UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Technologie IP multicast

Bc. Martin Němec

Diplomová práce
2014

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2013/2014**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin Němec**
Osobní číslo:	**I11396**
Studijní program:	**N2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Technologie IP multicast**
Zadávající katedra:	**Katedra softwarových technologií**

Zásady pro vypracování:

Cílem práce je popsat technologii IP multicast (její výhody a nevýhody, srovnání s unicastem, jaké jsou požadavky na technologii multicast). Dále představit stavební prvky multicastu a blíže popsat adresování (na L3 a na L2, mapování multicastových IPv4 adres na multicastové MAC adresy), protokol Internet group management protocol (IGMP) a IGMP Snooping, směrování multicastu a distribuční stromy. Teoretický popis bude obsahovat také směrovací protokol Protocol-Independent Multicast (PIM Dense Mode a PIM Sparse Mode). Praktická část bude obsahovat návrh a realizaci konfigurací multicastu na síťových zařízeních. Součástí tohoto výstupu bude odměření parametrů PIM protokolu na jednotlivých konfiguracích a jejich vyhodnocení.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

TIAN, Xiaohua. Scalable multicasting over next-generation internet: design, analysis, and applications. New York: Springer, c2013, xvii, 155 p. ISBN 978-146-1401-520.
HARTE, Lawrence. Introduction to data multicasting: design, analysis, and applications. Fuquay-Varina: Althos Publishing, c2008, viii, 72 s. ISBN 19-328-1355-1.
WILLIAMSON, Beau. Developing IP multicast networks: design, analysis, and applications. Indianapolis, IN: Cisco Press, 1999-. ISBN 15-787-0077-9.
MAUFER, Thomas A. Deploying IP multicast in the enterprise: design, analysis, and applications. Upper Saddle River: Prentice Hall, 1998, xvii, 275 s. ISBN 01-389-7687-2.

Vedoucí diplomové práce: **Ing. Soňa Neradová**
Katedra softwarových technologií

Datum zadání diplomové práce: **31. října 2013**
Termín odevzdání diplomové práce: **16. května 2014**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

prof. Ing. Antonín Kavička, Ph.D.
vedoucí katedry

V Pardubicích dne 15. listopadu 2013

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 16. 5. 2014 Bc. Martin Němec

Poděkování

Rád bych poděkoval vedoucí mé diplomové práce, Ing. Soně Neradové, že mi umožnila tuto práci realizovat a také za cenné rady a připomínky během jejího zpracování.

Anotace

Diplomová práce se zabývá technologií IP multicast. V teoretické části jsou popsány základní principy IP multicastu, jeho výhody a nevýhody. Dále je v této části popsán směrovací protokol PIM. Další část práce obsahuje popis konfigurace počítačové sítě a protokolu PIM-SM. Tato část se také zabývá měřením, porovnáním a vyhodnocením síťových parametrů pro různé konfigurace na této síti.

Klíčová slova

multicast, PIM, sparse mode, dense mode, IP, IGMP, distribuční strom, počítačová síť, směrování, router

Title

IP multicast technology

Annotation

My thesis deals with IP multicast technology. The theoretical part describes basic principles of the IP multicast technology, it's pros and cons. This part also describes multicast routing protocol PIM. The other part of my thesis contains a description of computer network configuration and configuration of multicast routing protocol PIM-SM. This part also deals with measurement, comparing and evaluation of network parameters in different cases of network configuration.

Keywords

multicast, PIM, sparse mode, dense mode, IP, IGMP, distribution tree, computer network, routing, router

Obsah

Seznam zkratek....10
Seznam obrázků....11
Seznam tabulek....12
1 Úvod....13
1.1 Cíle práce....13
1.2 Členění práce....14
2 Komunikace v počítačových sítích....15
2.1 Počítačová síť....15
2.2 Model ISO/OSI....17
2.3 Protokol IP....17
2.3.1 Směrování....18
2.3.2 Hlavička IP paketu....18
2.3.3 Adresace v IP....19
2.3.4 Nedostatek IP adres....21
2.3.5 Network Address Translation....21
2.3.6 IP verze 6 (IPv6)....23
2.3.7 Hlavička IPv6 paketu....24
2.3.8 Adresace v IPv6....25
2.4 Ethernet....26
2.4.1 Ethernetový rámec....27
2.4.2 Adresace v Ethernetu....28
2.4.3 Opakovače a přepínače....28
3 Technologie IP multicast....30
3.1 Principy multicastu....30
3.2 Výhody multicastu....31
3.2.1 Šířka pásma....31
3.2.2 Vytížení serveru....32
3.2.3 Zatížení sítě....32
3.3 Nevýhody multicastu....32
3.3.1 Nespolehlivý přenos....32

3.3.2 Zdvojené pakety....33
3.3.3 Zahlcení sítě....33
3.4 Adresace na L3 a L2....33
3.4.1 Adresace v IP....33
3.4.2 Adresace v IPv6....34
3.4.3 Adresace v Ethernetu....35
3.4.4 Mapování multicastových IP adres na ethernetové MAC adresy....36
3.4.5 Mapování multicastových IPv6 adres na ethernetové MAC adresy....37
3.5 Distribuční stromy....37
3.5.1 Zdrojové stromy....37
3.5.2 Sdílené stromy....38
3.6 Směrování multicastu....40
3.6.1 Reverse path forwarding....40
3.6.2 Multicastová směrovací tabulka....40
3.6.3 Práh TTL....41
3.6.4 Rozdělení multicastových routovacích protokolů....41
3.6.5 Dense mode protokoly....41
3.6.6 Sparse mode protokoly....42
3.6.7 Link-state protokoly....43
3.7 Protokol IGMP....43
3.7.1 IGMP verze 1....43
3.7.2 IGMP verze 2....44
3.7.3 IGMP verze 3....46
3.7.4 IGMP Snooping....49
4 Protocol Independent Multicast....50
4.1 PIM Dense Mode....50
4.1.1 Objevení sousedů....50
4.1.2 Směrování multicastového provozu....51
4.1.3 Pruning....52
4.1.4 Grafting....53
4.1.5 State-refresh....54
4.2 PIM Sparse Mode....54
4.2.1 Join message zprávy....54

4.2.2 Prune message zprávy....56
4.2.3 PIM zprávy....56
4.2.4 Zdroje multicastového provozu....56
4.2.5 Stromy nejkratších vzdáleností....58
5 Konfigurace počítačové sítě a multicastu....60
5.1 Zařízení v síti....60
5.1.1 Směrovače Cisco....60
5.1.2 Virtuální stroj jako směrovač....61
5.1.3 Koncová zařízení....62
5.2 Topologie a adresace....62
5.3 Konfigurace zařízení v síti....66
5.3.1 Konfigurace směrovačů Cisco 2811....66
5.3.2 Konfigurace virtuálního stroje....68
5.3.3 Konfigurace koncových zařízení....70
6 Měření parametrů multicastové komunikace....72
6.1 Porovnání zátěže procesoru směrovačů....72
6.2 Počty paketů protokolu PIM na linuxovém směrovači....76
6.3 Přístupová doba k datům skupiny....77
7 Závěr....82
Literatura....84
Příloha A – Konfigurace směrovače R1....87
Příloha B – Konfigurační soubor pimd.conf....90
Příloha C – Přiložené CD....91

Seznam zkratek

BGP	Border Gateway Protocol
CBT	Core-based Trees
DNS	Domain Name System
DVMRP	Distance Vector Multicast Routing Protocol
IP	Internet Protocol
MAC	Media Access Control
MOSPF	Multicast Open Shortest Path First
NAS	Network Attached Storage
NAT	Network Address Translation
NIC	Network Interface Controller
NTP	Network Time Protocol
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
SATA	Serial ATA
SPT	Shortest Path Tree
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol

Seznam obrázků

Obrázek 1 – Schéma sběrnicové topologie....16
Obrázek 2 – Schéma hvězdicové topologie....16
Obrázek 3 – Schéma kruhové topologie....16
Obrázek 4 – Směrování....18
Obrázek 5 – Hlavička IP paketu....19
Obrázek 6 – Příklad sítě s NAT....22
Obrázek 7 – Příklad sítě s využitím NAPT....23
Obrázek 8 – Hlavička paketu IP verze 6....24
Obrázek 9 – Ethernetový rámec....27
Obrázek 10 – Multicasting....30
Obrázek 11 – Streamování videa: unicast vs. multicast....31
Obrázek 12 – IPv6 multicastová adresa....34
Obrázek 13 – Příklad mapování IP adresy na ethernetovou MAC adresu....36
Obrázek 14 – Zdrojový strom....37
Obrázek 15 – Sdílený strom....38
Obrázek 16 – Jednosměrný sdílený strom....39
Obrázek 17 – Obousměrný sdílený strom....39
Obrázek 18 – Prune message....41
Obrázek 19 – Zpráva IGMP verze 1....43
Obrázek 20 – Zpráva IGMP verze 2....45
Obrázek 21 – Membership query v IGMPv3....46
Obrázek 22 – Membership report v IGMPv3....47
Obrázek 23 – Group Record....47
Obrázek 24 – Prvotní provoz v PIM-DM....51
Obrázek 25 – PIM-DM pruning....52
Obrázek 26 – Prune override....53
Obrázek 27 – Join message zprávy....55
Obrázek 28 – PIM register message zprávy....57
Obrázek 29 – Multicastový provoz po PIM register-stop zprávě....58
Obrázek 30 – PIM - Strom nejkratších vzdáleností....59
Obrázek 31 – Směrovač Cisco 2811....60
Obrázek 32 – Rozhraní nástroje VirtualBox....61
Obrázek 33 – VirtualBox s běžícím systémem....63
Obrázek 34 – Návrh budované sítě....64
Obrázek 35 – Konfigurace IP ve Windows....71
Obrázek 36 – Unicast vs. multicast....74
Obrázek 37 – Graf porovnání unicastu a multicastu....75
Obrázek 38 – Zatížení v klidu s jedním zdrojem....75
Obrázek 39 – Srovnání doby přístupu v různých situacích....79

Obrázek 40 – Přípojení PC4 do skupiny, jejíž provoz je směrován....79
Obrázek 41 – Přístupová doba při již směrovaném provozu....80
Obrázek 42 – Závislost přístupové doby PC3 na umístnění RP....81

Seznam tabulek

Tabulka 1 – Úkoly vrstev modelu ISO/OSI....17
Tabulka 2 – Třídy IP adres....20
Tabulka 3 – Privátní rozsahy IP adres....20
Tabulka 4 – Příklady zápisů stejné IPv6 adresy....25
Tabulka 5 – Skupiny IPv6 adres....26
Tabulka 6 – Přehled vybraných systémů Ethernet....27
Tabulka 7 – Příklady vyhrazených multicastových adres....34
Tabulka 8 – Hodnoty pole scope....35
Tabulka 9 – Sestavení State-Change Record....48
Tabulka 10 – Adresace zařízení v síti....65
Tabulka 11 – Výchozí brány osobních počítačů....66
Tabulka 12 – Přehled naměřených zatížení....73
Tabulka 13 – Počty paketů na linuxovém směrovači....76
Tabulka 14 – Přístup k datům po rychlém návratu....78
Tabulka 15 – Přístup k datům při prvním spojení....78

1 Úvod

Dnešní svět, plný multimédií, elektronických služeb a komunikace, si lze jen těžko představit bez počítačových sítí. Díky nim můžeme zasílat data na druhý konec budovy nebo i do desetitisíce kilometrů vzdálených míst. Těmito daty může být cokoliv od multimediálního obsahu po aktualizace operačního systému. Obzvlášť při přenosu zvuku a videa ovšem často narážíme na omezení týkající se kvality a kapacity spojení, které je způsobeno možnostmi dnešních technologií nebo technologií použitých k přenosu.

Stále větší požadavky na kvalitu a rychlost přenosu souvisí i s pokrokem v jiných odvětvích informačních technologií. Mílovými kroky kupředu se posunují některé multimediální standardy, které ještě před několika lety nebyly takřka známy. Za video zmiňme například dnešní standardy pro rozlišení obrazu, jako je například standard 4K (odpovídá čtyřnásobku rozlišení FullHD). Takové rozlišení u videosekvence má za následek obrovské množství přenášených dat, které musí být zpracováno. Pokud jsou multimédia tohoto typu přenášena počítačovou sítí, požadavky na tuto síť se zvyšují.

IP multicast je technologií, která nabízí úsporu síťových zdrojů zejména na poli streamovaných multimédií v reálném čase, která jsou zasílána více různým uživatelům. Běžnými příklady mohou být třeba internetové vysílání televizních nebo rozhlasových stanic, při kterém data samotného obsahu přijímají větší počty diváků či posluchačů. V případě klasické komunikace by docházelo k redundanci dat zasílaného obsahu, která má za následek obrovské požadavky na kvalitu a kapacitu spojení. Díky technologii IP multicast lze však takovéto redundantní zasílání dat odstranit a ušetřit tak kapacitu síťových zdrojů.

1.1 Cíle práce

Práce je rozdělena do třech částí, přičemž v každé z těchto částí lze vytyčit několik cílů. Cílem první části, teoretického popisu technologie IP multicast je především:

- zmapovat základy komunikace na IP sítích,
- popsat klíčové stavební prvky technologie IP multicast,
- zaměřit se na popis výhod a nevýhod této technologie oproti ostatním typům komunikace na paketových sítích,
- popsat principy multicastového směrovacího protokolu PIM.

Druhá část, konfigurace počítačové sítě a multicastu má za cíl:

- zvolit zařízení, ze kterých bude sestavena počítačová síť pro provoz multicastu,
- navrhnout topologii a adresaci počítačové sítě,

- popsat konfiguraci jednotlivých zařízení pro provoz multicastu.

Poslední, třetí část se soustředí na splnění následujících cílů:

- měření parametrů multicastového provozu,
- zhodnocení těchto parametrů pro různé případy (konfigurace).

1.2 Členění práce

Dokument je členěn do následujících sedmi kapitol.

1. **Úvod** je kapitola, která pojednává o tématu práce a jeho problematice. Dále představuje jednotlivé cíle každé části práce a popisuje způsob, jakým je práce logicky členěna.
2. Kapitola **Komunikace v počítačových sítích** popisuje základní principy komunikace mezi počítači v paketových sítích, popisuje protokoly IP a Ethernet.
3. V kapitole **Technologie IP multicast** jsou popsány stavební prvky IP multicastu, jeho výhody a nevýhody a principy komunikace na IP sítích.
4. Kapitola **Protocol Independent Multicast** obsahuje teoretický popis multicastového směrovacího protokolu PIM. Jsou zde popsány jeho varianty a funkce tohoto protokolu v IP sítích.
5. **Konfigurace počítačové sítě a multicastu** je kapitolou, ve které je popsána konfigurace vybraných síťových zařízení pro zprovoznění multicastové komunikace v počítačové síti.
6. **Měření parametrů multicastové komunikace** obsahuje metody, kterými byly měřeny různé parametry multicastového provozu. Naměřené hodnoty názorně zobrazuje a zhodnocuje jejich význam.
7. **Závěr** je celkovým shrnutím a zhodnocením diplomové práce.

Z hlediska logické výstavby práce lze kapitoly zařadit do třech částí:

- **teoretický popis technologie IP multicast**, do kterého patří kapitoly 2 až 4,
- **konfigurace počítačové sítě** odpovídající rozsahu kapitoly 5,
- **vyhodnocení parametrů multicastového provozu**, které odpovídá kapitole 6.

2 Komunikace v počítačových sítích

2.1 Počítačová síť

Pojem **počítačová síť** dnes zahrnuje množství rozmanitých prostředků a technologií, určených ke komunikaci jednotlivých počítačů mezi sebou. Obzvláště poslední dobou to již zdaleka nejsou jen počítače, které nalézáme mezi navzájem komunikujícími zařízeními. Stále větší podíl v tomto světě informací zaujímají zařízení jako chytré telefony (smartphony), tablety, chytrá datová úložiště (NAS), tiskárny, čtečky elektronických knih a spoustu dalších zařízení, pro které je nezbytná výměna dat s vnějším světem.

Počítačovou síť tedy můžeme definovat jako „dva nebo více počítačů (či jiných chytrých zařízení[1]) propojených nějakými prostředky, pomocí kterých jsou schopné si vyměňovat (sdílet) informace“. (Převzato z [6])

Základním kamenem pro takovou počítačovou síť je sdílené médium – prostředek skrze který proudí informace od jednoho uzlu ke druhému. Tímto prostředkem mohou být například: měděný kabel (kroucená dvoulinka, koaxiální kabel, ...), optické vlákno nebo éter[2] (bezdrátové technologie).

Dalším předpokladem k realizaci komunikace je, že jednotlivá zařízení mají rozhraní, pomocí kterého mohou po médiu komunikovat a vědí jakým způsobem s ostatními zařízeními komunikovat. Dnes nejběžnějšími rozhraními jsou například síťová karta (NIC), WiFi modul nebo Bluetooth modul (oba pro bezdrátovou komunikaci). Standardy, díky kterým zařízení vědí, jak spolu komunikovat se nazývají **síťové protokoly**.

Další nutností, díky které je počítač (či jiné zařízení) schopen komunikovat a sdílet informace s ostatními zařízeními, je softwarová implementace jednak samotných síťových protokolů a dále také obslužných aplikací. V dnešních moderních operačních systémech (Windows, Linux, OS X) je však implementace nejběžnějších síťových protokolů TCP/IP samozřejmostí. Stejně tak obsahují i běžné obslužné aplikace jako například internetový prohlížeč, SSH klient, SMB klient.

Počítačové sítě můžeme dělit podle několika kritérií. Jedním z nejběžnějších kritérií pro dělení počítačových sítí je rozsah. Podle rozsahu sítě rozlišujeme na:

- LAN (Local Area Network), jejíž rozsah je omezen na lokální patro, budovu, místnost,
- CAN (Campus Area Network), kam patří sítě přes více budov (kampus),
- MAN (Metropolitan Area Network), tedy na městskou (metropolitní síť),

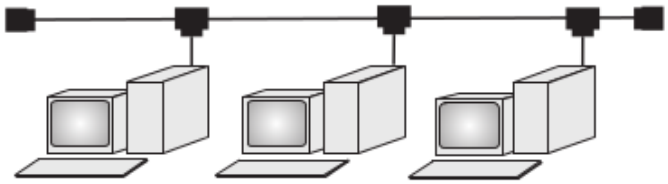
1 jako „chytré zařízení“ je v tomto kontextu označeno zařízení schopné se připojit do sítě

2 pojem „éter“ označuje hypotetickou substanci, zde je použit pro prostředí, ve kterém se šíří elektromagnetické záření

- WAN (Wide Area Network), u které je rozsah takřka neomezený. (Čerpáno z [7])

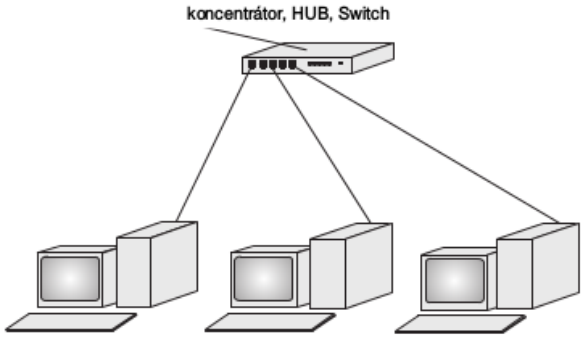
Dalším kritériem pro dělení počítačových sítí bývá jejich **topologie**. Topologie je způsob, jakým jsou zařízení v síti propojeny. Zároveň je prvkem síťového standardu a podstatně určuje výsledné vlastnosti sítě. Topologie počítačových sítí se dělí na:

- sběrnicovou topologii, kde je použito průběžné vedení a stanice se k tomuto vedení připojují pomocí odbočovacích prvků (obrázek 1),



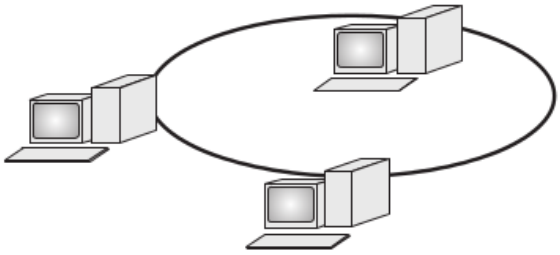
Obrázek 1 – Schéma sběrnicové topologie
Zdroj: Počítačové sítě pro začínající správce [5]

- hvězdicovou topologii, kde každá stanice je připojena vlastním kabelem do rozbočovače (např. hub, switch), který tvoří jakýsi střed sítě (obrázek 2),



Obrázek 2 – Schéma hvězdicové topologie
Zdroj: Počítačové sítě pro začínající správce [5]

- kruhovou topologii, ve které spojovací vedení stanic vytváří souvislý kruh (obrázek 3). (Převzato z [5])



Obrázek 3 – Schéma kruhové topologie
Zdroj: Počítačové sítě pro začínající správce [5]

2.2 Model ISO/OSI

Mezinárodní organizace pro normalizaci (angl. International Organization for Standardization) v osmdesátých letech vypracovala standard, který měl řešit tehdejší problém v různorodosti realizací počítačových sítí. Jelikož účelem počítačových sítí bylo a je vzájemné propojování, měl tento standard za úkol dát jasná pravidla pro přenos dat v počítačových sítích. Výsledný model se nazývá OSI (Open Systems Interconnection) a je známý též jako „referenční model ISO/OSI“. (Čerpáno z [5])

Tento model rozděluje síťovou komunikaci na vrstvy, kterých je sedm (tabulka 1). Základní myšlenkou je, že každá vrstva využívá služeb nižší vrstvy a poskytuje služby pro vyšší vrstvy. V rámci jednotlivých zařízení pak dochází ke komunikaci vrstev, které jsou na stejné úrovni.

Tabulka 1 – Úkoly vrstev modelu ISO/OSI

Zdroj: Počítačové sítě pro začínající správce [5]

Vrstva	Vysvětlení
Aplikační vrstva	Je určitou aplikací (např. oknem v programu) zpřístupňující uživatelům síťové služby. Nabízí a zajišťuje přístup k souborům (na jiných počítačích), vzdálený přístup k tiskárnám, správu sítě, elektronické zprávy (včetně e-mailu)…
Prezentační vrstva	Má na starosti konverzi dat, přenášená data mohou totiž být v různých sítích různě kódována. Tato vrstva zajišťuje sjednocení formy vzájemně přenášených údajů. Dále data komprimuje, případně šifruje… V praxi často splývá s relační vrstvou.
Relační vrstva	Navazuje a po skončení přenosu ukončuje spojení. Může provádět ověřování uživatelů, zabezpečení přístupu k zařízením…
Transportní vrstva	Typickou činností transportní vrstvy je dělení přenášené zprávy na pakety a opětovné skládání přijatých paketů do zpráv (při přenosu se mohou pakety pomíchat či ztratit).
Síťová vrstva	Je zodpovědná za spojení a směrování mezi dvěma počítači nebo celými sítěmi (tj. uzly), mezi nimiž neexistuje přímé spojení. Zajišťuje volbu trasy při spojení (mezi uzly bývá více možných cest pro přenos paketu)…
Linková vrstva	Uskutečňuje přenos údajů (datových rámců) po fyzickém médiu, pracuje s fyzickými adresami síťových karet, odesílá a přijímá rámce, kontroluje cílové adresy každého přijatého rámce, určuje, zda bude rámec odevzdán vyšší vrstvě…
Fyzická vrstva	Popisuje elektrické (či optické), mechanické a funkční vlastnosti: jakým signálem je reprezentována logická jednička, jak přijímací stanice rozezná začátek bitu, jaký je tvar konektoru, k čemu je který vodič v kabelu použit…

V praxi se tento model využívá spíše jen jako referenční, výkladový. Umožňuje především pochopit principy práce síťových prvků a patří k základní terminologii počítačových sítí.

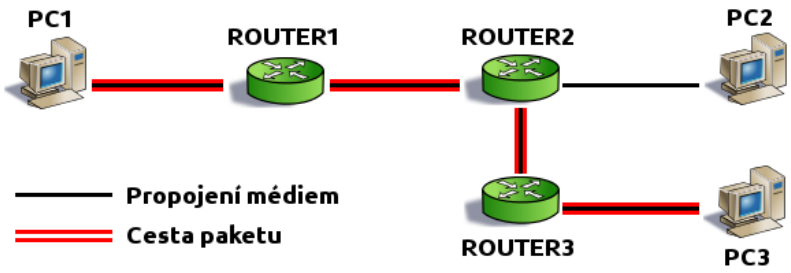
2.3 Protokol IP

Téměř všechny počítačové sítě a Internet jsou dnes budovány pomocí modelu **TCP/IP**. Srdcem tohoto modelu je protokol **IP** (Internet Protocol) operující na síťové vrstvě modelu

ISO/OSI. IP je nestavový a nespojový protokol zajišťující komunikaci pomocí bloků dat nazývaných pakety. IP paket má hlavičku, ve které se nachází různé informace o datech obsažených v těle paketu. Díky těmto informacím může paket i s daty, která nese, cestovat od odesílatele k příjemci.

2.3.1 Směrování

Mezi nejdůležitější informace v hlavičce patří adresa příjemce (adresáta). Tuto adresu využívají různé síťové prvky k doručení paketu k adresátovi. Těmito síťovými zařízeními jsou především směrovače (routery), které mají za úkol směrování (routing, routování) paketů podle cílové adresy k adresátovi. Proces směrování je naznačen na obrázku 4.



Obrázek 4 – Směrování
Zdroj: Vlastní zpracování

Na obrázku 4 počítač označený jako PC1 zasílá data počítači PC3. Pakety prochází postupně směrovači ROUTER1, ROUTER2 a ROUTER3, přičemž každý z nich paket přeposílá takovým směrem, aby postupně dorazil k adresátovi (PC3). Pro rozhodnutí, kterým směrem paket odeslat, používá směrovač tzv. směrovací (routovací) tabulku. Směrovací tabulku má každý směrovač svojí a jsou v ní záznamy, které říkají, jaké cílové adresy jsou směrovány jakým směrem.

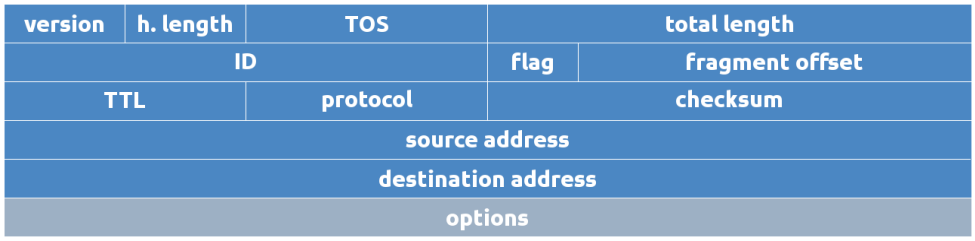
2.3.2 Hlavička IP paketu

Prvních 20 bajtů hlavičky IP paketu má pevnou podobu, další mohou být volitelné. Hlavička se skládá z následujících polí:

- *version* – první 4 bity hlavičky označují verzi protokolu IP,
- *header length* – další 4 bity indikují délku hlavičky IP paketu – tzn. včetně volitelných částí,
- *TOS* – 8 bitů dlouhé pole, jehož obsah označuje třídu, do které IP paket patří,
- *total length* – 16bitové pole, ve kterém je uvedena délka celého IP paketu v bajtech,
- *ID* – 16bitový identifikátor paketu, který je důležitý pro zpětné sestavení rozděleného paketu,
- *flag* – 3 bity jako příznaky (nultý bit je nevyužitý, první bit označuje, zda je možno

paket fragmentovat a druhý bit říká, zda očekávat další fragmenty paketu),

- *fragment offset* – 13bitové pole označující posun fragmentu,
- *TTL* (time-to-live) – 8bitové pole označující počet hopů (skoků). Jedná se o číslo vyjadřující počet směrovačů, kterými může paket projít, než bude zahozen,
- *protocol* – 8bitové pole indikující číslo protokolu vyšší vrstvy; toto číslo označuje protokol, jehož data paket ve svém těle nese,
- *checksum* – 16bitový kontrolní součet z hlavičky IP paketu,
- *source address* – 32bitová adresa odesílatele,
- *destination address* – 32bitová adresa příjemce,
- *options* – volitelná přídavná pole. (Čerpáno z [9])



Obrázek 5 – Hlavička IP paketu
Zdroj: Vlastní zpracování

2.3.3 Adresace v IP

Jak je znázorněno na obrázku 5, protokol IP používá 32bitové adresy k adresaci jednotlivých zařízení v síti. Těchto 32 bitů IP adresy se běžně zapisuje po jednotlivých oktetech v desítkové soustavě oddělených tečkami. Každý oktet tedy může nabývat hodnot `0x00` až `0xFF`, v desítkové soustavě zapsáno jako 0 až 255. Taková IP adresa může vypadat například: `169.78.231.17`, `192.168.51.100` nebo `255.255.255.255`.

