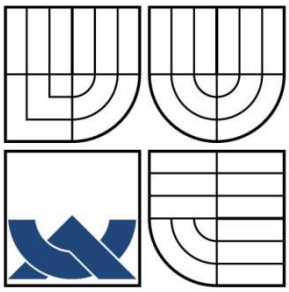
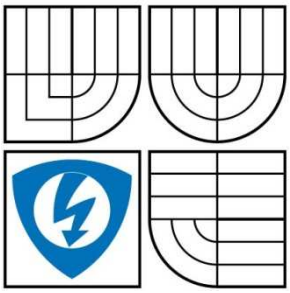


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKACNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

APLIKACE PRO MONITOROVÁNÍ MULTICASTOVÝCH RELACÍ

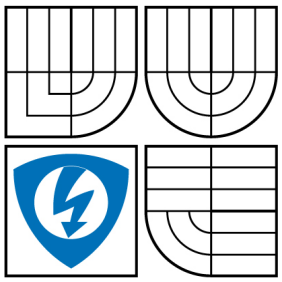
MONITORING APPLICATION FOR MULTICAST SESSIONS

DIPLOMOVÁ PRÁCE
MASTER´S THESIS

AUTOR PRÁCE BC. MARTIN KOPECKÝ
AUTHOR

VEDOUCÍ PRÁCE ING. MILAN ŠIMEK
SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Martin Kopecký	***ID:***	80547
Ročník:	2	***Akademický rok:***	2008/2009

NÁZEV TÉMATU:

Aplikace pro monitorování multicastových relací

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou monitorování multicastových relací v IP sítích. Zaměřte se především na zpracování příkazů v Cisco IOS. V programovacím jazyce JAVA navrhněte aplikaci, která bude monitorovat základní veličiny multicastových relací a vytvořte pro ni přehledné grafické rozhranní. Vytvořenou aplikaci otestujte na reálné multicastové síti.

DOPORUČENÁ LITERATURA:

[1] Maufer T. A.: Deploying IP Multicast in the Enterprise, Prentice-Hall Inc., ISBN: 0-13-89-897687-2

[2] Piotr Wróblewski, Algoritmy - Datové struktury a programovací techniky, Nakladatelství Computer Press, a.s

Termín zadání:	9.2.2009	***Termín odevzdání:***	26.5.2009

Vedoucí práce: Ing. Milan Šimek

prof. Ing. Kamil Vrba, CSc.

Předseda oborové rady

UPOZORNENÍ:

ABSTRAKT

Tématem této diplomové práce bylo seznámit se s možnostmi monitorování počítačových sítí a především monitorování multicastových relací. Navrhnout aplikaci pro monitorování těchto multicastových relací v IP sítích. Hlavním bodem práce bylo navržení přehledného grafického rozhraní a výpis multicastových informací ze síťových prvků experimentální sítě.

V první části jsou popsány možnosti monitorování počítačových sítí z hlediska použití protokolů a technik pro monitorování. V druhé části je popis experimentální počítačové sítě a několik základních příkazů nastavení multicastu v Cisco IOS a také příkazy pro kontrolu nastavení. V třetí části se práce věnuje popisu vytvořené aplikace pro monitorování multicastu v jazyce Java. V poslední části je testování aplikace na reálné multicastové síti a je zde uveden příklad, jak tuto aplikaci otestovat.

KLÍČOVÁ SLOVA

Multicast, SNMP, MIB, IP, Viewer, Monitoring, Cisco, IOS, OID, PIM, IGMP, SSM, ASM, JAVA, IP/TV, NMS, RMON

ABSTRACT

This work deals with a monitoring application for multicast sessions. The general aim is to develop the application for monitoring multicast sessions from network elements of a laboratory computer network.

The first part describes possibilities of monitoring computer networks in terms of monitoring techniques and protocols. The second part contains a topology of the laboratory computer network and several basic commands for setting of the multicast in Cisco IOS. The third part is devoted to the developed application for monitoring the multicast in Java language. The last part describes the testing on an actual multicast network and an example of such testing is stated there.

KEYWORDS

Multicast, SNMP, MIB, IP, Viewer, Monitoring, Cisco, IOS, OID, PIM, IGMP, SSM, ASM, JAVA, IP/TV, NMS, RMON

BIBLIOGRAFICKÁ CITACE

KOPECKÝ, M. *Aplikace pro monitorování multicastových relací.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 73 s. Vedoucí diplomové práce Ing. Milan Šimek.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma Aplikace pro monitorování multicastových relací jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedeného semestrálního projektu dále prohlašuji, že v souvislosti s vytvořením tohoto projektu jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení §11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení §152 trestního zákona č. 140/1961 Sb.

V Brně dne ---------- ----------

Podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce Ing. Milanovi Šimkovi, za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

V Brně dne ---------- ----------

Podpis autora

OBSAH

1. Úvod

V posledních letech stále dochází k velkému rozmachu v počítačových sítích. Vyvíjí se stále nové síťové protokoly, síťová řešení a nové monitorovací techniky a zabezpečení. Téměř každý počítač je zapojen do některé počítačové sítě, ať už lokální, tak velmi rozlehlé, jako je internet. V posledních letech jsou počítače nedílnou součástí téměř každého z nás. Počítače jsou potřeba v bankách, nemocnicích, státních institucích a v mnoha dalších oblastech. Klasický uživatel se často nesetká s odvětvím dohledových center, která monitorují a spravují dané úseky komunikace v počítačových sítích. S tímto velkým rozmachem užívání sítí je také důležitý rozvoj dohledových center, která se stávají stále potřebnější. Také každý již mohl slyšet pojem multicast. Multicast se rozvíjí a vyvíjí stále více, především pro multimediální přenosy dat. Již existuje mnoho projektů, kde se používá. Chceme-li například sledovat televizi ve vysoké kvalitě, využívat videokonference s mnoha účastníky, je vhodné použít technologii multicastu, ovšem není to nutné.

První část práce je zaměřena na teoretický základ a většinu důležitých pojmů, které jsou nezbytné. Především je potřeba se seznámit s funkcí dohledových center, která jsou zapotřebí, nejen pro monitorování počítačových sítí, ale také pro správu a údržbu. Monitoring je velice důležitý, především pro správce nebo administrátora, některé sítě nebo síťového úseku. Dochází k velkému rozmachu nástrojů, které se na monitoring zaměřují a usnadňují práci.

Další část navazuje plynule na předchozí rozebíranou problematiku monitorování počítačových sítí z pohledu správce sítě. Zde je rozebrán jeden z protokolů, který se v posledních letech rozvíjí a s jeho použitím se můžeme již setkat, téměř ve všech aplikacích umožňujících monitorování počítačových sítí. Důležité je pochopit funkci protokolu Simple Network Management Protocol (SNMP). Tento síťový protokol je rozebrán teoreticky a následně je uvedeno několik často používaných implementací.

Dále se práce věnuje problematice monitorování multicastových relací v IP sítích. Většina monitorovacích systému se zaměřuje na určitou část sítě. Správce sítě si specifikuje problém, který chtějí monitorovat a sledovat. Zde se jedná o sledování multicastových relací. Multicastových relací může být mnoho a jsou velice specifické. Pro monitorování multicastových relací v IP sítích, se používá již zmíněný protokol SNMP, ale není to podmínkou.

Po několika teoretických kapitolách se práce věnuje experimentální části. V úvodní části je naznačena topologie sítě a její zapojení v laboratoři. Také je zde navrhnuto adresní schéma sítě. Jsou zde uvedeny příklady nastavení multicastu na reálné experimentální síti a některé Cisco IOS příkazy použité na směrovačích ke kterým je uveden stručný popis.

Z důvodu nedostatku aplikací pro monitorování multicastových relací byla navržena aplikace pro monitorování multicastových relací v programovacím jazyce JAVA (JDK1.6). Jsou zde uvedeny nároky na aplikaci a její reálné využití v experimentální síti. Aplikace má přehledné grafické rozhraní, které je podrobně popsáno. Dále je popsána funkčnost aplikace a jsou uvedeny příklady práce s touto aplikací.

2. SPRÁVA A MONITOROVÁNÍ V POČÍTAČOVÝCH SÍTÍ

V současné době můžeme pozorovat velký rozvoj všech oblastí počítačových sítí. Lze říci, že složitost roste téměř exponenciálně vzhůru. Počítače a počítačové sítě nás obklopují téměř již ve všech oblastech života, proto je nesmírně důležitá funkčnost těchto sítí. Většina společností je již závislá na počítačových sítích jako je internet. Ovšem vyvíjí se také experimentální sítě například s multicastovým provozem. Je velmi důležité nejenom, aby síť fungovala jak má, ale aby v případě výpadku, byla síť co nejrychleji zprovozněna. Zavádí se tedy monitorování sítě a tím i urychlení odstraňování poruch. Především pro správce sítí, je monitorování velice důležitou složkou a téměř už nezbytným předpokladem ke správné funkčnosti, bezpečnosti a spolehlivosti sítě.

2.1. CÍLE SPRÁVY SÍTĚ

Cíle správy počítačové sítě jsou tedy jednoznačně dané, funkčnost, bezpečnost a spolehlivost. Důležitým faktorem je snadná obsluha sítě a rychlé reagování na změny v síti, tedy údržba a případné rozšiřování. Správa sítě je vlastně dohled nad správnou činností technického a také softwarového vybavení počítačové sítě.

Důležité je práce administrátora neboli správce sítě, který zajišťuje funkčnost dané počítačové sítě. Administrátor zastřešuje vrchol správy sítě, má na starost mnoho důležitých činností. Jak již bylo v úvodu vývoj nejrůznějších prvků a komponentů počítačových sítí se neustále zdokonaluje a vyvíjí, je potřeba tyto prvky v síti měnit a zdokonalovat tak funkčnost sítě. Administrátor se tedy stará o instalaci, zapojení aktivních prvků, konfigurace těchto prvků, návrh a realizace kabelových rozvodů a mnoho dalších činností. Především také dohled nad správnou funkcí těchto zapojených prvků.

V každé počítačové síti je použito programové vybavení, které je nezbytnou složkou. Programové vybavení lze rozdělit na dvě větší skupiny. Jedna z nich je software pro nastavování aktivních prvků v síti. Druhá z těchto skupin je uživatelský software. Do této skupiny patří například vzdálený přístup k aktivním prvkům například Telnet, SSH. Prostředky pro sdílení souborů, prohlížeče www, www servery pro snadnější administraci prvků přes webové rozhraní. Také je velmi důležité sledovat určité statistiky sítě, ze kterých lze předvídat problémy. K tomuto účelu je vhodné využívat v síti dostatečně vyspělé síťové prvky a všechny dostupné prostředky vzdálené správy například protokol SNMP nebo také Remote MONitoring (RMON). Pomocí těchto protokolů, lze ze sítě zjistit spousta důležitých informací. V následujících kapitolách bude rozebráno, jaké informace jsou potřeba pro správnou funkčnost.

2.2. SMYSL A PŘÍNOSY SPRÁVY SÍTÍ

Dnešní rozsáhlé sítě obsahují nepřeberné množství aktivních prvků, jako jsou rozbočovače, směrovače, servery, ale také samotné pracovní stanice a další. Každý administrátor má za úkol spravovat tyto prvky, je ovšem nemožné provádět správu fyzicky. Představme si velké budovy se stovkami pracovních stanic, velké města, jednotlivé státy a nakonec kontinenty, kde je potřeba spravovat určitý úsek sítě. Také si představme různé propojení prvků, různé technologie, síťové protokoly a také odlišnosti u síťových prvků různých výrobců.

Dříve se v prostředí velkých sálových počítačů zavedla strategie, kterou nazýváme Service Management. Garantovala nám zajištění určitých služeb a údržbu informačních systému. S postupem času se vše změnilo a tyto garantované služby se již přestaly nabízet a začali se zavádět distribuované systémy. Většinou se jedná o model klient-server, se kterým se v této práci ještě několikrát setkáme. Postupem času se také přecházelo na různé operační systémy, jako jsou UNIX a Microsoft Windows v různých implementacích založené na protokolech TCP/IP.

Na rozdíl od centralizované správy sálových počítačů se správa distribuovaných výpočetních systémů rozvíjí a přidávají se stále nové možnosti této implementace. Lze spravovat většinu síťových prvků a zařízení, což je jeden s největších kroků v před. [1]

Správa systému musí být robustní, musí vyhovovat všem novým výpočetním i komunikačním potřebám. Velice důležitá je spolehlivost, na kterou se v poslední době dbá především. Správa systémů je také nezanedbatelnou položkou v nákladech společností na IT.

2.3. SPRÁVA A MONITORING

Výrobci síťových produktů většinou dodávají software v podobě administračního rozhraní, pro nastavení veškerých parametrů daného zařízení, získání statistik a další možnosti. Administrační rozhraní bývají různé. Jedno z nich je Command Line Interface (CLI), jedná se o nastavování přes příkazový řádkový interpret. Většinou se k takovým zařízením přistupuje pomocí již zmíněného ssh nebo telnetu. Takovéto připojení na síťová zařízení používají většinou dobře znalí a zkušení administrátoři. Další možností pro nastavování je webové rozhraní. Toto rozhraní lze jednoduše obsluhovat pomocí webového prohlížeče. Tato volba nevyhovuje většině zkušenějších administrátorů.

Proto byl v rámci Internet Engineering Task Force (IETF) vyvinut protokol SNMP, který umožňuje monitoring síťových zařízení automatizovat a kromě toho jej činí do značné míry nezávislým na výrobci. SNMP protokol funguje na principu klient-server, funkčnost protokolu bude popsána v jedné z následujících kapitol.

Monitoring se poté provádí do značné míry jednoduše, stačí mít dobré programové vybavení na monitorování sítě pomocí tohoto protokolu. Můžeme sledovat řadu nejrůznějších statistik provozu sítě a daných síťových zařízení, jako je

například počet přijatých paketů, uptime, multicast relace a mnoho dalších volitelných položek, které nabízí SNMP protokol.

2.4. Správa sítí založená na technologii Java

V použití technologií rozvíjejících se v oblasti World Wide Web (WWW) serverů lze jít i dál a provádět celou správu sítě speciálními Common Gateway Interface (CGI) skripty, které jsou schopny zobrazovat SNMP informace. Také je velikou výhodou použít jazyk Java, kde lze zajistit lepší přenositelnost mezi různými operačními systémy. Také se vyvíjí různé Java applety, které lze pohodlně spouštět velice jednoduše. Nevýhoda je rychlost připojení. Stále se tedy častěji volí naprogramovat systém, který se spouští jako normální program. Ovšem tento úkol není pro každého. Většinou se tyto monitorovací systémy nabízí za nemalé finanční prostředky.

Použitelných nástrojů a metod pro sledování systému je celá řada. Technologie Java je velice přívětivá k použití SNMP protokolu a je mnoho open-source programů, kterých lze užít a sestavit si tak svůj profesionální program.[2]

2.5. Analýza provozu

Pro provádění analýzy provozu na lokální počítačové síti jsou dodávána i jednoúčelová speciální zařízení s poměrně širokou škálou vlastností, velmi často se zde však jedná o přenosné počítače s patřičným programovým vybavením. Jejich nevýhodou však bývá jejich poměrně velmi vysoká cena. Uvedeme si několik příkladů testování pomocí základních nástrojů, které se také využívají v profesionálních monitorovacích programech.

2.5.1. Sledování dostupnosti programu ping

Sledování dostupnosti zařízení na síti lze pomocí programu ping. Tento program je implementován ve většině operačních systému. Používá Internet Control Message Protocol (ICMP). Počítač, na kterém zadáme tento příkaz spolu s cílovou IP adresou, vyšle po síti žádost o odpověď (ICMP Echo Request) cílovému počítači a čeká na odezvu. Po obdržení odpovědi (ICMP Echo Response) zobrazí čas, který byl k této činnosti potřeba (Round Trip Time).

```
\C:\ >ping www.xxx.cz
Pinging www.xxx.cz [193.85.4.100] with 32 bytes of data:
Reply from 193.85.4.100: bytes=32 time=19ms TTL=249
Reply from 193.85.4.100: bytes=32 time=8ms TTL=249
Reply from 193.85.4.100: bytes=32 time=11ms TTL=249
Reply from 193.85.4.100: bytes=32 time=8ms TTL=249
```

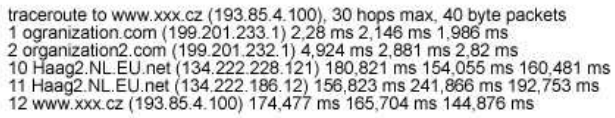
Obr. 2.1: Výstup příkazu ping v operačním systému MS Windows XP

Tímto velmi oblíbeným programem, lze jednoduše zjistit, zda daná IP adresa je dostupná či nikoliv. Tento program se velice osvědčil na základní zjištění dostupnosti.

Také je možnost, podle Time To Live (TTL) zjistit, jaká je propustnost sítě a její reakční schopnosti.

2.5.2. Příkaz traceroute

Další ze základních nástrojů je příkaz traceroute. Pokud potřebujeme zjistit, kudy procházejí data od zdroje k jeho cíly, použijeme tento příkaz. Výstupem tohoto příkazu je seznam směrovačů, přes které data postupně procházejí. Také se používá ICMP protokol a parametr Time Exceeded (TE).



Obr. 2.2: Výstup příkazu traceroute v operačním systému MS Windows XP

2.6. Síťový model správy podle ISO

Jelikož v minulosti bylo mnoho návrhů na správu sítí, bylo důležité navrhnout model správy sítě. Tento úkol si vzala na starosti mezinárodní organizace International Standards Organization (ISO), která standardizovala síťový management. Tento model se skládá z několika částí. Je popsán v dokumentu označeném OSI Management Framework. Tento dokument je čtvrtou částí standardu OSI Basic Reference Model (ISO/IEC 7498-4) [3], popisujícího síťový komunikační model.