Každá IP adresa se skládá ze dvou složek. Těmito složkami jsou:

- adresa sítě a
- adresa koncového uzlu (počítače) v této síti.

Protokol IP byl navrhnut tak, že IP adresy byly rozděleny do jednotlivých tříd. Podle toho, do které třídy adresa spadala, bylo více či méně prvních bitů adresy vyhrazeno pro adresu sítě. Třídy jsou navrhnuty tak, aby se snadno daly z adresy odvodit a díky tomu bylo na první pohled patrné, kolik bitů je vyhrazeno pro adresu sítě a kolik pro adresu uzlu. Počet bitů vyhrazených pro velikost uzlu udává, kolik zařízení je možno na této síti adresovat. Jednotlivé třídy i s jejich rozsahy IP adres a maximálními počty sítí a uzlů přehledně zobrazuje tabulka 2. (Čerpáno z [5], [8])

Tabulka 2 – Třídy IP adres

Zdroj: Packet guide to core network protocols [8]

Třída	Rozsah hodnot prvního oktetu	Binární hodnota prvních bitů	Maximální počet sítí	Maximální počet počítačů v síti
A	0–127	0	128	16 777 216
B	128–191	10	16 364	65 636
C	192–223	110	2 097 152	256
D	224–239	1110		
E	240–255	1111		

U adres třídy A je prvních osm bitů (první oktet) určeno pro adresu sítě a zbylých 24 bitů (3 oktety) pro adresu zařízení. První oktet může nabývat 256 různých hodnot, avšak do třídy A patří jen 128 z nich (0 až 127). Počítačů v síti může být tolik, kolik adres lze ze zbylých 24 bitů vytvořit, tj. 2^{24}. U adres třídy B je pro adresu sítě vyhrazeno 16 bitů a stejně tak 16 bitů je určeno pro adresu počítače. Počítačů u této třídy tedy může být 2^{16}, přičemž sítí je maximálně 2^{14} (první dva bity jsou fixní). Analogicky třída C, kde je pro adresu sítě vyhrazeno prvních 24 bitů, má maximum 2^{21} sítí a v každé síti nejvýše 2^{8} počítačů. Adresy ve třídě D jsou vyhrazeny pro IP multicast a zbylá třída E je označena jako rezervní. (Čerpáno z [8])

Aby nedocházelo ke konfliktu mezi IP adresami, organizace IANA (The Internet Assigned Numbers Authority) vyhradila v každé ze tříd A, B a C tzv. privátní adresové rozsahy. Tyto rozsahy slouží pro použití v lokálních sítích, nejsou tedy použity pro adresaci v Internetu. Tyto privátní rozsahy jsou znázorněné v Tabulce 3.

Tabulka 3 – Privátní rozsahy IP adres

Zdroj: Packet guide to core network protocols [8]

Třída	Rozsah privátních adres
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Pro větší flexibilitu v adresování sítí a počítačů, než nabízejí třídy IP adres, je společně s adresou uváděna i **maska sítě**.

Maska sítě jednoznačně určuje, jaká část IP adresy je adresou sítě a jaká část je adresou počítače. Je to 32bitové číslo, které se, stejně jako IP adresa, zapisuje v desítkové soustavě po jednotlivých oktetech oddělených tečkami. Binární operací `AND` mezi IP adresou a její maskou pak lze získat adresu sítě. (Čerpáno z [8])

Adresovat cílového příjemce paketu lze u protokolu IP čtyřmi různými způsoby:

- unicasting, kdy je adresován jeden konkrétní počítač,
- broadcasting, při kterém jsou adresovány všechny počítače v síti nebo v segmentu,
- anycasting, kdy jsou data zaslána nějakému z počítačů (nejlepšímu, nejbližšímu)[3],
- multicasting, který zasílá data několika zařízením (skupině). (Čerpáno z [2])

Unicastovými adresami jsou všechny adresy v dané síti kromě první IP adresy (všechny bity v adrese počítače nastaveny na 0) a poslední IP adresy (všechny bity v adrese počítače nastaveny na 1). V případě sítě `192.168.51.0` s maskou `255.255.255.0` jsou to tedy všechny adresy v rozsahu `192.168.51.1` – `192.168.51.254`. Zbylé dvě adresy mají jiné funkce. První adresa v síti (v tomto případě `192.168.51.0`) je adresou této sítě, poslední adresa v síti (zde `192.168.51.255`) je tzv. **broadcastovou adresou sítě**. Pakety, které mají v poli destination address vyplněnou broadcastovou adresu sítě, jsou rozeslány všem počítačům v této síti (resp. v broadcastové doméně).

2.3.4 Nedostatek IP adres

Jedním z největších problémů IP verze 4 je nedostačující počet adres pro všechna zařízení, která komunikují přes Internet. Počet možných IP adres je 2^{32}, tudíž přes 4 miliardy. V praxi je toto číslo poníženo o ty adresy, které jsou součástí vyhrazených rozsahů. To se ukázalo jako nedostačující. Jedním z řešení tohoto problému je použití techniky **NAT** (Network Address Translation).

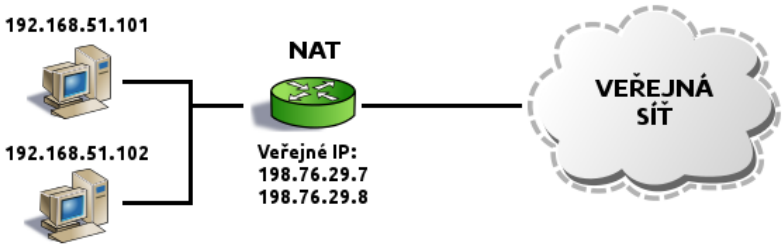
2.3.5 Network Address Translation

Network Address Translation neboli NAT, který je typicky implementován v nějakém zařízení (routeru), má za úkol překládat IP adresy na jiné. Lokální síť, která obsahuje několik privátních IP adres tak může komunikovat s vnější (veřejnou) sítí díky dynamickému mapování těchto privátních adres na veřejné adresy. Pokud je tedy v síti nižší nebo stejný počet privátních adres jako počet přidělených vnějších (veřejných), má každý počítač či zařízení s privátní (vnitřní) adresou garantovánu alespoň jednu veřejnou adresu, pod kterou bude při komunikaci se zařízeními ve veřejné síti vystupovat. V opačném případě bude maximální počet současně komunikujících počítačů omezen počtem přidělených veřejných adres. Některé z těchto veřejných adres lze rovněž mapovat staticky na konkrétní privátní adresu. Tím bude zaručeno, že konkrétní počítač je z vnější sítě vždy dostupný pod stejnou IP adresou. To umožňuje zařízením ve vnější síti uskutečnit komunikaci se zařízeními ve vnitřní síti, která by bez takovéhoto statického mapování nebyla tímto směrem (z vnější do privátní sítě) možná. (Čerpáno z [7], [10], [11])

Díky technice NAT lze adresy použité v lokální síti (privátní adresy) použít znovu v jakékoliv jiné lokální síti, aniž by hrozilo riziko kolize. Jakkoliv velká počítačová síť, která bude připojená k zařízení s funkcí NAT, bude moci komunikovat, aniž by adresy, které jsou pro počítače v této síti použité, byly odčerpány z rozsahu možných veřejných

3 anycasting byl zaveden až v IP verze 6

adres. Pokud uvážíme, že popisovanou veřejnou sítí je Internet, tato technika umožňuje úsporu přidělených IP adres, kterých je v IP verze 4 nedostatek.

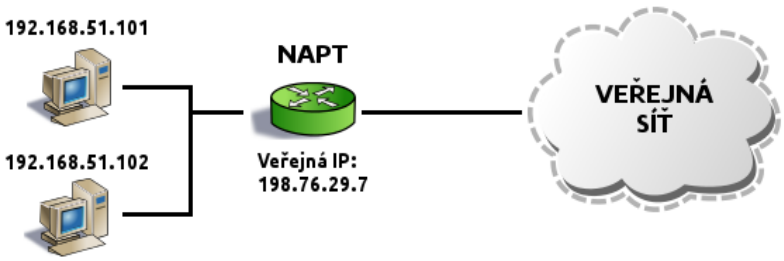


Obrázek 6 – Příklad sítě s NAT
Zdroj: Vlastní zpracování

Příklad takové privátní sítě využívající NAT je zobrazen na obrázku 6. Lokální síť obsahuje dva počítače s adresami z privátního rozsahu, které komunikují s veřejnou sítí (např. Internetem) za pomoci překladu adres. Pokud chce počítač s IP adresou `192.168.51.101` komunikovat s nějakým zařízením ve veřejné síti, zasílá pakety, které obsahují v poli *source address* hodnotu `192.168.51.101` a v poli *destination address* adresu odpovídajícího zařízení ve veřejné síti. Jakmile takové pakety dorazí na zařízení fungující jako NAT, je pro privátní adresu počítače z pole *source address* mapována jedna z veřejných adres, která je k dispozici – například `192.76.29.7`. NAT změní hlavičku paketu tak, že přepíše původní *source address* na nově zvolenou (veřejnou) adresu. Takto upravený paket putuje až k cílovému zařízení. Pakety, kterými cílové zařízení odpovídá, mají v IP hlavičce v poli *destination address* právě namapovanou veřejnou IP adresu a jakmile dorazí na NAT, je hodnota v tomto poli přepsána lokální adresou mapovanou k této veřejné (`192.168.51.101`). Na lokální síti již tedy paket bez problémů doputuje až k danému počítači.

Ve většině případů, které zahrnují i většinu domácích počítačových sítí a sítí v malých kancelářích, překládá zařízení obsahující NAT mnoho privátních IP adres na jednu veřejnou IP adresu. Konkrétně tato technika se nazývá **NAPT** (Network Address Port Translation), **PAT** (Port Address Translation) nebo **NAT Overload**. Použití této techniky tedy umožňuje souběžnou komunikaci více počítačů na lokální síti se zařízeními ve veřejné síti s použitím třeba i jen jedné veřejné IP adresy. Tato funkcionalita je uskutečňována mapováním nejen IP adres, ale celých párů IP adresa – číslo portu. Číslo portu představuje adresu na čtvrté vrstvě ISO/OSI modelu, kde nejčastěji používanými protokoly nad protokolem IP jsou spojový protokol TCP a nespojový protokol UDP. Číslo portu je šestnáctibitové číslo, pomocí kterého je adresován konkrétní proces na počítači. Je obsaženo v hlavičce TCP nebo UDP segmentu v polích *source port* a *destination port*, které označují odpovídající proces u odesílatele a adresáta. Toto mapování umožňuje zařízení s NAPTem jednoznačně identifikovat, pro které zařízení jsou pakety, přicházející

z veřejné sítě jako odpověď na zaslané pakety, určeny a následně je tomuto zařízení doručit. (Čerpáno z [7], [10], [11])



Obrázek 7 – Příklad sítě s využitím NAPT
Zdroj: Vlastní zpracování

Příklad sítě s využitím NAPT je vyobrazen na obrázku 7. Lokální síť obsahuje dva počítače s privátními adresami `192.168.51.101`, respektive `192.168.51.102`. Zařízení, které provádí NAPT, má k dispozici pouze jednu veřejnou IP adresu, a to `198.76.29.7`. Pokud komunikuje nějaká aplikace, například internetový prohlížeč, s nějakým webovým serverem ve veřejné síti, který má adresu `8.8.8.8`, má IP paket odcházející z počítače ve své hlavičce uvedenou zdrojovou adresu `192.168.51.101`, cílovou adresu `8.8.8.8` a v TCP hlavičce zdrojové číslo portu rovnající se tomu, které bylo internetovému prohlížeči přiděleno systémem, například `40000` a číslo cílového portu `80` (běžné pro webový server). Ve chvíli, kdy takovýto paket dorazí k NAPTu, namapuje se pro pár zdrojová adresa – zdrojový port nový pár, vytvořený z veřejné adresy a odpovídajícího čísla portu. NAPT potom pozmění IP hlavičku paketu a přepíše zdrojovou adresu na veřejnou, tedy `198.76.29.7`. Odpověď od webového serveru potom při průchodu přes NAPT nalezne podle cílového čísla portu odpovídající privátní adresu a opět změní hlavičku paketu. Může ovšem nastat případ, kdy internetový prohlížeč na druhém počítači v lokální síti chce komunikovat se stejným číslem zdrojového portu. V takovém případě musí NAPT zasáhnout do hlavičky TCP nebo UDP paketu a přepsat číslo zdrojového portu na jiné, které je v danou chvíli volné. Při přijmutí odpovědi se potom opět nalezne odpovídající pár IP adresa – číslo portu a dojde ke správnému doručení paketu.

2.3.6 IP verze 6 (IPv6)

NAT a další technologie, které slouží k řešení problému nedostatku IP adres, však tento problém pouze oddalují. Z toho důvodu byla v roce 1998 organizací IETF (The Internet Engineering Task Force) vydána další verze protokolu IP, a to verze 6 nazývaná IPv6. Změny oproti původnímu IP verze 4 se týkají především následujících kategorií.

- **Rozšířené možnosti adresace**. Adresa byla rozšířena z 32 na 128 bitů. Díky tomuto rozšíření je umožněno adresovat více zařízení (adresní rozsah má nyní 2^{128}

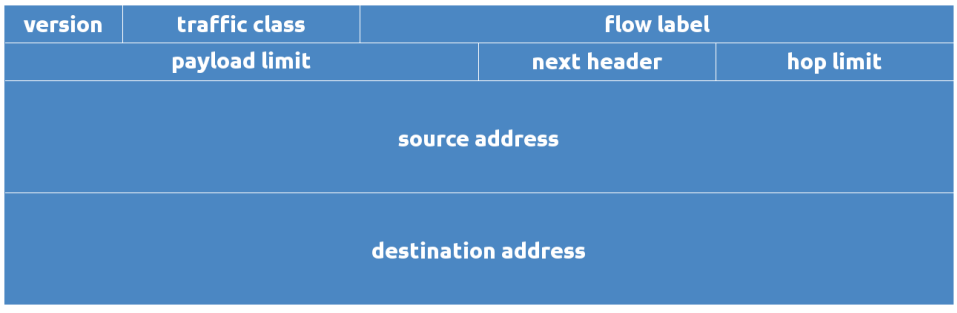
adres). Dále bylo přidáno pole *scope*, díky kterému byla zlepšena škálovatelnost multicastových adres. Byly zavedeny také anycastové adresy, díky kterým je možné adresovat některý ze skupiny počítačů.

- **Zjednodušení hlavičky**. Některá políčka známá z IP verze čtyři byla vyřazena, aby se zjednodušila práce s paketem a snížila režie.
- **Vylepšená podpora pro rozšíření a volby**. Změna způsobu, jakými jsou volitelné části hlavičky šifrovány, umožňuje efektivnější směrování a neklade tak přísné požadavky na délku volitelných částí. Zároveň přináší flexibilitu pro zavádění nových volitelných polí.
- **Identifikátory toku (flow labeling)**. Byla přidána nová vlastnost umožňující označit pakety, které patří do konkrétního toku dat (například QoS nebo real-time služby).
- **Autentizace a soukromí**. V IPv6 byla specifikována rozšíření pro podporu autentizace, integrity dat a volitelně i důvěrnosti dat. (Čerpáno z [7], [12], [13])

Jak již bylo zmíněno, v protokolu IPv6 došlo oproti verzi 4 ke zjednodušení hlavičky paketu. Sestává se z 8 polí, které dohromady mají fixní velikost 40 bajtů. Díky tomu je proces směrování více efektivní než u proměnné délky hlavičky v IP verze 4. Jelikož je délka fixní, není už třeba pole *header length*, které udávalo velikost hlavičky. Další pole byla odstraněna díky změně pravidel ohledně fragmentace. Pakety již nelze fragmentovat během cesty od odesílatele k adresátovi, může je fragmentovat pouze odesílatel. Dalším zjednodušením je vynechání pole *checksum*. Kontrolní součty hlavičky jsou implementovány v protokolech vyšších vrstev (TCP, UDP), a tak by zrušení tohoto pole nemělo mít vliv na spolehlivost. (Čerpáno z [7], [12], [13])

2.3.7 Hlavička IPv6 paketu

Schéma hlavičky IPv6 paketu je zobrazeno na obrázku 8.



Obrázek 8 – Hlavička paketu IP verze 6
Zdroj: Vlastní zpracování

Jak již bylo zmíněno, délka IPv6 hlavičky je fixní a má velikost 40 bajtů. Jednotlivá pole, která hlavička obsahuje, jsou:

- *version* – 4bitové číslo verze protokolu IP, zde tedy verze 6,
- *traffic class* – QoS třída, do které paket patří (8 bitů),
- *flow label* – pole o 20 bitech, které označuje tok, do kterého paket patří,
- *payload length* – délka dat, která paket přenáší (16 bitů),
- *next header* – 8bitové číslo, které udává typ následující hlavičky (typicky UDP, TCP nebo rozšiřující hlavička IPv6),
- *hop limit* – počet směrovačů, kterými může paket projít, než bude zahozen. Jedná se o 8bitové číslo, které je při průchodu směrovačem sníženo o jedna nebo zahozeno, pokud je jeho hodnota nulová,
- *source address* – 128bitová IPv6 adresa odesílatele,
- *destination address* – 128bitová IPv6 adresa příjemce. Tato adresa může být unicastová, multicastová nebo anycastová. (Čerpáno z [12], [13], [14])

Ve většině případů má IPv6 paket právě jednu hlavičku. Někdy je ale třeba k hlavičce přidat další informace, a jelikož je její délka fixní, není možnost je připojit přímo do ní. Z toho důvodu existují tzv. **rozšiřující hlavičky** (angl. extension headers), které připojení dalších informací umožňují. Tyto hlavičky jsou umístěny bezprostředně za první (hlavní) hlavičku paketu a jsou brány jako součást obsahu paketu. V takovém případě je v hlavní hlavičce, v poli *next header*, vyplněno číslo označující typ této hlavičky. (Čerpáno z [14])

2.3.8 Adresace v IPv6

Adresy v IPv6 jsou tedy, oproti IP verze 4, 128bitové. Zásadní změna proběhla i v zápisu adres. Ten nyní není v dekadickém tvaru, jak bylo u původní verze zvykem, nýbrž hexadecimálním. Další změnou je oddělovač skupin, který se změnil z tečky na dvojtečku a samotná velikost skupiny, která se zvýšila z původních osmi bitů na šestnáct bitů. Takových skupin je tedy osm (tj. 8 × 16 bitů). Příklad zápisu takové IPv6 adresy je: `AA76:0000:0000:0000:0012:A322:FE33:2267`. Počáteční nuly mohou být ve kterékoliv skupině ořízntuty na jednu. Zároveň jakýkoliv počet po sobě jdoucích skupin, obsahujících pouze nuly, lze zkrátit dvěma dvojtečkami. U mnoha adres se tak výrazně zkrátí délka zápisu. Takové případy jsou zobrazeny v Tabulce 4. (Čerpáno z [7], [12], [13])

Tabulka 4 – Příklady zápisů stejné IPv6 adresy

Zdroj: Network Warrior [7]

AA76:0000:0000:0000:0012:A322:FE33:2267
AA76:0:0:0:12:A322:FE33:2267
AA76::12:A322:FE33:2267

Stejně jako u IP verze 4, i ve verzi 6 jsou vyhrazené některé rozsahy adres pro různé účely. Jedná se opět o speciální adresy typu zpětné smyčky nebo multicastu. V IPv6 však některé

tyto adresy prošly proměnou a nyní jsou nahrazeny například celými rozsahy (tak je tomu u zpětné smyčky) nebo se celá adresa rozděluje na jednotlivá pole, které mají různé funkce (multicastové adresy).

IPv6 tedy rozděluje adresy do několika skupin, podle jejich použití. Tyto skupiny společně s binárním prefixem, který tato skupina má, jsou přehledně zobrazeny v Tabulce 5.

Tabulka 5 – Skupiny IPv6 adres

Zdroj: IPv6 – Theory, Protocol and Practise [13]

Typ adresy	Binární prefix	Zápis v IPv6
Nespecifikovaná adresa	00...0 (128 bitů)	::/128
Loopback (lokální smyčka)	00...1 (128 bitů)	::1/128
Multicast	11111111	FF00::/8
Link-local adresa	1111111010	FE80::/10
Site-local adresa	1111111011	FEC0::/10
Unicast	všechno ostatní	

- **Nespecifikovaná adresa** (angl. Unspecified address) je adresa, ve které je všech 128 bitů nastavených na nuly. Taková adresa není nikdy žádnému zařízení přiřazena. Používá se například pro inicializaci, pro pole *source address* ve chvíli, kdy zařízení ještě nezískalo svou vlastní adresu.
- **Loopback**, adresa s nastaveným pouze posledním bitem na jedna, odpovídá lokální smyčce z IP verze 4 (127.0.0.1). Nikdy není přiřazena žádnému fyzickému rozhraní a nesmí se ani vyskytovat v poli *source address* hlavičky paketu.
- **Multicast** pro adresování určité skupiny zařízení.
- **Link-local adresa** je taková adresa, která není žádným routerem směrována dále. Slouží například pro sítě, ve kterých se nenachází žádný směrovač anebo pro automatickou konfiguraci IP adresy zařízení.
- **Site-local** adresa slouží k adresaci všech zařízení na síti (v organizaci). Pakety s takovouto adresou, jakožto adresou příjemce, nejsou směrovány pryč ze sítě.
- **Unicast** odpovídá klasické unicastové adrese z IP verze 4. (Čerpáno z [13])

2.4 Ethernet

Ethernet je technologií, hojně používanou na lokálních sítích (LAN). Má vztah k první a druhé vrstvě ISO/OSI modelu. Mezi její největší výhody, díky kterým se Ethernet stal tak populárním, patří především nízká cena, vysoká spolehlivost a flexibilita sítě. Technologie Ethernet zahrnuje několik standardů vytvořených organizací IEEE (Institute of Electrical and Electronics Engineers). (Čerpáno z [15])

Původní standard Ethernet o rychlosti 10 Mb/s byl poprvé vydán v roce 1980 konsorciem DECIntel-Xerox (známé jako DIX Ethernet standard). Zanedlouho přišla otevřená standardizace Ethernetu od IEEE vydaná pod číslem 802.3. Tento standard byl publikován v roce 1985 pod názvem *„IEEE 802.3 Carrier Sense Multiple Access with Collicion Detection (CSMA/CD) Access Method and Physical Layer Specifications“*. Dnes je běžně označován jako *10BASE2 (Ethernet 10BASE2)*. (Čerpáno z [15])

Postupem času s příchodem nových médií, mezi které patří kroucená dvoulinka a optická vlákna, vznikaly další varianty desetimegabitového Ethernetu, lišící se právě používaným médiem. Dále byl vytvořen stomegabitový Ethernet (100 Mb/s), gigabitový Ethernet (1 Gb/s) a desetigigabitový Ethernet (10 Gb/s). Tabulka 6 přehledně zobrazuje vybrané ethernetové systémy. (Čerpáno z [15])

Tabulka 6 – Přehled vybraných systémů Ethernet
Zdroj: Zpracováno dle [15]

IEEE Identifikátor	Rychlost	Médium
10BASE5	10 Mb/s	tlustý koaxiální kabel
10BASE2	10 Mb/s	tenký koaxiální kabel
10BASE-T	10 Mb/s	kroucená dvoulinka
10BASE-F	10 Mb/s	optické vlákno
100BASE-TX	100 Mb/s	kroucená dvoulinka alespoň kategorie 5
100BASE-FX	100 Mb/s	vícevidové optické vlákno
1000BASE-SX	1 Gb/s	vícevidové optické vlákno
1000BASE-LX	1 Gb/s	jednovidové nebo vícevidové optické vlákno
1000BASE-T	1 Gb/s	kroucená dvoulinka alespoň kategorie 5e
10GBASE-T	10 Gb/s	kroucená dvoulinka alespoň kategorie 6

2.4.1 Ethernetový rámec

Bloky dat, pomocí kterých se v Ethernetu přenášejí data z jednoho zařízení ke druhému, se nazývají **ethernetové rámce** (Ethernet Frames).

Obrázek 9 – Ethernetový rámec
Zdroj: Vlastní zpracování

Tento rámec „obaluje“ přenášená data dalšími potřebnými informacemi, díky kterým mohou jednotlivé hardwarové prvky s rámci pracovat. Struktura rámce je zobrazena na obrázku 9. (Čerpáno z [15])

Takový ethernetový rámec se skládá z polí:

- *preamble*, což je 64bitová sekvence signalizující začátek nového rámce,
- *destination address*, 48bitové hardwarové (MAC) adresy cílového rozhraní,
- *source address*, 48bitové hardwarové (MAC) adresy vysílajícího rozhraní,
- *type/length*, používané pro označení protokolu přenášeného v poli *data* nebo pro uložení informace o délce rámce,
- *data*, ve kterém jsou přenášena samotná data, která musí mít minimálně 46 bajtů a maximálně 1500 bajtů,
- *frame check sequence* (FCS), které nese kontrolní součet (CRC) z celého rámce. (Čerpáno z [15])

2.4.2 Adresace v Ethernetu

Ethernetový rámec je od odesílatele zaslán všem rozhraním na sdíleném médiu. Tato rozhraní mají vlastní 48bitovou adresu (MAC adresu). Ve chvíli, kdy rámec dorazí na jednotlivá rozhraní, provede se porovnání cílové adresy ethernetového rámce s adresou rozhraní, kdy v případě neshody je takovýto rámec zahozen. V opačném případě je rámec přijat a jeho data jsou předána vyšší vrstvě. Ethernetová 48bitová adresa se zapisuje jako posloupnost šesti hexadecimálních dvojic číslic oddělených dvojtečkami. Příklad takovéto ethernetové MAC adresy tedy může být například `3C:97:0E:19:9E:30`. (Čerpáno z [15])

V Ethernetu lze, podobně jako v IP adresovat i skupinu cílových zařízení (multicast) nebo všechna cílová zařízení na segmentu (broadcast). Pro takovéto případy jsou opět vyhrazeny speciální adresy. V případě multicastu jsou to adresy z rozsahu od `01:00:5E:00:00:00` do `01:00:5E:7F:FF:FF`. Pro multicastové skupiny je tedy vyhrazeno 23 bitů (2^{23} ethernetových adres). Broadcastová adresa má naproti tomu všechny bity nastavené na jedničku (`FF:FF:FF:FF:FF:FF`). Pokud se tato vyskytne v poli *destination address* ethernetového rámce, přijmou tento rámec ke zpracování všechna zařízení na daném segmentu. Takovýto segment sítě, kde všechna zařízení přijmou paket s broadcastovou adresou, se nazývá **broadcastová doména**. (Čerpáno z [15])

2.4.3 Opakovače a přepínače

Jedním ze základních stavebních prvků média pro provoz Ethernetu jsou kromě samotné kabeláže také opakovače a přepínače. Díky nim lze snadno vytvořit hvězdicovou topologii, která nabízí flexibilitu a škálovatelnost takto postavené sítě. Zároveň tato aktivní zařízení zesilují (opakují) signály, které jsou na dlouhých kabelech náchylné k rušení. (Čerpáno z [15])

Prvním takovým zařízením je ethernetový opakovač (hub, repeater hub). Takové zařízení obsahuje několik ethernetových portů pro připojení několika zařízení ke sdílenému médiu.

Práce opakovače je omezena na prosté opakování signálu všemi ostatními porty mimo port, kterým signál přišel. V praxi tedy dochází k zasílání ethernetových rámců všem zařízením, které jsou k opakovači připojeny. (Čerpáno z [15])

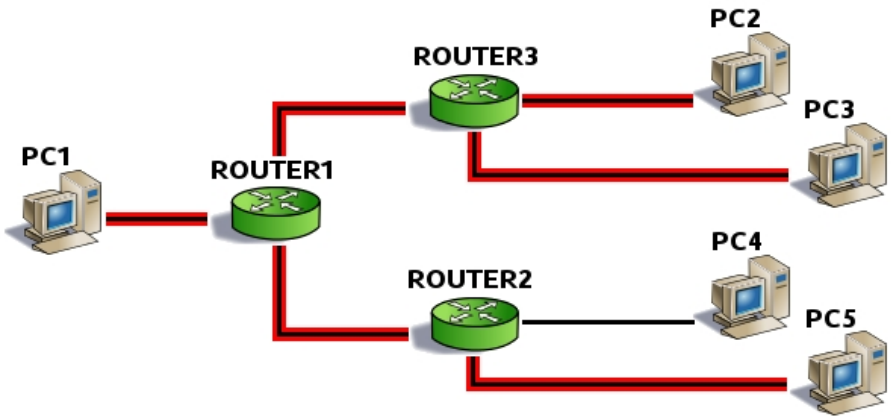
Naproti tomu ethernetový přepínač (switch, switching hub) je zařízení, které je schopné rozhodnout, kterým směrem má zaslat ethernetové rámce na základě cílové MAC adresy. Rozhodnutí provádí na základě databáze hardwarových (MAC) adres, kterou se sám naučí. V první fázi přepínač funguje stejným způsobem jako opakovač, nicméně zároveň si ukládá MAC adresy, které přečte v poli *source address* ethernetového rámce s příslušným rozhraním na které takový rámec přišel, do vnitřní databáze. U dalších rámců, které přichází na různá rozhraní přepínač čte cílovou MAC adresu a pokud tato již je v databázi, nerozešle rámec na všechna rozhraní, ale pouze na rozhraní uvedené k této hardwarové adrese. (Čerpáno z [15])

3 Technologie IP multicast

3.1 Principy multicastu

V počítačových sítích lze cílové stanice adresovat různými způsoby. Na jedné straně je to **unicastová komunikace**, při které je adresováno jedno koncové zařízení, kterému jsou data doručena. Na druhém konci tohoto pomyslného spektra to je **komunikace broadcastová**, kdy vysílající zařízení adresuje všechna ostatní zařízení na dané části počítačové sítě. V takovém případě je daný blok dat (rámec, paket) zaslán jednou a například na každém přepínači rozeslán všemi porty dále tak, aby všechna cílová zařízení tato data přijala. Na pomyslný prostředek, mezi unicasting a broadcasting, patří adresování určité skupiny počítačů a zařízení nazývané **multicasting**. (Čerpáno z [1], [2])

Multicasting je komunikace jednoho zařízení s několika jinými zařízeními (one-to-many), nebo komunikace několika zařízení s několika jinými zařízeními (many-to-many). Rozdíl oproti unicastu spočívá v tom, že blok dat, který je zaslaný jednou, je doručen několika zařízením. Při unicastové komunikaci lze stejného výsledku, doručení bloku dat několika zařízením, dosáhnout při opakovaném zaslání stejných dat těmto zařízením. To ovšem způsobuje výrazné navyšování nároků na přenosovou rychlost. Ve chvíli, kdy počítač například streamuje video o datovém toku 1 Mb/s dvaceti různým počítačům, při unicastové komunikaci potřebuje šířku pásma 20 Mb/s. V praxi bývá toto číslo díky režii ještě vyšší. Naproti tomu při využití multicastové komunikace není třeba stejné bloky dat zasílat znovu a znovu, a tak jsou nároky na šířku pásma daleko nižší, a tím i vyšší efektivita využití potenciálu sítě. V tomto konkrétním případě je pak potřebná šířka pásma 1 Mb/s (opomeneme-li režii). Příklad multicastové komunikace je vyobrazen na obrázku 11. (Čerpáno z [1], [2], [3], [16])



Obrázek 10 – Multicasting
Zdroj: Vlastní zpracování

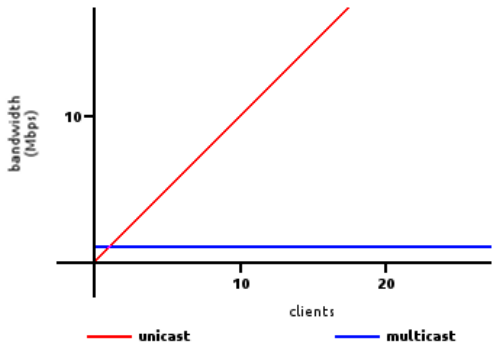
V příkladu zobrazeném na obrázku 10 komunikuje počítač označený jako PC1 s počítači PC2, PC3 a PC5. Jelikož všem zasílá stejná data (streamování videa), využívá k tomu multicastovou komunikaci. V takovém případě zašle každý blok dat pouze jednou a jednotlivé routery (ROUTER1, ROUTER2 a ROUTER3) směrují pakety (a v případě potřeby je zkopírují na více svých rozhraní) postupně k cílovým počítačům. Tím je ušetřena šířka pásma, protože PC1 zasílá každý paket pouze jednou a není třeba jednotlivé pakety pro různé adresáty znovu sestavovat.

3.2 Výhody multicastu

V různých podnikových sítích, které mají mnoho připojených uživatelů (zařízení), vyvstává požadavek na přístup více uživatelů ke stejným informacím v přibližně stejném čase. Díky využití multicastu pro distribuci takovýchto informací lze často snížit celkové nároky na šířku pásma sítě. Běžným příkladem zdroje takovýchto informací je například server, který streamuje multimediální obsah v reálném čase. (Čerpáno z [1], [2])

3.2.1 Šířka pásma

Jednou z největších výhod při použití multicastu je bezesporu úspora šířky pásma. Při použití klasického unicastu stoupá potřebná šířka pásma lineárně s připojením dalších a dalších uživatelů. Naproti tomu při použití multicastu je potřebná šířka pásma se stoupajícím počtem připojených uživatelů stále stejná. Graf těchto závislostí je zobrazen na obrázku 11. (Čerpáno z [1], [2])



Obrázek 11 – Streamování videa: unicast vs. multicast

Zdroj: Vlastní zpracování

Na obrázku je příklad, který odpovídá potřebné šířce pásma (svislá osa) pro streamování videa o datovém toku 1 Mbps v závislosti na počtu souběžně přijímajících klientů (vodorovná osa) pomocí unicastu a multicastu. Z obrázku je zřejmé, že potřebná šířka pásma je pro unicast přímo úměrná počtu připojených uživatelů, zatímco pro multicast je konstantní a odpovídá, i pro větší počet souběžných klientů, potřebné šířce pásma pro

jednoho uživatele při unicastu. Nutno podotknout, že na uvedeném obrázku je pro účely výkladu opomenuta režie.

3.2.2 Vytížení serveru

Využitím multicastu například pro streamování videa, které sleduje množství klitetů, lze znatelně ušetřit náklady na výkon zprostředkujícího serveru. V případě použití unicastu vzniká s každým dalším připojeným klientem další režie, což má za následek větší nároky na hardwarové komponenty použité na zařízení, které klientům danou službu nabízí. Jedná se zejména o výkon procesoru, operační paměť, výkon síťového rozhraní. Jakmile se v takovém případě začnou připojovat další klienti, které server musí obsloužit, dojde nutně k úplnému využití některé z těchto komponent a taková následně nebude schopna obsloužit další klienty v reálném čase. To bude mít za následek pořízení dalších a dalších serverů. (Čerpáno z [1], [2])

V případě multicastu ovšem zvýšení počtu klientů nebude zvyšovat nároky na jednotlivé komponenty, protože server potom streamuje multimediální data pouze jednou, a to pro všechny uživatele. Tím nevzniká požadavek na zvyšování výkonu jednotlivých komponent nebo dokonce pořizování dalších serverů. (Čerpáno z [1], [2])

3.2.3 Zatížení sítě

S úsporou šířky pásma úzce souvisí celkové zatížení síťových prvků, především směrovačů. Díky nižším nárokům na šířku pásma se snižuje i množství paketů, které sítí proudí a jsou potažmo zpracovávány jednotlivými směrovači. Nemusí to ovšem platit bez vyjímky. V případě že je směrovač nucen přijatý paket směrovat do více svých rozhraní najednou (je nucen vytvořit novou kopii pro každé rozhraní), klade to další nároky na hardwarové prostředky směrovače – především procesor a paměť. Pokud tedy směrovač nemá implementován efektivní mechanismus pro obsluhu takovýchto situací, může doba zpracování paketů značně narůstat s počtem rozhraní, kterými je třeba paket poslat. Na starších typech směrovačů bylo třeba pro každý nový paket alokovat novou část paměti, což vedlo k jejímu neúspornému využívání. Při velkém počtu kopií paketu pak byl směrovač nucen alokovat velké množství paměti. Nové směrovací algoritmy tento problém řeší předáváním ukazatele na původní paket (není tedy třeba alokovat nové zdroje), a tak šetří paměť i procesor. (Čerpáno z [1])

3.3 Nevýhody multicastu

Ačkoliv multicast přináší řadu výhod, které mohou zefektivnit využití například vnitropodnikové sítě, je stále třeba mít na mysli i omezení, které ze samotné podstaty multicastu plynou. Některé z nich jsou vysvětleny v této kapitole.

3.3.1 Nespolehlivý přenos

Multicastová komunikace je v protokolu IP, stejně jako unicastová, nespolehlivá. Pro

unicastovou komunikaci spolehlivost zajišťují protokoly vyšší vrstvy (typicky TCP na čtvrté vrstvě modelu ISO/OSI). Jelikož ale multicast je komunikace jeden k více (one-to-many), není nad IP multicastem možné protokol TCP použít. Při použití multicastu je běžně na čtvrté vrstvě ISO/OSI modelu použit protokol UDP (User Datagram Protokol), který je nespolehlivý. Při takovýchto technologiích je tedy nutné, aby aplikace, která využívá multicast, byla připravena, že některé pakety nemusí nezbytně dorazit k cíli. (Čerpáno z [1])

3.3.2 Zdvojené pakety

Jelikož směrovače zasílají kopie multicastových paketů několika různými rozhraními najednou, je riziko, že jedna z cílových stanic obdrží tentýž paket vícekrát než jednou, mnohem vyšší, než je tomu například při unicastu. Takovýto problém nastává především v sítích, jejichž topologie obsahuje více redundantních cest od odesílatele k adresátovi a použitý multicastový routovací protokol ještě nezkonvergoval a tudíž neodstranil redundantní cesty. (Čerpáno z [1])

3.3.3 Zahlcení sítě

Unicastová komunikace v IP sítích, kde je jako protokol na čtvrté vrstvě ISO/OSI modelu zvolen protokol TCP, zabraňuje zahlcení sítě a vyčerpání jejích zdrojů. Je to díky protokolu TCP, který implementuje mechanismy pro nastavení rychlosti datového přenosu. Jelikož při použití multicastu nelze pracovat s protokolem TCP (díky jeho one-to-many povaze), není zde implementovaná žádná ochrana proti vyčerpání šířky pásma, hardwarových prostředků směrovače a tím následnému zahlcení sítě. Nutno podotknout, že stejným problémem trpí při použití transportního protokolu UDP i unicastová komunikace. (Čerpáno z [1])

3.4 Adresace na L3 a L2

Narozdíl od unicastových adres, které identifikují právě jedno zařízení v IP síti, multicastové adresy specifikují libovolnou skupinu zařízení, která se k této skupině připojila a přejí si přijímat data zaslaná této skupině. (Čerpáno z [1])

3.4.1 Adresace v IP

Pro adresování takovýchto zařízení v protokolu IP jsou využity adresy ze třídy D. Tyto adresy začínají binárním prefixem `1110` a z toho je plynoucí rozsah adres třídy D od `224.0.0.0` do `239.255.255.255`. Z tohoto bloku adres vyhradila organizace IANA rozsah `224.0.0.0` až `224.0.0.255` pro použití v rámci jednoho segmentu sítě. Pakety s takovýmito adresami nejsou směrovači směrovány dále. (Čerpáno z [1], [2], [16])

IANA dále vyčlenila několik různých multicastových adres pro různé účely. Některé z nich jsou v privátním rozsahu a nejsou směrovány do jiných sítí, než na které byly zaslány. Takové pakety se dostanou pouze na zařízení v místní síti. Jiné adresy, jako například

skupina `224.0.1.1` pro NTP (Network Time Protocol), jsou veřejné a směrovače je mohou směrovat mezi jednotlivými sítěmi. Některé vybrané příklady z těchto adres s uvedeným významem jsou zobrazeny v Tabulce 7. (Čerpáno z [1])

Tabulka 7 – Příklady vyhrazených multicastových adres

Zdroj: Developing IP Multicast Networks [1]

Adresa	Využití	Vysvětlení
224.0.0.1	Všechna koncová zařízení	Adresuje všechna zařízení v daném segmentu sítě, která podporují multicast.
224.0.0.2	Všechny multicastové směrovače	Adresuje všechny směrovače na daném segmentu sítě, které podporují multicast.
224.0.0.4	DVMRP směrovače	Adresuje všechny směrovače používající routovací protokol DVMRP
224.0.0.5	OSPF směrovače	Adresuje všechny směrovače používající routovací protokol OSPF
224.0.0.9	RIP2 směrovače	Adresuje všechny směrovače používající routovací protokol RIP2
224.0.1.1	NTP	Protokol pro synchronizaci data a času

Dalším z vyčleněných rozsahů u multicastových adres je rozsah od `239.0.0.0` do `239.255.255.255`. Tyto adresy se nazývají adresy s administrativně omezeným rozsahem (angl. Administratively Scoped Multicast Addresses) a jsou využívány v privátních multicastových doménách. Určením jsou podobné unicastovým privátním rozsahům – slouží pro použití v privátních sítích a nejsou směrovány na Internet. (Čerpáno z [1], [16])

3.4.2 Adresace v IPv6

V protokolu IP verze 6 byl vyhrazen pro multicastové adresy rozsah začínající binárním prefixem `11111111`, zkráceně tedy `FF00::/8`. Další bity v multicastové IPv6 adrese mají speciální významy. Struktura IPv6 adresy je zobrazena na obrázku 12.

Obrázek 12 – IPv6 multicastová adresa

Zdroj: Vlastní zpracování

IPv6 multicastová adresa je rozdělena na čtyři pole:

- prvních osm bitů, které jsou pevně určeny a všechny mají binární hodnotu 1,
- pole *flags* (příznaky), z nichž první tři bity jsou rezervovány pro pozdější použití (tyto jsou nastaveny na 0) a čtvrtý bit označuje zda tato adresa patří mezi velmi

známé (angl. well-known) adresy (potom má hodnotu `0`) či je to přechodná (angl. transient) multicastová adresa (hodnota `1`),

- pole *scope* (rozsah), čtyřbitové pole, které je určeno k omezení rozsahu multicastové skupiny,
- *group ID* (identifikátor skupiny), identifikuje multicastovou skupinu. (Čerpáno z [13])

IPv6 tedy přináší několik nových vylepšení pro multicastovou adresaci. Pole *scope*, sloužící k omezení rozsahu multicastové skupiny, může nabývat 2^4, tedy šestnácti hodnot. Tyto hodnoty s přiřazenými rozsahy přehledně zobrazuje tabulka 8.

Tabulka 8 – Hodnoty pole scope
Zdroj: IPv6 – Theory, Protocol and Practise [13]

Value	Scope
0x0	reserved
0x1	interface-local scope
0x2	link-local scope
0x3	reserved
0x4	admin-local scope
0x5	site-local scope
0x8	organization-local scope
0xE	global scope
0xF	reserved

Všechny ostatní hodnoty, kterých může pole *scope* nabývat a nejsou uvedeny v Tabulce 8, nemají přiřazenou žádnou funkci. Nejrestriktivnější rozsah mají adresy, jejichž pole *scope* obsahuje hodnotu `0x1`, tedy interface-local scope. Takové pakety nejsou zaslány po žádné fyzické lince a smějí být obslouženy pouze v rámci vysílajícího zařízení. Dalším možným rozsahem platnosti je link-local scope. Takové pakety nejsou směrovány a zůstávají pouze v rámci daného segmentu sítě. Jejich ekvivalentem z IP verze 4 je rozsah `224.0.0.0./24`. Pole scope nastavené na hodnotu admin-local (`0x5`) označuje nejmenší rozsah, který musí být administrativně nakonfigurován, nevychází tedy z fyzické topologie sítě. Site-local scope omezuje rozsah na jednu lokalitu (budovu, společnost). Hodnota organization-local scope odpovídá rozsahu několika lokalit jedné organizace (komunikace například skrze VPN). Poslední, global scope, jsou adresy, které jsou směrované přes internet. (Čerpáno z [13], [17], [18])

3.4.3 Adresace v Ethernetu

U ethernetových MAC adres je vyhrazen poslední (nejméně významný) bit prvního oktetu pro signalizaci, zda je daná adresa a potažmo ethernetový rámec unicast nebo

multicast/broadcast. Pokud je tento bit nenastaven (má hodnotu `0`), je tato adresa unicastová, v opačném případě se jedná o multicastovou nebo broadcastovou adresu. Multicastové MAC adresy při použití IP multicastu začínají 24bitovým prefixem `01:00:5E`, následovaným dalším bitem nenastaveným (s hodnotou `0`). Tím zbývá pouze 23 bitů pro určení multicastové skupiny. (Čerpáno z [1], [2], [15])

Většina běžných ethernetových přepínačů nejsou schopny rozpoznat zařízení, která poslouchají dané multicastové skupině, a tak rámce určené pro multicastovou skupinu jednoduše opakují na všechna svá rozhraní (stejně jako rámce s broadcastovou adresou). Některé moderní high-end přepínače však obsahují implementaci metod pro rozpoznání zařízení poslouchajících multicastovým skupinám (IGMP snooping) a dokáží tak omezit propagaci multicastových rámců jen na potřebná rozhraní. (Čerpáno z [1], [15])

3.4.4 Mapování multicastových IP adres na ethernetové MAC adresy

Jak již bylo zmíněno, ethernetové multicastové MAC adresy začínají hexadecimálním prefixem `01:00:5E` následovaným nenastaveným bitem. Tato specifikace ponechává pouze 23 bitů pro identifikaci multicastové skupiny. Naproti tomu dvaatřicetibitové multicastové IP adresy začínají binárním prefixem `1110`, a tak na identifikaci skupiny zbývá 28 bitů. Pro potřeby multicastu je nutné 28 bitů označujících IP multicastovou skupinu namapovat do 23 bitů pro ní vyhrazených uvnitř adresy ethernetového rámce. (Čerpáno z [1], [2], [15])

Řešením tohoto problému je jednoduché oříznutí prvních 5 bitů identifikátoru IP multicastové skupiny. Tím se ovšem ztrácí část informace, což s sebou přináší nevýhodu v podobě kolize různých IP adres, které se mapují na jednu stejnou ethernetovou MAC adresu. Multicastových IP adres, které se dají namapovat na stejnou multicastovou MAC adresu je tedy 2^5, tj. 32. Problém vzniká například ve chvíli, kdy nějaký počítač přijímá pakety skupiny `224.1.1.1`. Nastaví tedy svůj hardware (ethernetovou síťovou kartu), aby procesoru zaslala přerušení, až obdrží vhodný rámec, a to s adresou `01:00:5E:00:01:01`. Nicméně v síti existuje i server, který zasílá pakety pro skupinu `224.128.1.1`. Tyto pakety cestují v rámcích, které mají cílovou adresu taktéž `01:00:5E:00:01:01`. Procesor v počítači, který této skupině nenaslouchá je tedy přerušen, a tím je i nižší efektivita využití jeho procesorového času. (Čerpáno z [1], [2], [15])

Obrázek 13 – Příklad mapování IP adresy na ethernetovou MAC adresu

Zdroj: Vlastní zpracování

Na obrázku 13 je vyobrazen příklad mapování multicastové IP adresy `224.1.1.1` (na obrázku nahoře) na multicastovou ethernetovou MAC adresu `01:00:5E:00:01:01`

(dole). Bílé bity jsou pevně stanovené (prefixy pro multicastové adresy pro IP a multicast). Žlutě označené bity jsou ty, které se při mapování ztrácejí. Černě označené bity v obou adresách jsou shodné (namapované) bity.

3.4.5 Mapování multicastových IPv6 adres na ethernetové MAC adresy

U ethernetové MAC adresy je pro namapování multicastové IPv6 adresy vyčleněn hexadecimální prefix `33:33`. Z toho plyne, že zbylých 32 bitů je tedy volných. Identifikátor skupiny u IPv6 je dlouhý 112 bitů. Mapování mezi IPv6 multicastovou adresou a ethernetovou adresou tedy probíhá, podobně jako u IPv4, oříznutím prvních bitů. V tomto případě jich je ovšem 80. (Čerpáno z [19])

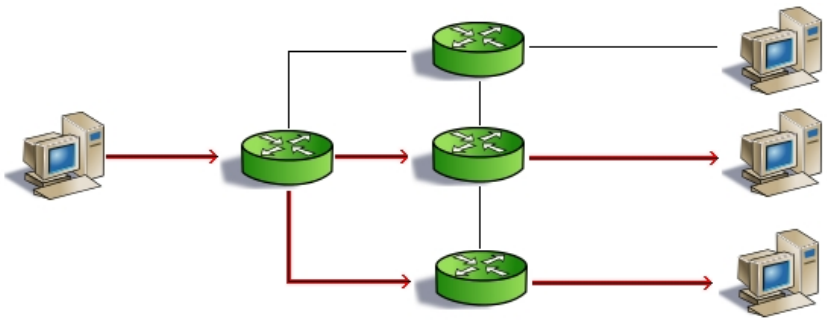
3.5 Distribuční stromy

Při použití unicastové komunikace prochází paket sítí z bodu A do bodu B skrze jednotlivé směrovače a další síťová zařízení. Pro popis této cesty při použití multicastu, kdy paket cestuje do více cílových zařízení současně, se používají takzvané multicastové distribuční stromy. Ty se dělí do dvou skupin:

- **zdrojové stromy** (angl. source trees),
- **sdílené stromy** (angl. shared trees). (Čerpáno z [1])

3.5.1 Zdrojové stromy

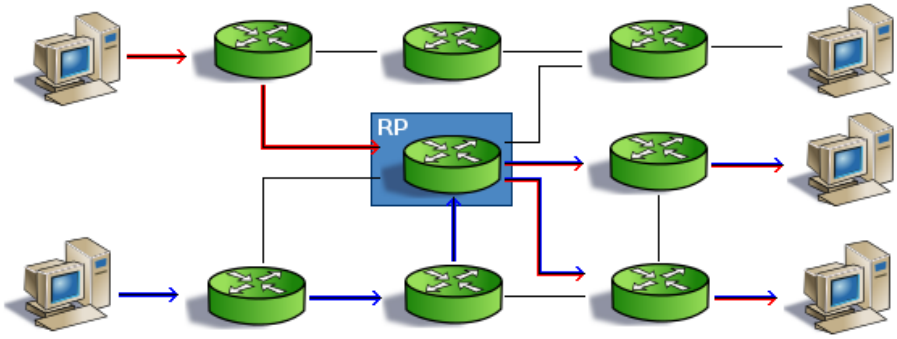
Zdrojový strom je nejjednodušším typem multicastového distribučního stromu. Jeho kořen je umístěn ve zdroji multicastového vysílání a jeho listy jsou účastníci multicastové skupiny, která je příjemcem tohoto vysílání. Tento strom využívá nejkratší cesty od kořene k listům (od vysílače k cílovým stanicím, které jsou členy tohoto stromu), a tak bývá označován jako SPT (shortest path tree). Příklad takového zdrojového stromu je zobrazen na obrázku 14. (Čerpáno z [1], [2])



Obrázek 14 – Zdrojový strom
Zdroj: Vlastní zpracování

3.5.2 Sdílené stromy

Narozdíl od zdrojových stromů, které mají svůj kořen umístěn ve zdroji (vysílači) multicastových paketů, sdílené stromy používají kořen, který je umístěn na nějakém místě v síťové topologii. Takovýto kořen se nazývá, v závislosti na použitém multicastovém směrovacím protokolu, **rendezvous point** (RP, bod setkání) nebo **core** (jádro). Sdílené stromy jsou pak označovány také jako RP trees (RPT) nebo core-based trees (CBT). V případě sdílených stromů vysílače zasílají pakety směrem ke kořeni stromu, odkud jsou pak dále distribuovány směrem k příjemcům (počítačům přihlášeným k multicastové skupině). Příklad takovéhoto sdíleného stromu je zobrazen na obrázku 15. (Čerpáno z [1], [2])



Obrázek 15 – Sdílený strom
Zdroj: Vlastní zpracování

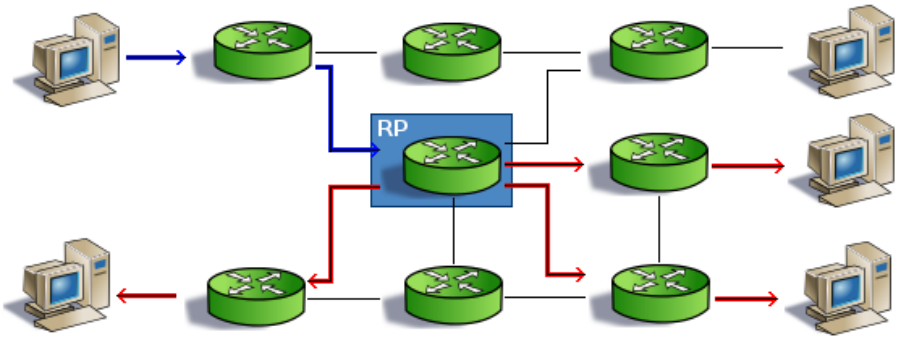
Na příkladu je naznačen sdílený strom, ve kterém jsou dva vysílače (počítače vlevo, od kterých vedou červené a modré šipky), které zasílají data určená pro multicastovou skupinu směrem k rendezvous pointu. Ten pak tato data přeposílá cílovým počítačům, přihlášeným k této multicastové skupině (počítače vpravo, ke kterým vedou červeno-modré šipky).