Správa výkonu je první část modelu. Měří výkonnost a zatížení jednotlivých systémů sítě. Monitorují se zde různé parametry zatížení jak operačního systému a programů, tak šířka přenosového pásma a různé odezvy. Zavadí se dva důležité druhy managementu, reaktivní a proaktivní. Reaktivní management znamená reakce na překročení určitých limitů, lze nastavit určitou akci. Většinou se nastavuje informační zpráva o stavu sítě, která se odešle administrátorovi. Proaktivní management znamená lepší plánování do budoucna a předcházení určitým problémům dříve než nastanou.

Konfigurační management. Sleduje nastavení konfigurace sítě a řeší její optimální chod, z důvodu vlivu na síťové prvky sítě. Veškeré zjištěné informace se ukládají do databáze pro snadný další přístup.

Management účtů je sledování parametrů využití sítě jednotlivými uživateli. Tyto informace ve formě přehledných reportů umožní správci sítě lépe zjišťovat poplatky uživatelů, zjišťovat jejich chování v síti a rozdělovat úměrně provoz mezi ostatní uživatele.

Poruchový management je detekce chyb a poruch sítě, jejich izolace chodu sítě. Zaznamenávají se do souboru. Poté jsou uživatelé nebo správce sítě upozorněni na vznik problému. Tato část tohoto modelu je obzvlášť obsáhlá a důležitá, protože to je základní problém sítí a proto se zavádí vlastně celý monitoring počítačových sítí.

Bezpečnostní management řídí přístup k síťovým zdrojům podle stanovených pravidel tak, aby nemohlo dojít k neoprávněnému přístupu do sítě. Zde se nastavují další parametry jako je přihlášení, zadání uživatelského jména a hesla. Lze zde detekovat případné pokusy o zdolání bezpečnosti systému a následné blokování uživatelů.

3. SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

3.1. MINULOST A BUDOUCNOST

V minulosti prvních počítačových sítí se administrátoři setkávali s menšími problémy než tomu je v této době, jak již bylo zmíněno rozmanitost dnešních počítačových sítí je obrovská a také s tímto aspektem narůstají možnosti chyb v síti. Administrátoři z dřívějších dob používali nástroje jako je například ICMP protokol, ping a jejich možnosti, k různým odhalením chyb. Jelikož brzy možnosti těchto nástrojů již nestačili, tak se programátoři rozhodli vyvinout nový protokol zaměřený přímo na monitorování sítě. První nástroj byl protokol Simple Gateway Monitoring Protocol (SGMP). Tento protokol umí monitorovat brány (Gateway), ovšem to brzy nestačilo. Poté již programátoři začínají nazývat další verzi protokolu SNMP, ovšem ještě zdaleka ne v tak rozmanité formě. V tuto dobu umí SNMP pracovat pouze na Transmission Control Protocol/Internet Protocol (TCP/IP) sítích. V roce 1993 byl SNMP rozšířen o možnosti pracovat na sítích AppleTalk a Internet Packet Exchange (IPX). Poté se objevuje standard Remote Network MONitoring (RMON), který umožňuje monitorovat celé podsítě jako jeden celek a nemusí se dotazovat všech zařízení. Vývojáři navrhli nový bezpečný a spolehlivý protokol Common Management Information Protocol (CMIP), který byl zastřešující z těchto monitorovacích protokolů měl nahradit SNMP, ovšem nestalo se tak z jednoho prostého důvodu. Tento protokol měl o mnoho větší nároky na přenosové cesty, a tedy režie sítě byla o mnoho větší než u protokolu SNMP. Proto se dále rozvíjel především protokol SNMP a stal se standardem pro testování a správu. Používá se již velmi rozmanitě, především z hlediska finančního.

3.2. VERZE SNMP PROTOKOLU

Při vzniku protokolu SNMP bylo cílem vytvořit pro správce univerzální centralizovaný nástroj pro sledování, kontrolu stavu a vzdálené řízení sítí. SNMP pracuje na aplikační vrstvě modelu Open Systems Interconnection Basic Reference Model OSI/ISO. Tak jako každý protokol měl SNMP v minulosti mnoho nedostatků. Přicházejí na řadu úpravy a různé verze protokolu. SNMP používá User Datagram Protocol (UDP) porty 161 pro agenta a 162 pro manažera. Manažer může posílat žádosti z různého dostupného portu. Odezva agenta bude poslána zpátky do zdroje. A manažer přijme na portu 162.

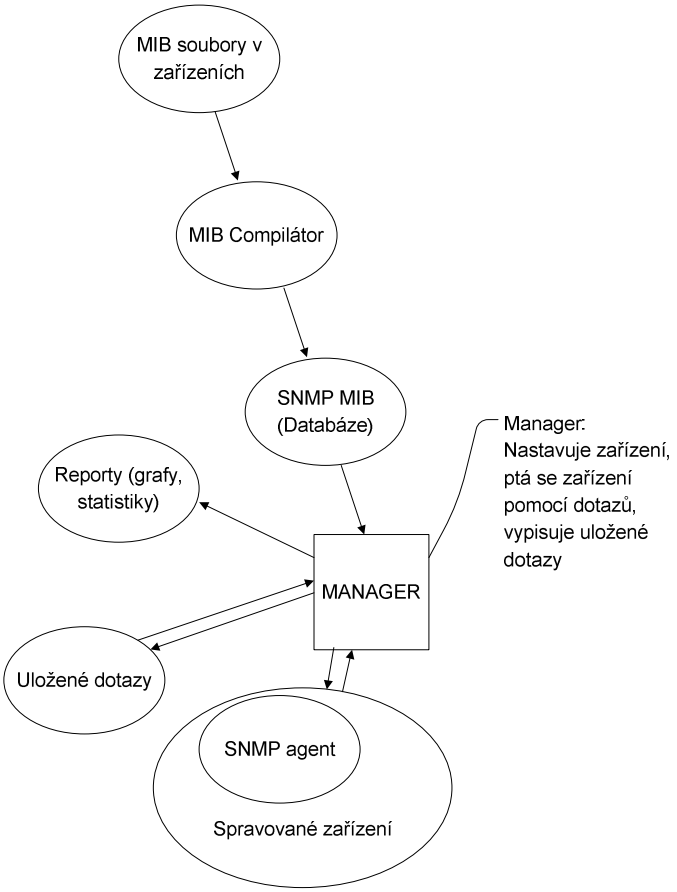
První verze protokolu se nazývá SNMPv1. Tato první verze byla kritizovaná především za bezpečnost v dnešní době velice důležitý prvek. Autentifikace klientů je vykonávána jen řetězcem komunity, ve skutečnosti druh hesla, který je přenášen v Protokol Data Unit (PDU).

Přichází na řadu další verze protokolu SNMPv2. Zlepšení tohoto protokolu nedoznalo větších změn především v části bezpečnosti, proto také tato verze není stále optimální z tohoto hlediska. Bezpečnost je v podstatě založena na první verzi s minimálními úpravami. Funkčnost a výkon této verze již je na tom o poznání lépe. Zdokonalení je především k získávání informací a zapouzdření více žádostí do jedné. V protokolu SNMPv2 je definováno celkem 6 základních operací pro komunikaci mezi centrální řídicí stanicí Network Management Systém (NMS) a agenty v jednotlivých sledovaných zařízeních. 1. Get dovoluje NMS stanici zjistit hodnotu vybraného objektu od SNMP agenta. 2. GetNext dovoluje NMS stanici získat hodnotu dalšího objektu ve stromové struktuře Management information base (MIB). 3. GetBulk tato operace byla přidána, aby se eliminovala potřeba zadávat velkého množství žádostí GetNext pro přenos větších objemů SNMP dat. 4. Set dovoluje NMS stanici nastavit hodnotu vybraného objektu v agentu, přístup je řízen podle názvu komunity. 5. Inform dovoluje výměnu trap zpráv mezi několika Network Management System (NMS).

Na řadu přichází verze 3, která již doznala nemalých změn v oblasti bezpečnosti. Je přidána autorizace a zabezpečené připojení hesla. Také podpora IPv6 a nejenom IPv4. Verze je o poznání lepší nejenom z hlediska bezpečnosti, ale také výkonu. Ochrana dat se provádí šifrovacím algoritmem Data Encryption Standard (DES). Negativa jsou ve větší režii sítě, ovšem stále zanedbatelné než u jiných protokolů pro monitorování. Implementace tohoto protokolu není úplně ideální. Důvod je jednoduchý, jelikož stále síť funguje na starších prvcích, které podporují pouze předchozí verze a také různí výrobci prozatím nezavádí také verzi 3.

3.3. Model typu Manager – Agent

Architektura SNMP protokolu funguje podle modelu Manager – Agent a umožňuje přenos a komunikaci mezi správcem sítě tedy managerem a agenty na jednotlivých síťových zařízeních. K tomu vyžaduje, aby každé zařízení sítě poskytovalo jisté základní informace o sobě samém a stejně tak usnadnilo přidání dalších informací, specifických pro dané zařízení. Tyto základní a přídavné informace se spolu nazývají Management Information Base (MIB). MIB databáze bude rozebrána jako samostatná kapitola v této práci.



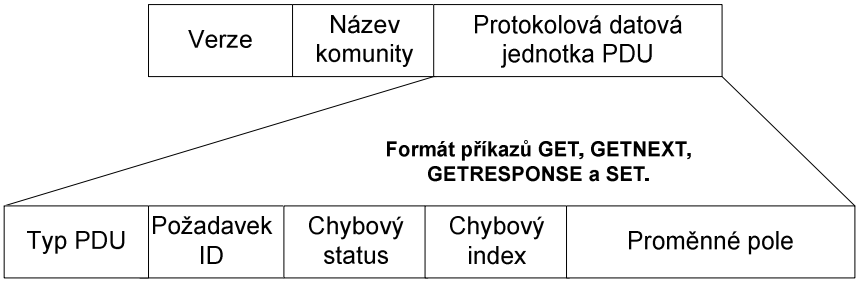
Obr. 3.1: Základní model Manager-Agent

Protokol definuje dva typy zařízení na síti, se kterými už jsme se setkali výše. Managery a Agenty. Navíc mohou existovat tzv. proxy agenti, které kontaktuje manager místo vlastních agentů. SNMP Manager je program, který běží na síťové stanici. U větších systémů jde většinou o vyhrazenou výkonnou pracovní stanici s běžícím software Network Management System (NMS). Funkce tohoto SNMP Manageru pak spočívá v dotazování jednotlivých SNMP Agentů pomocí SNMP operací. Smyslem je získat všechny potřebné informace o daném zařízení, které agent reprezentuje. SNMP Manager poskytuje většinou grafické rozhraní, které umožňuje prezentaci získaných dat, sledování síťových alarmů a archivaci dat např. k analýze časového vývoje. SNMP Agent - je malý program, běžící na síťovém zařízení, který jej reprezentuje a odpovídá na dotazy SNMP Managera. Agent proto neustále monitoruje a sbírá informace o všech dostupných funkcích a stavech daného zařízení. K získání informací o daném zařízení, manager musí vyslat požadavek na dané zařízení a projít informace poskytované agentem. Musí projít celou stromovou strukturou MIB až k objektu, který obsahuje potřebná data, aby mohl získané informace interpretovat. Informace mohou být také vyslány agentem bez vyžádání managerem. Jestliže agent detekuje jisté nestandardní podmínky, jako např. hardwarovou poruchu, vyšle tuto informaci, zvanou trap, sám bez vyžádání. To je důležité pro zajištění okamžité informovanosti např. o vážnějších problémech. Tento druh informací k managerovi se

nazývá polling aktivita, což je procedura vyžádání informací a je nastavitelná v jistých intervalech. Pro většinu informací není nutné kontinuální monitorování, neprovádí se také z důvodu zbytečné zátěže sítě, a tak kombinace polling aktivity managera a trap aktivity agenta zajišťují potřebnou efektivitu. V lepších programech je tato možnost provedená tlačítkem start a stop polling.

3.4. Formát SNMP zpráv

Tak jako každý protokol používá různé zapouzdření zpráv, které se posílají po síti, také SNMP protokol používá svoje specifické zapouzdření. SNMP zprávy se skládají ze dvou hlavních částí. Hlavička zprávy a její vlastní Protokol Data Unit (PDU) viz obr. 3.2. Hlavička je velice důležitá, především jde zde o určení číslo verze SNMP protokolu a také název komunity. Ovšem je zbytečné přenášet tuto informaci v každé zprávě, jak to protokol provádí. Do budoucna by tato drobnost mohla být vyřešena. Vlastní datová část zprávy obsahuje jeden z příkazů SNMP protokolu a příslušný operand, což je položka objektu, která je předmětem komunikace. Poté se definují také speciální zprávy, které se nazývají trapy, také již zmíněné v této práci. Jedná se o informační zprávu. Struktura a význam této zprávy je na obrázku 3.2. Také SNMP obsahuje ještě jeden typ zprávy. GetBulk – request, což je požadavek na zaslání objemného seznamu setříděných podle identifikátoru. Struktura této zprávy a její význam je na obrázku 3.4.



Obr. 3.2: Formát SNMP zpráv

Jednotlivá pole mají následující význam:

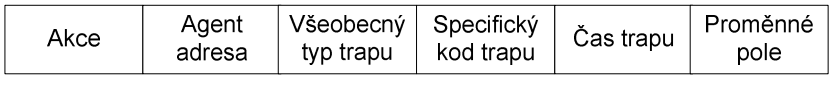
Typ PDU - 0 Get-request, 1 GetNext-request, 2 Get-response, 3 Set-request, 4 Trap, 5 Inform

Požadavek ID - přiřazuje požadavky s odpověďmi.

Chybový status - indikuje chybu a její typ.

Chybový index - přiřazuje chybu dané proměnné z pole variable bindings.

Proměnné pole - obsahuje vlastní data SNMP PDU, přiřazuje daným proměnným jejich aktuální hodnoty (vyjma Get a GetNext příkazů).



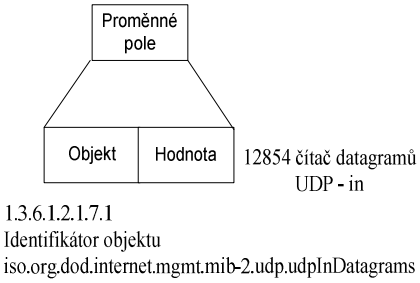
Obr. 3.3: Typ zprávy Trap

Akce - identifikuje typ objektu, který vygeneroval trap.
Agent adresa - je adresa objektu, který vygeneroval trap.
Všeobecný typ trapu, specifický kod trap - identifikují typ a kód trapu.
Čas trapu - čas mezi poslední reinicializací sítě a vygenerováním trapu.
Proměnné pole - seznam proměnných, které obsahují relevantní informace k danému trapu.

Typ PDU	Požadavek ID	Počet proměnných	Maximum opakování	Proměnné pole

Obr. 3.4: Typ zpávy GetBulk – request

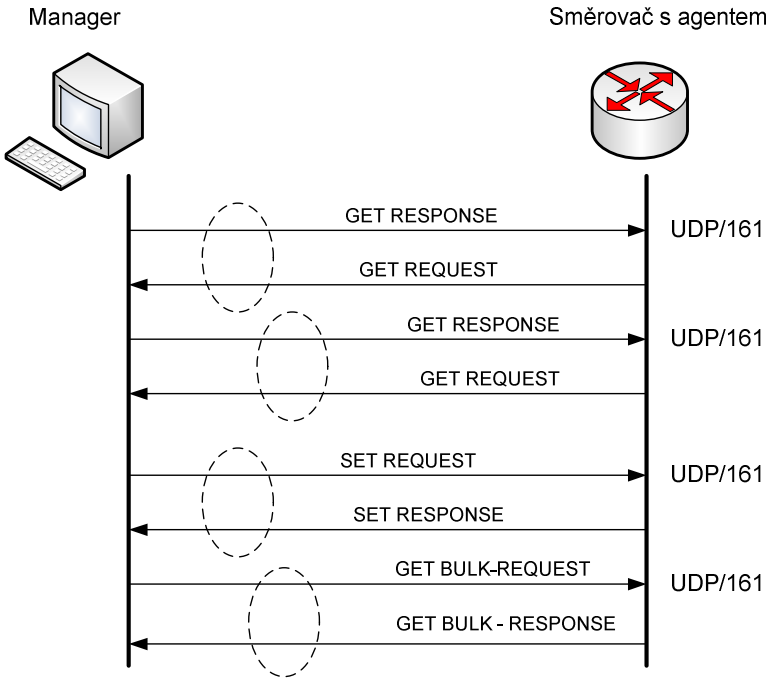
Typ PDU - 0 Get-request, 1 GetNext-request, 2 Get-response, 3 Set-request, 4 Trap, 5 Inform
Požadavek ID - přiřazuje požadavky s odpověďmi.
Počet proměnných - počet proměnných v seznamu Objekt-Hodnota, pro které se očekává, v odpovědi, pouze jedna hodnota (skalární objekty).
Maximum opakování - určuje maximální počet hodnot pro každou proměnnou (mimo skalární objekty).