Sdílené distribuční stromy se dají, podle směru, kterým provoz stromem putuje, rozdělit na dva typy:

- **jednosměrné**, kde data ve stromu proudí pouze jedním směrem, a to od kořene stromu ke klientům,
- **obousměrné**, kde multicastový provoz může téci v opačném směru tak, aby obsloužil všechny přijímače. (Čerpáno z [1], [2])

Jednosměrné sdílené stromy dovolují, aby multicastový provoz tekl pouze směrem, a to od kořene k přijímačům tohoto provozu. Vysílače jsou tedy odkázání na to využít nějaký vlastní prostředek k tomu, aby dopravily multicastová data ke kořeni stromu. Jednou z takovýchto metod, kterou směrovací multicastové protokoly používají, je například zasílání multicastového provozu pomocí zdrojového stromu. V případě, že zdrojový strom bude mít kořen ve vysílači multicastového provozu a kořen sdíleného stromu (rendezvous

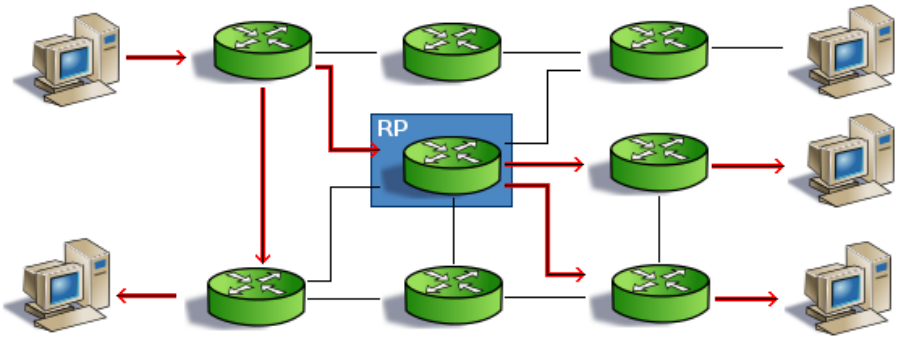
point) se stane členem tohoto stromu, je komunikace mezi vysílačem a sdíleným stromem navázána. Zároveň je tím zaručeno, že data od vysílače ke kořeni sdíleného stromu putují nejkratší cestou. Příklad jednosměrného sdíleného stromu je zobrazen na obrázku 16. (Čerpáno z [1])



Obrázek 16 – Jednosměrný sdílený strom
Zdroj: Vlastní zpracování

Na zobrazeném příkladu je jeden vysílač, a to počítač v levém horním rohu obrázku. Směrovač uprostřed je zvolen jako rendezvous point, od kterého jsou multicastová data distribuována pomocí sdíleného stromu třem koncovým počítačům (červené šipky). Vysílající stanice zasílá data směrem k rendezvous pointu pomocí stromu nejkratších vzdáleností (SPT).

Oproti jednosměrným, obousměrné sdílené stromy dovolují, aby data proudila oběma směry stromu. To umožňuje aby vysílač zasílal data proti směru stromu. Příklad takovéhoto obousměrného stromu je zobrazen na obrázku 17. (Čerpáno z [1])



Obrázek 17 – Obousměrný sdílený strom
Zdroj: Vlastní zpracování

Obousměrný sdílený strom, který je uveden na obrázku má kořen opět v prostředním směrovači. Vysílač, který je vlevo nahoře zasílá data prvnímu směrovači, který je posílá oběma směry stromu (směrem k rendezvous pointu a zároveň směrem k přijímači vlevo dole).

3.6 Směrování multicastu

V případě unicastové komunikace směrují směrovače jednotlivé pakety jednou cestou směrem od zdroje k adresátovi na základě IP adresy příjemce. Každý router se rozhoduje, kam paket zaslat, na základě cílové adresy a jejího vyhledání (nebo nadřazeného bloku adres) ve své routovací tabulce. Tím získá informaci, kterým svým rozhraním má paket zaslat. V případě multicastu ovšem takovýto způsob nelze použít, protože paket je adresován skupině cílových zařízení. Z toho důvodu může být rozhraních, kterými má paket opustit směrovač, více. Směrování multicastových paketů je proto více komplexní, než směrování unicastových paketů. (Čerpáno z [1], [16])

3.6.1 Reverse path forwarding

Techniku směrování na základě zpětné cesty (angl. reverse path forwarding) využívá většina multicastových směrovacích protokolů. Když multicastový paket dorazí na rozhraní směrovače, směrovač vykoná RPF kontrolu (angl. RPF check). Pokud je tato kontrola úspěšná, je paket na základě dalších kritérií směrován dále, v opačném případě je paket zahozen. (Čerpáno z [1], [2], [16])

RPF kontrola je vlastně ujištění, zda rozhraní směrovače, na které paket dorazil, je ve směru ke zdroji multicastového provozu. To zabraňuje vzniku smyček ve směrování paketu. Rozhodování probíhá na základě zdrojové adresy paketu (cílová je označení multicastové skupiny), podle které je určeno, zda paket zahodit nebo směrovat dále. Samotné určení, zda paket prošel kontrolou či nikoliv je odlišné pro různé směrovací protokoly. V některých případech směrovače udržují vlastní multicastovou routovací tabulku, na základě které se rozhodují. Mezi tyto protokoly patří například DVMRP (Distance Vector Multicast Routing Protocol). Jinou technikou je rozhodnutí na základě klasické unicastové routovací tabulky směrovače. Takto se chovají například protokoly PIM (Protocol Independent Multicast) nebo CBT (Core Based Tree). (Čerpáno z [1], [2], [16])

3.6.2 Multicastová směrovací tabulka

Každý distribuční strom může být v paměti směrovačů uložen v takzvaných multicastových směrovacích tabulkách (angl. multicast route table, multicast forwarding cache). V této tabulce jsou záznamy, které určují, k jakým příchozím rozhraním náleží která odchozí rozhraní. Rozdíl je u obousměrných sdílených stromů, u kterých nezáleží na tom, které z rozhraní je příchozí a které odchozí (multicastový provoz může proudit oběma směry). Směrovače pro každou multicastovou skupinu běžně určí příchozí rozhraní, na kterém provádí RPF kontrolu. V případě změny multicastového provozu (změny v distribučním stromu) je směrovač nucen přepočítat, které z rozhraní bude příchozí, aby správně reagoval na změny v síti. (Čerpáno z [1], [2])

3.6.3 Práh TTL

Každý směrovač, který směruje paket dále, sníží jeho hodnotu TTL o jedna. Pokud tato hodnota dosáhne nuly, je paket zahozen. Na směrovačích podporujících multicast lze na jednotlivá jejich rozhraní aplikovat takzvaný práh TTL (angl. TTL threshold), který představuje hranici, pod kterou nesmí TTL příchozího multicastového paketu být, jinak je paket zahozen. (Čerpáno z [1])

Tato technika umožňuje administrativní dohled nad multicastovým provozem a nazývá se také TTL scoping (stanovení rozsahu za pomoci TTL). Díky nastavení těchto hranic v síti je možno například udržet daný multicastový provoz v rámci určité oblasti sítě. (Čerpáno z [1])

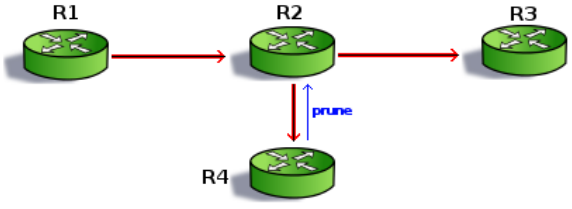
3.6.4 Rozdělení multicastových routovacích protokolů

Multicastové routovací protokoly lze rozdělit do třech skupin, podle způsobu zasílání multicastového provozu:

- **dense mode protokoly**, do kterých patří DVMRP a PIM-DM,
- **sparse mode protokoly**, kam patří například PIM-SM a CBT,
- **link-state protokoly**, kam se řadí MOSPF. (Čerpáno z [1], [2])

3.6.5 Dense mode protokoly

Dense mode protokoly jsou multicastové směrovací protokoly, určené pro sítě a služby, ve kterých většina zařízení na síti přijímá multicastový provoz – jsou členem této multicastové skupiny. K doručování paketů se využívají stromy nejkratších vzdáleností (SPT). Práce takového dense mode směrovacího protokolu je rozesílat pakety do všech částí sítě. Tomuto procesu se říká **flooding** (zamořování). V takovém případě je multicastový paket, který dorazí na rozhraní směrovače, rozeslán na všechna ostatní rozhraní tohoto směrovače. Takovýmto způsobem se všechny multicastové pakety dostanou ke všem zařízením na síti, i těm, které se z multicastové skupiny odhlásí. Z důvodů ušetření zdrojů pak může směrovač, k jemuž nějakému rozhraní není připojeno žádné zařízení této multicastové skupiny, dát takovéto rozhraní do stavu **pruned** (potlačeno). V takovém případě nebude zasílat multicastové pakety na toto rozhraní. (Čerpáno z [1], [2], [16])



Obrázek 18 – Prune message
Zdroj: Vlastní zpracování

Na obrázku 18 je zobrazen příklad sítě s multicastovým provozem za použití dense mode protokolu. Zdroj vysílání zasílá multicastový provoz směrovači R1, ten ho dále přeposílá směrovači R2, který replikuje pakety na všechna svá zbývající rozhraní – směrovačům R3 a R4. Ve chvíli, kdy za směrovačem R4 není žádné zařízení přihlášené k multicastové skupině, zašle směrovači R2 takzvanou **prune message** (zprávu o odříznutí), díky které si směrovač R2 zařadí příslušné rozhraní do stavu pruned. To způsobí, že další multicastové pakety již nebude na toto rozhraní zasílat a směrovač R4 tedy žádné další nebude přijímat. (Čerpáno z [1], [2], [16])

Zařazení rozhraní do stavu pruned je časově omezené. Tento čas je různý v závislosti na použitém routovacím protokolu. Jakmile toto časové omezení vyprší, je rozhraní opět vyjmuto ze stavu pruned a vráceno do původního stavu. V takovém případě může opět směrovač, pokud stále nemá na svém segmentu sítě zařízení náležící do skupiny, zaslat novou prune message, díky které bude rozhraní opět přeřazeno zpět do stavu pruned. (Čerpáno z [1], [2])

Další technika, která se u dense mode protokolů využívá je tzv. **grafting** (roubování). Jedná se rychlé znovupřipojení segmentu sítě, který je ve stavu pruned. Směrovač ihned zjistí, pokud se některé ze zařízení přihlásí k multicastové skupině a zašle takzvanou **graft message** (zprávu o naroubování) směrem ke zdroji vysílání. Sousední směrovač, který měl příslušné rozhraní ve stavu pruned, může tento stav ihned zrušit a multicastový provoz je tak zasílán novým účastníkům. (Čerpáno z [1])

3.6.6 Sparse mode protokoly

Narozdíl od dense mode protokolů, sparse mode protokoly nepřeposílají pakety všemi rozhraními a nezamořují síť multicastovým provozem. Jsou určené pro sítě, kde se jen menší část uživatelů přihlašuje k multicastové skupině. (Čerpáno z [1])

Směrovače, tedy nerozesílají multicastový provoz do doby, dokud není explicitně vyžádán. Směrovač, ke kterému jsou připojena zařízení, která se přihlásí ke skupině, zasílá zprávy o připojení (angl. **join messages**) směrem ke zdroji multicastového vysílání. Zasíláním těchto zpráv o připojení až ke kořeni stromu – rendezvous pointu, popřípadě k core, dojde k vybudování nové větve sdíleného stromu. Tyto zprávy se musí zasílat periodicky, jinak dojde ke smazání stavů na rozhraních směrovačů (doba platnosti). (Čerpáno z [1], [2], [16])

V některých případech (PIM-SM), jsou používány i zprávy o připojení k vytvoření stromu nejkratších vzdáleností (SPT). Tyto můžou sloužit ke zkrácení cesty multicastového provozu díky vynechání kořene sdíleného stromu. (Čerpáno z [1]).

V případě, že multicastový provoz již dále není potřebný, lze u sparse mode protokolů zasílat **prune message** zprávy (zprávy o potlačení). Například pokud směrovač zjistí, že už nemá připojená žádná zařízení, které multicastovému provozu naslouchají, posílá tuto prune message směrem ke kořeni stromu, aby ostatní směrovače již nemusely multicastový

provoz tímto směrem zasílat a zároveň nemusely čekat na vypršení doby platnosti. V takovém případě to je z hlediska úspory síťových zdrojů efektivnější řešení. (Čerpáno z [1])

3.6.7 Link-state protokoly

Link-state protokoly, podobně jako dense mode protokoly, používají k doručování multicastového provozu stromy nejkratších vzdáleností (SPT). Narozdíl od nich však nepoužívají mechanismus rozesílání paketů všemi rozhraními kromě příchozího. Oproti tomu zasílají speciální multicastové informace o stavu linky, díky kterým identifikují, kde se nachází zařízení připojená k dané multicastové skupině. Každý směrovač pak využívá tyto informace k sestavení nejkratší cesty ke všem příjemcům multicastového provozu. (Čerpáno z [1]).

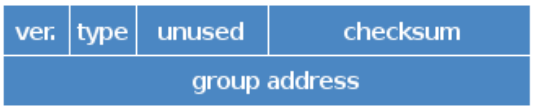
3.7 Protokol IGMP

Internet Group Management Protocol (IGMP) je jedním ze stavebních kamenů IP multicastové komunikace. Jedná se o protokol, který je primárně určen ke komunikaci mezi cílovými zařízeními a směrovači. Základními zprávami, které pomocí tohoto protokolu počítače zasílají směrovači, jsou požadavky o příjem provozu multicastové skupiny a požadavky o ukončení příjmu tohoto provozu. Protokol IGMP je k těmto účelům využíván nehledě na zvolený multicastový směrovací protokol. IGMP je nedílnou součástí protokolu IP a všechna zařízení, která si přejí přijímat multicastový provoz, musí protokol IGMP implementovat. IGMP pakety jsou zasílány uvnitř IP paketů, u kterých je v poli *protocol*, vyplněno číslo 2 (značí IGMP). Tyto pakety mají dále nastaveno pole *TTL* na hodnotu 1. Znamená to, že IGMP zprávy nejsou směrovány a dostanou se pouze na nejbližší směrovač. (Čerpáno z [1], [2], [16], [20])

Směrovače si udržují pro jednotlivé multicastové skupiny seznam rozhraní, za kterými jsou zařízení náležící těmto skupinám. Tyto seznamy budují na základě IGMP zpráv, které koncová zařízení směrovači zasílají. Těmito rozhraními potom zasílají multicastový provoz odpovídajícím koncovým zařízením. (Čerpáno z [1])

3.7.1 IGMP verze 1

První verze protokolu IGMP (IGMPv1) byla definována v RFC 1112 a vydána roku 1989.



Obrázek 19 – Zpráva IGMP verze 1
Zdroj: Vlastní zpracování

Zpráva protokolu IGMP verze 1 obsahuje pole:

- *version*, určující verzi protokolu (1),
- *type*, které určuje typ zprávy (membership query nebo membership report),
- *checksum*, kontrolní součet,
- *group address*, což je adresa multicastové skupiny, jíž se zpráva týká. (Čerpáno z [1], [2])

Směrovač, který je na daném segmentu sítě zodpovědný za zasílání IGMP zpráv, zasílá v případě IGMPv1 periodicky zprávu typu **membership query** (dotaz na členství) všem stanicím v této lokální síti (`224.0.0.1`). Standardní nastavení doby, po které se opakuje zasílání těchto zpráv, je 60 sekund. Počítač, který je členem multicastové skupiny, zašle IGMP zprávu typu **membership report** (zpráva o členství) na multicastovou adresu skupiny, které je členem. Tím se směrovače dozví, že na této lokální síti jsou zařízení, která si přejí přijímat multicastový provoz dané skupiny a mohou toto rozhraní zařadit do seznamu rozhraní pro tuto skupinu. Pokud je v lokální síti více zařízení, která si přejí dostávat provoz dané multicastové skupiny, nemusí již zasílat zprávu membership report. Výsledkem tohoto procesu je, že směrovače znají multicastové skupiny, jejichž provoz mají na tuto lokální síť (příslušným rozhraním) zasílat. (Čerpáno z [1], [2], [10])

IGMPv1 používá takzvaný **report suppression mechanism** (mechanizmus potlačování zpráv) aby omezil počet IGMP paketů na lokální síti. Ve chvíli, kdy IGMP membership query dorazí na koncové zařízení, začne odpočítávání časovače pro každou multicastovou skupinu, které je tento počítač členem. Každý takový časovač je počátečně nastaven na náhodnou hodnotu mezi 0 a 10 sekundami. Počítač zasílá zprávu membership report až po vypršení tohoto časovače a to jen v případě, že během odpočítávání nedostal stejnou zprávu od jiného počítače v síti. Díky tomu je omezen počet zpráv typu membership report na lokální síti. (Čerpáno z [1], [10])

Proces přihlášení počítače k dané multicastové skupině lze urychlit, pokud počítač ihned při vzniku takovéhoto požadavku zašle směrovači membership report. Jakmile směrovač obdrží takovýto membership report, zařadí dané rozhraní do svého seznamu pro tuto multicastovou skupinu a začne na něj multicastové pakety rozesílat. Počítač tak nemusí čekat, než vyprší interval a směrovač rozešle své membership query. (Čerpáno z [1], [10])

V případě, že daný segment sítě obsahuje více směrovačů než jeden, je volba o tom, který z nich bude zodpovědný za zasílání zpráv, nechána na použitém multicastovém směrovacím protokolu. (Čerpáno z [1])

3.7.2 IGMP verze 2

Druhá verze protokolu IGMP byla standardizována organizací IETF v listopadu roku 1997 a přinesla několik úprav oproti původní verzi. (Čerpáno z [1], [10])

V IGMP verze 2 jsou membership query zprávy rozděleny do dvou kategorií: **general query** (obecný dotaz), který má stejnou funkci jako membership query z první verze

a **group-specific query**, který představuje dotaz na jednu konkrétní multicastovou skupinu. Proces zasílání membership query a membership report je totožný s tím v první verzi. (Čerpáno z [1], [10])

Zpráva má, oproti první verzi, trochu odlišný formát. Formát zprávy v IGMP verze 2 je zobrazen na obrázku 20.

Obrázek 20 – Zpráva IGMP verze 2
Zdroj: Vlastní zpracování

Pole *type* bylo sloučeno s polem *version* a nyní zabírá celých 8 bitů. Hodnoty jednotlivých zpráv používaných v IGMP verze 2 jsou nastaveny tak, aby zaručily zpětnou kompatibilitu s předchozí verzí. Nevyužité místo nyní vyplňuje pole *maximum response time*, které dává směrovači možnost zadat maximální čas, do kterého musí zařízení odpovědět. Tento čas počítače používají jako horní limit pro náhodné číslo, kterým inicializují svůj časovač po obdržení membership query. Směrovač tak může regulovat latenci procesu přihlášení do skupiny. (Čerpáno z [1], [10])

Druhá verze IGMP obsahuje nový typ zprávy, takzvanou **leave group messag**e (zpráva o opuštění skupiny). Tyto zprávy zasílají počítače ihned při opuštění multicastové skupiny na adresu `224.0.0.2` (všechny směrovače na tomto segmentu). Směrovač v takovém případě, když obdrží zprávu o opuštění skupiny, rozešle group-specific query, kterým se ptá, zda je na této síti nějaké zařízení, které si přeje multicastový provoz této skupiny přijímat. Pokud takové zařízení na síti je, zašle membership report pro tuto skupinu a směrovač tak nepřestává zasílat multicastový provoz na příslušné rozhraní. Naproti tomu, pokud takové zařízení již na této síti není a směrovač neobdrží membership report v odpovídajícím čase, je zařízení odstraněno ze seznamu pro tuto skupinu a multicastový provoz této skupiny již není dále zasílán. (Čerpáno z [1], [2], [10])

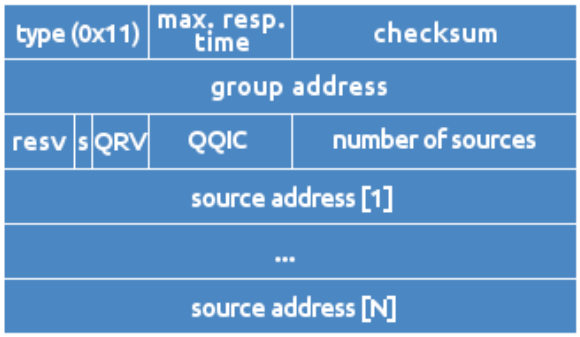
Další důležitou vlastností IGMP verze 2 je možnost volení směrovače zodpovědného za zasílání zpráv. Taková možnost v předchozí verzi chyběla a volba zodpovědného směrovače byla ponechána na multicastovém routovacím protokolu. IGMP verze 2 používá pole *group address* ve zprávě general query ke zvolení zodpovědného směrovače. (Čerpáno z [1], [10])

Každý směrovač na síti po svém startu zasílá zprávu general query, ve které je v poli *group address* adresa jeho rozhraní do této sítě. Zprávy jsou zasílány všem zařízením na síti (`224.0.0.1`). Pokud některý směrovač přijme tuto zprávu, porovná zdrojovou adresu zprávy se svou vlastní adresou odpovídajícího rozhraní. Zodpovědným směrovačem se stává ten, který má nejnižší IP adresu na rozhraní do této sítě. Tento proces se periodicky opakuje, aby v případě například havárie směrovače byl zvolen nový. (Čerpáno z [1], [10])

3.7.3 IGMP verze 3

Poslední verze IGMP, verze 3, byla vydána v roce 2002. Tato verze přináší významné změny oproti předchozím verzím. Jedním z největších zlepšení je možnost počítačů zvolit si zdroj nebo zdroje multicastového vysílání dané skupiny. (Čerpáno z [1], [2], [21])

Zpráva IGMP verze 3 doznala oproti předchozím verzím značných změn. Samotné implementace IGMP verze 3 jsou však zpětně kompatibilní se staršími verzemi. Na obrázku 21 je vyobrazena struktura IGMP membership query zprávy. (Čerpáno z [2], [21])



Obrázek 21 – Membership query v IGMPv3
Zdroj: Vlastní zpracování

Prvních 64 bitů je stejných jako u předchozí verze. V poli *type* je pro membership query hodnota `0x11`. Pole *maximum response time*, *checksum* a *group address* mají stejný účel jako ve verzi 2. Pole, která jsou ve verzi 3 nová:

- *resv* (reserved), vyhrazené pro pozdější účely, nyní je ignorováno,
- *s flag* (příznak s), pokud je nastaven na 1, dává směrovačům najevo, aby neposílaly odpovědi na příchozí periodicky posílané membership query,
- *QRV* (querier's robustness variable), hodnota mezi 0 a 7, značí kolikrát zařízení opakují zasílání zprávy,
- *QQIC* (Querier's Query Interval Code), hodnota intervalu, po kterém směrovač zodpovědný za zasílání membership query posílá zprávy,
- *number of sources*, počet zdrojových adres obsažený v tomto membership query,
- *source address [i]*, zdrojové adresy, které jsou pro danou multicastovou skupinu dostupné. (Čerpáno z [21])

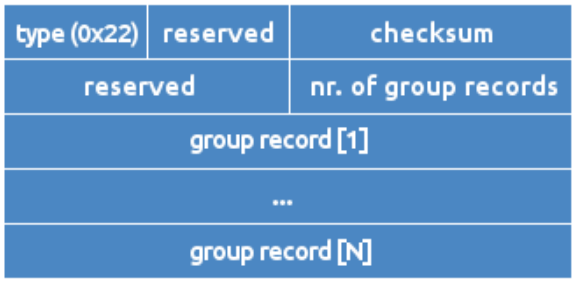
Membership query mohou být v této verzi IGMP 3 různé typy:

- **general query** (obecný dotaz), kterou zasílá směrovač, aby se dozvěděl kompletní seznam multicastových adres, kterým si přejí počítače na této síti naslouchat,
- **group-specific query** (dotaz na skupinu) zasílá směrovač aby zjistil, zda si některý počítač na síti přeje přijímat provoz jedné konkrétní skupiny,

- **group-and-source-specific query** (dotaz na skupinu a zdroj) zasílá směrovač aby se dozvěděl, provoz kterých zdrojů dané multicastové skupiny si počítače přejí přijímat. (Čerpáno z [21])

General query zprávy jsou zasílány všem zařízením na síti (skupina `224.0.0.1`), group-specific a group-and-source specific query zprávy jsou zasílány na adresu skupiny, jíž se dotaz týká. (Čerpáno z [21])

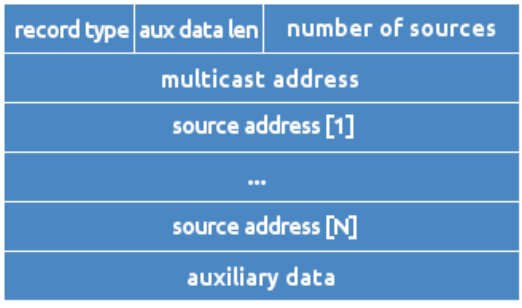
Struktura membership report zprávy je oproti předchozím verzím taktéž do značné míry změněna. Schéma membership report je zobrazeno na obrázku 22.



Obrázek 22 – Membership report v IGMPv3
Zdroj: Vlastní zpracování

Nově se skládá z několika bloků nazývaných **group record**, kdy každý odpovídá některé multicastové skupině a zvoleným zdrojům multicastového provozu. Jednotlivá pole, které membership report obsahuje jsou:

- *type*, které má hodnotu `0x22`, značí IGMPv3 membership report,
- *reserved*, jsou pole, která jsou ignorována, rezervována pro pozdější využití,
- *number of group records*, počet záznamů typu group record,
- *group record [i]*, záznamy group record, odpovídající multicastovým skupinám. (Čerpáno z [21]).