Obr. 3.5: Příklad obsahu Proměnné pole

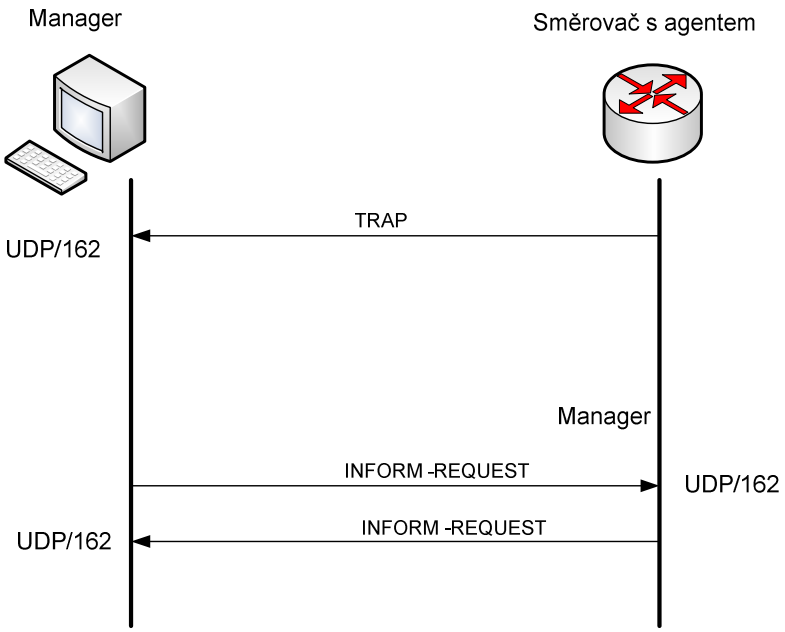
3.4.1. KOMUNIKACE SNMP PROTOKOLU

Komunikace v modelu manager-agent je znázorněná na obrázku 3.6. Manager posílá zprávu s požadavkem na směrovač, který je nastaven i jako agent pro sběr informací. Vysílání tohoto požadavku je přes port UDP/161. Následně dostává odpověď od agenta. Tato komunikace probíhá pro běžné zprávy protokolu SNMP. Poté je možno nastavovat různý objekt v agentovi, přes zprávy Set Request. V komunikaci je také definována zpráva Get Bulk-Request, kde v jédné takové zprávě je několik požadavků na objekt v agentovi. [4]



Obr. 3.6: Komunikace mezi managerem a agentem, základní zprávy

Na dalším obrázku 3.7 je zobrazena komunikace trap zpráv, které vysílá sám agent ze směrovače. Trap zprávy se posílají směrem k managerovi, kde manager přijímá tyto SNMP zprávy na portu UDP/162. Následně si manager ověřuje zprávami Inform stav daného objektu.

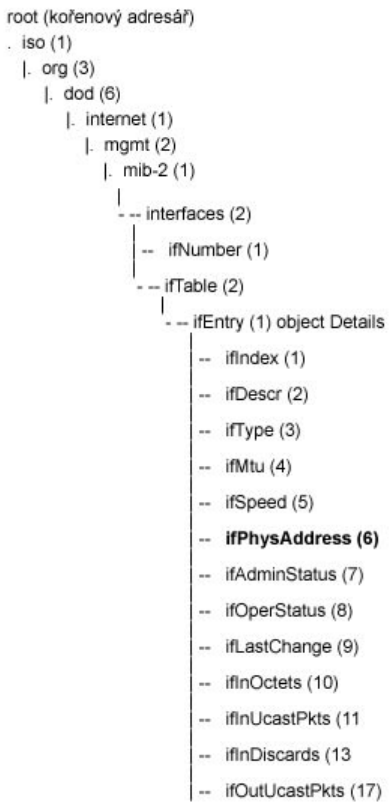


Obr. 3.7: Komunikace mezi managerem a agentem, Trap zprávy

3.4.2. Management Information Base (MIB)

Jedná se o databázi, která popisuje sadu objektů, které jsou potřebné ke správě daného zařízení. Na dané zařízení se může implementovat několik takovýchto databází, záleží na okolnostech, co vše je potřeba monitorovat a spravovat. MIB popisuje strukturu, ale také formát dat. MIB je tedy datová hierarchická stromová struktura, která odpovídá danému konkrétnímu zařízení a je objektově orientována jako sada SNMP objektů, relací a operací na a mezi objekty. Moduly v MIB musí vyhovovat syntaktickým pravidlům podmnožiny jazyka Abstract Syntax Notation One (ASN.1) a seskupují dohromady odpovídající příkazy a definice. Tyto moduly se uchovávají v ASCII souboru. Dokonalá znalost databáze MIB je především důležitá pro programátory SNMP nástrojů, ale především pro výrobce zařízení. MIB databáze jsou někdy velice rozsáhlé a obsahují mnoho objektů. Každý objekt zařízení musí mít dané místo ve stromové struktuře, je to velice důležité především z hlediska odkazování při SNMP operacích. [6]

Stromová organizace databáze MIB se také označuje jako Global Naming Tree. Každý uzel v této struktuře obsahuje popis a poté taky integer hodnotu, vše je naznačeno na obrázku 3.8.



Obr. 3.8: MIB struktura - Global Naming Tree

Skládá se z objektů root, subtree a leaf . Na nejvyšší úrovni jsou například uzly 0-CCIT, 1-ISO a další. Poté se přidělují jednotlivým výrobcům jejich vlastní podstromy, což je někdy nevýhoda, jelikož rozmanitost takovýchto databází neúměrně stoupá. Adresování je pomocí jména daného uzlu, tedy Object Identifier (OID). Adresa je tvořena sekvencí číselných integerů na cestě z root přes subtree až k danému objektu typu leaf. Tato decimální notace reprezentuje tedy cestu ke každé z funkcí nebo schopností daného zařízení. Struktura může připomínat, některé prvky jako v systémech UNIX. Adresa může být ve tvaru 1.3.6.1.2.1.2.1.2.1.**6**, jak je z obrázku patrné cesta postupuje podle daných OID až na konec stromové struktury. Například tato adresa nás odkazuje na cestu k získání fyzické adresy na daném rozhraní.

3.4.3. SNMP OBJEKTY A JEJICH TYPY

SNMP objekty mají dva typy, skalární a tabulární hodnoty. První z nich může nabývat pouze jednoduché nestrukturované hodnoty. SNMP dovoluje ještě tři jiné typy skalárních hodnot (NULL, Opaque a Network Address), které se ale nepoužívají. V tabulce 3.9 jsou uvedené hodnoty pro skalární i tabulární objekty. Přesto nelze provádět SNMP operace nad tabulkami jako celkem, ale jen nad jednotlivými skalárními objekty, tedy hodnotami v tabulce. Jednoduchý příklad je směrovací tabulka směrovače.

Tab. 3.9 - Skupina udp, skalární objekty a tabulární objekt

Skalární objekt			
Název	*Datový typ*	*R/W*	*Popis*
udpInDatagrams	Čítač	-	Počet UDP datagramů doručených do uživatelských procesů
udpNoPorts	Čítač	-	Počet UDP datagramů, pro které neexistoval proces na cílovém portu
udpInErrors	Čítač	-	Počet UDP nedoručených (chybových) datagramů
udpOutDatagrams	Čítač	-	Počet UDP datagramů vyslaných
Tabulární objekt			
Název	*Datový typ*	*R/W*	*Popis*
udpLocalAddress	IP adresa	-	Lokální IP adresa pro proces
udpLocalPort	[0.....65535]	-	Číslo portu pro proces

Je několik datových typů. Čítač, který je uveden na obrázku je nezáporný integer, který se stále postupně zvětšuje, až dosáhne max. hodnoty (232-1) a poté začíná od nuly. Absolutní hodnota je méně důležitá než rozdíl delta od posledního vzorku, ze kterého lze usuzovat na rychlost změn. Jak je na obrázku patrné používá se

například na výčet počtu UDP datagramů. Dalším datovým typem může být Míra (Gauge), také je tento typ nezáporný integer, jehož hodnota může vzrůstat, ale i klesat, nikdy ovšem nepřekročí maximální hodnotu. Hodnota je maximální, když je informace větší nebo stejná jako toto maximum. Dalším typem je TimeTicks. Také se jedná o nezáporný integer, který reprezentují v setinách sekundy čas od dané doby. Zjišťování například uptime určitého zařízení. IP adresa je datový typ o délce 32bitů. Řetězec Octet [0 až 65535], je sekvence bytů, která vyjadřuje řetězec znaků nebo libovolné binární data, používá se především pro zjištění MAC adresy zařízení.[4]

3.5. Bezpečnost přístupu

Velice důležitou, dříve opomíjenou stránkou, je bezpečnost. SNMP přistupuje k objektům a poté probíhá určitá komunikace po síti posílání SNMP zpráv a ty je potřeba zabezpečit. Zabezpečení přístupu k objektům se řeší pomocí přístupových práv, které se přidělují SNMP agentům a managerům. Způsob zabezpečení je celkem jednoduše vymyšlen. V každém příkazu je obsažen název komunity, který byl již v této práci zmíněn. Funguje jako kombinace jména a hesla. Správce definuje přístup k objektům pomocí možnosti čtení a zápisu. Prakticky se musí shodovat možnosti čtení a zápisu jak na zařízení, tak na agentovi a poté se příkazu vyhoví, v opačném případě se zpráva zahodí. Nejpoužívanější název komunity je default. U SNMP zařízení je pro veřejné zprávy pouze čtení a pro privátní je povolen i zápis.

Celkově ovšem není zabezpečení SNMP protokolu na nejlepší úrovni, ovšem je několik druhů zabezpečení. Jeden způsob je ověřovat názvy komunit. Je možné přidávat, měnit a odebírat komunity. Z důvodu zabezpečení není vhodné vytvářet komunitu s názvem Veřejná. Definuje se seznam a poté se zpracovávají pouze požadavky určité komunity, také se dají nastavovat práva určité komunity. Další možností je ověřování pomocí ověřovací depeše. Kontroluje se platnost názvu a adresa hostitele. Jakmile agent obdrží požadavek, u kterého není správně název komunity nebo není členem seznamu, agent pošle ověřovací depeši správcům a označí tím, že ověření selhalo. Tato možnost je většinou v základním nastavení.

3.6. Další vývoj protokolu SNMP

Některá omezení protokolu SNMP vyplývají přímo z jeho architektury, která používá pasivní agenty, jež jsou aktivováni pouze SNMP dotazy. Takto zvolená architektura je nešetrná vůči přenosovému pásmu z hlediska pravidelného dotazování agentů od aplikací. V SNMP protokolu není definována komunikace mezi managery, takže funkce managementu se nedá použít u více správců současně, to omezuje tento protokol u opravdu velkých společností, kde by tato možnost byla velice oceňována. Také je velice obtížné získat jedním příkazem více informací. Komunikace mezi agentem a managerem není také úplně optimální. Agent upozorní managera na

problém a ten se musí dotazovat na další podrobnosti, navíc agent neví, jestli zpráva od něj byla doručena managerovi.

Protokol má ale i několik předností, tou největší je bezesporu jeho velké rozšíření a popularita. Je také velice univerzální, lze použít na mnoho prvků z počítačových sítí, ale i na nejrůznější senzory a další elektrotechnické prvky. Pro všechny pro a proti protokolu, lze říci, že v současnosti neexistuje k SNMP protokolu lepší alternativa na monitoring a správu v počítačových sítích.

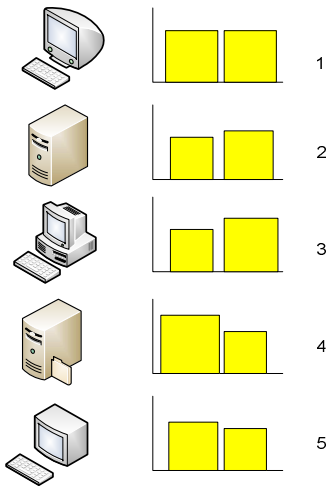
4. REMOTE MONITORING (RMON)

4.1. POPIS STANDARDU

Tento standard vznik především z několika hledisek nedokonalosti SNMP protokolu. Při vývoji tohoto standartu byla pozornost zaměřena na co nejdokonalejší detekce poruch na síti, také analýza dat pro potřeby proaktivního managementu, ladění výkonnosti a plánování změn a v neposlední řadě dálkové monitorování segmentů a i přes Wide Area Network (WAN) spoje. Základní koncepcí tedy bylo vytvořit inteligentního agenta, který by uměl přijaté informace zpracovat a uložit pro další čtení. Tyto informace se ukládají na správcovské konzoly a měly by být k dispozici i historicky. RMON umožňuje sběr nejrůznějších statistik a údajů o Ethernet i Token Ring segmentech. Poté správce sítě má lepší možnosti, může se podívat na chybové informace a zjistit, kde má síť problémy a poté se ještě může podívat historicky na zatíženost určitého segmentu. Výhoda v historických statistikách je především v plánování a optimalizaci sítě. RMON standard definuje skupiny informací, které mohou být monitorovány síťovým analyzátorem nebo sondou, což je v případě SNMP agent. Řešení tohoto standardu je typické distribuované řešení, stejně jako klasický SNMP model má RMON také dvě části. První část tvoří agent a druhou správcovská aplikace, která běží na centrální konzole. Z této aplikace definujeme agentům jejich nastavení a tedy definice informací, které mají poskytovat. V síti může být mnoho agentů, většinou kolik má síť segmentů, tolik je potřeba agentů. Agenti sbírají statistické údaje a odlehčují tak práci managerům a v případě RMON aplikacím. Celkově tedy zatížení sítě je menší než u SNMP.

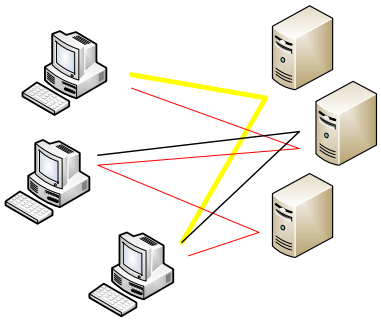
4.2. FILOSOFIE RMON

Vlastní filosofie RMON je výhodná v sítích, kde se prolínají topologie Ethernet a Token Ring. Ve standardu RMON byla databáze MIB rozšířena o 9 nových skupin.
1. Statistika informuje o statistikách týkajících se přenesených paketů a jejich velikosti, kolizí Ethernet, všesměrového vysílání z hlediska segmentu, portu nebo uživatele. 2. Historie dává přehled o historickém vývoji stejných údajů jako v bodu 1. Vzorkovací periodu může určit uživatel, délka testování a perioda je pochopitelně omezena kapacitou paměti Agenta. Někdy bývá rozdělena do 2 skupin nastavení parametrů a vlastní historická data. 3. Alarmy umožňuje uživateli nastavit maximální a minimální hodnoty sledovaných údajů, jejichž překročení je zaznamenáno a je na něj upozorněno, je-li podporována 9. skupina. 4. Hostitelé informuje o statistických údajích z hlediska jednotlivých síťových uzlů. 5. Top N hostitelů stejné informace jako v bodě 4 seřazené podle dosažených hodnot. Například 5 stanic s největším provozem. Obrázek ilustruje tuto situaci.



Obr. 4.1: Top N stanic s největším provozem

6. Matice provozu data o vzájemné komunikaci dvojic uzlů.



Obr. 4.2: Matice provozu, komunikace jednotlivých uzlů

7. Filtry umožňují nastavit omezení sledovaných paketů jen na ty, které uživatele zajímají. 8. Lovení paketů umožňuje zachytávat určité pakety a zapamatovat si je pro pozdější předání Manažeru. 9. Události umožňuje zasílat zprávy na uživatelskou konzoli. Také v případě RMON se záhy ukázalo, že by neškodila další rozšíření, takže byly brzy přidány i další skupiny. V současnosti je nejnovější verzí RMON 2, která umožňuje monitorovat sítě až do aplikační úrovně. Mezi nejznámější firmy, které jako první uvedly na trh RMON sondy, patřily firmy Armon Networking, Axon Networks a Frontier Software Development. Díky svým pokročilým řešením s nimi spolupracují i takový giganti jako Nortel Network,3Com a Cisco.

4.3. Přínosy standardu

Na základě výše uvedeného popisu jednotlivých skupin specifikace RMON si můžeme udělat představu, jaké velké množství údajů nám RMON agenti poskytují. Je jich opravdu hodně a tak máme-li management aplikaci a zařízení, podporující RMON

specifikaci, základní otázkou se pak stává správná interpretace získaných hodnot. Musíme nejenom vědět, co jednotlivé údaje znamenají, ale důležitá je i představa, jaké hodnoty jsou běžné a jaké jsou již kritické. Z toho pak vyplývají různé nastavení prahových hodnot alarmů.

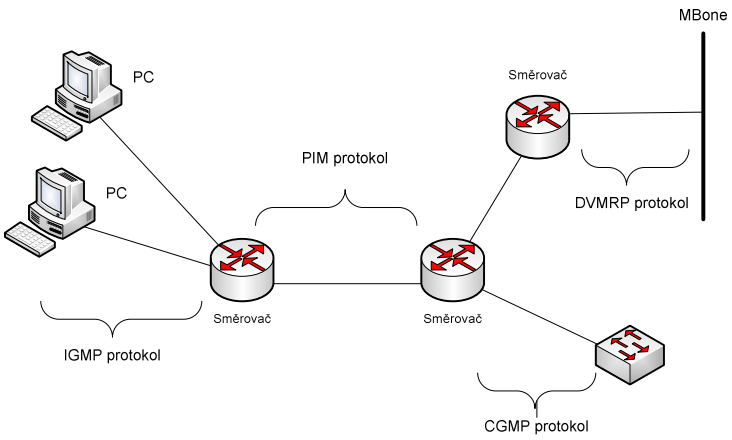
Přínosy jsou především schopnost spolupráce produktů různých výrobců. Díky standardizaci je většinou možné jednoduše integrovat agenty do většiny SNMP správních konzol, takže nejsme odkázáni na produkty jen jednoho výrobce. Dalším přínosem je výkonné monitorování a analýza. Aplikace jako jsou zachycení a analýza paketů, sledování trendů, statistika vzájemné komunikace mezi uzly a systém alarmů poskytují silné nástroje nejen na sledování podrobného aktuálního stavu naší sítě a proaktivní management systémem včasného varování při všech událostech, ale poskytují i podklady při plánování úprav sítě. Velkým přínosem je zatěžování komunikace, kde je RMON velice šetrný. Proto také můžeme spravovat takové zařízení i přes WAN spoje. Také rozšiřitelnost tohoto standardu je již veliká, jelikož byl navržen tak, že dovoluje snadné rozšiřování na LAN a WAN sítě.