Obrázek 23 – Group Record
Zdroj: Vlastní zpracování

Na obrázku 23 je zobrazeno schéma záznamu group record. Skládá se z následujících polí:

- *record type*, typ záznamu, který může nabývat hodnot: current-state record dělící se na `MODE_IS_INCLUDE` a `MODE_IS_EXCLUDE`, filter-mode-change record dělící se na `CHANGE_TO_INCLUDE_MODE` a `CHANGE_TO_EXCLUDE_MODE` nebo source-list-change record (`ALLOW_NEW_SOURCES, BLOCK_OLD_SOURCES)`,
- *aux data len*, které signalizuje délku přídavných dat,
- *number of sources*, signalizující kolik zdrojových adres je přítomno v tomto záznamu,
- *multicast address* značí adresu skupiny, které se tento záznam týká,
- *source address [i]* jsou zdrojové adresy v tomto záznamu,
- *auxiliary data* jsou přídavná data, v IGMPv3 se nepoužívají. (Čerpáno z [21])

Proces fungování protokolu IGMP verze 3 lze popsat zvlášť pro koncová zařízení, která přijímají multicastový provoz (počítače, směrovače) a zařízení, která na lokální síti tento provoz zprostředkovávají (směrovače). Z pohledu koncových zařízení existují dvě události, na které protokol IGMP verze 3 reaguje nějakou z akcí: změna stavu naslouchajícího rozhraní a příjem IGMP dotazu (membership query). (Čerpáno z [21])

Při změně stavu naslouchajícího rozhraní, například při změně zdroje, od kterého chce počítač dostávat multicastový provoz, vysílá zařízení state-changed report. Rozhraní je pro multicastovou skupinu nastaveno na jeden z filtrovacích módů (**filter mode**) **exclude** nebo **include**. Dále si rozhraní společně s tímto módem udržuje seznam zdrojových adres (source list), na které je tento mód aplikován. Mód include společně se zdrojovými adresami značí, že počítač chce zasílat multicastová data této skupiny pouze od zmíněných zdrojů. V případě módu exclude jsou však zdroje, které jsou v seznamu, potlačeny a multicastová data jsou přijímána od všech ostatních. Zpráva pak obsahuje jednotlivé záznamy group record, jejichž typ a obsah je závislý na porovnání filtrovacího módu a seznamu zdrojů pro danou multicastovou adresu, a to před a po změně. Výsledkem je zpráva, která obsahuje záznamy group record odpovídající aktuálně změněnému stavu rozhraní. V tabulce 9 je zobrazen klíč k sestavování takovéto zprávy na základě minulého a nového stavu rozhraní. Aby bylo předejito možnosti, že některé multicastové směrovače nezachytí zprávu o změně stavu, je tato poslána několikrát, podle nastavení hodnoty *QRV*. (Čerpáno z [21])

Tabulka 9 – Sestavení State-Change Record

Zdroj: RFC3376 [21]

Minulý stav rozhraní	Nový stav rozhraní	Zasílaný State-Change Record
INCLUDE (A)	INCLUDE (B)	ALLOW(B-A), BLOCK (A-B)
EXCLUDE (A)	EXCLUDE (B)	ALLOW(A-B), BLOCK (B-A)
INCLUDE (A)	EXCLUDE (B)	TO_EX (B)
EXCLUDE (A)	INCLUDE (B)	TO_IN (B)

Po přijetí membership query zprávy zařízení neodpovídá okamžitě, ale čeká náhodný čas, ze shora ohraničený hodnotou pole *max response time*. Takové zařízení může dostávat různé typy zpráv membership query. Jakmile časovač vyprší, zařízení zašle membership report zprávu, ve které jsou záznamy typu current-state record obsahující filtrovací mód a seznam zdrojů, na všechny multicastové adresy, kterým dané zařízení naslouchá, případně na multicastovou adresu, jíž se membership query zpráva týká. (Čerpáno z [21])

Směrovač, který potřebuje znát skupiny, jejichž provoz má na připojenou síť zasílat, posílá periodicky general query, tedy obecné dotazy. Díky tomu získá od zařízení informace o tom, jaký provoz má směrovat do dané sítě. V případě, že některé zařízení na síti opustí skupinu, zasílá směrovač group-specific query zprávu, díky které se dozví, zda jsou na síti ještě nějaká zařízení, která chtějí provoz této skupiny přijímat. Jsou tedy posílány v reakci na state-change record, který zaslal některý ze systémů v síti. Aby se směrovač dozvěděl, zda provoz od některých zdrojů skupiny už nemá směrovat, zasílá group-and-source-specific query zprávy, díky kterým zjistí, zda je na síti nějaké zařízení, které si přeje dostávat provoz od konkrétních zdrojů multicastového vysílání. Tyto dotazy jsou zasílány pouze v reakci na state-change record zaslaný některým ze systémů na síti. (Čerpáno z [21])

Volba směrovače, zodpovědného za posílání dotazů, je shodná s mechanizmem představeným u IGMP verze 2. (Čerpáno z [21])

3.7.4 IGMP Snooping

Problémem stále zůstává adresace na druhé vrstvě ISO/OSI modelu, kde v případě například ethernetové multicastové MAC adresy jsou tyto multicastové rámce zasílány všemi rozhraními ethernetového přepínače a tím dochází k vysokým počtům ethernetových rámců na lokálních sítích. Jednou z technik, která tento problém řeší je takzvaný **IGMP Snooping**. (Čerpáno z [1], [16])

Jedná se v podstatě o analýzu IGMP zpráv, kdy přepínač rozpoznává, která multicastová data má zasílat jakým svým rozhraním na základě přihlašování počítačů ke skupinám a na základě jejich odhlašování. V případě procházejících membership report zpráv si přepínač zařadí příslušný port do multicastové CAM tabulky, kde jej přiřadí k odpovídající multicastové skupině. Naopak pokud zařízení opustí multicastovou skupinu, může směrovač dané rozhraní z tabulky odstranit. Na základě těchto poznatků se přepínač postupně dozví, že data té či oné multicastové skupiny má zasílat pouze například dvěma rozhraními, namísto všech a tím dochází k úspoře síťových zdrojů. (Čerpáno z [1], [16], [22])

4 Protocol Independent Multicast

PIM (angl. Protocol Independent Multicast) je multicastový směrovací protokol, který ke svému fungování využívá unicastové směrovací tabulky jednotlivých směrovačů. Narozdíl od některých jiných multicastových směrovacích protokolů (např. MOSPF) je tedy nezávislý na použitém směrovacím protokolu v síti a není rozhodující, jestli je směrovací tabulka směrovače naplněna například staticky nebo pomocí nějakého unicastového směrovacího protokolu (RIP, OSPF, BGP, atd.). (Čerpáno z [1], [2], [16])

Protokol PIM dokáže operovat v jednom ze dvou módů tak, aby pokryl potřeby kladené na směrování multicastového provozu v jednotlivých sítích. Tyto módy jsou:

- **dense mode**, určený pro sítě, ve kterých bude větší počet koncových zařízení přijímat multicastový provoz,
- **sparse mode**, určený pro sítě, ve kterých se k multicastové skupině připojuje jen menší část koncových zařízení. (Čerpáno z [1], [2], [16])

4.1 PIM Dense Mode

Jak bylo zmíněno výše, PIM-DM (PIM dense mode) je protokol, který není závislý na tom, jaký unicastový směrovací protokol je v síti použit. PIM-DM používá takzvané **flood-and-prune** chování, tzn. že je pro něj přirozené zasílat multicastový provoz do všech částí sítě a je na směrovačích, aby potlačily zasílání provozu tam, kde to není třeba. Tento proces je také označován termínem **data pushing** (tlačení dat), čímž je poukázáno na implicitní rozesílání multicastového provozu do všech segmentů sítě. Jelikož PIM-DM je dense mode protokol, jako prostředek k doručování multicastového provozu cílovým stanicím využívá sdílené stromy (SPT). (Čerpáno z [1], [2], [16])

Ve chvíli, kdy nějaký zdroj multicastového provozu začne rozesílat data, PIM-DM předpokládá, že všechna zařízení v síti si přejí tato data přijímat. Multicastový provoz se tedy začne rozesílat do všech částí sítě, přičemž díky algoritmu RPF je zaručeno, že nevzniknou smyčky ve směrování. Pokud některé části sítě neobsahují žádné zařízení, které je členem multicastové skupiny, je na směrovačích, aby provoz do této části sítě potlačily (**pruning**). Tento stav (prune state) je časově omezený a po vypršení tohoto času bude multicastový provoz do této sítě opět zasílán. Pokud je multicastový provoz do některé části sítě potlačován (pruned) a v téže části sítě se objeví zařízení, které se přihlásí do multicastové skupiny, směrovač tuto část sítě opět připojí k multicastovému provozu. Takovému procesu se říká **grafting** (roubování). (Čerpáno z [1], [23])

4.1.1 Objevení sousedů

Směrovač protokolu PIM zasílá periodicky zprávy pojmenované jako **PIM hello** na

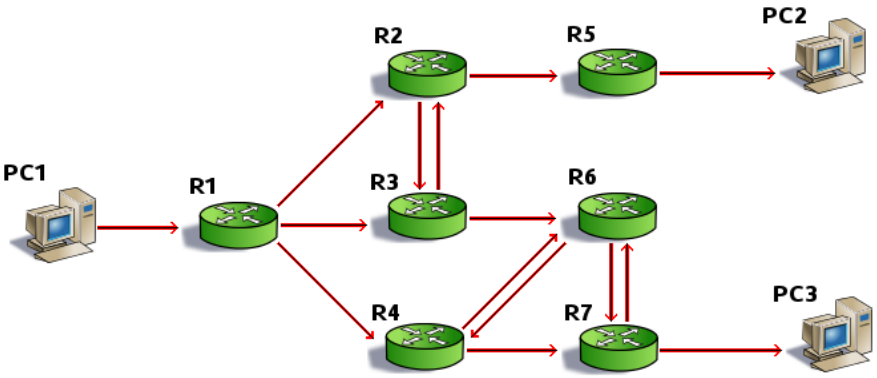
všechna svá rozhraní, na kterých je PIM nastaven jako aktivní. Díky těmto zprávám, zasílaným skupině `224.0.0.13` (všechny PIM směrovače), se směrovač dozví, které další směrovače protokolu PIM v síti jsou. PIM hello zprávy jsou zasílány typicky po 30 sekundách a pokud od některého směrovače tato zpráva nepřišla po trojnásobnou dobu (typicky 90 sekund), je tento směrovač považován za nefunkční. (Čerpáno z [1], [23])

Udržování sousedství je důležité z hlediska vytváření a udržování distribučních stromů. Dále jsou tyto zprávy také používány ke zvolení zodpovědného směrovače (angl. designated router). (Čerpáno z [1])

4.1.2 Směrování multicastového provozu

Jedním ze základních algoritmů, které PIM-DM používá, je RPF (reverse path forwarding). Díky této technice jsou multicastové pakety, které dorazí na rozhraní směrovače, kontrolovány, zda přicházejí ze žádoucího směru. Protokol PIM-DM k tomu používá unicastovou směrovací tabulku, ve které vyhledá záznam nejlépe se shodující se zdrojovou adresou multicastového paketu. Pokud se rozhraní uvedené k tomuto záznamu shoduje s rozhraním, jímž paket na směrovač dorazil, je paket dále zpracováván, v opačném případě je paket zahozen. (Čerpáno z [1])

V prvotní fázi tedy začíná protokol PIM-DM směrovat pakety, u nichž skončí test RPF s kladným výsledkem, všemi ostatními rozhraními mimo to, kterým daný paket na směrovač dorazil. Nutno podotknout, že tento multicastový provoz je rozesílán pouze rozhraními, které mají alespoň jednoho PIM souseda nebo přímo připojená koncová zařízení, patřící do multicastové skupiny. Příklad takové sítě, ve které je protokol PIM-DM v prvotní fázi, je zobrazen na obrázku 24. (Čerpáno z [1], [2])



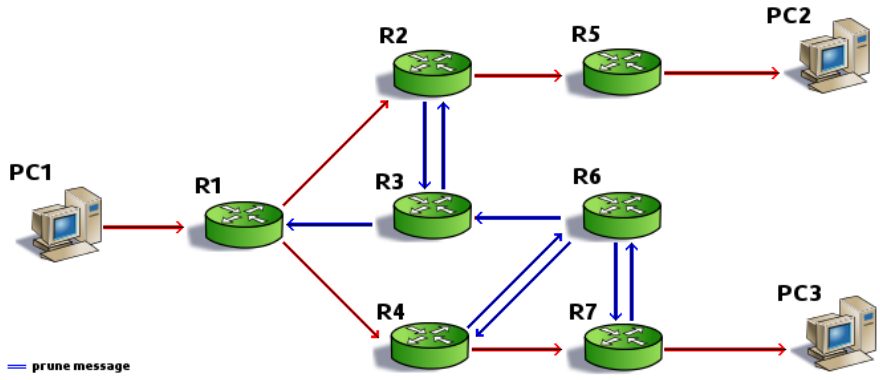
Obrázek 24 – Prvotní provoz v PIM-DM
Zdroj: Vlastní zpracování

Každý ze směrovačů na obrázku přijímá multicastový provoz právě jedním rozhraním, pro které dopadne RPF kontrola kladně (takový provoz dostává R1 od PC1, R2 od R1, R3 od R1, R4 od R1, R5 od R2, R6 od R3 a R7 od R4). Zároveň však každý ze směrovačů rozesílá provoz všemi ostatními rozhraními, tj. i těmi, které nevedou k cílovým počítačům

(PC2 a PC3) nebo můžou potažmo způsobit smyčky ve směrování (např. R6 směrem k R4). Díky RPF je však provoz, který by mohl způsobit smyčku ve směrování, zahazován (v případě, že takováto smyčka neexistuje v samotné konfiguraci směrovacích tabulek). Počítače PC2 a PC3 jsou přihlášeny k multicastové skupině a dostávají její provoz.

4.1.3 Pruning

Pruning, neboli „potlačení provozu“, je technika, díky níž PIM šetří síťové zdroje. Směrovače, které zjistí, že některými porty jim přichází provoz, který nepřeposílají nikam dále, zasílají tzv. **prune message** zprávy (zprávy o potlačení), kterými informují sousední směrovače o tom, že nepotřebují multicastový provoz na tomto rozhraní přijímat. Tyto zprávy musí být zasílány periodicky (typický interval je 3 minuty). Jedním takovým důvodem potlačení multicastového provozu může být negativní výsledek RPF kontroly. Pokud na rozhraní přijde multicastový paket, protokol PIM-DM provede RPF kontrolu vůči unicastové směrovací tabulce. Pokud zdrojová adresa paketu neodpovídá rozhraní nejlepší shody ve směrovací tabulce, paket je zahozen a směrovač na toto rozhraní zasílá svému PIM sousedovi prune message zprávu. Soused po přijetí této zprávy uvede své vlastní rozhraní do stavu pruned. Tímto rozhraním dále nezasílá multicastový provoz této skupiny, a to až do vypršení tohoto stavu (tento stav má dočasnou životnost a proto je zprávy nutno zasílat periodicky). Další situací, při které směrovač emituje prune message zprávy, je pokud je tento směrovač listem v síti a zároveň nemá připojené žádné počítače, které by patřily k multicastové skupině. Pokud má takovýto směrovač všechna rozhraní, kromě toho, kterým multicastový provoz přijímá, ve stavu pruned, zasílá sám prune message zprávy směrem ke zdroji multicastového provozu. Příklad použití těchto pravidel v PIM síti je zobrazen na obrázku 25. (Čerpáno z [1], [23])



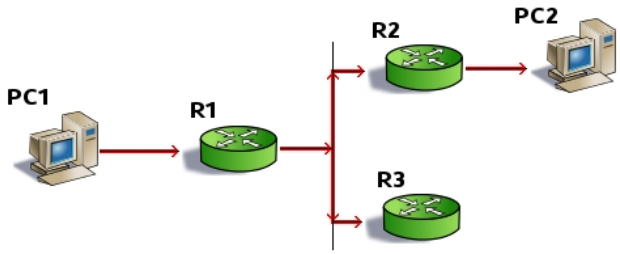
Obrázek 25 – PIM-DM pruning

Zdroj: Vlastní zpracování

Obrázek zachycuje stejnou síť, která je zobrazena i na obrázku 24, nicméně ve fázi, kdy směrovače postupně zasílají prune message zprávy (modré šipky). Tyto zprávy mezi směrovači R4 a R6, R2 a R3, R6 a R7 jsou zasílány z důvodu negativního výsledku RPF. Směrovače po obdržení těchto zpráv vědí, že dále již nemusí zasílat provoz, který by byl jejich sousedy zahozen. Směrovač R6 má všechna rozhraní, kromě příchozího, ve stavu

pruned, a proto i ten zasílá prune message zprávy směrovači R3. Ze stejného důvodu pak směrovač R3 zasílá tyto zprávy směrovači R1. Výsledkem je zdrojový distribuční strom, který doručuje multicastový provoz počítačům přihlášeným k multicastové skupině (PC2 a PC3). (Čerpáno z [1])

Dalším případem, který může nastat v síti, kde je na jednom segmentu více směrovačů, je zasílání prune message zpráv směrovači, po kterém ovšem směrování multicastového provozu vyžadujeme. Jedná se o případ, kdy jeden ze směrovačů, který je listem v síti, zasílá prune message. V daném segmentu sítě je i jiný směrovač, který má přímo připojená cílová zařízení přijímající multicastový provoz. Zprávy prune message jsou zasílány na multicastovou adresu `224.0.0.13` (všechny PIM směrovače), a tak zprávu o potlačení obdrží všechny směrovače na daném segmentu. Pokud nějaký z nich multicastový provoz potřebuje, zašle takzvanou PIM join message, kterou dá směrovači, zasílajícímu tento provoz, najevo, že potlačení provozu se nemá uskutečnit. Příklad takovéto jednoduché sítě je vyobrazen na obrázku 27. (čerpáno z [1])



Obrázek 26 – Prune override
Zdroj: Vlastní zpracování

Na síti uvedené v příkladu je zdroj multicastového provozu PC1, který zasílá provoz směrovači R1. Ten dále zasílá multicastové pakety na sdílené médium – pro směrovače R2 a R3. Směrovač R2 má přímo připojeného člena multicastové skupiny PC2. Naproti tomu R3 je listem v síti. R3 podle očekávání, protože je listem a nepotřebuje multicastový provoz, začne zasílat prune message zprávy na multicastovou adresu `224.0.0.13`. Směrovač R1 zprávu obdrží a v tu chvíli spustí časovač (typicky nastavený na 3 sekundy). Tuto zprávu zároveň obdrží i směrovač R2, který potřebuje dostávat multicastový provoz, aby ho mohl směrovat k PC2. Aby provoz nebyl potlačen, zasílá směrovač R2 PIM join message. Jelikož směrovač R1 obdrží tuto zprávu ještě před uplynutím časovače, k potlačení provozu (pruning) nedojde a PC2 o své multicastové pakety nepřijde.

4.1.4 Grafting

Grafting neboli roubování je technika, kterou PIM-DM využívá k opětovnému připojení dříve potlačených (pruning) větví distribučního stromu. Pokud se na části sítě, kterou obsluhují směrovače, jejichž rozhraní jsou ve stavu pruned, přihlásí nějaký počítač k odběru provozu multicastové skupiny, je tato část sítě připojena zpět do distribučního stromu. Aby směrovače nemusely čekat na vypršení pruned stavů rozhraní, zasílají

v takovém případě tzv. **graft message** zprávu. Sousední směrovač po obdržení této zprávy odpovídá **graft-ack** zprávou. V tomto momentě je zrušen stav pruned na odpovídajícím rozhraní a multicastový provoz dané skupiny je znovu zasílán do této části sítě. (Čerpáno z [1], [23])

4.1.5 State-refresh

Aby se omezilo opakované zamořování sítě a následné potlačování provozu (pruning), používá protokol PIM-DM takzvaný state-refresh mechanismus (obnovení stavu). Jedná se o zprávy **state refresh message**, které jsou zasílány směrovačem přímo připojeným ke zdroji multicastového provozu. Tyto zprávy jsou zasílány napříč celou sítí, takže je obdrží každý PIM směrovač v distribučním stromu. Pokud směrovač tuto zprávu obdrží na své rozhraní a tato zpráva projde RPF kontrolou, obnoví se stav všech pruned rozhraní – tedy nastaví časovače u rozhraní v pruned stavu pro tuto multicastovou skupinu na původní hodnotu. Tím se zabrání opětovnému zaslání multicastového provozu do všech částí sítě (po vypršení směrovačů i do těch, kde jsou rozhraní ve stavu pruned). (Čerpáno z [23])

4.2 PIM Sparse Mode

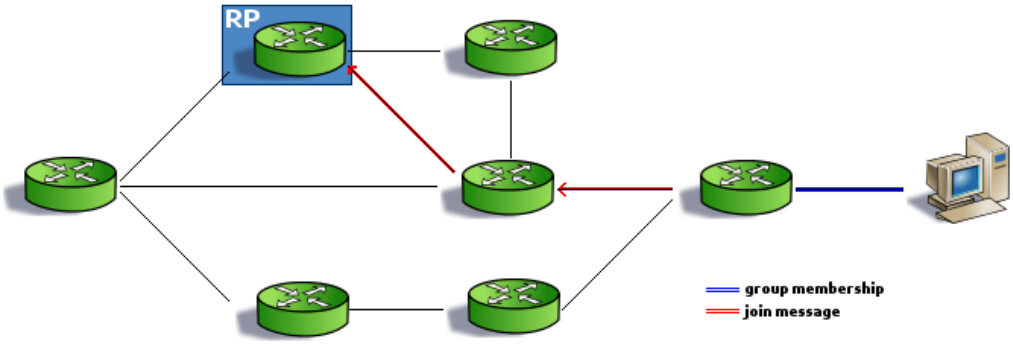
Protokol PIM-SM (PIM sparse mode) je, podobně jako jeho dense mode varianta, multicastový směrovací protokol, který ke směrování multicastových paketů využívá unicastovou směrovací tabulku a zároveň je nezávislý na tom, jaký unicastový směrovací protokol je v síti použit. Namísto techniky data pushing, používané v PIM-DM, je zde využívána varianta označovaná jako **data pulling** (tahání dat). Toto označení poukazuje na fakt, že data jsou zasílány jen na explicitní vyžádání. Multicastový provoz je směrován do jednotlivých částí sítě jen v případě, že přijde požadavek na zasílání provozu tímto směrem. Až na základě tohoto požadavku je tedy provoz jednotlivými směrovači směrován k cíli. (Čerpáno z [1], [2])

Základem protokolu PIM-SM je sdílený strom (shared tree, RP tree), jehož kořen je umístěn v některém prvku (směrovači) v síti a nazývá se rendezvous point (RP). Směrem k tomuto kořeni, k rendezvous pointu, zasílají vysílače multicastový provoz, který je tímto následně směrován sdíleným stromem směrem k přijímačům. Směrovače, které mají přímo připojená koncová zařízení patřící do multicastové skupiny (tj. zařízení která si přejí přijímat multicastový provoz), zasílají takzvané **join message** zprávy (zprávy o připojení do skupiny) směrem ke kořeni stromu. Naopak pokud multicastovou skupinu opustí, zasílají **prune message** zprávy (zprávy o potlačení), kterými dají směrovačům najevo, že provoz již není třeba zasílat. (Čerpáno z [1], [24])

4.2.1 Join message zprávy

Distribuční sdílený strom, používaný v protokolu PIM-SM, má svůj kořen v bodě rendezvous point, který se nachází na některém místě v síti. Po přihlášení počítače do multicastové skupiny, pokud je tento první, který je ke směrovači přímo připojen, zasílá

směrovač join message zprávu směrem k rendezvous pointu. Tato zpráva obsahuje adresu multicastové skupiny, o jejíž provoz počítač stojí. Každý ze směrovačů po cestě si ve své paměti přiřadí dané rozhraní k multicastové skupině obsažené ve zprávě join message. Takto se zachová každý směrovač do chvíle, dokud join message nedorazí na rendezvous point nebo na směrovač, který již v paměti záznam této skupiny má (je tedy součástí sdíleného stromu). Příklad sítě, na které vzniká takový sdílený strom je zobrazen na obrázku 27. (Čerpáno z [1], [24])



Obrázek 27 – Join message zprávy
Zdroj: Vlastní zpracování

Počítač na obrázku se přihlásí k odebírání multicastového provozu dané skupiny. Jelikož je tento počítač prvním počítačem v síti, který se do multicastové skupiny přihlašuje a směrovač, ke kterému je připojen tedy ještě nepatří do distribučního stromu pro tuto multicastovou skupinu, vytvoří záznam pro tuto skupinu a rozhraní směrem k počítači zařadí mezi ty, jimiž se má provoz této skupiny zasílat. Směrovač byl donucen vytvořit záznam pro tuto multicastovou skupinu a tudíž zasílá PIM join message zprávu směrem k rendezvous pointu (rozhraní, kterým tuto zprávu zaslat nalezne pomocí unicastové směrovací tabulky). Další směrovač na cestě k rendezvous pointu, po obdržení join message zprávy, opět vytvoří záznam pro tuto skupinu a příchozí rozhraní do ní zařadí. Pokračuje zasláním join message zprávy dále směrem k RP. Rendezvous point tak obdrží join message zprávu pro danou multicastovou skupinu. Jelikož pro tuto skupinu ještě záznam nemá, vytvoří ho a příslušné rozhraní zařadí. V tuto chvíli je sestavený distribuční strom z RP až k počítači, který se přihlásil do skupiny. (Čerpáno z [1], [24])

Jelikož stav multicastového záznamu na směrovači má časový limit, po kterém je tento z paměti směrovač vymazán (tento limit je defaultně nastaven na 3 minuty), jsou zprávy join message zasílány periodicky (standardně po 1 minutě). Tento způsob zabraňuje zbytečnému zasílání provozu do některých částí sítě v případě, že by například prune message zpráva z nějakého důvodu nedorazila k cíli v pořádku a větev distribučního stromu určená k odebrání by zůstala aktivní. (Čerpáno z [1], [24])

4.2.2 Prune message zprávy

V případě, že po odhlášení počítače od multicastové skupiny (např. zasláním IGMP leave message) již na daném segmentu nezbývá žádné další zařízení, které by stálo o multicastový provoz, směrovač vyřadí toto rozhraní ze seznamu těch, kterými zasílá provoz dané multicastové skupiny. Pokud je tento seznam prázdný, nalezl se směrovač ve stavu, ve kterém provoz multicastové skupiny již nepotřebuje. V tu chvíli zasílá takzvanou prune message zprávu směrem k rendezvous pointu. Sousední směrovač po přijetí této zprávy analogicky opět vyřadí příslušné rozhraní ze seznamu a díky tomu se provoz skupiny do segmentu sítě, který ho již nepotřebuje, přestane zasílat. Pokud i tento směrovač po odebrání rozhraní ze skupiny skončí s prázdným seznamem rozhraní pro tuto skupinu, opět posílá prune message směrem k RP, čímž postupně dochází k odebrání větve distribučního stromu, pokud ta již není třeba. (Čerpáno z [1], [24])

V případě že segment sítě obsahuje více směrovačů a mohlo by dojít k odebrání větve stromu, která být odebrána nemá, protokol PIM-SM používá techniku prune override stejným způsobem jako je tomu v dense mode variantě protokolu PIM. (Čerpáno z [1], [24])

4.2.3 PIM zprávy

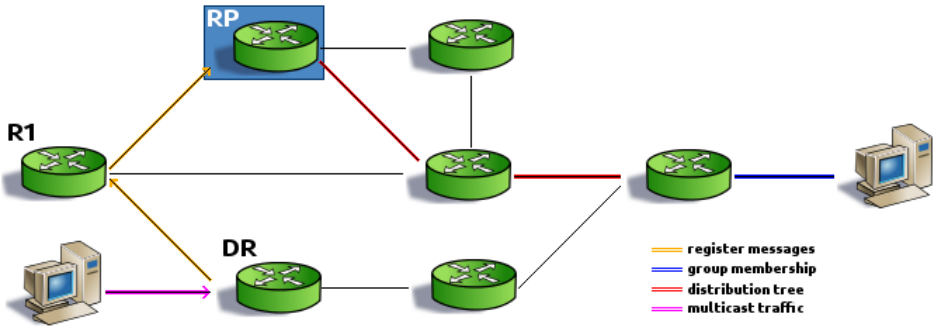
Zprávy join message a prune message, zasílané v protokolu PIM-SM jsou PIM zprávy, které mají přesně definovaný formát. Tyto zprávy obsahují seznamy join a seznamy prune, obsahující několik multicastových skupin. Počet multicastových skupin v seznamu může být i 0. Možnost zahrnout do jedné zprávy několik různých multicastových skupin značně zvyšuje efektivitu periodického zasílání těchto zpráv. Jeden takový záznam v join/prune seznamu obsahuje zejména:

- **adresu multicastového zdroje**, tj. adresu zdroje multicastového provozu, o který je žádáno (join) či kterého se směrovač vzdává (prune), a je-li zároveň nastaven wildcard příznak, potom je zde uvedena adresa rendezvous pointu,
- **multicastovou adresu skupiny**, což je adresa multicastové skupiny, které se join, prune záznam týká,
- **wildcard příznak** (wildcard flag), který říká, zda se tento join/prune záznam týká sdíleného stromu,
- **RP příznak**, jakožto příznak říkající, zda má být tato zpráva směrovači směrována dále směrem ke kořeni stromu. (Čerpáno z [1], [24])

4.2.4 Zdroje multicastového provozu

V tuto chvíli jsou popsány principy vybudování sdíleného distribučního stromu s kořenem v bodě rendezvous point. Následuje popis způsobů, kterými jsou data od zdrojů multicastového provozu zasílána směrem k rendezvous pointu tak, aby je tento mohl distribuovat ke koncovým zařízením náležícím do multicastové skupiny. Zodpovědný

směrovač (designated router), ke kterému je zdroj multicastového provozu připojen tyto jednotlivé pakety zabalí (encapsulate) do takzvaných **PIM register message** zpráv, které zasílá rendezvous pointu. Díky tomu se rendezvous point dozví o tom, že daný zdroj multicastového provozu zasílá data do skupiny a zároveň tak přijímá první pakety multicastového provozu. Rendezvous point tato data rozbalí a rozešle distribučním stromem k cílovým zařízením. Na obrázku 28 je zobrazen příklad počítačové sítě, ve které zdroj multicastového provozu zasílá PIM register message zprávy. (Čerpáno z [1], [24])



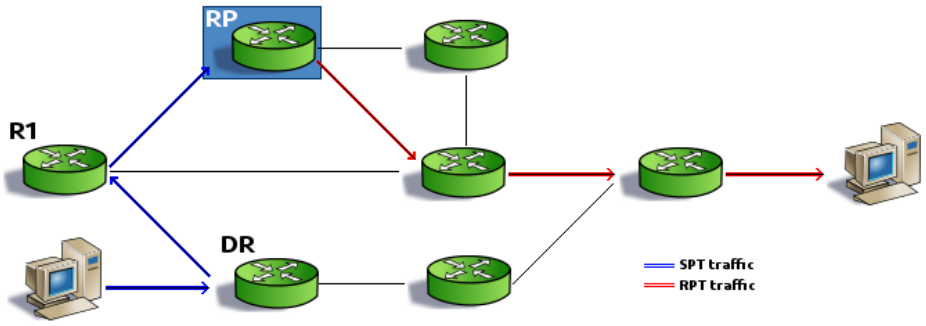
Obrázek 28 – PIM register message zprávy
Zdroj: Vlastní zpracování

V příkladu znázorněném na obrázku zasílá počítač v levém dolním rohu multicastový provoz pro skupinu, jejíž rendezvous point je vyznačen obdélníkem s nápisem „RP“ a která obsahuje jeden počítač přihlášený do této skupiny (vpravo). Příslušnost počítače ke skupině je znázorněna modře. Sdílený distribuční strom vedoucí od rendezvous pointu k cílovým směrovačům je vyznačen červeně. Zdroj multicastového provozu tedy zasílá pakety (fialová šipka) určené pro multicastovou skupinu na svůj zodpovědný směrovač (designated router), označený písmeny „DR“. Tento směrovač tyto pakety zabalí (encapsulate) do PIM register message zpráv, které zasílá směrem k RP (znázorněno žlutými šipkami). Rendezvous point po přijetí těchto zpráv jednotlivé pakety rozbalí a původní data rozešle po sdíleném distribučním stromu jednotlivým příjemcům (počítač vpravo). Tím se multicastový provoz dostane od vysílače ke všem účastníkům této multicastové skupiny.