5. MULTICAST V IP SÍTÍCH

Multicastové komunikace se používají zatím jen velmi zřídka, proto se jedná většinou jen o experimentální sítě. Multicast je poměrné nová technologie. Steve Deering je první, kdo se zmínil o multicastu ve své disertační práci. Tento typ komunikace se výborně hodí na přenosy, kdy jeden, či více zdrojů posílá stejná data velkému počtu příjemců. Základní myšlenka je jednoduchá. Ideální příklad je internetové vysílání televize či rozhlasu. Klient, který chce vysílání přijímat, se přihlásí do tzv. multicastové skupiny, která má přidělenou IP adresu s třídy D. Na základě členství v této skupině může požadovaná data přijímat. Zdroj dat však vysílá data jen jednou, o duplikaci a distribuci dat po síti se starají směrovače, které musí podporovat multicast. Nedochází tak ke zbytečnému zatěžování sítě. Je zapotřebí sledovat a monitorovat, zda směrovače neposílají data tam, kam nemají. Také je vhodné monitorovat, jak je síť zatížena, přehled multicastových klientů, kteří sdílejí multimediální přenos dat, také sledovat funkčnost protokolů, které jsou pro tuto komunikaci zvoleny, nejčastěji se jedná o protokol IGMP. Stinnou stránkou této technologie je nespolehlivý přenos dat pomocí UDP. Nutno podotknout, že nemáme možnost ztracené pakety znovu obnovit. U multimediálních přenosů tato ztráta paketů není velkým problémem, projeví se pouze zhoršenou kvalitou dat. [14]

5.1. SMĚROVACÍ PROTOKOLY PRO MULTICAST

Směrování v multicastové síti je velice neobvyklá záležitost, vzhledem k rozšíření multicastu. Byly vyvinuty speciální směrovací protokoly. S jejich názvy jste se již mohli setkat, popis samotných protokolů je nad rámec této práce. Je zde uveden, přehled několika z nich. Implementace protokolů pro multicast se může lišit na síťových prvcích různých firem, neboť některé protokoly jsou proprietární. Uvedené protokoly podporují směrovače Cisco a jejich grafické znázornění je na obrázku 5.1.



Obr. 5.1: Příklad použití multicast protokolů

• IGMP (Internet Group Management Protokol) - se využívá mezi klienty na LAN a směrovačem, umožňuje klientům přihlásit se do multicastové skupiny.
• PIM (Protocol Independent Multicast) – se využívá mezi směrovači k směrování multicastového provozu přes IP síť.
• DVMRP (Distance Vector Multicast Routing Protocol) – se využívá v MBone (multicast bacbone of internet). Tato experimentáln síť zatím nebyla uvedena. Na směrovačích Cisco lze nakonfigurovat směrování z PIM do DVMRP
• CGMP (Cisco Group Management Protocol) – se využívá na směrovačích připojených k přepínačům Catalyst, kde poskytuje podobné služby jako IGMP. [7]

5.2. PROTOCOL INDEPENDET MULTICAST (PIM)

PIM, je jak název napovídá, protokolově nezávislý. To je myšleno tak, že tento protokol využívá pro své potřeby unicastové směrovací tabulky směrovače a nezáleží na tom, jaký dynamický směrovací protokol tyto tabulky vytvořil. Protokol lze nakonfigurovat do 4 režimů. Dense mode, sparse mode, sparse-dense mode, bidirectional.

5.2.1. DENSE MODE (DM)

Označuje se většinou jako PIM-DM. Funkčnost protokolu v tomto módu je taková, že data se posílají do všech větví multicastového stromu, i když ve větvích není žádný zájemce o vysílání multicastu. Poté účastníci, kteří nepožadují toto vysílání, pošlou zprávu směrem ke kořenu stromu, aby odřezal tuto větev. Zabrání se tak zbytečnému zatěžování přenosového pásma. Tato zpráva se nazývá prune a je nutné je jí obnovovat, jelikož směrovače do těchto větví po určité době provoz obnoví. Pokud tomu je naopak a připojí se do stromu nový zájemce o vysílání, připojí se nová větev a směrovače odesílají opět požadovaná data. Tato zpráva se nazývá graft. Každý paket směrovač testuje mechanismem Reverse Path Forwarding (RPF), aby nedocházelo k nekonečným smyčkám. Dense modu je vhodný pro využití v rychlých lokálních sítích, kde je většina uživatelů členem nějaké multicastové skupiny, v jiném případě zbytečně zaplavuje síť nevyžádanými daty.

5.2.2. SPARSE MODE (SM)

Označuje se jako PIM-SM, pro distribuci dat využívá sdílený strom a tzv. pull model. V tomto modelu se data neposílají do žádné části sítě, která si o ně sama nezažádala. Pokud se připojí zájemce o data, pošle nadřazený směrovač zprávu o připojení ke kořenu. Tato zpráva se nazývá Join. Tím se sestaví nová větev a následně mohou být data směrována k zájemci. Zpráva Join má časově omezenou platnost, tudíž

musí být obnovována, jinak je přenos dat ukončen. Pokud již ve větvi není žádný člen, směrovač sám pošle do kořene zprávu graft a větev se odřízne. V tomto modelu se jedná o lepší rozložení zátěže na směrovačích. Protože PIM-SM využívá sdílený strom, je nutné, aby v síti byl nakonfigurován alespoň jeden RP, který je kořenem stromu a udržuje informace o skupinách a zdrojích. Všechny Join zprávy jsou směrovány právě k RP, který o požadavku informuje i zdroj dat. Data putují po sdíleném stromu, to znamená, že jdou nejdříve k RP a odtamtud jsou dále směrovány k příjemcům. Směrovače firmy Cisco, mají defaultně nastavený mechanismus, který umožňuje, v případě že je směrování dat přes RP neefektivní, vytvořit zdrojový strom a posílat data nejkratší cestou. Mechanismus funguje tak, že směrovače se dozvídají o zdrojích dat ze sdíleného stromu přijímáním dat přes RP. Když směrovač vyšle Join message ve tvaru (Zdroj - S, Skupina - G) směrem k RP, každý směrovač na cestě k RP zkontroluje svou unicastovou směrovací metriku RP s metrikou zdroje dat, pokud je metrika zdroje dat lepší, vybuduje nový zdrojový strom a přestane vysílat data přes strom sdílený. Výhodou oproti modelu dense je, že směrovače nemusí počítat pro každý zdroj nový strom. Pokud si představíme masový provoz pomocí sparse mode, je nutné předpokládat, že každý poskytovatel multimediálních služeb bude mít svůj vlastní RP, tím vzniká problém komunikace mezi RP. Spase mode se dobře přizpůsobuje v sítích větších rozměrů a nezatěžuje síť odesíláním nevyžádaných dat

5.2.3. Sparse-dense mode

Tento mod je pouze kombinací výše zmíněných, využívá se v sítích, kde se zároveň využívají jak klasické multicastové přenosy tak novější SSM. Protokol se sám přepne do modu jaký třeba pro přenos a to v závislosti na tom o jakou se jedná multicastovou skupinu. Pro jeho funkci musí být nakonfigurován RP

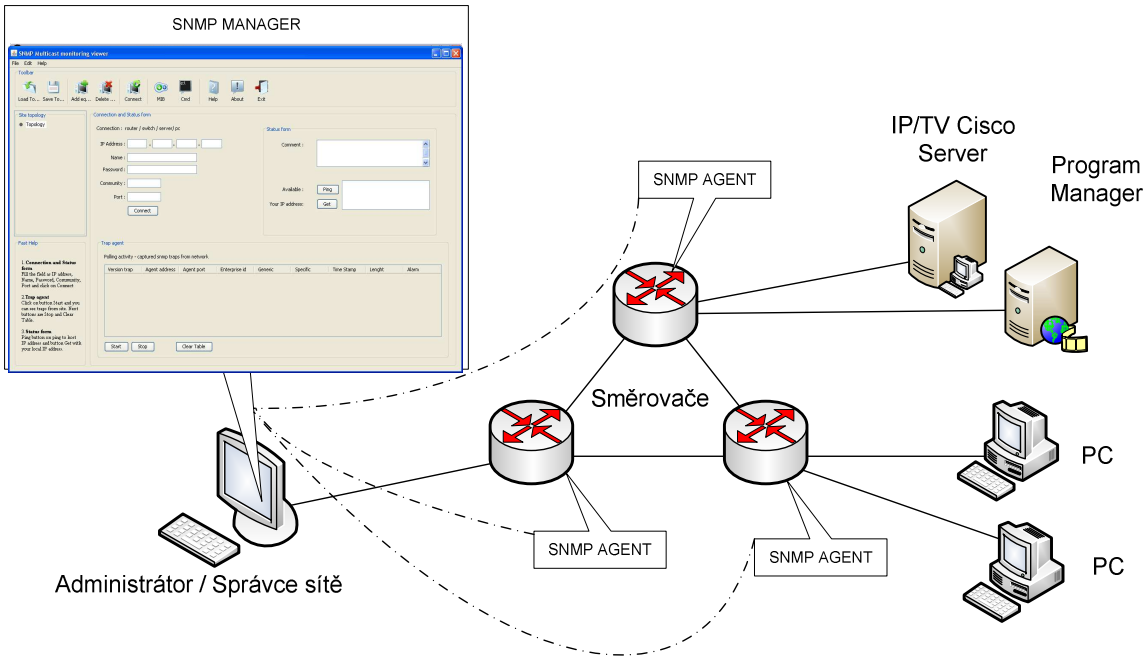
5.2.4. Bidirectional PIM

Tento protokol je rozšířením protokolu PIM, je navrženo pro podporu komunikace many-to-many v rámci jedné domény. Klasický sdílený strom je jednosměrný, to znamená, že na to aby mohla být data posílána k RP je vybudován zdrojový strom a teprve potom jsou data odeslána dolů do větví k příjemcům. Data ze zdroje nemohou být posílána sdíleným stromem směrem k RP. Pokud je tato možnost povolena, jedná se o dvousměrný sdílený strom, který využívá bidir-PIM.

5.3. Monitorování správcem sítě

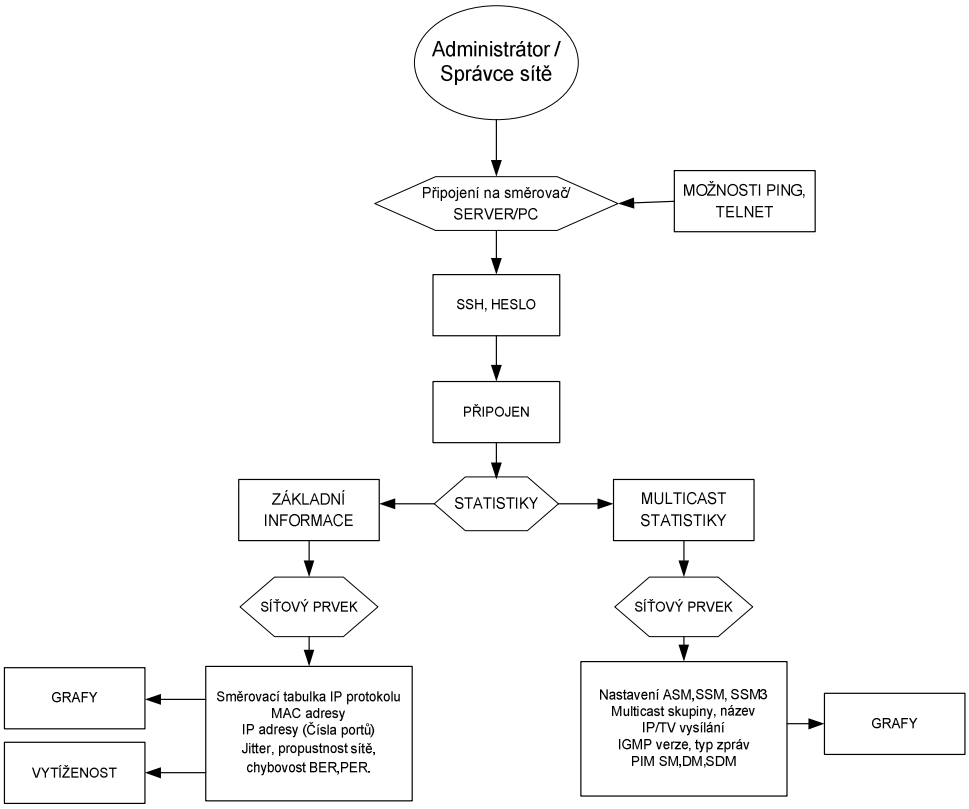
Na obrázku 5.2 je znázorněno monitorování sítě z pohledu správce sítě. Na monitorovací stanici je spuštěna aplikace, která zastává roli managera. IP/TV Cisco server a jeho Program manager jsou zde jenom pro ilustraci, abychom věděli, že po

počítačové síti bude generován multicast provoz a možnost sledovat multicastové relace.



Obr. 5.2: Monitorování sítě z pohledu správce sítě

Parametrů je celá řada. Důležité je především databáze MIB a podpora v zařízeních, na kterých chceme monitorovat dané parametry. V této práci se jedná především o menším přehledu těch nejdůležitějších. Na obrázku 5.3 jsou znázorněny postupně kroky, které správce sítě provádí, aby mohl zjistit požadovaný parametr. Správce sítě má možnost sledovat základní statistiky, ale také multicast statistiky.



Obr. 5.3 Přístup ke statistikám z pohledu správce sítě

5.3.1. MONITORING ZÁKLADNÍ INFORMACÍ

Každý správce sítě musí znát dobře celou topologii sítě, kterou spravuje. Pomocí dobrého programového vybavení je schopen monitorovat celou počítačovou síť, také i vzdáleně a usnadní si tak velice hledání případného problému. Základní informace o síti jsou nezbytnou součástí každého monitorovacího programu. Správce sítě by měl mít perfektní přehled o všech síťových komponentách dané sítě.

Základních informací o počítačové síti je celá řada, mezi nejznámější a důležité informace patří například jméno hosta, ip adresu, služby běžící na daném síťovém prvku, aktuální dobu od zapnutí prvku, nainstalovaný software a další. Spektrum základních informací je velice široké. K důležitým základním informacím je potřeba také znát nastavení daného síťového prvku, který je monitorován. Jedná se o nastavení ip adres na daných portech a také výpisy směrovacích tabulek. Ve směrovacích tabulkách lze nalézt například (čísla portů, na kterých probíhá komunikace, zdrojové a cílové ip adresy, masky sítí, jejich fyzické adresy, nastavení rychlostí na portech.

Pro správce sítě je nezbytné analyzovat také provoz na daném síťovém prvku a v dané počítačové síti. Do analýzy patří zpoždění přenosu paketů IP Packet Transfer Delay (IPTD), což je zpoždění dané časovým úsekem mezi dobou vyslání a dobou přijmutí paketu, poměr chybných paketů IP Packet Error Ratio (IPER) k počtu přenesených paketů ze zvolené množiny paketů, poměr ztracených paketů IP Packet Loss Ratio

(IPLR) k počtu přenášených paketů ze zvolené množiny paketů a dalších mnoho statistik přenosu dat.

5.3.2. Monitoring Multicast informací

Určité programy pro monitorování jsou mnohdy speciálně vyvíjeny, nejenom pro monitorování základních veličin, ale většinou pro monitorování dalších potřebných informací. Tyto speciální informace jsou například multicastové relace v ip sítích. S multicastovým zapojením sítě se setkáváme velice zřídka, většinou se jedná o experimentální sítě, ovšem je zapotřebí vyvíjet nástroje i pro tuto skupinu experimentálních sítí. V multicastových sítích můžeme sledovat také mnoho veličin.

Mezi základnější veličiny patří například sledování parametrů nastavení protokolů na daných síťových prvcích. Monitoring položek protokolu IGMP, který je základním pro multicastové relace. Sledované položky jsou například verze IGMP protokolu, příchozí multicastové pakety na dané rozhraní, zprávy po připojení do multicastové skupiny, také zprávy pro odpojení ze skupiny, výpisy do jaké skupiny daný účastník patří. Poté nastavení samotného multicastu, tedy monitoring protokolů PIM. Sledované položky jsou nastavení módu pro PIM protokol, doba trvání paketů pro PIM protokol a mnoho dalších nastavení protokolu PIM. Také sledování multicastové routovací tabulky je důležité, zde jsou položky jako příchozí, multicastové pakety, odchozí mulitcastové pakety, nastavený protokol a také další volitelné položky. V předchozí kapitole bylo pojednáno o analýze základních informací, zde je analýza velice podobná ovšem provádí se analýza multicastových relací.

6. EXPERIMENTÁLNÍ SÍŤ

6.1. POPIS EXPERIMENTÁLNÍ SÍTĚ

Pro ověření funkčnosti aplikace pro monitorování multicastových relací je potřeba využít experimentální síť s podporou multicastových technologií, která je vybudovaná v laboratoři. Prvky sítě jsou především směrovače s podporou multicastu a také snmp protokolu. Síť se také skládá Cisco Content Engine 566 v modu Program Manager, Cisco IP/TV server 3442 a IP/TV Viewer. IP/TV server zpracovává multimediální data, buď z karty na zachytávání videa, nebo z pevného disku. Data převede do formátu vhodného k přenosu a pomocí protokolu RTP jsou data vysílána na pokyn Program manageru přes multicastové směrovače k příjemcům. Příjemci, kteří chtějí přijímat data, musí být zaregistrovaní v multicastové skupině a mít nainstalovaný IP/TV Viewer, který přehrává distribuovaný obsah. Celý přenos řídí Program manager, ten má také funkci jako server, který přijímá, zpracovává a vyřizuje žádosti na vysílání. Přes jeho webové rozhraní se vytváří a spravují programy. Koncový uživatel při výběru programu komunikuje s Program managerem, který jeho požadavek obslouží a dá pokyn TV serveru vyslat data novému příjemci. Přihlášení do multicastových skupin probíhá přes TV viewer, bez vědomí uživatele. Příjemce předem neví, jaký TV server se stará o zasílání dat, což umožňuje v sítí využívat více TV serverů, aniž by uživatel musel předem znát jejich adresy. O vybrání a přiřazení vhodného TV serveru se stará opět Program manager. Takto funguje multicastové vysílání na experimentální síti a zajišťuje generování provozu. Tento provoz je důležitý především pro monitorování.

Další důležitou položkou je nastavení směrovačů. Každý směrovač je nadefinován podle adresního rozsahu, všechna rozhraní a také je na všech směrovačích zapnuta podpora protokolu snmp. Je důležité znát model klient-server, který již byl zmíněn v kapitole o snmp. Takto je realizována také experimentální síť v laboratoři. Kde klienti jsou směrovače a server je stanice, z které se dotazujeme na určité snmp dotazy. Ve vyvíjené aplikaci se administrátor připojí na daný směrovač, jehož IP adresu musí znát z topologie sítě a bude mít možnost monitorovat jak základní informace o síti pomocí snmp protokolu, tak také multicastové relace, například při sledování, určitého streamovaného videa či zvuku, uživatelem v experimentální síti. Dále je široké spektrum možností monitoringu pomocí snmp protokolu. Multicastové relace jsou probrány v předchozích kapitolách. Program by měl být přenositelný do většiny systémů s podporou Javy.

6.1.1. NASTAVENÍ SMĚROVAČŮ PRO MULTICAST

V základním nastavení multicastu, lze směrovače nastavit v několika módech s několika různými protokoly, které již byly uvedeny v předchozích kapitolách. Tyto základní nastavení směrovačů jsou například sparse mode s auto-RP, sparse mode s anycast RP, sparse mode s bootstrap router, sparse mode s single static RP, sparse mode s SSM a sparse mode s Bidirectional PIM. V experimentální síti je použit sparse mode s Source specific Multicast (SSM). Tento mód podporuje komunikaci od jednoho zdroje k několika příjemcům. Jedná se o velice rozvíjené a současně používané nastavení. Nastavuje se protokol PIM-SSM a také IGMP ve verzi 3. Odlišnosti od klasického nastavení jsou především v protokolu IGMP, který definuje INCLUDE mode. Základní nastavení je v tab. 6.1.

Tab. 6.1 – Základní nastavení směrovačů pro PIM-SSM

Krok	Příkaz (parametry)
1	Router> **enable**
Popis:	*Přepnutí do privilegovaného EXEC módu. Vyžadováno heslo pokud je nastaveno.*
2	Router# configure terminal
Popis:	*Přepnutí do konfiguračního režimu.*
3	Router(config)# **ip multicast-routing [distributed]**
Popis:	*Zapnutí multicastového směrování* • *Použití distibuted povoluji multicastové distribuované přepínání*
4	Router(config)# **ip pim ssm {default | range *access-list*}**
Popis:	*Konfigurace SSM:* • *Default – defunje SSM adresní rozsah IP access listů například 232/8.* • *Range – Specifikuje standartní IP access list*
5	Router(config)# **interface ethernet 1**
Popis:	*Výběr rozhraní pro konfiguraci*
6	Router(config-if)# **ip pim sparse-mode**
Popis:	*Zapnutí PIM protokolu na rozhraní ve sparse-módu.*
7	Opakovat kroky 1-6 pro každé rozhraní, na které bude užívat IP multicast.
8	Router(config-if)# **ip igmp version 3**
Popis:	*Zapnutí IGMPv3 na rozhraní, defaultně nastaveno IGMPv2. U verze 3 je je vyžadováno SSM.*
9	Opakovat krok 8 na všech rozhraních připojených k hostům.
10	Router(config-if)# **end**
Popis:	*Ukončení konfigurace.*

Tab. 6.2 – Ověření nastavení na směrovači

Krok	Příkaz (parametry)
1	**Router# show ip igmp groups {*group-name* | *group-address* | *interface-type interface-number*} [detail]**
Popis:	*Příkaz zobrazuje multicastové skupiny, které jsou přímo připojené na směrovač a které se připojily pomocí IGMP protokol. Možnost zadat jejich jméno adresu nebo také typ rozhraní pro detailnější informace.*
2	**Router# show ip mroute**
Popis:	*Zobrazí multicastovou směrovací tabulku. Tabulka zobrazuje zda je multicastová skupina nastavená na SSM nebo vypisuje hostitelské zprávy SSM.*

Pro zobrazení multicastových informací používáme několik základních příkazů, které používáme po připojení na směrovač. V navrhované aplikaci se používá protokol snmp a vypisování těchto údajů do tabulek více o této metodě v popisu aplikace.

Tab. 6.3 – Multicast mrinfo a mtrace příkazy na směrovačích

Krok	Příkaz (parametry)
1	**Router > enable [heslo]** **Router# mrinfo [host-name | host-address] [source-address | interface]** **Router# mrinfo** 147.229.151.250 [version 12.4] [flags: PMSA]: 147.229.151.250 -> 147.229.151.249 [1/0/pim/querier] 147.229.151.233 -> 147.229.151.234 [1/0/pim] 147.229.151.241 -> 147.229.151.242 [1/0/pim]
Popis:	*Příklad pro zobrazení sousedících multicastových směrovačů.*
2	**Router# mtrace {source-name | source-address} [destination-name | destination-address] via [group-name | group-address]** **Router2# mtrace 10.10.3.5 147.229.151.150 via 224.0.1.40** Type escape sequence to abort. Mtrace from 10.10.3.5 to 147.229.151.150 via group 224.0.1.40 From source (?) to destination (UC-249-10.utko.feec.vutbr.cz) Querying full reverse path... 0 UC-249-10.utko.feec.vutbr.cz (147.229.151.150) -1 147.229.151.249 PIM [10.10.3.0/24] -2 147.229.151.250 PIM [10.10.3.0/24] -3 147.229.151.242 PIM [10.10.3.0/24]
Popis:	*Příklad pro zobrazení cesty od zdroje k cíli multicastovým stromem.*

Tab. 6.4 – Multicast příkazy pro výpisy informací na směrovačích

Krok	Příkaz (parametry)
1	**Router# show ip mroute** IP Multicast Routing Table Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected, L - Local, P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement, U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel, z - MDT-data group sender, Y - Joined MDT-data group, y - Sending to MDT-data group Outgoing interface flags: H - Hardware switched, A - Assert winner Timers: Uptime/Expires Interface state: Interface, Next-Hop or VCD, State/Mode (*, 239.255.255.255), 00:17:36/00:02:38, RP 147.229.151.250, flags: S Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: FastEthernet0, Forward/Sparse, 00:17:36/00:02:38 (147.229.151.227, 239.255.255.255), 00:02:42/00:01:09, flags: PT Incoming interface: FastEthernet0, RPF nbr 147.229.151.249 Outgoing interface list: Null (*, 239.255.255.250), 00:18:30/00:02:43, RP 147.229.151.250, flags: S Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: Vlan1, Forward/Sparse, 00:18:30/00:02:43 (*, 224.2.127.254), 00:17:36/00:02:36, RP 147.229.151.250, flags: S Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: FastEthernet0, Forward/Sparse, 00:17:36/00:02:36 --More--
Popis:	*Výpis ze směrovače S3.*
2	**Router# show ip pim interface FastEthernet1/0** Address Interface Ver/ Mode Nbr/ Count Query/ Intvl DR/ Prior DR 147.229.151.250 FastEthernet0 v2/S 1 30 1
Popis:	*Výpis protokolu PIM na rozhraní FastEthernet1/0*
3	**Router# show ip mcache** IP Multicast Fast-Switching Cache (147.229.151.227/32, 239.255.255.255), FastEthernet0, Last used: never, Semi-fast (147.229.151.227/32, 224.2.127.254), FastEthernet0, Last used: never, Semi-fast (147.229.151.233/32, 224.3.8.8), FastEthernet1, Last used: never, MinMTU: 1500 FastEthernet0 MAC Header: 01005E0308080018B9E33DC00800

	(147.229.151.241/32, 224.3.8.8), Vlan1, Last used: never, MinMTU: 1500 FastEthernet0 MAC Header: 01005E0308080018B9E33DC00800 (*, 232.3.10.11), Null, Last used: never, Semi-fast (147.229.151.226/32, 232.3.10.11), FastEthernet0, Last used: 00:00:00, MinMTU: 1500 Vlan1 MAC Header: 01005E030A0B0018B9E33DC00800 (*, 232.3.10.10), Null, Last used: never, Semi-fast (147.229.151.226/32, 232.3.10.10), FastEthernet0, Last used: 00:00:00, MinMTU: 1500 Vlan1 MAC Header: 01005E030A0A0018B9E33DC00800
Popis:	*Příklad výpisu ze směrovače, při nastavené multicastové distribuci (MDS).*
4	**Router# show ip pim rp mapping** PIM Group-to-RP Mappings This system is a candidate RP (v2) Group(s) 224.0.0.0/4 RP 147.229.151.250 (?), v2 Info source: 147.229.151.249 (?), via bootstrap, priority 0, holdtime 150 Uptime: 14:39:49, expires: 00:02:13 Group(s) 224.3.0.0/16 RP 147.229.151.249 (?), v2 Info source: 147.229.151.249 (?), via bootstrap, priority 0, holdtime 150 Uptime: 14:40:20, expires: 00:02:14
Popis:	*Příklady výpisu mapování multicastových skupin a jejich parametry.*
5	**Router# show ip rpf 10.10.3.5** RPF information for ? (10.10.3.5) RPF interface: Vlan1 RPF neighbor: ? (147.229.151.242) RPF route/mask: 10.10.3.0/24 RPF type: unicast (rip) RPF recursion count: 0 Doing distance-preferred lookups across tables
Popis:	*Příkaz vypisuje informace získané z rpf o adrese 10.10.3.5.*

6.1.2. NASTAVENÍ TRAP ZPRÁV NA SMĚROVAČÍCH

Jak již bylo uvedeno SNMP protokol obsahuje zprávy, které jsou automaticky odesílány z daného zařízení. Zprávy jsou odesílány při změně některé kontrolované hodnoty. Pro sledování sítě jsou tyto zprávy velice užitečný nástroj, administrátor

ihned nalezne, na jakém prvku se změnila určitá hodnota. Základní nastavení a příklad použití trap zpráv je v tab. 6.5 a v tab. 6.6.

Tab. 6.5 – Nastavení trap zprav snmp s PIM

Krok	Příkaz (parametry)
1	**Router(config)# snmp-server enable traps pim [neighbor-change | rp-mapping-change | invalid-pim-message]**
Popis:	*Zapnutí odesílání zpráv pim.* • *neighbor-change - nastavení odesílání zpráv ze směrovače, při změně rozhraní na zapnuto nebo vypnuto.* • *rp-mapping-change – odesílání zpráv při změně nastavení RP, ovšem jeli aktivován jeden z módů pro RP, nikoliv SSM.* • *invalid-pim-message – zprávy při špatných PIM operacích. Při příjmu join a prune zpráv se špatnou adresou zdroje například.*
2	**Router(config)# snmp-server host *host-addr* [traps | informs] *community-string* pim**
Popis:	*Specifikuje příjemce zpráv PIM s community string buď public nebo private.*
3	**Router# show running-config**
Popis:	*Kontrola nastavení pomocí výpisu na směrovači.*

Tab. 6.6 – Příklad nastavení trap zpráv s PIM

Krok	Příkaz (parametry)
1	**router(config)# snmp-server host 10.10.3.5 traps version 2 public pim**
Popis:	*Nastavení PIM trap zpráv posílaných přes SNMPv2 na zařízení s ip adresou 10.10.3.5.*
2	**router(config)# snmp-server enable traps pim neighbor-change**
Popis:	*Nastavení odesílání zpráv o změně PIM nastavení.*
3	**router(config)# interface ethernet0/0** **router(config-if)# ip pim sparse-dense-mode**
Popis:	*Zapnutí sparse-dense módu na rozhraní Ethernet 0/0.*

Důležité je specifikovat trap zprávy SNMP pro zařízení na které mají být odesílány. Nastavení SNMP trap zpráv na zařízení je v tab. 6.7.

Tab. 6.7 – Popis parametrů nastavení trap snmp zpráv

Krok	Příkaz (parametry)
1	**snmp-server host *host-addr* [traps | informs] [version {1 | 2 | 3 [auth | noauth | priv]}]** ***community-string*** **[udp-port *port*] [*notification-type*]**

Popis:	*Zapnutí odesílání zpráv pim.* • *Traps – defaultně nastaveno, posílání trap zpráv* • *Informs – posílání dalších informačních zpráv.* • *Version – Verze SNMP protokolu k odeslání trap zpráv. Verze 3 je bezpečný mod s použitím hesla.* o *1—SNMPv1 – Verze 1 není podporováná u inform zpráv.* o *2c – SNMPv2* o *3 - SNMPv3 – Zabezpečený mod pro posílání trap zpráv. (auth – zapnutí Message Digiest (MD5), no auth – defaultně, priv – zapnutí Data Encryption Standard(DES)* • *Udp-port – port příjemce defaultně 162.* • *Notification – type – odesílání různých položek, které lze sledovat.*
2	**no snmp-server host *host-addr* [traps | informs]**
Popis:	*Vypnutí snmp trap zpráv.*

6.1.3. OBJEKTY MIB DATABÁZE NA SMĚROVAČÍCH

Velice důležité je nastavení SNMP protokolu na směrovačích. Jak již bylo popsáno v předchozích kapitolách směrovače obsahují MIB tabulku s objekty OID, které nesou mnoho informací o stavu daného zařízení. Tato MIB tabulka z objekty, je hierarchicky členěná a administrátor si díky přístupu pomocí protokolu SNMP, zjistí daný objekt OID a k němu již přistupuje pomocí daného softwarového nástroje. Tabulka obsahuje základní objekty definované IETF organizací. Rozšířené objekty jsou Cisco IOS-Specific MIBs, které jsou pro multicatové informace. Přehled některých multicastových informací z této MIB tabulky jsou uvedeny v tab. 6.8.

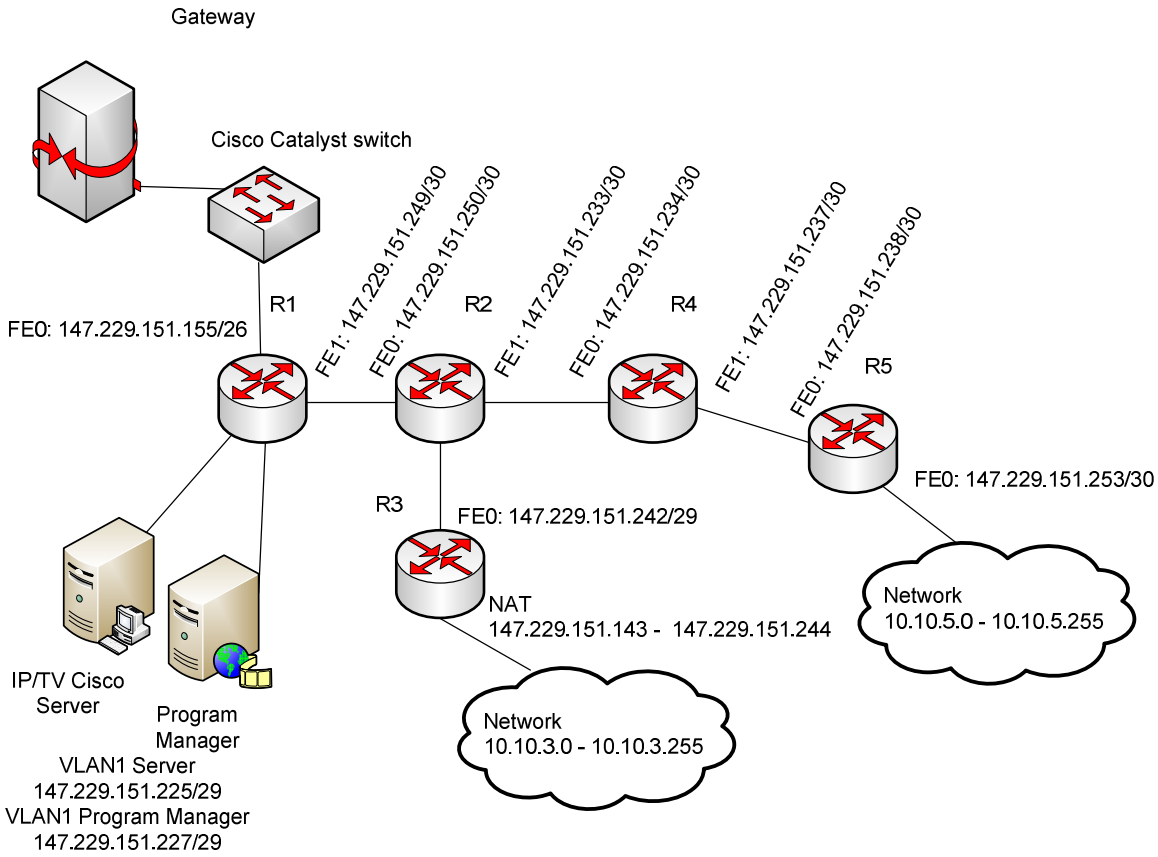
Tab. 6.8 – OID objekty v MIB tabulce

Jméno trap zprávy a OID číslo v MIB	Popis
pimNeighborLoss 1.3.6.1.3.61.1.3.1.2.1	*Trap signalizuje ztrátu sousedství se sousedícím připojeným zařízením. Trap zpráva je generovaná, pokud sousedícímu vyprší časový interval a směrovač nemá ostatní sousedící na stejném rozhraní s nižší IP adresou než svojí.*
ciscoPimInterfaceUp 1.3.6.1.4.1.9.9.184.2.0.1	*Trap signalizuje obnovení PIM protokolu na rozhraní. Generuje se, když se změní stav na aktivní. Identifikuje také rozhraní, které se zapojí do směrovače.*
ciscoPimInterfaceDown 1.3.6.1.4.1.9.9.184.2.0.2	*Trap signalizuje ztrátu PIM na rozhraní. Tento trap je generován při vymazaní této hodnoty z v MIB tabulce, položka PimInterfaceTable.*
ciscoPimRPMappingChange 1.3.6.1.4.1.9.9.184.2.0.3	*Tento trap indetifikuje změnu mapování RP. Pokud se změní RP mapování nebo je přidán nový RP, vymazaná cache tabulka s RP nebo je v ní změna, generuje se tento trap. Typ změny je definován položkou pimRPMappingChangeType. V případě, že se změní existující hodnota na jiný typ přepíše se položka*

	modifiedOldMapping a následně po změně je nastaveno modifiedNewMapping. Nastavování RP mapování by mělo být kompromisem.
ciscoPimInvalidJoinPrune 1.3.6.1.4.1.9.9.184.2.0.5	*Trap zpráva, která identifikuje o špatné join nebo prune zprávě, která je posílaná po multicastové síti.*

6.2. Adresní rozsah

Pro experimentální síť byl vyhrazen adresový prostor 147.229.151.224/27, což odpovídá 32 IP adresám. Vzhledem k tomu, že se síť skládá z 5 směrovačů a 2 serverů, bylo nutné tento prostor dále rozdělit na menší podsítě. Všechna zařízení jsou umístěna v místnosti PA-249 v budově Purkyňova 118 a jsou připojeny do universitní počítačové sítě a internetu. Adresní schéma je znázorněné v tab. 6.10.