Zasílání PIM register message zpráv, které ve svém těle obsahují pakety původního multicastového provozu, není ovšem efektivní. Prvním důvodem je, že samotné zabalování (encapsulation) a rozbalování (decapsulation) jsou další operace, které pro velké množství paketů mohou zkonzumovat velké množství hardwarových zdrojů směrovačů. Z tohoto důvodu zasílá rendezvous point, po příchodu prvních PIM register paketů, join message zprávu směrem ke zdroji tohoto multicastového provozu. Tím se vlastně RP stane listem stromu nejkratších vzdáleností (SPT), který má kořen ve zdroji multicastového provozu. Jakmile zodpovědný směrovač zdroje provozu obdrží tuto join zprávu, začne posílat nezabalený provoz směrem k RP. V tuto chvíli rendezvous point dostává od zdroje provoz, který není zabalen a díky tomu již nepotřebuje dostávat PIM register message zprávy. RP

tedy zašle takzvanou **PIM register-stop message** zprávu směrem ke zdroji provozu, kterou dá najevo, že již dále nepotřebuje dostávat PIM register message zprávy. V tuto chvíli zodpovědný směrovač připojený ke zdroji multicastového provozu přestane provádět zabalování a dále již nebude posílat PIM register message zprávy. (Čerpáno z [1], [24])

V případě že ke sdílenému stromu nejsou připojena žádná koncová zařízení, která by naslouchala provozu dané multicastové skupiny, rendezvous point taktéž zasílá PIM register-stop zprávy, kterými dá najevo, že provoz této skupiny nepotřebuje tímto kanálem dostávat. Na obrázku 29 je vyobrazena síť ve stavu, kdy RP zaslal PIM register-stop zprávy a zodpovědný směrovač připojený ke zdroji provozu přestal zasílat PIM register message zprávy. (Čerpáno z [1], [24])



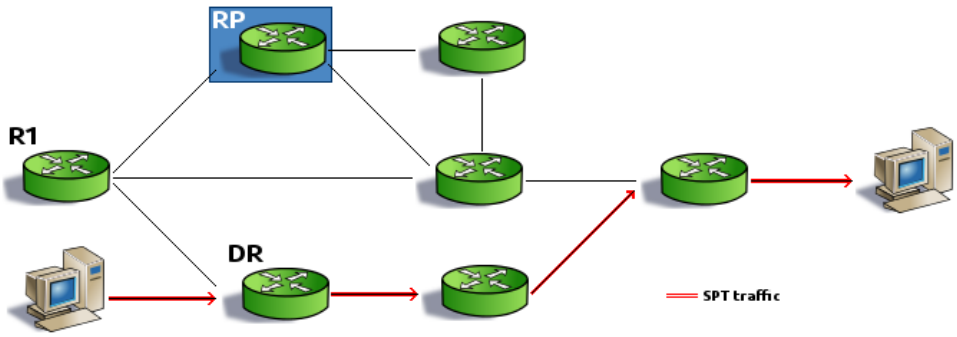
Obrázek 29 – Multicastový provoz po PIM register-stop zprávě
Zdroj: Vlastní zpracování

Na obrázku jsou zobrazeny dva distribuční stromy. První z nich, strom nejkratších vzdáleností, který vznikl díky join message zprávám zaslaných rendezvous pointem směrem ke zdroji a obsahuje pouze jednu větev, je znázorněn modrými šipkami. Směrovače, které jsou v cestě tohoto stromu, mají ve svých multicastových tabulkách záznamy typu (S,G), kde písmeno S označuje zdroj multicastového provozu a písmeno G označuje skupinu, pro kterou je tento provoz určen. Ke každému tomuto záznamu si směrovač udržuje seznam rozhraní, kterými má odpovídající provoz zasílat. Naproti tomu sdílený strom je na obrázku vyznačen červenými šipkami a směrovače, ze kterých je tento strom sestaven v paměti udržují záznamy typu (*,G), kde znak hvězdičky označuje všechny možné zdroje pro tuto multicastovou skupinu a písmeno G značí onu skupinu, pro kterou jsou multicastová data zasílána. K těmto záznamům směrovače opět udržují seznam rozhraní, kterými mají odpovídající provoz zasílat. V případě těchto záznamů je, narozdíl od záznamů typu (S,G), odpovídající provoz jakýkoliv provoz určený skupině G (z jakéhokoliv zdroje). (Čerpáno z [1], [24])

4.2.5 Stromy nejkratších vzdáleností

Cesta multicastového provozu od zdroje k cílovým zařízením přes rendezvous point může být často zbytečně dlouhá, neoptimální. Pro zlepšení odezvy a snížení celkového zatížení sítě používá protokol PIM-SM stromy nejkratších vzdáleností, které se vytváří pro

jednotlivé zdroje multicastového provozu. Směrovače, které jsou zodpovědné pro členy multicastové skupiny, zasílají po obdržení prvních paketů ze sdíleného stromu join message zprávy směrem ke zdroji, jehož provoz přijímají. Tyto zprávy obsahují adresu multicastového zdroje, a tak jednotlivé směrovače, na které dorazí, vytváří záznamy typu (S, G) (pokud je ještě v paměti vytvořeny nemají). Tyto join message zprávy postupně dorazí až ke směrovači, který je připojen přímo ke zdroji nebo k nějakému směrovači, který již stejný (S, G) záznam obsahuje. V obou případech se daná cesta připojí ke stromu nejkratších vzdáleností s kořenem ve zdroji S. Jakmile je tato větev stromu připojena, získává směrovač připojený ke koncovému zařízení dvě kopie stejných dat. Směrovač proto začne zahazovat pakety z daného zdroje, přicházející skrze sdílený strom a zároveň zašle prune message zprávu směrem k rendezvous pointu. Tím dojde k odebrání větve ze sdíleného stromu a cílové zařízení dostává multicastový provoz pouze skrze strom nejkratších vzdáleností (SPT). Takovýto scénář je naznačen na obrázku 30. (Čerpáno z [1], [24])



Obrázek 30 – PIM - Strom nejkratších vzdáleností
Zdroj: Vlastní zpracování

V síti zobrazené na obrázku došlo k vytvoření stromu nejkratších vzdáleností od zdroje (počítač vlevo dole) až k jedinému účastníku multicastové skupiny (počítač vpravo). Zodpovědný směrovač, který je přímo připojen k přijímači, proto zaslal prune message zprávu a tím odebral větev, jíž byl součástí, ze sdíleného stromu. Jelikož RP již dále nepotřebuje přijímat provoz od zdroje, protože ve sdíleném stromu nezbyly žádné přijímače, zasílá prune message zprávy směrem ke zdroji multicastového provozu. Multicastový provoz tak již dále nebude zasílán rendezvous pointu a jediná cesta, kterou je nyní provoz směrován, je nejkratší cesta směrem k přijímači.

5 Konfigurace počítačové sítě a multicastu

Počítačová síť, na níž budou realizovány multicastové konfigurace, se bude snažit přibližně odrážet středně velkou podnikovou síť, která pojme řádově stovky připojených počítačů. Aby se však na takové síti projevily některé vlastnosti a přednosti multicastové komunikace, je její topologie v některých ohledech záměrně přizpůsobena tomuto faktu (například míra redundance). Na této síti bude zprovozněno směrování multicastového provozu. Jako multicastový směrovací protokol bude použit PIM-SM, jakožto směrovací protokol, který je obecně doporučovaný pro směrování multicastu v počítačových sítích. Tato kapitola popisuje způsoby konfigurace jednotlivých zařízení v síti pro účely testování a měření parametrů směrování multicastového provozu. V síti jsou pominuta například nastavení různých přístupových zabezpečení, firewallů, atp.

5.1 Zařízení v síti

V praxi se dnes setkáváme ve velké míře s počítačovými sítěmi, ve kterých nacházíme různá síťová zařízení od různých jednotlivých výrobců. Funkcionalita různých síťových protokolů v takovýchto sítích potom často závisí na podpoře těchto protokolů v jednotlivých zařízeních a verzích těchto protokolů, které dané zařízení (jeho firmware nebo operační systém) podporuje.

5.1.1 Směrovače Cisco

Směrovače Cisco řady 2800 jsou zařízení, která jsou výkonným řešením pro sítě malého a středního rozsahu. Obsahují operační systém Cisco IOS, který podporuje širokou škálu protokolů, používaných v dnešních počítačových sítích.

Směrovače této řady, konkrétně Cisco 2811, jsou použity jako hlavní směrovače v sestavované počítačové síti. Tato zařízení obsahují operační systém Cisco IOS verze 15.0. Směrovač Cisco 2811 je zobrazen na obrázku 31.

Obrázek 31 – Směrovač Cisco 2811

Zdroj: www.cisco.com

Směrovače Cisco řady 2800 mohou, díky své modularitě, disponovat různými rozhraními. Z pohledu této práce jsou důležitá rozhraní, kterými použité směrovače disponují, tato:

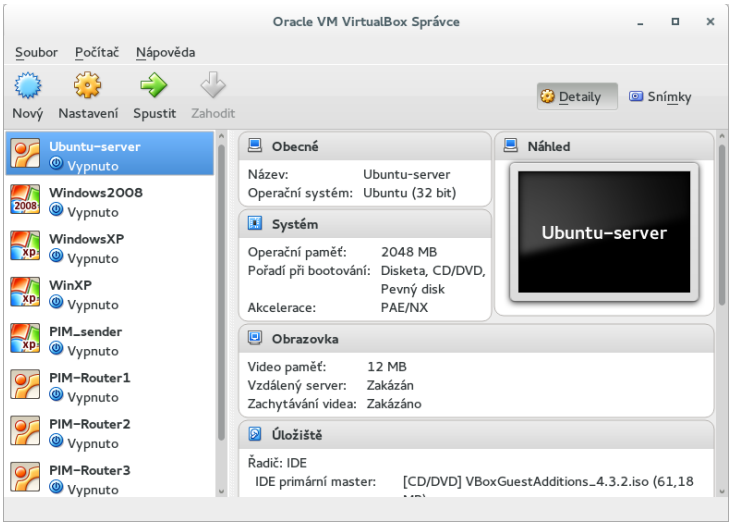
- sériová rozhraní, označovaná jako Smart Serial cable interface,

- rozhraní FastEthernet, umožňující připojení ethernetové sítě rychlostí až 100 Mb/s.

5.1.2 Virtuální stroj jako směrovač

Virtualizace je v dnešním světě informačních technologií již běžným pojmem. Díky virtualizaci lze snadno ušetřit náklady za hardware i za provoz. Zároveň umožňuje rychlé nasazení systémů a jejich pohodlnou správu. Ve spoustě dnešních počítačových sítích se lze běžně setkat s virtualizovaným strojem, který plní funkci serveru a poskytuje nejrůznější služby. Nezřídka kdy je třeba, aby tento server plnil zároveň funkci směrovače (například směroval provoz skrze VPN tunel nebo i jako směrovač pro běžný provoz v lokální síti) nebo NAPTu. Díky robustnosti dnešních operačních systémů dokáže takovéto nastavení často usnadnit přístup administrátora k různým dalším síťovým prvkům nebo počítačům. Pro simulaci takovéhoto virtualizovaného stroje bude v sestavované síti použit virtualizační nástroj VirtualBox od firmy Oracle.

VirtualBox je virtualizační software, který je šířený pod licencí GNU (GPL) verze 2. Tento nástroj umí virtualizovat jak platformu x86, tak i platformu AMD64/Intel64. Další výhodou tohoto produktu je, že je multiplatformní – běží na platformách Microsoft Windows, Linux, Mac OS a Solaris. Zároveň podporuje velké množství operačních systémů, které na virtuálních strojích poběží. Rozhraní VirtualBoxu spuštěného v desktopovém prostředí Gnome je zobrazeno na obrázku 32. (Čerpáno z [25])



Obrázek 32 – Rozhraní nástroje VirtualBox

Zdroj: Vlastní zpracování

Pro běh nástroje VirtualBox, a potažmo tedy samotného virtuálního stroje, je vyhrazen běžný osobní počítač s následující konfigurací:

- procesor Intel Pentium Dual-Core E5200 2,5 GHz,
- operační paměť 4,00 GB (2 × 2 GB) DDR2 800 MHz,

- pevný disk Seagate Barracuda ST3160815AS – 160 GB,
- operační systém Microsoft Windows 7 Enterprise (64-bitový).

Operační systém, zvolený pro běh na virtuálním serveru, je 32bitová verze Ubuntu 12.04.4 Server. Tento systém poskytuje řadu výhod, mezi něž bezesporu patří: přímočará a jednoduchá instalace, snadná konfigurace a podpora běžných serverových služeb. Díky balíčkovacímu systému a softwaru dostupnému v repozitářích je tento systém ideální pro účely požadovaného virtuálního stroje.

Konfigurace samotného virtuálního stroje v nástroji VirtualBox je následující:

- maximální využití procesoru 100 %,
- počet využívaných jader procesoru – jedno jádro,
- operační paměť 1024 MB,
- pevný disk SATA 8 GB, formát *vdi*, dynamicky alokované,
- síťová karta připojena k síťovému mostu,
- síťová karta připojena k virtuální síti pouze s hostujícím systémem.

5.1.3 Koncová zařízení

Koncová zařízení (počítače), která jsou z pohledu této práce zdroji a příjemci multicastového provozu, jsou běžné osobní počítače obsahující následující konfiguraci:

- procesor Intel Pentium Dual-Core E5200 2,5 GHz,
- operační paměť 4,00 GB (2 × 2 GB) DDR2 800 MHz,
- pevný disk Seagate Barracuda ST3160815AS – 160 GB,
- operační systém Microsoft Windows 7 Enterprise (64-bitový).

Operační systémy Windows jsou celosvětově nejrozšířenější platformou na osobních počítačích. Jejich jednoduché a intuitivní rozhraní do značné míry odstiňuje uživatele od problematiky správy a konfigurace operačního systému. Podpora multimédií v těchto systémech dosahuje taktéž vysoké úrovně. Díky těmto kladům je tento systém logickou volbou pro koncová zařízení (osobní počítače) v sestavované počítačové síti.

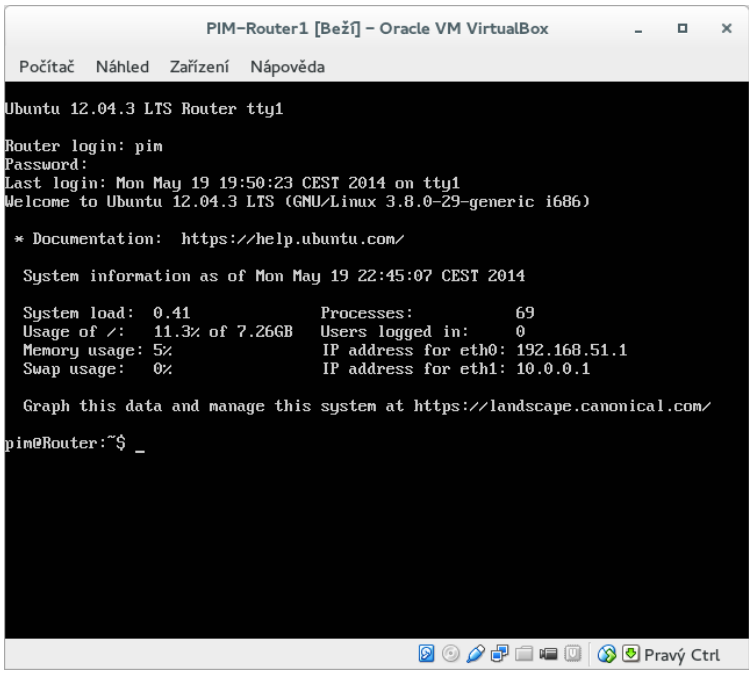
5.2 Topologie a adresace

Základ sítě bude sestaven ze směrovačů Cisco 2811. Ty budou tvořit takzvané jádro (core) počítačové sítě. Každý z těchto směrovačů může například ve firemní síti zprostředkovávat konektivitu pro jedno oddělení, budovu, pobočku, atd. Tyto směrovače budou mezi sebou propojeny sériovým rozhraním a budou uspořádány tak, aby v síti vznikly redundantní cesty. Důvody pro redundanci jsou zřejmé. Jedná se především o zajištění dostupnosti

síťových zdrojů i v případě výpadku některého ze zařízení. Pro účely této práce jsou redundantní spoje na sestavované síti nezbytné pro umožnění testování některých parametrů na jednotlivých konfiguracích multicastu. Sériový port nacházející se na směrovačích Cisco 2811, označovaný jako Smart Serial Interface, podporuje několik různých sériových rozhraní. Rozhraní použité pro přenos dat mezi jednotlivými směrovači v sestavované síti je rozhraní V.35. Po tomto rozhraní lze na použitých směrovačích přenášet data, dle nastavení taktovací frekvence, rychlostí až 8 Mb/s.

Směrovače jsou zároveň vybaveny ethernetovými rozhraními (FastEthernet), díky čemuž umožňují připojení segmentů lokálních sítí (například přepínačů, na které budou napojena koncová zařízení). Počet koncových zařízení bude dán kapacitou přepínačů připojených k těmto rozhraním. V tomto ohledu je třeba brát v úvahu výkon těchto zařízení a zároveň omezení plynoucí z protokolů používaných na druhé vrstvě ISO/OSI modelu (například STP).

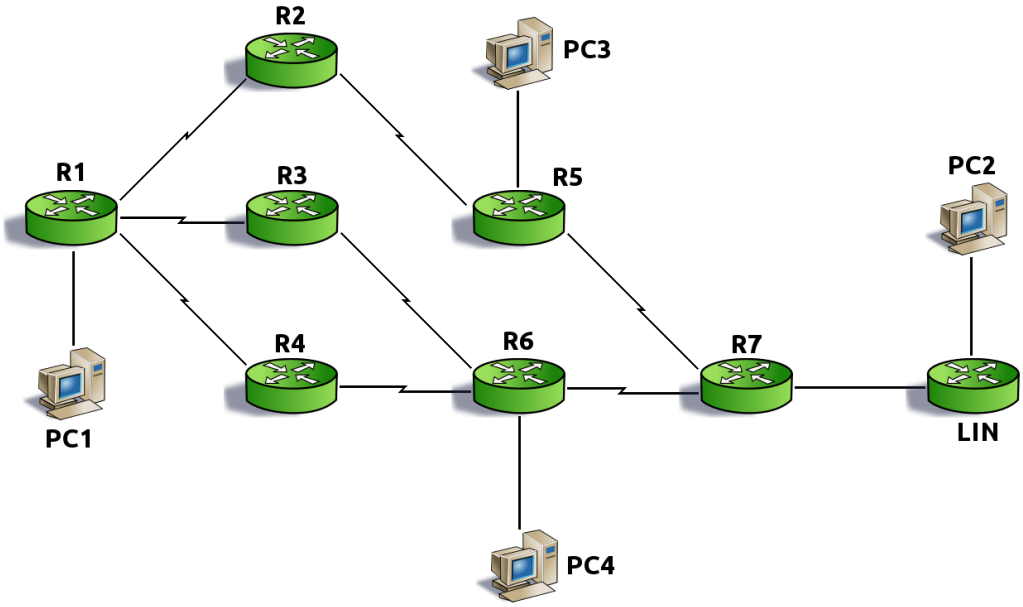
Počítač, na kterém poběží virtuální stroj obsahující systém Ubuntu bude v této síti plnit funkci směrovače. Jedno ze svých dvou virtuálních ethernetových rozhraní je připojeno k síťovému mostu. Toto nastavení znamená, že systém může přes toto rozhraní komunikovat stejným způsobem, jako by bylo fyzickým rozhraním, které obsahuje hostující počítač. Díky tomu lze virtuální stroj pomocí ethernetového rozhraní hostujícího počítače připojit k jednomu ze směrovačů Cisco 2811. Tím v síti vznikne další směrovač – virtuální stroj. Na obrázku 33 je zobrazen nástroj VirtualBox se spuštěným operačním systémem Ubuntu Server.



Obrázek 33 – VirtualBox s běžícím systémem

Zdroj: Vlastní zpracování

Pro účely této práce postačí, že koncová zařízení budou připojena jen k některým směrovačům v síti. Zároveň nebude využito ethernetových přepínačů a počítače tak budou připojeny přímo ke směrovačům. Rozmístění tří osobních počítačů se systémy Windows je vybráno tak, aby prokrylo různé části sítě. Dalším koncovým zařízením se stane počítač, na kterém běží virtuální stroj. Díky virtuální ethernetové síti mezi hostovaným a hostujícím systémem jsou tato zařízení logicky propojena. Hostující systém (Windows) tedy bude představovat čtvrté koncové zařízení v budované síti a komunikace mezi ním a virtualizovaným směrovačem bude probíhat stejným způsobem, jako při přímém propojení. Topologie této sítě je znázorněna na obrázku 34.



Obrázek 34 – Návrh budované sítě
Zdroj: Vlastní zpracování

Jak je znázorněno na obrázku, jádro sítě tvoří směrovače Cisco 2811 (R1 až R7). Tyto směrovače jsou spolu propojeny pomocí sériových rozhraní takovým způsobem, aby díky vzniklým redundancím byla zaručena konektivita mezi zbývajícími směrovači i v případě havárie některého z nich.

K těmto směrovačům, konkrétně směrovačům R1, R5 a R6, jsou přímo připojeny tři osobní počítače (PC1, PC3 a PC4), které odpovídají vybraným pracovním stanicím ve vnitropodnikové síti.

Ke směrovači R7 je dále připojen osobní počítač s virtuálním strojem a virtualizovaným operačním systémem Ubuntu Server. Tento virtuální stroj, který bude v síti fungovat jako linuxový směrovač, je na obrázku označen jako LIN. Počítač PC2 obsahuje systém Microsoft Windows, na kterém běží zmíněný virtuální stroj LIN. S ním je propojen virtuální ethernetovou sítí, díky které je vlastně přímo připojen ke směrovači LIN (tato síť je znázorněna spojnicí mezi směrovačem LIN a počítačem PC2).

Adresace IP této sítě je zvolena tak, aby nebylo plýtváno jednotlivými rozsahy IP adres. Pro adresaci jsou zvoleny privátní rozsahy adres. Adresy z privátního rozsahu `10.0.0.0/8` jsou použity pro adresaci segmentů mezi směrovači. Protože tyto spoje jsou dvoubodové (takzvaně point-to-point), jsou pro adresaci rozhraní na těchto segmentech použity masky `255.255.255.252`. Pro adresaci lokálních sítí obsahujících koncová zařízení jsou využity adresy privátního rozsahu `192.168.0.0/16`. Na těchto částech sítě se mohou nacházet řádově desítky připojených koncových zařízení, proto je pro adresaci těchto segmentů zvolena maska `255.255.255.0`. Adresaci všech zařízení, zobrazených na obrázku 34, přehledně zobrazuje tabulka 10.

Tabulka 10 – Adresace zařízení v síti

Zdroj: Vlastní zpracování

Zařízení	Rozhraní	Adresa	Maska	Soused
R1	Serial 0/0/0	10.0.0.1	255.255.255.252	R2
	Serial 0/0/1	10.0.0.5	255.255.255.252	R3
	Serial 0/1/0	10.0.0.9	255.255.255.252	R4
	FastEthernet 0/0	192.168.51.1	255.255.255.0	PC1
R2	Serial 0/0/0	10.0.0.2	255.255.255.252	R1
	Serial 0/0/1	10.0.0.13	255.255.255.252	R5
R3	Serial 0/0/0	10.0.0.6	255.255.255.252	R1
	Serial 0/0/1	10.0.0.17	255.255.255.252	R6
R4	Serial 0/0/0	10.0.0.10	255.255.255.252	R1
	Serial 0/0/1	10.0.0.21	255.255.255.252	R6
R5	Serial 0/0/0	10.0.0.14	255.255.255.252	R2
	Serial 0/0/1	10.0.0.25	255.255.255.252	R7
	FastEthernet 0/0	192.168.53.1	255.255.255.0	PC3
R6	Serial 0/0/0	10.0.0.18	255.255.255.252	R3
	Serial 0/0/1	10.0.0.22	255.255.255.252	R4
	Serial 0/1/0	10.0.0.29	255.255.255.252	R7
	FastEthernet 0/0	192.168.54.1	255.255.255.0	PC4
R7	Serial 0/0/0	10.0.0.26	255.255.255.252	R5
	Serial 0/0/1	10.0.0.30	255.255.255.252	R6
	FastEthernet 0/0	10.0.1.1	255.255.255.252	LIN
LIN	eth0	10.0.1.2	255.255.255.252	R7
	eth1	192.168.52.1	255.255.255.0	PC2
PC1	Místní síť	192.168.51.2	255.255.255.0	R1
PC2	VirtualBox host only	192.168.52.2	255.255.255.0	LIN
PC3	Místní síť	192.168.53.2	255.255.255.0	R5
PC4	Místní síť	192.168.54.2	255.255.255.0	R6

Dalším úkolem v této síti je naplnit směrovací tabulky směrovačů. K tomuto účelu je použit směrovací protokol RIP verze 2. RIP je směrovací protokol, sloužící k distribuci směrovacích informací napříč sítí. Ačkoliv není tak robustní jako jiné směrovací protokoly (např. OSPF, EIGRP), díky jednoduché administraci a přímočaré konfiguraci je vhodným protokolem pro výměnu směrovacích informací mezi jednotlivými směrovači na sestavované síti.