Obr. 6.9: Fyzické zapojení sítě

U každého síťového prvku je zobrazena jeho IP adresa a rozhraní ke kterému patří. Na směrovačích tři a pět je nakonfigurován překlad adres Network Address Translation (NAT). Tento překlad adres je zde nastaven z důvodu nedostatku volných IP adres. Každá privátní síť umožňuje připojit 254 systémů. Pro přístup do internetu se jejich požadavky překládají na veřejné IP adresy. V tabulce jsou znázorněny všechny důležité informace o rozdělení IP adres.

Tab 6.10 - Adresní rozsah experimentální sítě

Podsíť č.	Adresa podsítě	Rozsah	Všesměrová adresa	Síť/prefix
1	147.229.151.224	.225-230	.231	**147.229.151.224/29**
2	147.229.151.232	.233-234	.236	**147.229.151.232/30**
3	147.229.151.236	.237-238	.239	**147.229.151.236/30**
4	147.229.151.240	.241-246	.247	**147.229.151.240/29**
5	147.229.151.248	.249-250	.251	**147.229.151.248/30**
6	147.229.151.252	.253-254	.255	**147.229.151.252/30**

IP/TV server a Program manager je připojen do směrovače S1, který zároveň připojuje experimentální síť do sítě univerzitní přes bránu s IP adresou 147.229.151.129. Připojení do univerzitní sítě nám umožňuje rozšířit rozsah multicastového vysílání do celé učebny PA-249, což rozšíří i možnosti další analýzy sítě do budoucna. Technicky je tato experimentální síť schopna rozšířit vysílání do dalších učeben, ale provoz by musel být povolen správci universitní sítě, neboť v současné době je blokován firewally. Pro účely vyvíjené aplikace nebylo toto rozšíření využito.

7. APLIKACE PRO MONITOROVÁNÍ MULTICASTOVÝCH RELACÍ V IP SÍTÍCH

7.1. ÚVOD DO APLIKACE

Aplikace SNMP Multicast monitoring viewer slouží k monitorování experimentálních sítí a také jako síťový analyzátor. Aplikace byla navrhnutá v jazyce Java a je použitelná téměř na všech platformách s podporou javy. Důvod navrhování aplikace v tomto programovacím jazyce je především dobrá podpora síťových protokolů. Také již zmiňovaná přenositelnost aplikace na více platforem. Hlavní nasazení aplikace je především kvůli monitorování mutlicastových relací a monitorování provozu v řešení IP/TV v experimentální síti na Ústavu Telekomunikací v laboratoři č. 249 v Brně. Výstupem z aplikace jsou informace ze síťových zařízení přehledně graficky zpracovány do tabulek a také zpracování některých informací v podobě grafů.

SNMP Multicast monitoring viewer, lze modifikovat a také nasadit v současných počítačových sítích. Velkou předností aplikace je snadná manipulace a rychlé zjištění stavu počítačové sítě s pohledu správce sítě. Oproti jiným aplikacím je SNMP Multicast monitoring viewer velice přehledný díky grafickému rozhraní GUI (Graphical User Interface), které je velice intuitivní a pro uživatele přívětivé. V oblasti softwaru sledování sítí je obrovský rozmach a to především díky použití snmp protokolu a díky podpoře výrobců síťových prvků, kteří tento protokol implementují. Hlavní podstatou aplikace je připojení na síťové zařízení a snadné získání informací, které jsou nezbytné pro každého správce sítě. Aplikace je také schopná nezabezpečeně monitorovat síť a odchytávat alarmy z daných síťových prvků na kterých jsou nastaveny.

Důvody k nasazení aplikace jsou tedy především analýza provozů síťových zařízení, analýza problémů v počítačové síti a bezpečné získávání informací ze síťových zařízení.

Shrnutí výhod aplikace SNMP Monitoring viewer :

- Aplikace je schopná pracovat na více platformách díky podpoře JAVA.
- Snadná manipulace s programem díky GUI
- Monitoring základních informací o síťových prvcích počítačové sítě
- Monitoring multicastových informací o síťových prvcích počítačové sítě
- Zobrazování některých výsledků pomocí grafů
- MIB browser pro získání vlastního OID

7.2. POŽADAVKY NA PC A POČÍTAČOVOU SÍŤ

Aplikace je snadno spustitelná na všech platformách s podporou javy. Nároky na pc jsou minimální, jelikož je program tvořen na bázi posílání snmp zpráv na síťové zařízení typu požadavek – odpověď. Aplikace tedy nijak významně nezatěžuje procesor. Nároky jsou především na počítačovou síť. Aplikace pracuje již po připojení k téměř každému síťovému zařízení s podporou snmp protokolu. Všechny možnosti aplikace fungují po připojení do větší sítě s podporou multicastu. V této větší síti by měl být provoz videa či rozhlasu, tedy IP/TV a podpora protokolu PIM a IGMP, pomocí nichž se monitoruje většina multicastových relací.

7.3. GRAFICKÝ NÁVRH PROGRAMU A STRUČNÝ POPIS

Grafický návrh aplikace byl pečlivě sestavován tak, aby zaujal na první pohled svojí jednoduchostí a přehledností. Skládá se s mnoha grafických komponent a formulářů, které usnadňují práci s danými veličinami.

SNMP Multicast monitoring viewer obsahuje mnoho formulářů. První z těchto formulářů je přihlášení do aplikace (Login to aplication), který slouží k přihlášení do další části aplikace. Je zobrazen na obr. 7.1. Obsahuje položky jméno k přihlášení (Login) a heslo pro vstup do aplikace (Password).

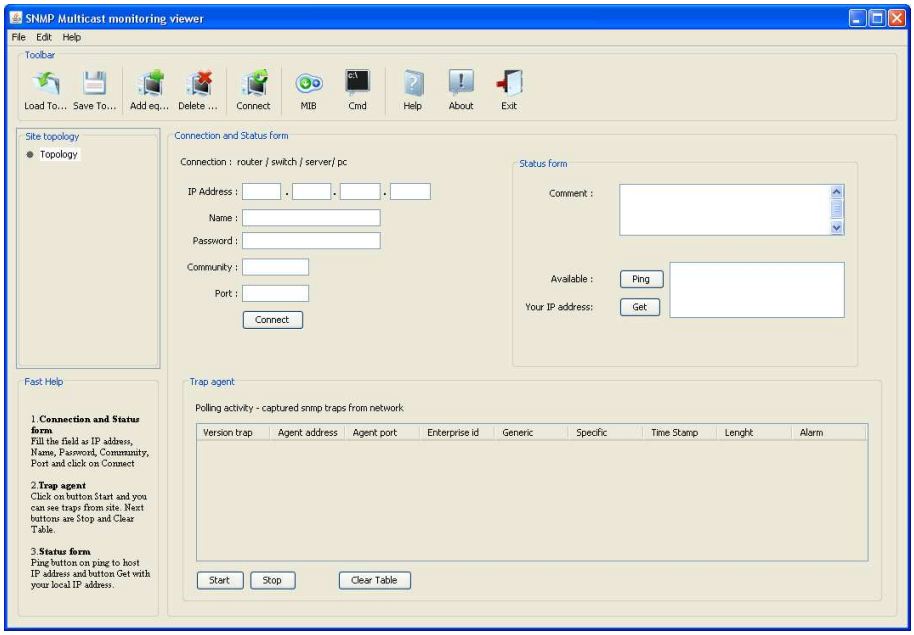
Obr. 7.1 – Login okno

Po potvrzení zadaných údajů se zobrazí hlavní okno aplikace, které má mnoho částí. Je zobrazeno na obr. 7.2. V horní části aplikace je nástrojová lišta (Toolbar) s tlačítky pro ovládání, která bude popsaná v dalších kapitolách. V levé části aplikace je stromová struktura topologie (Topology). Pod stromovou strukturou sítě je rychlý návod (Fast Help), pro snadnější orientaci ihned po prvním spuštění. Pravá část programu pro připojení (Connection and Status form) se opět skládá z několika dalších částí. Jsou zde položky pro vyplnění daných veličin. Adresa zařízení, na kterou se aplikace má připojit a z které budou získávány informace (IP address), jméno daného zařízení (Name) a heslo pro přístup k tomuto zařízení (Password), které by mělo být

využito ve vyšší verzi aplikace do budoucna. Další položka je skupina (Community), slouží pro SNMP protokol. Položka (Port) slouží pro další potřeby protokolu SNMP. Poslední položkou v tomto formuláři je potvrzovací tlačítko pro připojení na dané síťové zařízení (Connect).

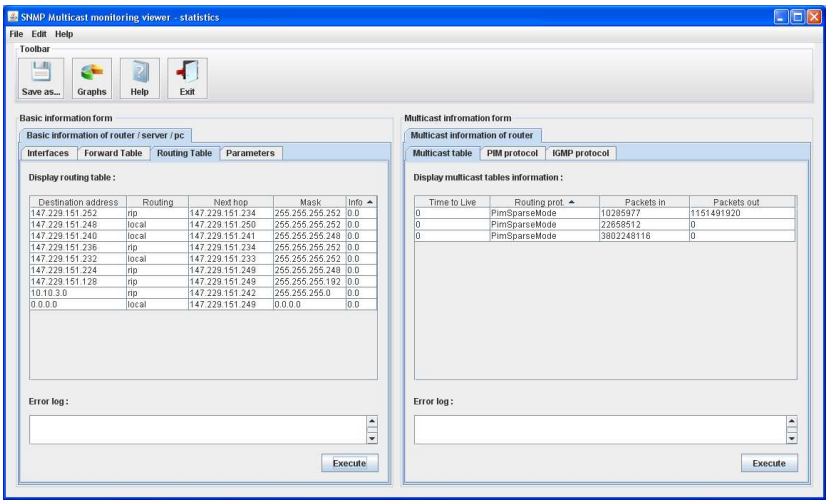
Formulář pro status (Status form), kde si uživatel může ověřit například dostupnost dané IP adresy. Tento formulář obsahuje položku komentáře k danému síťovému prvku nadefinované při zadávání topologie sítě (Comment), poté dostupnost pomocí programu ping (Availaible) a zjištění vlastní IP adresy (Your IP address).

Posledním formulářem je agent pro sledování trap zpráv (Trap agent) z počítačové sítě, k níž je aplikace připojena. V tabulce je poté následně zachytávaná komunikace. Toto zachytávání lze zapnout a také vypnout tlačítky.



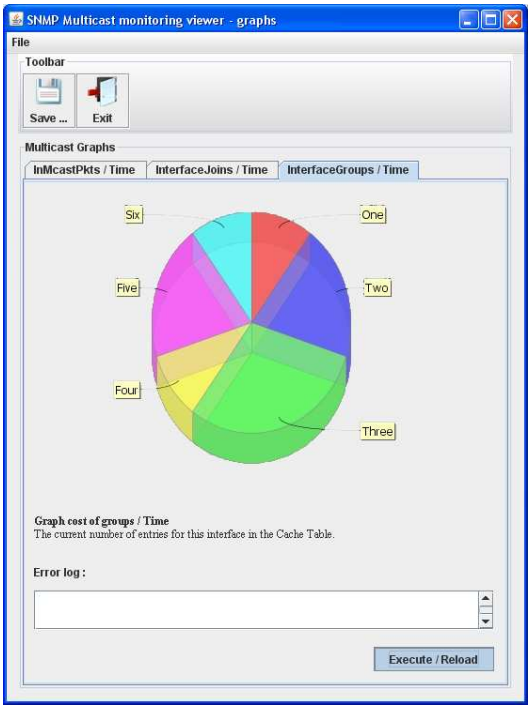
Obr. 7.2 – Hlavní okno aplikace

Okno pro monitorování statistik, které se zobrazí, po úspěšném připojení je zobrazeno na obr. 7.3. Také obsahuje nástrojovou lištu (Toolbar). V levé části formuláře, jsou záložky se základními statistikami a informacemi daného síťového zařízení (Basic information form). Další záložky v tomto panelu budou podrobněji popsány v části o funkčnosti tohoto formuláře. V pravé části programu jsou záložky s již zmíněnými multicast informacemi (Multicast information form), také budou popsány v jedné z následujících kapitol o funkčnosti formuláře.



Obr. 7.3 – Okno pro sledování statistik

Převážná většina monitorovacích aplikací zpracovává výsledky do uživatelsky vhodné podoby pro snadnou orientaci z pohledu správce sítě. Také v této aplikaci jsou přehledně všechny statistiky vypsány. Ovšem je zde také možnost monitorování některých statistik a zobrazení do grafů. Grafy jsou pro multicastové informace. V jednotlivých záložkách je krátký popis daného grafu. Okno pro grafy je na obr. 7.4.

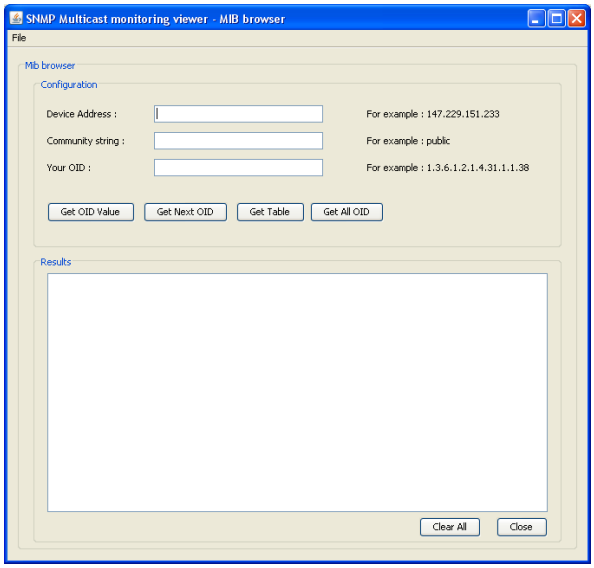


Obr. 7.4 – Okno pro vykreslování grafů

Další částí aplikace je okno MIB browser. Jedná se o okno, ve kterém lze nalézt, své OID číslo a zjistit tak informaci z daného síťového zařízení. MIB browser je znázorněn na obr. 7.5. MIB browser se skládá ze dvou částí, první z nich je konfigurace (Configuration) a druhou částí jsou výsledky (Results).

V první části se definuje adresa zařízení, z kterého se budou vypisovat informace (Device Address), poté položka skupina (Community string), zde se volí buď public pro veřejnou skupinu a zprávy SNMP protokolu, a nebo private pro privátní sledované položky. V neposlední řadě je zde číslo OID (Your OID), pro přístup k dané položce v MIB tabulce. Také je zde několik tlačítek. První z nich je tlačítko pro získání jedné dané hodnoty (Get OID Value), kterou uživatel zadá. Další tlačítko je pro získání další hodnoty dalšího prvku v pořadí v hierarchické struktuře MIB databáze, pomocí snmp zpráv get next, které již byly popsány v přechozích kapitolách. Třetí tlačítko zobrazí celou MIB tabulku pod daným OID (Get Table). Poslední tlačítko vypíše všechny hodnoty z MIB pod daným OID, vypíše všechny hodnoty.

V druhé části, je okno pro vypisování výsledků, kde se zobrazí hodnoty ze síťového zařízení v případě úspěšného vypsání a nebo se zobrazí chybové hlášení.



Obr. 7.5 – MIB browser

7.4. Popis nástrojové lišty (Toolbar)

7.4.1. Nástrojové lišty

Hlavni okno aplikace obsahuje nástrojovou lištu zobrazenou na obr. 8.6. skládá se z mnoha standardních tlačítek, ale také další tlačítka pro funkce této aplikace, tlačítka jsou doplněná o obrázky pro snadnou orientaci. Nástrojová lišta je velice intuitivní a přehledná. Také v okně monitorovaní statistik na obr. 7.7. je obsažena nástrojová lišta. Některé tlačítka jsou stejná jako v předchozím případě. Každé tlačítko má svůj popis. Obě nástrojové lišty jsou vyjímatelné z okna, uchopením na levé straně a uživatel je schopen si přizpůsobit vzhled aplikace podle jeho potřeb.

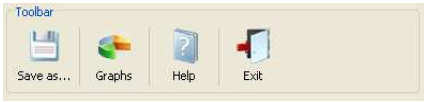
Nástrojová lišta v hlavním okně je rozdělena na 5 částí. V první části jsou tlačítka pro načtení topologie počítačové sítě (Load Topology), které vyvolá formulář

pro načtení souboru a druhé tlačítko pro uložení uživatelem nadefinované topologie (Save Topology). Topologii počítačové sítě je zapotřebí po vytvoření uložit. Další tlačítka jsou pro nadefinování topologie. Přidávání prvků topologie (Add equipment), po stisku tlačítka se objeví formulář, pro zadávání síťového zařízení. Tlačítko odstranit síťové zařízení (Delete equipment), zobrazí další formulář na odstranění daného síťového zařízení.

Obr. 7.6 – Nástrojová lišta pro hlavní okno

Tlačítko pro připojení (Connect), kterým se připojíme na dané síťové zařízení, pokud je ovšem síťové zařízení dostupné a zobrazí se okno pro sledování statistik. V další části nástrojové lišty jsou tlačítka pro externí nadstavbu programu. Tlačítko MIB. Po stisku tohoto tlačítka se zobrazí MIB browser. V této části je i tlačítko pro vyvolání příkazové řádky (Cmd), kde si může uživatel zadávat klasické příkazy. Poslední část jsou tlačítko nápovědy (Help), o programu (About) a v neposlední řadě tlačítko pro ukončení programu (Exit).

Nástrojová lišta v okně statistik obsahuje pouze 4 tlačítka. Tlačítko pro uložení načtených dat (Save as). Další tlačítko pro zobrazení grafů (Graphs), které otevře okno pro grafy. Také jsou zde tlačítka nápovědy (Help) a také ukončení tohoto okna (Exit). Do budoucna bude tato lišta rozšířena o několik dalších tlačítek.



Obr. 7.7 – Nástrojová lišta okno sledování statistik

7.4.2. Funkční tlačítka – menu

Položky menu jsou v každém okně aplikace jiné, v následujících tabulkách je shrnut popis všech tlačítek a jejich klávesové zkratky. V tabulce 7.8 jsou uvedeny položky menu z hlavního okna.

Tab. 7.8 – Funkční tlačítka pro hlavní okno

Hlavní okno Položka menu	Volby	Klávesová zkratka	Popis
File			
	Load topology	Shift + O	*Načtení topologie*
	Save topology	Shift + S	*Uložení topologie*
	Add equipment	Shift + A	*Přidání síťového zařízení*
	Delete equipment	Shift + D	*Vymazání síťového zařízení*

	Restart equipment	Alt + Shift + R	*Restart zařízení*
	Exit	Shift + Q	*Ukončení programu*
Edit			
	Connect	Ctrl + Shift + C	*Připojení na síťového zařízení*
	Mib	Shift + M	*Otevření MIB browseru*
	Command line	Shift + L	*Otevření příkazové řádky*
Help			
	Help	F1	*Nápověda*
	About	F2	*O programu*

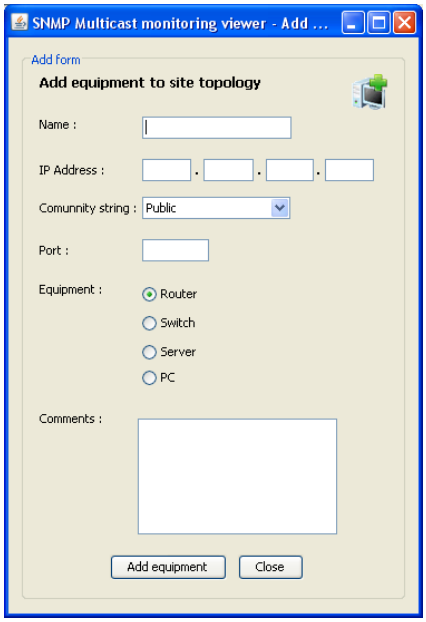
V další tabulce tab. 7.9 jsou uvedeny položky menu z okna sledování statistik.

Tab. 7.9 – Funkční tlačítka pro okno sledování statistik

Okno sledování statistik			
Položka Menu	Volby	Klávesová zkratka	Popis
File			
	Save as	Ctrl + Shift + S	*Uložení statistik*
	Exit	Ctrl + Shift + Q	*Ukončení okna*
Edit			
	Graphs	Ctrl + Shift + G	*Otevření okna pro grafy*
Help			
	Help	F1	*Nápověda*

7.4.3. Formulář pro přidání síťového zařízení

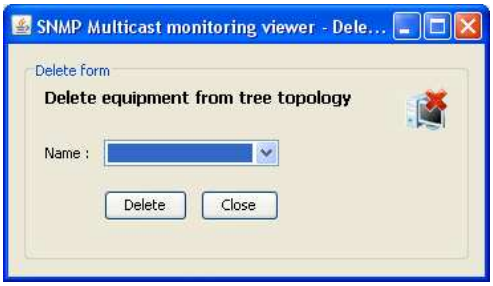
Pro přidávání síťového zařízení se objeví nový formulář. Obsahuje položky pro přidávání jména síťového zařízení (Name), ip adresu (IP address), pro určení skupiny u snmp protokolu (Community string), dále potom port pro další využití protokolu SNMP, pro určení druhu zařízení je zde položka (Equipment) a pro komentář k síťovému zařízení položka (Comments). Formulář je zobrazen na obr. 7.10.



Obr. 7.10 – Formulář pro přidání síťového zařízení

7.4.4. Formulář pro mazání síťového zařízení

Další formulář je také pro práci s topologií sítě, kterou si uživatel definuje. Tento formulář slouží pro mazání síťových zařízení. Formulář je zobrazen na obr. 7.11.



Obr. 7.11 – Formulář pro odstranění síťového zařízení

7.4.5. Formulář informací o programu

Informace o programu, autor a verze programu jsou zobrazeny na obr. 7.12.

Obr. 7.12 – Formulář s informacemi o programu

7.5. FUNKCE APLIKACE

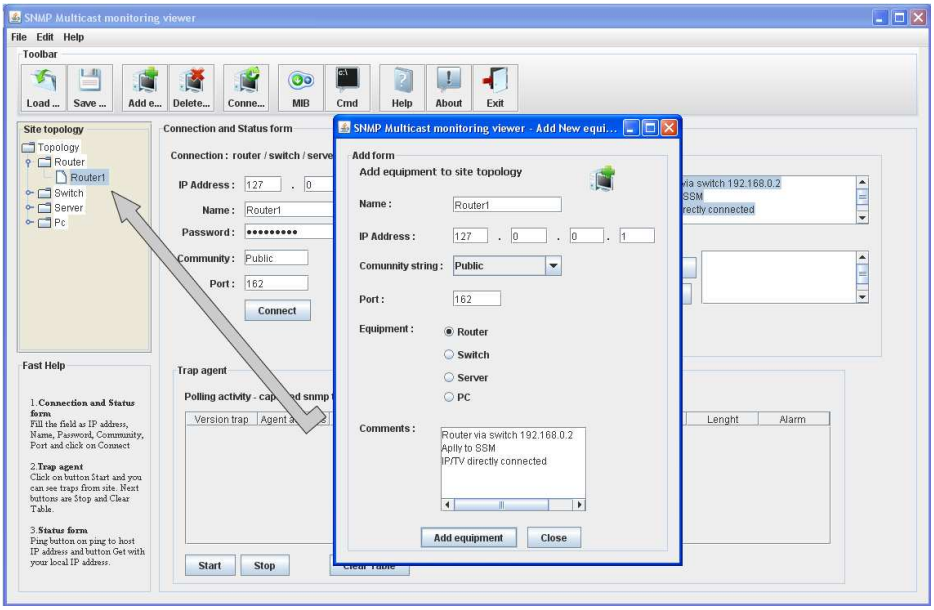
Popis funkce aplikace je rozdělena do tří podkategorií, pro podrobnější vysvětlení. V každé podkategorii jsou názorné příklady práce s daným formulářovým oknem a výstupy z dané části aplikace.

Stručný popis chování celé aplikace. Po spuštění se zobrazí hlavní okno, kde se definuje topologie počítačové sítě, s možností topologii uložit či načíst ze souboru. Zobrazení doplňkových informací je také obsaženo v hlavním okně aplikace. Aktuální změny v počítačové síti, lze monitorovat pomocí SNMP trap zpráv, které v hlavním okně přijímá Trap Agent. Po připojení na síťové zařízení se zobrazí okno sledování statistik, kde je několik druhů statistik, jak základní informace ze zařízení, tak multicastové informace a následná možnost uložení výsledků. Další volbou je vyvolání okna pro grafy. Aplikace je schopna zobrazit různé průběhy gráfů.

7.5.1. FUNKCE HLAVNÍHO OKNA

V první části aplikace je základním krokem nadefinovat vlastní topologii sítě. Správce sítě zná topologii sítě a také ip adresy síťových zařízení ty jsou nadefinovány do topologie sítě pro usnadnění práce s vyplňování údajů do formulářových polí. Nadefinování topologie se provádí přes tlačítko Add equipment v nástrojové liště, zobrazí se formulář pro vyplnění údajů. Důležité je vyplnit jméno a ip adresu a také o jaké zařízení se jedná. Po stisknutí tlačítka Add se síťový prvek přidá do stromové struktury topologie. Názorný příklad přidávání síťového zařízení je na obr. 7.13.

Poté si lze uložit topologii pomocí tlačítka Save topology. Uživatel si vybere adresář a do něj si soubor uloží. Pro načtení topologie ze souboru slouží tlačítko Load Topology. Všechny nadefinované síťové zařízení se zobrazí ve stromové struktuře a již uživatel nemusí vyplňovat položky těchto zařízení. Příklad uložení a načtení topologie je velmi jednoduchý a není jej třeba znázorňovat na obrázku.

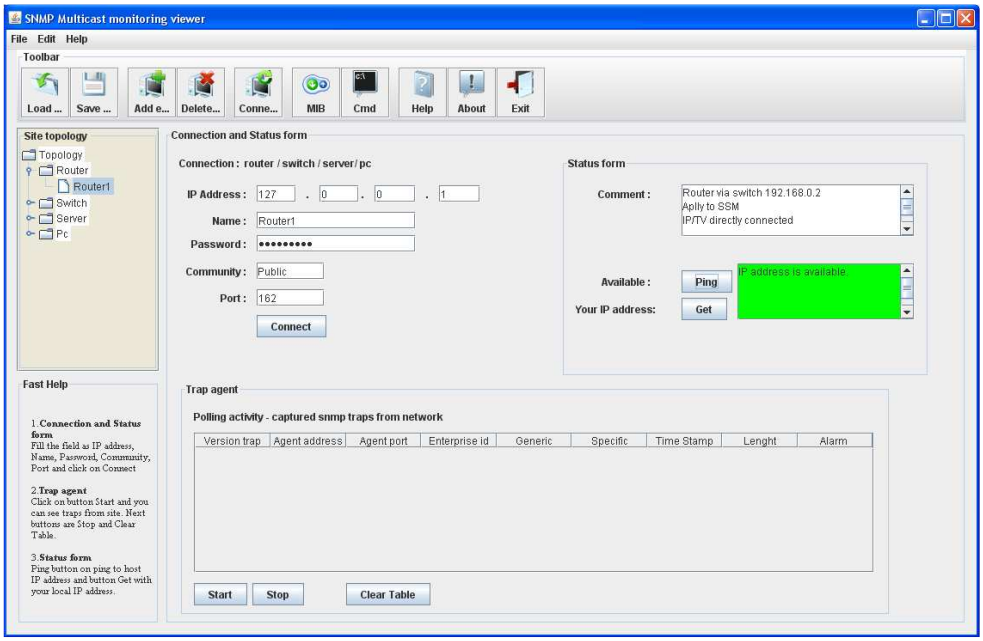


Obr. 7.13 – Přidávání síťového zařízení do topologie sítě

Smazání položky je také velice jednoduché. Stačí stisknout tlačítko Delete equipment a po zobrazení formuláře vybrat pouze položku, kterou chceme odstranit.

Další částí v hlavním okně je připojení daný síťový prvek. Po kliknutí do stromové struktury topologie na daný síťové zařízení jsou vyplněny položky formuláře. Důležitou částí je položka IP adresy a skupiny. Položka password, bude také využívána do budoucna pro protokol SNMPv3. Tyto hesla nejsou z důvodu bezpečnosti ukládaná do topologie sítě. Také je možnost nadefinování síťového zařízení, které není ve stromové struktuře. Poté stačí stisknout tlačítko Connect. Názorný příklad správného vyplnění formuláře je na obr. 7.14. Pokud je některá položka špatně nadefinována objeví se dialogové okno s neúspěšným připojením, buď z důvodu nedostupnosti daného síťového zařízení nebo pro špatně zadané údaje a je potřeba připojení opakovat nebo změnit položky ve formuláři. Pokud je připojení úspěšné zobrazí se okno sledování statistik, popis funkce tohoto okna se nachází v následující kapitole.

V hlavním okně je také část s doplňkovými příkazy (Status form). Lze zde ověřit dostupnost adresy pomocí programu ping, pokud je ip adresa dostupná vybarví se textové pole na zeleno, pokud není ip adresa dostupná, zobrazí se chybová hláška. Také je zde obsaženo tlačítko pro určení rozhraní počítače, na kterém je aplikace spuštěna. Tlačítko Get.



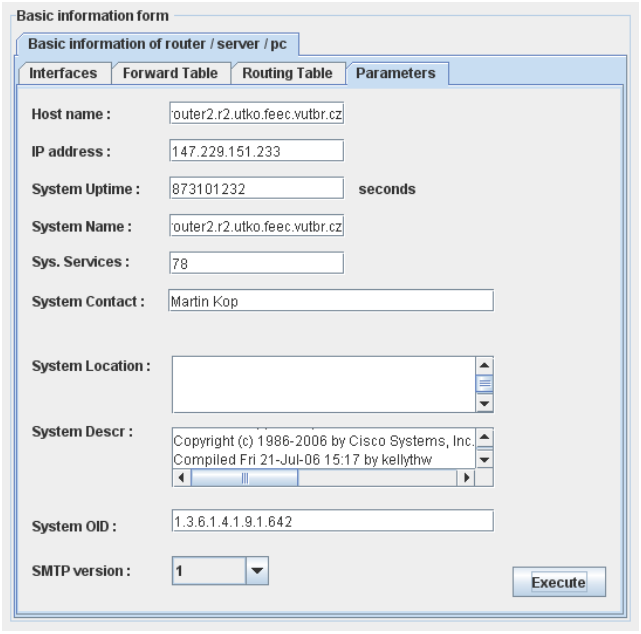
Obr. 7.14 – Názorné vyplnění hlavního okna

V poslední části je sledování počítačové sítě pomocí zpráv SNMP trap. Tabulka, která se nazývá Trap agent, slouží pro příjem zpráv od SNMP agentů, kteří jsou definovaní na daných síťových zařízeních a neustále monitorují počítačovou síť. Po stisknutí tlačítka Start, začne příjem těchto zpráv a následně jsou přehledně vypisovány do tabulky. Tyto příchozí zprávy se nazývají Trapy, také již byly probrané v předchozích kapitolách. Komunikace probíhá na portech 162 a 161. Nastavení těchto agentů je velice rozmanité. V tabulce se například zobrazují informace o stavu síťových zařízení, u kterých se změní stav. Je-li například připojený směrovač dostupný zda nikoliv. Po stisku tlačítka Stop je příjem zpráv zastaven. Tabulku lze vymazat tlačítkem Clear Table. Funkce Trap agenta je lépe znázorněna v kapitole o testování aplikace.

7.5.2. Funkce okna sledování statistik

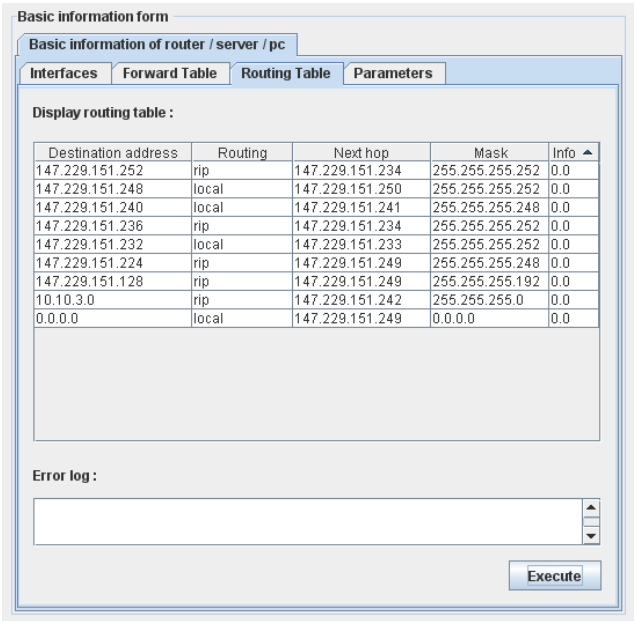
Primární funkcí tohoto okna je posílat SNMP dotazy na dané síťové zařízení a poté přijmout odpověď a tu následně zpracovat přehledně do tabulek. V levé části okna jsou základní informace, které jsou řazené v záložkách pro přehlednost. Tyto informace jsou získávány pomocí snmp protokolu a přístupu do tabulky MIB na daném síťové zařízení. Pro tuto každou záložku byly nadefinovány OID čísla pro příjem daných informací. V záložce parametry (Parameters) jsou základní informace o daném síťovém zařízení. Záložka obsahuje jméno (Host name), ip adresa zařízení na něhož se posílají SNMP dotazy (IP address), poté čas který určuje, jak dlouho je zařízení zapnuté (System uptime), také jeho jméno v systému (System name), počet spuštěných služeb, které jsou nastavené na síťovém prvku (System services), kontaktní údaje na zařízení (System Contact, System Location) , popis zařízení (System Description) a v neposlední řadě číslo OID (System OID), což je číslo pro přístup do dané MIB tabulky o kterém bylo

pojednáno v předchozích kapitolách. A také možnost nastavení SNMP zpráv pro verzi SNMPv1 nebo SNMPv2. Obrázek 7.15.