Směrovací tabulky na osobních počítačích budou obsahovat pouze výchozí bránu – adresu směrovače, který obstarává provoz pro jejich segment sítě a skrze který komunikují se zbytkem sítě. Tabulka 11 zobrazuje nastavení výchozí brány pro všechny koncové počítače v síti.

Tabulka 11 – Výchozí brány osobních počítačů
Zdroj: Vlastní zpracování

Počítač	Výchozí brána
PC1	192.168.51.1
PC2	192.168.52.1
PC3	192.168.53.1
PC4	192.168.54.1

5.3 Konfigurace zařízení v síti

Způsob konfigurace jednotlivých zařízení se odvíjí od operačního systému, firmwaru či rozhraní, které tato zařízení obsahují.

5.3.1 Konfigurace směrovačů Cisco 2811

Směrovače Cisco 2811, použité k sestavení jádra budované sítě, lze konfigurovat přes rozhraní příkazové řádky (CLI) operačního systému IOS. K tomuto rozhraní lze přistupovat připojením na konzolový port směrovače pomocí sériové komunikace a použitím obslužné aplikace (putty, minicom). Další možností je, po nakonfigurování vzdáleného přístupu, přihlášení ke konzoli směrovače přes protokoly Telnet nebo SSH.

Po připojení k příkazové řádce systému IOS směrovače se uživatel nachází v neprivilegovaném módu. Tento mód nabízí uživateli pouze přehledy různých nastavení směrovače. Pro více možností je třeba vstoupit do takzvaného privilegovaného módu, ve kterém se obor možností administrátora rozšíří. Vstupu do privilegovaného módu zadáním příkazu *enable*.

Po vstupu do privilegovaného módu má administrátor možnost vstoupit do globálního konfiguračního terminálu zadáním příkazu *configure terminal*. V tomto režimu lze konfigurovat chování směrovače. Aby administrátor mohl konfigurovat konkrétní rozhraní tohoto směrovače, musí vstoupit do režimu konfigurace tohoto rozhraní. To udělá

příkazem:

```
Router(config)# interface if
```

ve kterém slovo *if* zastupuje název rozhraní, které si administrátor přeje konfigurovat. Konfigurace IP adresy rozhraní se provádí v režimu konfigurace příslušného rozhraní příkazem

```
Router(config-if)# ip address A.B.C.D E.F.G.H
```

kde *A.B.C.D* je IP adresa zařízení a *E.F.G.H* je maska podsítě. Další nezbytností, která se týká sériových rozhraní, je nastavit taktovací frekvenci hodinového signálu. Tento postup je třeba provést na tom konci sériového spoje, který je za zdroj hodinového signálu zodpovědný (DCE rozhraní). Od frekvence hodinového signálu se odvíjí přenosová rychlost po tomto spoji. Frekvence hodinového signálu se nastavuje v konfiguračním módu příslušného rozhraní příkazem

```
Router(config-if)# clock rate value
```

kde zástupné slovo *value* zastupuje hodnotu frekvence. Nakonec je třeba zapnout komunikaci na tomto rozhraní. To lze udělat prostým zadáním příkazu

```
Router(config-if)# no shutdown
```

po jehož zpracování začne směrovač obsluhovat pakety přicházející (nebo odcházející) na toto rozhraní.

Konfigurace směrovacího protokolu RIP se v operačním systému IOS provádí v konfiguračním módu směrovacího protokolu. Do konfiguračního módu směrovacího protokolu RIP lze vstoupit z globálního konfiguračního módu zadáním příkazu

```
Router(config)# router rip.
```

V tomto módu lze uskutečnit všechna nastavení ohledně směrovacího protokolu RIP. Příkazem *version* administrátor nastaví verzi protokolu RIP, která bude v případě sestavované sítě, verze 2. Příkaz *no auto-summary* vypne automatickou sumarizaci podsítí do vyšších celků. Dále je třeba pomocí příkazu *network* nastavit lokální sítě, jejichž směrovací informace se mají propagovat mezi směrovači v síti. Syntaxe zmíněných příkazů je následující:

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

Router(config-router)# no auto-summary

Router(config-router)# network A.B.C.D
```

kde slovo *number* je zástupným symbolem pro číslo verze a sestava znaků *A.B.C.D* v příkazu *network* je adresou sítě, informace o níž se mají propagovat ostatním

směrovačům. Příkazů *network* administrátor zadá tolik, o kolika sítích přípojených ke směrovači mají být informace v celé síti známy.

Aby směrovače Cisco 2811 směrovaly multicastový provoz, je třeba směrování multicastu zapnout. To se provede zadáním následujícího příkazu:

```
Router(config)# ip multicast routing
```

v globálním konfiguračním módu systému IOS. Následně je třeba pro jednotlivá rozhraní zapnout multicastový směrovací protokol. V tomto případě to bude multicastový směrovací protokol PIM-SM. Zapnutí PIM-SM protokolu na jednotlivých rozhraních se provádí příkazem:

```
Router(config-if)# ip pim sparse-mode
```

v konfiguračním módu příslušného rozhraní. Zapnutí protokolu PIM-SM je nezbytné na všech rozhraních, které se mají směrování multicastového provozu účastnit. Pro správnou funkci protokolu PIM-SM je třeba, aby všechny směrovače, které na směrování multicastového provozu participují, znali adresu směrovače, který je rendezvous pointem. Metod jak nastavit rendezvous point je několik (automaticky, staticky). V budované síti o osmi směrovačích postačí statická konfigurace rendezvous pointu. Příkaz

```
Router(config)# ip pim rp-address A.B.C.D
```

zadaný v globálním konfiguračním módu systému IOS nastaví staticky nakonfigurovaný rendezvous point pro všechny multicastové skupiny na adresu *A.B.C.D*.

Příklad konfigurace směrovače R1 je dodán jako Příloha A k textu práce.

5.3.2 Konfigurace virtuálního stroje

Virtuální stroj, který v síti plní úlohu směrovače, má nainstalovaný operační systém Ubuntu Server. Tento směrovač disponuje dvěma ethernetovými rozhraními, které systém interpretuje jako eth0 a eth1. V defaultní konfiguraci zde administrátor pracuje v příkazovém řádku linuxového shellu Bash. Způsobů jak nakonfigurovat statickou IP adresu rozhraním směrovače je více. Lze využít například linuxový nástroj *ip*, který je součástí běžné instalace Ubuntu Server 12.04, nebo nástroj *ifconfig* dostupný v balíčku net-tools v repozitářích systému. S využitím například nástroje *ifconfig*, lze nastavit IP adresu danému rozhraní následujícím způsobem:

```
root@router:~# ifconfig interface A.B.C.D/mask up
```

kde *interface* značí rozhraní, na kterém se IP adresa nastavuje, *A.B.C.D* je IP adresa, která bude tomuto rozhraní přiřazena a *mask* je síťová maska podsítě, v níž se dané rozhraní nachází. Díky příznaku *up* na konci příkazu se rozhraní zapne. Takto nastavená IP adresa není perzistentní a po restartování systému na rozhraní nezůstane nastavena. Pro perzistenci IP adres pro jednotlivá rozhraní je třeba editovat konfigurační soubor

/etc/network/interfaces, kde lze zadefinovat adresy pro jednotlivá rozhraní.

V základní instalaci systém Ubuntu Server pakety nesměruje. Aby tak činil, je třeba nastavit parametr *ip_forward* linuxového jádra na hodnotu 1. To lze za běhu systému učinit zapsáním hodnoty 1 do souboru */proc/sys/net/ipv4/ip_forward*. Jednoduše lze tohoto docílit příkazem

```
root@router:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

který přes operátor přesměrování výstupu zapíše hodnotu 1 do tohoto souboru. Po restartování systému se však hodnota v tomto souboru opět nastaví na původní, tedy 0. Aby toto nastavení zůstalo perzistentní, je třeba upravit příslušné nastavení v souboru */etc/sysctl.conf*.

Pro zprovoznění směrovacího protokolu RIP je v systému Ubuntu 12.04 nutné mít nainstalovaný nějaký nástroj, který tuto funkci poskytuje. Jedním takovým je směrovací software Quagga. Tento nástroj je obsažen v repozitářích pro Ubuntu Server 12.04 jako balíček quagga. Quagga umožňuje zprovoznění několika různých směrovacích protokolů, mezi nimiž se RIP nachází. Konfigurace tohoto nástroje je možná skrze konfigurační soubory, nebo přes vzdálený přístup k příkazové řádce jednotlivých směrovacích protokolů.

V konfiguračním souboru */etc/quagga/daemons* lze jednotlivé směrovací protokoly zapnout nebo vypnout. Struktura tohoto souboru je jednoduchá – na řádcích jsou názvy služeb jednotlivých směrovacích protokolů následované rovnítkem a slovem *yes*/*no* podle toho, zda má být konkrétní směrovací protokol aktivní. V případě virtuálního stroje v budované síti je nastaven příznak *yes* u služby směrovacího protokolu RIP – ripd.

Konfigurace samotného protokolu RIP se potom nachází v konfiguračním souboru */etc/quagga/ripd.conf*. Konfigurační příkazy jsou velmi podobné těm, které jsou použity v systému IOS na směrovačích Cisco. Administrátor může například nastavit vzdálený přístup k příkazové řádce služby ripd nastavením názvu zařízení (*hostname*) a hesla (*password*) v souboru *ripd.conf*. Služba příkazové řádky k daemonu ripd naslouchá na portu 2602 a lze se k ní připojit přes protokol Telnet.

Konfigurace směrovacího protokolu RIP směrovacího softwaru Quagga z příkazové řádky je prakticky totožná s konfigurací protokolu RIP v systému IOS na směrovačích Cisco. Sítě, které se mají propagovat skrze protokol RIP se zde zadávají, oproti implementaci v IOS, včetně masky podsítě. Postupná konfigurace směrovacího protokolu RIP po přihlášení do příkazové řádky služby ripd:

```
Router# configure terminal

Router(config)# router rip

Router(config-router)# version 2
```

```
Router(config-router)# network A.B.C.D/mask
```

kde *A.B.C.D* je IP adresa sítě, která se má propagovat pomocí protokolu RIP a *mask* je maska této sítě.

Aby systém Ubuntu Server nainstalovaný na virtuálním stroji mohl směrovat multicastový provoz, je nutné vypnout parametr linuxového jádra *rp_filter* na rozhraních, které se mají účastnit multicastového směrování. Parametr jádra rp_filter představuje nastavení, které říká, zda má být takzvaný Reverse Path Filter (RP Filter) na daném rozhraní aktivní. Tento filtr přestavuje základní ochranu proti útoku IP address spoofing. Funguje tak, že po přijetí paketu na rozhraní, na kterém je RP Filter aktivní, přečte zdrojovou adresu tohoto paketu. Pokud je tato adresa směrovatelná tímto rozhraním (rozhodnutí na základě směrovací tabulky), pak je paket zpracován nebo směrován. V opačném případě je paket zahozen. V případě aktivního RP Filteru nebude směrování multicastového provozu fungovat správně. (Čerpáno z [26])

Změnu parametru *rp_filter* lze učinit příkazem

```
root@router:~# echo 0 > /proc/sys/net/ipv4/conf/*/rp_filter
```

který přesměruje výstup příkazu *echo* (0) do všech souborů *rp_filter* nacházejících se v podsložkách adresáře */proc/sys/net/ipv4/conf/*. Pro perzistenci takového nastavení je opět třeba editovat příslušné nastavení v souboru */etc/sysctl.conf*.

Implementací protokolu PIM-SM pro unixové systémy je služba pimd. Je obsažena v balíčku pimd v repozitářích systému Ubuntu. Služba pimd se konfiguruje přes konfigurační soubor /etc/pimd.conf. V tomto souboru jsou obsaženy příkazy, které modifikují chování služby pimd. Nejdůležitější z těchto příkazů jsou:

- *default_source_preference*, což je hodnota která se používá při volbě směrovače, který bude zasílat multicastový provoz na segment sítě s více směrovači,
- *rp_address*, kterým je definována adresa rendezvous pointu pro skupiny uvedené v příkazu,
- *switch_data_treshold*, kterým jsou určeny podmínky, za jakých směrovač, který je listem, začne přijímat multicastový provoz ze stromu nejkratších vzdáleností (SPT). (Čerpáno z [27])

Konfigurační soubor pimd.conf ze směrovače LIN je přiložen jako příloha B k textu práce.

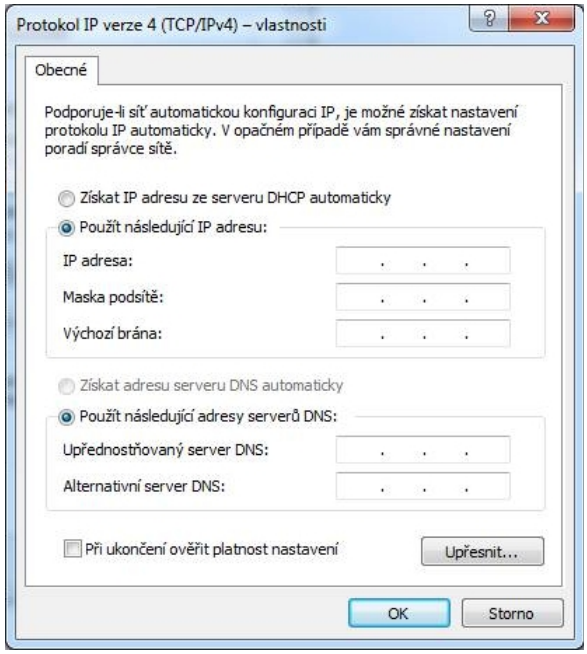
5.3.3 Konfigurace koncových zařízení

Osobní počítače připojené k síti obsahují systém Microsoft Windows 7. Jelikož se jedná o koncová zařízení, konfigurace zahrnuje nastavení IP adresy rozhraní a výchozí brány, tj. směrovače, který pro tento segment sítě zprostředkovává komunikaci se zbytkem sítě. V budované síti bude výchozí brána pro jednotlivé osobní počítače rovna adrese

ethernetového rozhraní směrovače, ke kterému je tento počítač připojen.

Systémy Windows jsou založeny na grafickém uživatelském rozhraní, a tak i konfigurace zde probíhá v tomto prostředí. Nicméně alternativou je konfigurace v příkazové řádce pomocí příkazu *netsh*.

Cest k oknu s nastavením IP adresy, masky sítě a výchozí brány je několik (v tomto okně lze nastavit i DNS servery). Jedna z těchto cest vede přes Ovládací Panely, Nastavení Síťového adaptéru a následné vyvolání okna vlastností adaptéru. Na obrázku 35 je zobrazeno okno konfigurace protokolu IPv4 nad ethernetovým adaptérem (ve Windows označované jako Připojení k místní síti).



Obrázek 35 – Konfigurace IP ve Windows

Zdroj: Vlastní zpracování

6 Měření parametrů multicastové komunikace

Všechna zařízení v sestavené síti jsou nakonfigurovány tak, aby spolu navzájem dokázala komunikovat. Dále je na všech směrovačích v síti (se systémy IOS i Linux), nakonfigurováno směrování multicastového provozu pomocí sparse mode protokolu PIM-SM. Tato kapitola obsahuje porovnání různých parametrů v síti za různých konfigurací multicastového provozu, který je v síti přítomen.

Daty, která jsou přenášena pomocí multicastové komunikace, bývají ve velké míře multimédia – video a zvuk. Pro účely testování multicastového provozu na navrhnuté síti proto bude mezi koncovými zařízeními přenášeno video. Jako testovací videosekvence je vybrán krátký film Sintel, který je volně dostupný ke stažení pod licencí Creative Commons na webových stránkách *www.sintel.org*. Verze která byla v síti streamována je kódovaná pomocí kodeku H264 a má rozlišení 1280 × 544 pixelů.

Jako nástroj pro streamování této videosekvence bude použit multimediální přehrávač VLC, který je projektem neziskové organizace VideoLAN. VLC je jednoduchý, rychlý a výkonný přehrávač, který podporuje velké množství multimediálních formátů. Zároveň nabízí podporu pro streamování multimédií pomocí různých aplikačních protokolů.

Aplikačním protokolem, vhodným pro přenášení dat videosekvence v reálném čase, je protokol RTP, který je k tomuto účelu přímo navržen.

6.1 Porovnání zátěže procesoru směrovačů

Zpracovávání paketů různých síťových protokolů i směrování běžného provozu v síti vyžaduje ve větší či menší míře procesorový čas směrovače. Na sestavené síti bylo postupně měřeno průměrné vytížení procesoru během pětiminutového intervalu. Jelikož měření byla prováděna za dobu pěti minut během zasílání streamu, nemá na výsledky vliv umístění rendezvous pointu, protože v době měření dostávaly všechny přijímače data streamu skrze stromy nejkratších vzdáleností (SPT).

Vytížení procesoru na směrovačích Cisco 2811 bylo prováděno spuštěním příkazu

```
Router# show processes cpu
```

který zobrazuje zátěž procesoru: aktuální, průměrnou za minutu a za pět minut.

Na směrovači s operačním systémem Ubuntu Server bylo měření zátěže procesoru prováděno periodickým zapisováním aktuální zátěže procesoru zobrazené ve výstupu příkazu top po jedné sekundě po dobu pěti minut. Z těchto hodnot byla následně sestavena průměrná zátěž procesoru za daných pět minut.

Zátěž procesoru byla změřena na všech směrovačích v síti za následujících podmínek:

a) v klidovém stavu, kdy na síti není žádný zdroj ani přijímač streamu,
b) při unicastovém vysílání, kdy zdroj PC1 zasílá stream počítačům PC2, PC3 a PC4,
c) při unicastovém vysílání, kdy zdroj PC1 zasílá stream počítačům PC2, PC3 a PC4 a zároveň zdroj PC2 zasílá stream počítačům PC1, PC3 a PC4,
d) při multicastovém vysílání, kdy zdroje PC1 a PC2 jsou vysílače a na síti nejsou žádné přijímače
e) při multicastovém vysílání, kdy zdroj PC1 je vysílačem a počítač PC2 je přijímačem,
f) při multicastovém vysílání, kdy zdroj PC1 je vysílačem a počítače PC2, PC3 a PC4 jsou příjemci,
g) při multicastovém vysílání, kdy zdroj PC1 zasílá stream, který přijímají počítače PC2, PC3 a PC4 a zároveň PC2 zasílá ve stejné multicastové skupině stream, který přijímají počítače PC1, PC3 a PC4,
h) při multicastovém vysílání, kdy zdroj PC1 zasílá stream, který přijímají počítače PC2, PC3 a PC4 a zároveň PC2 zasílá v jiné multicastové skupině stream, který přijímají počítače PC1, PC3 a PC4.

Následující tabulka (tabulka 12) shrnuje jednotlivá měření.

Tabulka 12 – Přehled naměřených zatížení

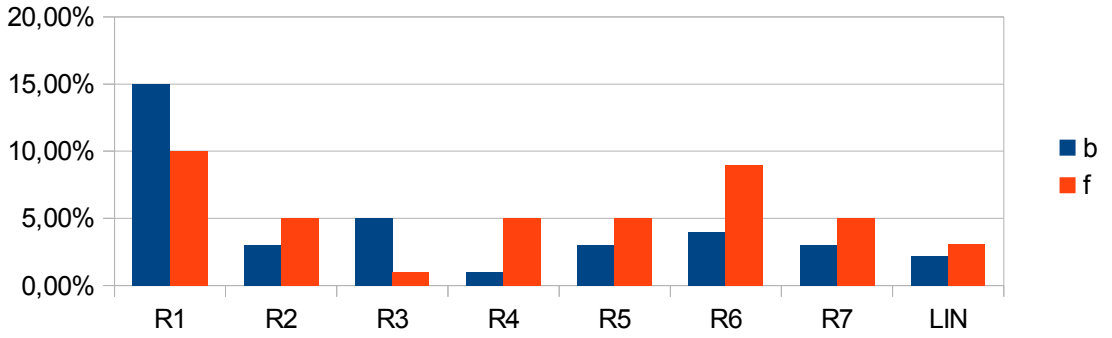
Zdroj: Vlastní zpracování

Případ	R1	R2	R3	R4	R5	R6	R7	R8
a	1 %	1 %	1 %	1 %	1 %	1 %	1 %	1,01 %
b	15 %	3 %	5 %	1 %	3 %	4 %	3 %	2,16 %
c	20 %	3 %	5 %	2 %	5 %	7 %	19 %	17,75 %
d	4 %	1 %	1 %	1 %	1 %	1 %	1 %	1,83 %
e	7 %	1 %	1 %	4 %	5 %	5 %	5 %	4,22 %
f	10 %	5 %	1 %	5 %	5 %	9 %	5 %	3,10 %
g	13 %	4 %	1 %	8 %	9 %	16 %	17 %	5,90 %
h	15 %	5 %	1 %	7 %	8 %	17 %	17 %	5,30 %

Zatížení procesoru směrovače stoupá úměrně s počtem paketů které směrovačem prochází. V případě multicastového provozu ovšem procesorový čas spotřebovává i zpracovávání paketů multicastového provozu, které musí být zreplikovány na více rozhraní.

První porovnání lze provést mezi případem b) a případem f), ve kterých vždy počítač PC1 zasílá provoz pro tři přijímače – počítače PC2, PC3 a PC4. Toto porovnání nabídne představu o rozdílech zatížení směrovačů při použití unicastové a multicastové komunikace. Rozdíly mezi zátěží na procesorech v těchto případech jsou přehledně zobrazeny v grafu na obrázku 36. Nutno podotknout že v případě unicastu přichází na

směrovač R1 trojnásobné množství paketů streamu a z toho vyplývá i vyšší vytížení linky mezi PC1 a R1. Další nevýhodou unicastové komunikace při použití protokolu RTP při této konfiguraci je, že pakety streamu jsou sítí směrovány i v době, kdy cílové stanice tato data nepřijímání.



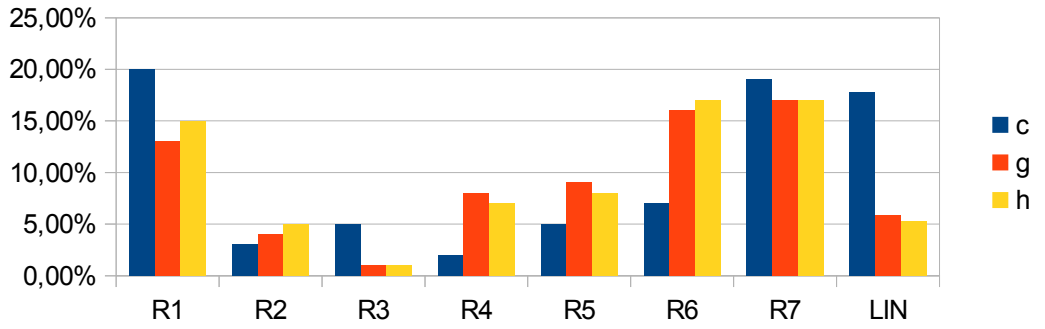
Obrázek 36 – Unicast vs. multicast
Zdroj: Vlastní zpracování

Z grafu (obrázek 36) je patrné, že více směrovačů má vyšší zatížení procesoru při použití multicastu. Obzvláště se to projevuje u směrovače R6, který v případě unicastu směruje provoz pro cíle PC2 i PC4. V případě multicastu přichází na jeho rozhraní pouze polovina paketů streamu, nicméně je musí replikovat na dvě svá rozhraní a dále udržovat informace o multicastových skupinách, což ústí ve větší vytížení procesoru v případě multicastu. Naproti tomu procesor směrovače R1, který je přímo připojen ke zdroji streamování, je znatelně více vytížen při unicastovém provozu. V tu chvíli na rozhraní směrovače přichází trojnásobné množství paketů streamu oproti multicastu a procesor směrovače je pouhým unicastovým směrováním vytížen více, než replikováním paketů na dvě svá rozhraní v případě multicastového provozu. V případě stoupajícího počtu přijímačů se rozdíly mezi unicastovou a multicastovou komunikací na této síti budou zvyšovat.

Dalšími případy vhodnými k porovnání jsou ty, kdy jsou zasílány různé streamy ze dvou různých zdrojů s tím, že vždy zbylé tři počítače jsou příjemci tohoto provozu. Jedná se o případy: c), kde probíhá unicastová komunikace, g), kdy je komunikace multicastová a oba zdroje provozu zasílají stream stejné skupině a h), kdy komunikace je opět multicastová, ale zdroje zasílají provoz různým multicastovým skupinám. Naměřené hodnoty jsou opět porovnány v grafu.

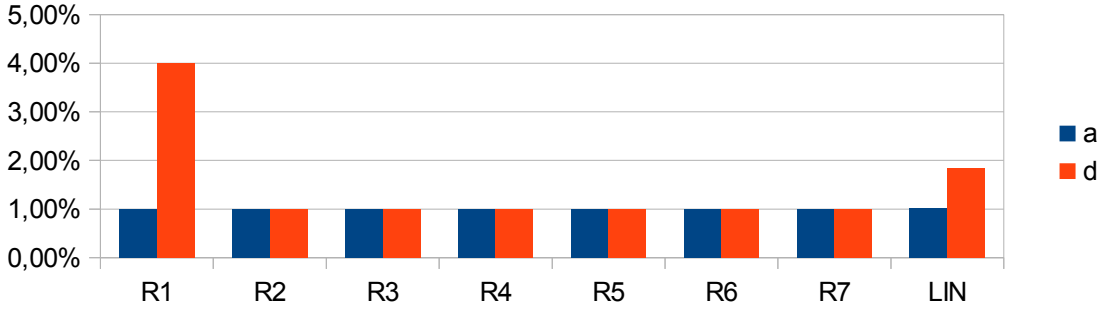
V případě dvou zdrojů streamu je v grafu (obrázek 37) opět patrný rozdíl mezi multicastovou a unicastovou komunikací na směrovačích přímo připojených ke zdrojům vysílání. Obzvláště výrazný je tento rozdíl na linuxovém směrovači běžícím ve virtuálním stroji (LIN). Tento směrovač má pouze dvě rozhraní a tak nemusí multicastový provoz replikovat na více rozhraní (jako je tomu u směrovače R1) Naproti tomu na směrovači R6 je výrazně nižší zátěž při použití unicastové komunikace. Tento směrovač je připojen do

čtyřech sítí, přičemž na dvě rozhraní dostává multicastový provoz, který dále zasílá každý na své další dvě rozhraní. Rozdíly mezi multicastovou komunikací, kdy zdroje vysílají ve stejné skupině nebo ve dvou různých skupinách jsou při tomto počtu vysílačů (skupin) zanedbatelné.



Obrázek 37 – Graf porovnání unicastu a multicastu
Zdroj: Vlastní zpracování

V bodě a) byla měřena zátěž procesorů směrovačů na síti, kam nebyl zasílán žádný provoz. V bodě d) byla tato zátěž měřena v případě, kdy PC1 a PC2 zasílaly stream pro multicastovou skupinu, nicméně na síti nebyly žádné přijímače. Srovnání naměřených hodnot je zobrazeno v grafu (obrázek 38).



Obrázek 38 – Zatížení v klidu s jedním zdrojem
Zdroj: Vlastní zpracování

Z grafu je zřejmé, že v celé síti nedochází k vytížení procesorů směrovačů většímu než je to, které bylo naměřeno v klidu. Vyjímkou jsou procesory směrovačů R1 a LIN, které jsou přímo připojeny ke zdrojům multicastového provozu. Tyto směrovače proto musí obsluhovat multicastové pakety, které jsou zasílány počítači PC1 a PC2.

6.2 Počty paketů protokolu PIM na linuxovém směrovači

Dalším sledovaným parametrem byl počet paketů protokolu PIM, které přišly na rozhraní linuxového směrovače. Výsledky tohoto měření prozradí, kolik režie způsobuje protokol PIM. Pro změření počtů paketů byl použit linuxový nástroj iptables.

Pro změření počtů protokolu PIM byly do iptables přidána následující pravidla příkazy:

```
root@router:~# iptables -I INPUT -p pim
```

pro měření počtu přijatých PIM paketů a

```
root@router:~# iptables -I OUTPUT -p pim
```

pro měření počtu zaslaných PIM paketů. Následně byly čítače paketů vynulovány příkazem

```
root@router:~# iptables -Z
```

a zobrazeny po pěti minutách zachytávání příkazem

```
root@router:~# iptables -L -vxn
```

který zobrazuje počet paketů vyhovujících jednotlivým pravidlům, která iptables obsahuje.

Podmínky, při kterých byly změřeny počty PIM paketů na linuxovém směrovači, jsou:

a) klidový stav, kdy na síti není žádný zdroj ani přijímač,
b) kdy PC1 je vysílačem PC2 je přijímačem multicastového provozu, rendezvous point se nachází na rozhraní Serial 0/0/0 směrovače R2,
c) kdy vysílače různých skupin jsou PC1 a PC2, přijímače jsou vždy zbylá tři PC a rendezvous point je umístěn na rozhraní Serial 0/0/0 směrovače R2,
d) kdy PC1 je vysílačem PC2 je přijímačem multicastového provozu, rendezvous point se nachází na rozhraní eth0 směrovače LIN,
e) kdy vysílače různých skupin jsou PC1 a PC2, přijímače jsou vždy zbylá tři PC a rendezvous point je umístěn na rozhraní eth0 směrovače LIN.

Výsledky jednotlivých měření jsou shrnuty v následující tabulce (tabulka 13).

Tabulka 13 – Počty paketů na linuxovém směrovači
Zdroj: Vlastní zpracování

a		b		c		d		e	
příchozí	odchozí	příchozí	odchozí	příchozí	odchozí	příchozí	odchozí	příchozí	odchozí
35	25	43	30	61	41	50	27	68	28

Dle očekávání je na linuxovém směrovači nejnižší režie v případě, kdy na síti není žádný zdroj ani přijímač multicastového provozu. Počty PIM paketů stoupají přibližně úměrně s počtem multicastových skupin, které na síti jsou. V případě, že byl rendezvous point přesunut na směrovač LIN, na kterém probíhalo měření, zvýšil se počet přijatých PIM paketů, ale naopak se snížil počet odchozích PIM paketů. Nutno podotknout, že měření je prováděno během streamování, kdy všechny přijímače získávají data ze stromů nejkratších vzdáleností (SPT). V součtech tedy nejsou zahrnuty například PIM register zprávy.

6.3 Přístupová doba k datům skupiny

Jedním z klíčových parametrů pro uživatele využívajícího služby IP multicastu, je doba, po jaké začnou přicházet data zasílaná multicastové skupině, do níž se uživatel přihlásil. Existují případy, kdy může každá sekunda, o kterou by uživatel přišel při prvním spuštění multimediálního obsahu, přenášeného multicastem, být velmi důležitá (sportovní přenosy, bezpečnostní kamery). Cílem této kapitoly je zjistit dopady různých stavů sítě na přístupovou dobu k datům, které jsou příslušné multicastové skupině zasílány.

Přístupová doba k datům multicastové skupiny je v této práci definována jako rozdíl času obdržení prvního paketu multicastového provozu skupiny a času odeslání prvního IGMP membership report paketu, kterým o provoz této skupiny koncové zařízení žádá. Měření byla prováděna na osobních počítačích s operačním systémem Windows. Nástrojem pro změření doby mezi odeslání IGMP a přijetí prvního UDP paketu náležícího do streamu je síťový analyzátor Wireshark. Vypovídající hodnota přístupové doby, která je zde uváděna, je průměrná hodnota sestavená z deseti replikací stejného měření za stejných podmínek.

Zkoumaná veličina byla měřena na různých konfiguracích, kterými jsou:

a) rendezvous point na rozhraní Serial 0/0/0 směrovače R2, zdroj vysílání PC1 a přístupová doba byla měřena na PC2, PC3 a PC4,
b) rendezvous point na rozhraní Serial 0/0/0 směrovače R2, zdroj vysílání PC1, příjemci streamu PC2, PC3 a PC4 a přístupová doba byla měřena na PC2, PC3 a na PC4, přičemž během měření přijímali ostatní účastníci skupiny multicastová data,
c) rendezvous point na rozhraní eth0 směrovače LIN, zdroj vysílání PC1, přístupová doba byla měřena na PC2, potom na PC3,
d) rendezvous point na rozhraní eth0 směrovače LIN, zdroj vysílání PC1, příjemci streamu PC2, PC3 a PC4 a přístupová doba byla měřena na PC2, potom na PC3, přičemž během měření přijímali ostatní účastníci skupiny multicastová data,
e) rendezvous point na rozhraní eth0 směrovače LIN, zdroj vysílání PC2 a přístupová doba byla měřena na PC1
f) rendezvous point na rozhraní eth0 směrovače LIN, zdroj vysílání PC2, příjemci streamu PC1, PC3 a PC4 a přístupová doba byla měřena na PC1, přičemž během měření přijímali ostatní účastníci skupiny multicastová data.

Ve všech těchto případech byla přístupová doba změřena za dvou podmínek. První měření odpovídalo návratu uživatele k zavřenému streamu. Jedná se o přístupovou dobu ve chvíli, kdy uživatel zavřel přehrávač videa, který před tím přijímal multicastový stream, a nyní se chce ke streamu opět připojit (řádově v rámci sekund). Na jednotlivých směrovačích tedy nevyprší stavy multicastových záznamů pro jednotlivá rozhraní a směrovače tak žádají přímo o připojení ke stromu nejkratších vzdáleností (SPT). Druhé měření probíhalo po několikaminutové odmlce, kdy multicastové záznamy již jednotlivé směrovače ze své paměti vymazali a je tedy třeba se nejprve připojit ke sdílenému stromu.

Přehled naměřených hodnot prvních měření (rychlého návratu ke streamu, kdy ještě nevypršely časovače pro multicastové záznamy na směrovačích) na počítačích PC1, PC2, PC3 a PC4 pro jednotlivé případy popsané výše zobrazuje tabulka 14. Prázdná pole v tabulce znamenají, že tento konkrétní případ nebyl měřen.

Tabulka 14 – Přístup k datům po rychlém návratu

Zdroj: Vlastní zpracování

Počítač	a	b	c	d	e	f
PC1					20,9 ms	14,5 ms
PC2	3 254,9 ms	2 722,7 ms	2 397,4 ms	2 654,1 ms		
PC3	18,1 ms	9,6 ms	22,2 ms	15,9 ms		
PC4	18,5 ms	8,6 ms				

Hodnoty naměřené ve druhém měření, kdy se uživatel připojuje ke streamu poprvé, případně po delší odmlce, zobrazuje tabulka 15.

Tabulka 15 – Přístup k datům při prvním spojení

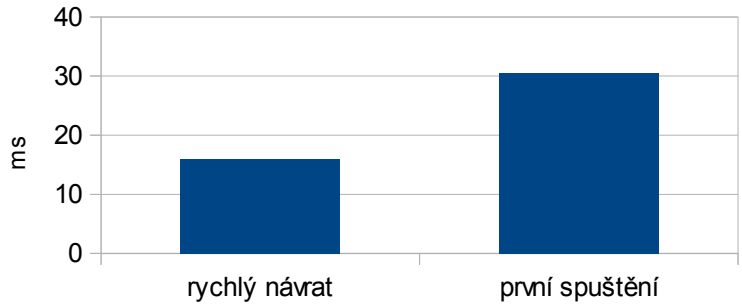
Zdroj: Vlastní zpracování

Počítač	a	b	c	d	e	f
PC1					42 ms	31,9 ms
PC2	2 717,3 ms	2 332 ms	2 439,1 ms	2 913,9 ms		
PC3	27,3 ms	12,6 ms	64,1 ms	21,6 ms		
PC4	36,1 ms	8,9 ms				

Z výsledků lze pozorovat, že směrovač běžící na virtuálním stroji se službou pimd výkonově zaostává za směrovači Cisco v případě zprostředkování multicastového provozu pro připojené příjemce.

Naměřené časy na směrovačích Cisco dokazují, že průměrná přístupová doba při rychlém znovupřipojení do skupiny, kdy se směrovače připojují přímo ke stromu nejkratších vzdáleností, je znatelně nižší než v případě prvního spojení, kdy je třeba připojit se ke sdílenému stromu. Průměrné hodnoty pro směrovače Cisco z naměřených hodnot zvlášť

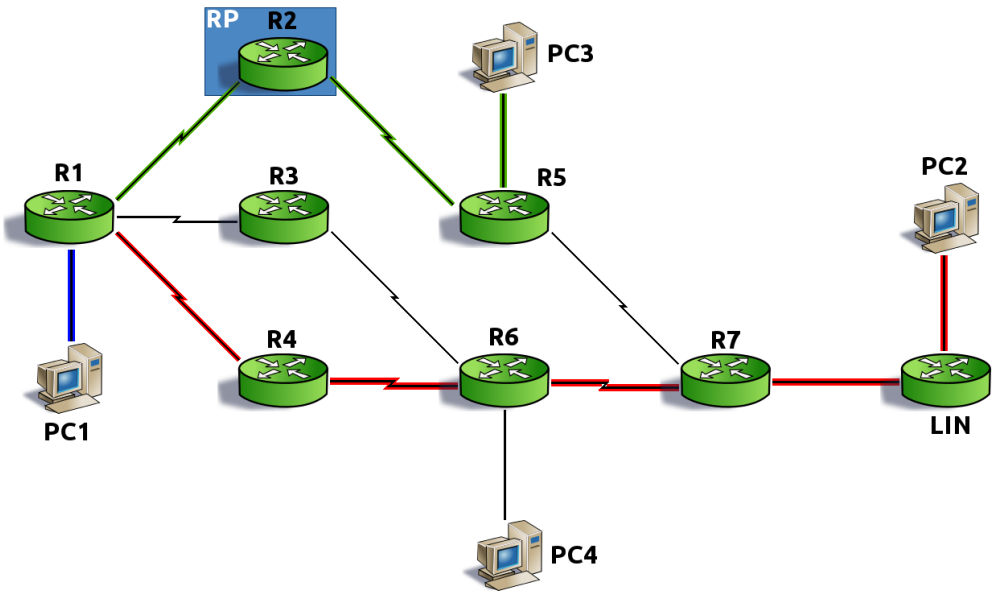
pro obě tabulky graficky zobrazuje následující graf (obrázek 39).



Obrázek 39 – Srovnání doby přístupu v různých situacích

Průměrná doba přístupu ke streamu v případě prvního spuštění značně převyšuje dobu přístupu při rychlém návratu k již dříve přijímanému streamu. V rámci jednotlivých hodnot však lze vypozorovat vliv multicastového provozu, který je již v síti směrován na přístupovou dobu.

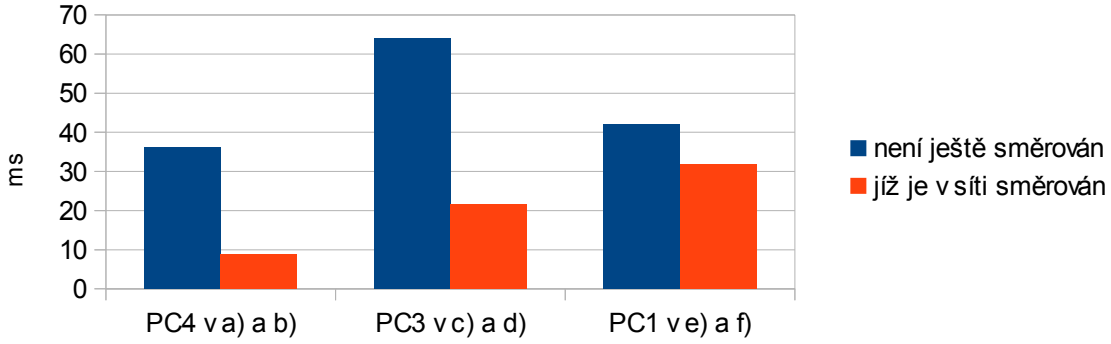
Takovým případem je třeba srovnání hodnoty prvotního přístupu ke streamu na počítači PC4 v měřeních a) a b). V prvním případě v síti není ještě multicastový provoz směrován, a tak se musí směrovač R6 stát členem sdíleného stromu s kořenem v rendezvous pointu (R2). V případě, kdy je však multicastový provoz této skupiny, konkrétně pro zdroj PC1, již směrovačem R6 směrován (směruje pakety streamu stromem nejkratších vzdáleností pro PC2), získává PC4 data provozu zasílaného počítačem PC1 ihned po přijetí IGMP membership report zprávy směrovačem R6. Popsaný případ je zobrazen na obrázku 40.



Obrázek 40 – Přípojení PC4 do skupiny, jejíž provoz je směrován
Zdroj: Vlastní zpracování

Multicastový provoz je ze zdroje PC1 směrován stromem nejkratších vzdáleností k PC2 (větev označena červeně) a k PC3 (větev označena zeleně). Jakmile počítač PC4 zašle IGMP membership report zprávu o příslušnosti k této multicastové skupině, směrovač R6 mu ihned začne zasílat pakety streamu. To je možné díky faktu, že směrovač R6 již pakety multicastového provozu získává díky tomu, že je členem stromu nejkratších vzdáleností pro zdroj PC1. Mimo to se R6 zároveň stane členem sdíleného stromu, aby přijal pakety od případných dalších zdrojů multicastového provozu pro tuto skupinu.

Srovnání prvotní přístupové doby ke streamu, který v síti ještě není směrován s přístupovou dobou ke streamu, který je již v síti různými směrovači směrován zobrazuje následující graf (obrázek 41). Na ose *y* uvedeného grafu je vynášena přístupová doba ke streamu v milisekundách. Na ose *x* tohoto grafu jsou uvedeny jednotlivé počítače s popisem, kterých případů měření se uvedený sloupec grafu týká.

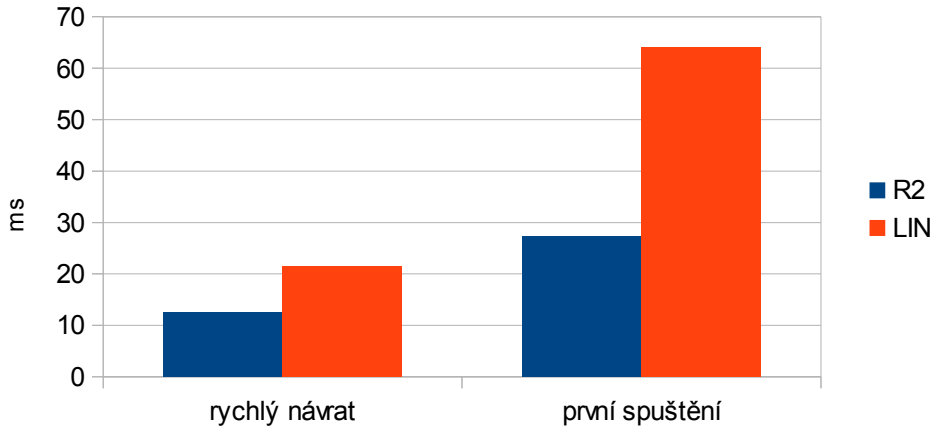


Obrázek 41 – Přístupová doba při již směrovaném provozu

Z grafu vyplývá, že prvotní připojení ke streamu je znatelně rychlejší v případě, kdy je provoz již v síti směrován. Rozdíly jsou také závislé na konkrétních cestách již směrovaného provozu – jak dlouho trvá směrovači připojit se ke stromu nejkratších vzdáleností pro tento zdroj a získat tím cílový provoz. V případě b) je multicastový provoz v síti před přihlášením počítače do skupiny směrován přímo na přes jeho sousední směrovač a tak doba přístupu k takovým datům je minimální. Naproti tomu v případě f) musí sousední směrovač zasílat join message směrem k rendezvous pointu a při této cestě narazí na strom nejkratších vzdáleností až po dvou hopech (skocích) a proto rozdíl v přístupové době mezi případy e) a f) není tak výrazný, jako je tomu v případě a) a b). V počítačových sítích s většími latencemi by se rozdíly s největší pravděpodobností mohly ještě mnohonásobně zvětšit.

V dalším porovnání je testováno, zda je doba přístupu k multicastovému provozu, ovlivněna umístěním rendezvous pointu. Jako příklad lze uvést přístup k datům streamu vysílače R1 na počítači PC3. V prvním případě je rendezvous point umístěn na směrovači R2 a jeho rozhraní Serial 0/0/0, ve druhém případě je umístěn na linuxovém virtualizovaném směrovači LIN a jeho rozhraní *eth0*. Porovnání přístupové doby v obou

případech je zobrazeno na grafu (obrázek 42).



Obrázek 42 – Závislost přístupové doby PC3 na umístnění RP

Rozdíl v přístupové době je z grafu patrný jak pro rychlý návrat, kdy směrovače ještě obsahují multicastové směrovací záznamy, tak pro přístup k datům při prvním připojení ke skupině. V obou případech získá počítač PC3 data mnohem dříve, pokud bude rendezvous point umístěn na směrovači R2. Rendezvous point je v takovém případě umístěn přímo v cestě nejkratší vzdálenosti mezi směrovačem R5 (sousední směrovač počítače PC3) a zdrojem multicastového provozu PC1. Cesty paketů provozu, které ve druhém z případů musí putovat přes celou síť, jsou mezi zdrojem vysílání a rendezvous pointem kratší a přístup ke streamu je v takovém případě rychlejší.

7 Závěr

Diplomová práce se zabývá problematikou technologie IP multicast. Tato technologie umožňuje do značné míry ušetřit systémové prostředky síťových prvků, zejména procesorový čas směrovačů v síti a šířku pásma na jednotlivých síťových spojích. Použití multicastu lze doporučit především pro streamovaná multimédia v reálném čase, která jsou díky své povaze pro přenos pomocí multicastu vhodná. To však neznamená, že všechna ostatní data nejsou pro multicast vhodná.

Zároveň také nelze opomenout, že použití multicastové komunikace má své limity v podobě nespolehlivého přenosu a není vhodné pro každý typ dat, který je napříč počítačovými sítěmi přenášen. Dalším faktem, který je nutné zmínit, je, že samotné směrování multicastových paketů přináší směrovačům značnou zátěž, a proto je použití této technologie potřeba dopředu zvážit. Pokud se ale dá počítat s větším množstvím příjemců datového přenosu, je využití směrovačů o mnoho efektivnější než by tomu bylo u klasické unicastové komunikace.

Cílem diplomové práce bylo navrhnout počítačovou síť pro provoz multicastového provozu porovnat jeho různé parametry.

Byla navržena počítačová síť, která obsahuje různé typy směrovačů s různým operačním systémem. Síť dále obsahuje několik koncových zařízení, které mohou být zdroji nebo přijímači multicastového provozu. Všechna zařízení jsou nakonfigurována pro směrování multicastového provozu pomocí sparse mode varianty protokolu PIM. Konfiguraci provázelo několik problémů. Mezi těmito lze zmínit například nutnost změny parametru linuxového jádra rp_filter, bez které směrování multicastového provozu na směrovači se systémem Ubuntu Server nefunguje správně.

Na navržené síti byly změřeny a porovnány různé parametry multicastového provozu. Jednalo se o procentuální zatížení procesorů jednotlivých směrovačů, počty paketů protokolu PIM, které musel obsloužit linuxový směrovač a doba trvání doručení prvních paketů provozu po přihlášení se k multicastové skupině.

Výsledkem měření bylo, že použití multicastového provozu na navržené síti je z hlediska využití procesorů směrovačů efektivnější až při větším počtu příjemců. V opačném případě byly procesory některých směrovačů více vytíženy odbavováním multicastových paketů než při směrování unicastových.

Měřením doby přístupu k přenášeným paketům bylo zjištěno, že tento čas je znatelně kratší, pokud se zařízení hlásí do multicastové skupiny opakovaně. Velký vliv na dobu přístupu má také přítomnost požadovaného provozu v síti. Pokud již na některém z potřebných směrovačů požadovaný multicastový provoz existuje, je doba přístupu znatelně kratší. Podíl na přístupové době má také poloha rendezvous pointu v síti.

Navržená síť může sloužit jako referenční pro konfiguraci multicastu v podnikových sítích různého rozsahu. Zároveň nabízí možnost pro využití v laboratorních podmínkách, je připravena pro konfiguraci různých síťových protokolů a analýzu jejich kvalitativních i kvantitativních znaků.

Všechny cíle diplomové práce byly splněny. Jsem rád, že se mi dostalo možnosti toto téma realizovat. Tato práce pro mě byla velkým přínosem a prohloubila mé znalosti dané problematiky.

Literatura

1. WILLIAMSON, Beau. *Developing IP multicast networks*. Indianapolis: Cisco Press, 1999. ISBN 15-787-0077-9.

2. HARTE, Lawrence. *Introduction to data multicasting.* Fuquay-Varina: Althos Publishing, 2008. ISBN 19-328-1355-1.

3. TIAN, Xiaohua. *Scalable multicasting over next-generation internet: design, analysis, and applications.* New York: Springer, 2013. ISBN 978-146-1401-520.

4. MAUFER, Thomas A. *Deploying IP multicast in the enterprise.* Upper Saddle River: Prentice Hall, 1998. ISBN 01-389-7687-2.

5. HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce.* 3. aktualiz. vyd. Brno : Computer Press, 2006. ISBN 80-251-0892-9.

6. Introduction to IP Multicast [online]. [cit. 2014-05-01]. Dostupné z: http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/ip-multicast/prod_presentation0900aecd80310883.pdf

7. DONAHUE, Gary A. *Network warrior.* 2nd ed. Beijing: O'Reilly, 2011. ISBN 978-1-449-38786-0.

8. HARTPENCE, Bruce. *Packet guide to core network protocols.* Sebastopol: O'Reilly Media, 2011. ISBN 14-493-0653-5.

9. SETH, Sameer a VENKATESULU, M. Ajaykumur. *TCP/IP architecture, design and implementation in Linux.* Los Alamitos: IEEE Computer Society, 2008. ISBN 978-047-0147-733.

10. SRISURESH, P. a HOLDREGE, M. *RFC 1112 – Host Extensions for IP Multicasting* [online]. ©1989 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc1112.txt

11. SRISURESH, P., EGEVANG, K. *RFC 3022 – Traditional IP Address Translator* [online]. ©2001 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc3022.txt

12. DEERING, S., HINDEN, R. *RFC 2460 – Internet Protocol, Version 6 (IPv6) Specification* [online]. ©1998 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc2460.txt

13. LOSHIN, Pete. *IPv6 theory, protocol, and practice.* 2nd ed. San Francisco: Morgan Kaufmann, 2004. ISBN 15-586-0810-9.

14. RACHERLA Sangam a DANIEL Jason. *IPv6 Introduction and Configuration.* IBM Redbooks, 2012. ISBN 9780738450551.

15. SPURGEON, Charles E. *Ethernet: The Definitive Guide.* Boston: O´Reilly, 2000. ISBN 15-659-2660-9.

16. RACHERLA, Sangam a RACHERLA Oglaza. Sebastian. *IP multicast protocol configuration.* IBM Redbooks, 2012. ISBN 9780738450568.

17. DEERING, S., HABERMAN, B., JINMEI T., NORDMARK E. a ZILL, B. *RFC 4007 – IPv6 Scoped Address Architecture* [online]. ©2005 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc4007.txt

18. HINDEN, R. a DEERING, S. *RFC 4291 – IP version 6 Addressing Architecture* [online]. ©2006 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc4291.txt

19. CRAWFORD, M. *RFC 2464 – Transmission of IPv6 Packets over Ethernet Networks* [online]. ©1998 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc2464.txt

20. FENNER, W. *RFC 2236 – Internet Group Management Protocol, Version 2* [online]. ©1997 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc2236.txt

21. CAIN, B., DEERING, S., KOUVELAS, I., FENNER, B. a THYAGARAJAN, A. *RFC 3376 - Internet Group Management Protocol, Version 3* [online]. ©2002 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc3376.txt

22. CHRISTENSEN, M., KIMBALL, K. a SOLENSKY F. *RFC 4541 – Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches* [online]. ©2006 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc4541.txt

23. ADAMS, A., NICHOLAS, J. a SIADAK, W. *RFC 3973 – Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised)* [online]. ©2005 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc3973.txt

24. FENNER, B., HANDLEY, M., HOLBROOK, H. a KOUVELAS, I. *RFC 46001 – Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)* [online]. ©2006 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc4601.txt

25. Oracle VM VirtualBox [online]. ©1995–2014 [cit. 2014-05-01]. Dostupné z: https://www.virtualbox.org/

26. Reverse Path Filtering. *The Linux Documentation Project* [online]. [cit. 2014-05-01]. Dostupné z: http://tldp.org/HOWTO/Adv-Routing-HOWTO/lartc.kernel.rpf.html

27. Ubuntu Manpage. *pimd – PIM-SM v2 dynamic multicast routing daemon* [online]. ©2010 [cit. 2014-05-01]. Dostupné z: http://manpages.ubuntu.com/manpages/precise/man8/pimd.8.html

28. TCP/IP Protocol: Real-time Transport Protocol. [online]. [cit. 2014-05-01]. Dostupné z: http://www.linux.org/threads/tcp-ip-protocol-real-time-transport-protocol-rtp.4965/

29. SCHULZRINNE, H., CASNER, S., FREDERICK R. a JACOBSON, V. *RFC 3550 – RTP: A Transport Protocol for Real-Time Applications* [online]. ©2003 [cit. 2014-05-01]. http://www.ietf.org/rfc/rfc3550.txt

Příloha A – Konfigurace směrovače R1

```
R1#show running-config
Building configuration...


Current configuration : 1586 bytes
!
! Last configuration change at 20:19:13 UTC Mon Jan 27 2014
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
ip source-route
!
!
ip cef
!
!
ip multicast-routing
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
voice-card 0
!
!
!
license udi pid CISCO2811 sn FCZ131820CB
vtp domain CCNA_Troubleshooting
```

```
vtp mode transparent
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.51.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.0.0.1 255.255.255.252
 ip pim sparse-mode
 clock rate 8000000
!
interface Serial0/0/1
 ip address 10.0.0.5 255.255.255.252
 ip pim sparse-mode
 clock rate 8000000
!
interface Serial0/2/0
 ip address 10.0.0.9 255.255.255.252
 ip pim sparse-mode
 clock rate 8000000
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Integrated-Service-Engine1/0
 no ip address
 shutdown
 no keepalive
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.51.0
```

```
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
ip pim rp-address 10.0.1.2
!
!
!
!
control-plane
!
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
line aux 0
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

Příloha B – Konfigurační soubor pimd.conf

```
default_source_preference     101  # smaller is better
default_source_metric         1024 # smaller is better

# The phyint setting MUST BE AFTER default_source_*,
# BUT MUST BE BEFORE everything else
# By default, all non-loopback multicast capable interfaces
# are enabled.
#phyint de1 disable

# Smaller value means "higher" priority
#cand_rp time 30 priority 20

# Bigger value means  "higher" priority
#cand_bootstrap_router priority 5

# Static rendez-vous point
rp_address 10.0.1.2 224.0.0.0/4

# All multicast groups
group_prefix 224.0.0.0 masklen 4

#
switch_data_threshold rate 0 interval 5
switch_register_threshold rate 0 interval 5
```

Příloha C – Přiložené CD

Na přiloženém CD se nachází text diplomové práce v elektronické podobě.