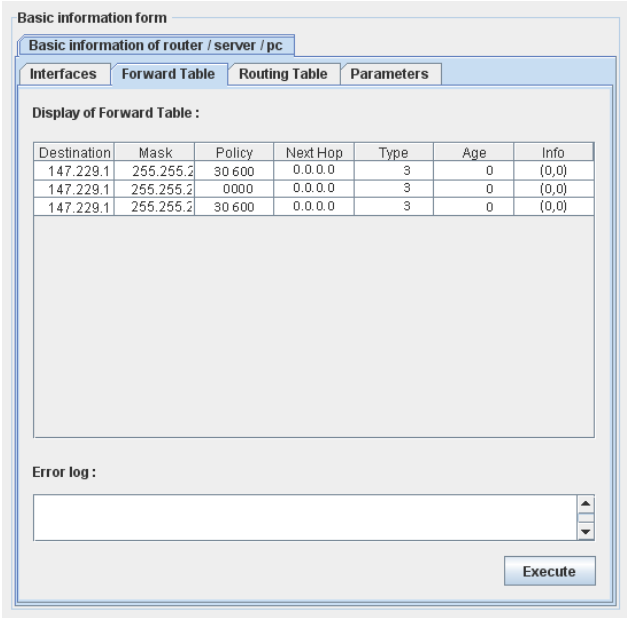
Obr. 7.15 – Základní parametry

Další záložkou je směrovací tabulka (Routing Table) zobrazená na obr. 7.16. OID je 1.3.6.1.2.1.2.2.1. Zde jsou informace o směrovací tabulce. Ip adresy cílových zařízení (Destination address), směrovací protokol (Routing), skok na další síťový prvek (Next Hop) a masky ip adres (Mask), případné další informace (Info). V dolní části je okno pro výpis chybových hlášení v případě špatného příjmu SNMP odpovědí.



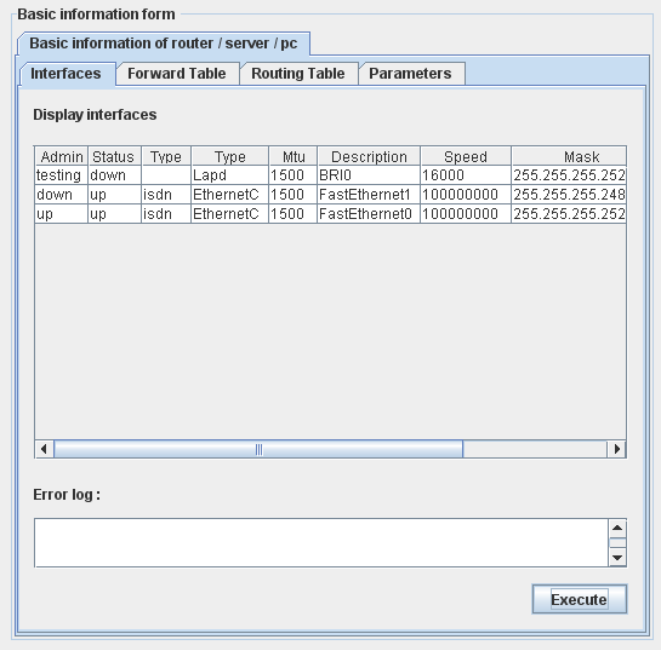
Obr. 7.16 – Směrovací tabulka

Na následujícím obr. 7.17 jsou informace o směrování na další síťový prvek. OID u těchto statistik je 1.3.6.1.2.1.4.24.2.1.1. První položka je cílová adresa (Destination address), maska síťového rozhraní (Mask), dalé aplikovaná politika na rozhraní například číslo access listu (Policy), skok na další směrovač (Next Hop), typ rozhraní (Typ), počet sekund od poslední změny na rozhraní (Age) a dodatkové informace (Info).



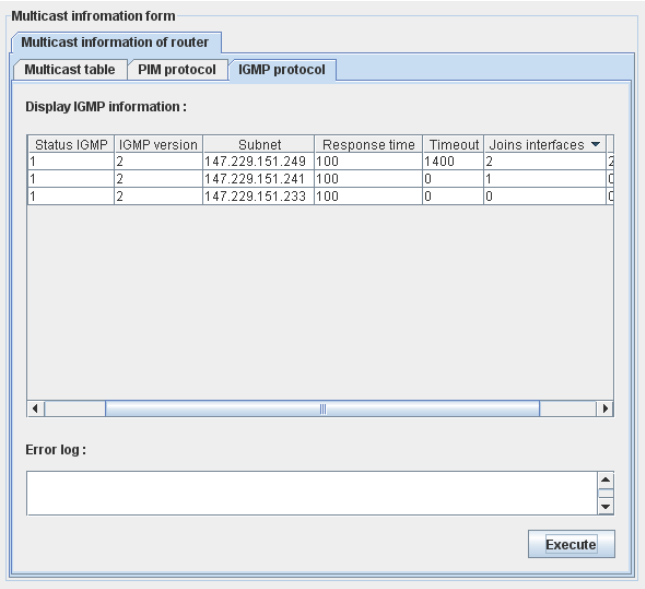
Obr. 7.17 – Informace o softwaru na síťovém zařízení

Poslední položkou v levé části je záložka s rozhraními na daném síťovém prvku (Interfaces). Základní OID je 1.3.6.1.2.1.2.2.1. Zde je mnoho parametrů, které jsou důležité z hlediska přehledu nastavení jednotlivých rozhraní. Položka (Admin status), která identifikuje nastavení rozhraní, dále položka fyzického stavu rozhraní (Status), položky typu rozhraní jsou dvě. První pro určení například isdn linky a druhá pro druh, například ethernet nebo serial link (Type), další položka je maximální velikost paketu přenesená na daném rozhraní (MTU), popis rozhraní (Description), rychlost linky (Speed), maska daného rozhraní (Mask), ip adresa rozhraní (IP address). Obrázek 7.18.



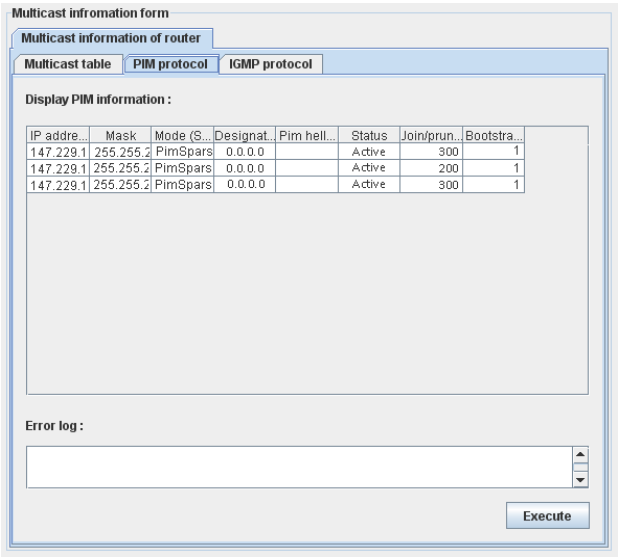
Obr. 7.18 – Položky vypisované na rozhraní

V pravé části okna sledování statistik jsou multicastové informace. Také zde je několik záložek pro sledování různých veličin. Zde jsou uvedeny některé protokoly, pomocí nichž, lze sledovat multicastové relace. Jedná se o protokol PIM a IGMP a také multicastovou směrovací tabulku. Také pro multicast informace ze zařízení se přistupuje do tabulky MIB přes dané OID. Na obr. 7.19 je zobrazena záložka s protokolem IGMP, která obsahuje mnoho sledovaných položek. OID je pro záložku IGMP 1.3.6.1.2.1.85.1.1.1. První položka je stav IGMP protokolu, jednička znamená, že je protokol aktivní (IGMP Status). Verze IGMP (IGMP version), podsíť (Subnet), další je čas maximální odezvy zpráv IGMP (Response Time), doba vypršení (Timeout), dále položka počtu připojených rozhraní (Join Interfaces), poslední položkou, která udává počet multicastových skupin na daném rozhraní je (Groups).



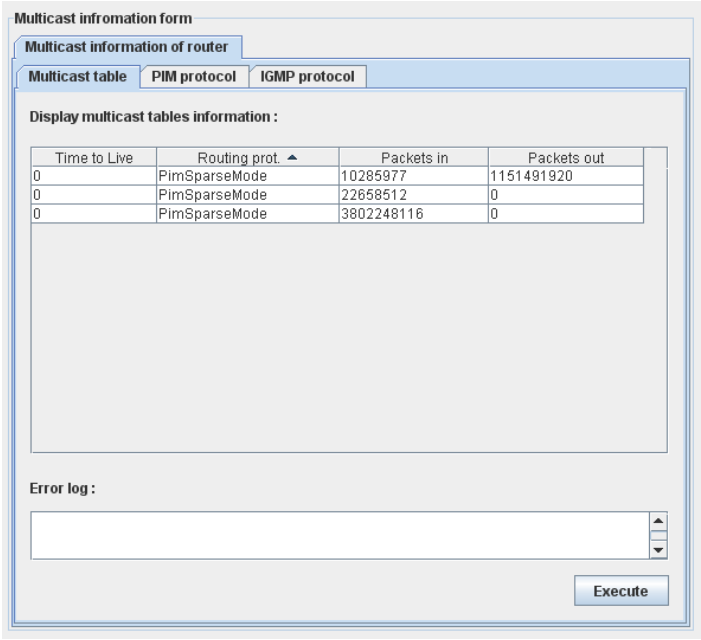
Obr. 7.19 – IGMP protokol a jeho veličiny

Další záložka je monitorování PIM protokolu, je zobrazena na obr. 7.20. Tento protokol je masivně nasazen v experimentální síti. Na obrázku je opět mnoho informací, které uživatele zajímají. Základní OID pro PIM protokol je 1.3.6.1.3.61.1.1.2.1. Jako první položka je ip adresa rozhraní na kterém je aplikováno PIM (IP address PIM), poté maska (Mask), další položkou je mód PIM protokolu, jestli se jedná o sparse-mode či dense-mode (Mode), adresa designated směrovače, ovšem pokud se jedná o spojení point-to-point je adresa 0.0.0.0 (Designated router), frekvence s jakou přicházejí PIM hello pakety na rozhraní (PIM hello pkt), položka, která identifikuje PIM na rozhraní (Status), frekvence jakou jsou zprávy join a prune přenášeny na rozhraní (Join/Prune int), hodnota, která definuje bootstrap směrovač, pokud je nastaven (Bootstrap router).



Obr. 7.20 – PIM protokol a jeho veličiny

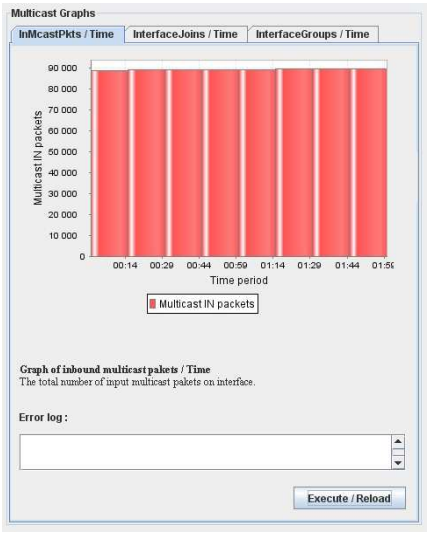
Poslední záložka je multicastová směrovací tabulka. OID této tabulky je 1.3.6.1.2.1.83.1.1.4.1. V této tabulce je opět několik důležitých veličin. Hodnota, která definuje jestli, budou multicastové pakety směrovány zda nikoliv (Time To Live), směrovací protokol na daném rozhraní (Routing protocol), počet příchozích multicastových paketů na rozhraní (Packets in), počet odchozích multicastových paketů (Packets out). Obrázek 7.21.



Obr. 7.21 – Multicastová směrovací tabulka

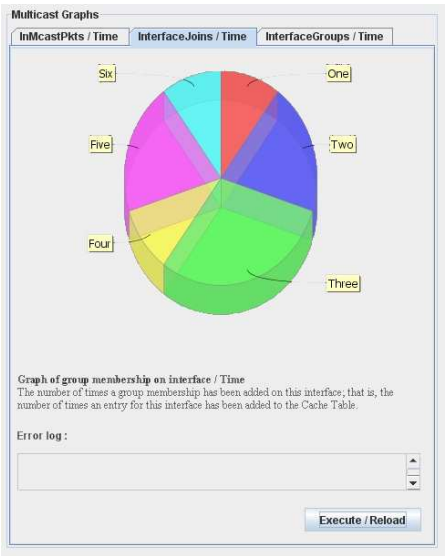
7.5.3. FUNKCE OKNA GRAFŮ

Poslední dílčí částí aplikace jsou grafy. Mulicastové grafy jsou tři. První graf (InMcastPkts / Time), který udává počet příchozích multicastových paketů vztaženo opět k času. Na obr. 7.22 je znázorněn graf při experimentálním měření a testování aplikace.



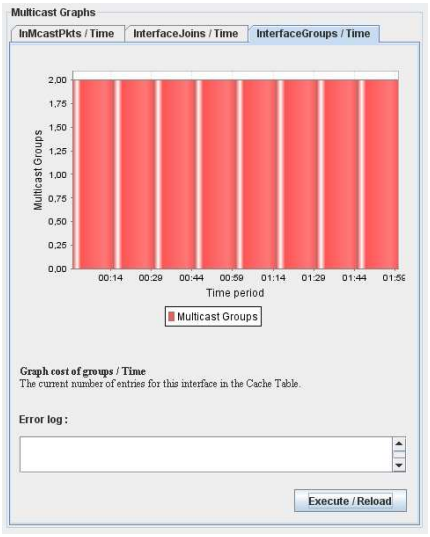
Obr. 7.22 – Graf odeslaných multicastových paketů

Na druhém grafu (InterfaceJoins / Time) je zobrazen počet zpráv protokolou IGMP. Lze sledovat aktivitu uživatelů, kteří tyto zprávy generují. Každou barvou jsou znázorněny zprávy od jiného uživatele. Tento graf je opět experimentální a je znázorněn na obr. 7.23.



Obr. 7.23 – Aktivita uživatelů sledovaná pomocí IGMP

Posledním grafem (InterfaceGroups / Time) je znázorněno kolik skupin bylo vytvořeno na daném rozhraní. Opět je tato hodnota vztažená k jednotce času a také tento graf je experimentální a pouze přibližuje funkčnost aplikace. Tento graf je znázorněn na obr. 7.24.



Obr. 7.24 – Počet multicastových skupin

7.6. DALŠÍ VÝVOJ PROGRAMU

Aplikace je v první plně funkční verzi. Do budoucna by se měla rozšířit o nastavování jednotlivých síťových zařízení, lepší zpracování grafů. Dále potom by aplikace měla být zdokonalená z hlediska zabezpečení a to díky možnostem protokolu SNMP verze 3, který již obsahuje prvky zabezpečení. Aplikace by do budoucna měla obsahovat terminál pro připojení na síťové zařízení přes SSH. Z hlediska multicastových relací by mohla aplikace také mít možnost nastavování jednotlivých parametrů multicastu. Časová náročnost vyvíjení, zdokonalování a testování aplikace je velice vysoká.

8. TESTOVÁNÍ APLIKACE

Všechny vyvíjené aplikace je potřeba důkladně otestovat a to především z důvodu jejich nasazení v reálných podmínkách na počítačových sítích. Aplikace by měla být stabilní, měla by být ošetřená z hlediska uživatelských kroků a nastavení, v neposlední řadě by také měla být rychlá. Vyvíjená aplikace pro monitorování multicastových relací byla otestována na reálné multicastové síti, která již byla popsána v předchozích kapitolách. Aplikace je schopna ihned monitorovat základní veličiny, ovšem u multicastových relací, je situace poněkud složitější. U multicastových relací je zapotřebí generovat určitý provoz na experimentální síti. Tento provoz je generován pomocí Cisco Content Engine 566 v modu Program Manager, Cisco IP/TV server 3442 a IP/TV Viewer. Poté již je aplikace schopna monitorovat multicastové relace. Testování aplikace a její části jsou rozděleny do několika podkapitol, ve kterých jsou také postupy testování a výsledky.

8.1. TESTOVÁNÍ TRAP ZPRÁV V HLAVNÍM OKNĚ

Po spuštění aplikace a správném zadání jména admin a hesla 1234, se zobrazí hlavní okno ve kterém je část s tabulkou nazvanou Trap agent, ve tabulka přijímá SNMP trap zprávy z různých síťových zařízení. Ovládání této části aplikace je velice triviální, po stisku tlačítka start začne aplikace přijímat pomocí SNMP protokolu tyto specifické trap zprávy. Důležitou podmínkou je, mít nastavené tyto SNMP zprávy nadefinované pomocí příkazů, které již byly znázorněny v kapitole 6.1.1.

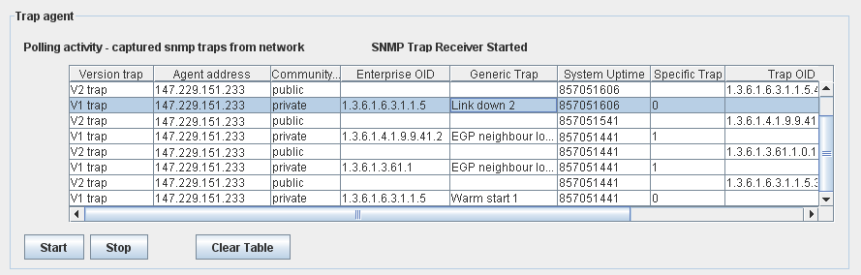
Testování této části aplikace proběhlo na směrovači označeném jako S3 s ip adresou 147.229.151.233. Počítač, na kterém byla aplikace spuštěna, byl připojen do sítě přes port FastEthernet 0/9 a jeho adresa byla přiřazena směrovačem pomocí DHCP 10.10.3.5.

Tab. 8.1 – Použité příkazy na směrovači S3

Krok	Příkaz (parametry)
1	**Router(config)# snmp-server host 10.10.3.5 traps version 1 public ipmulticast**
Popis:	*Nastavení posílání snmp trap zpráv na adresu 10.10.3.5 ve verzi 1 a s věřejnou community string a také je povoleno sledování multicastu.*
2	**Router(config)# snmp-server enable traps ipmulticast**
Popis:	*Příkaz pro povolení zasílání snmp zpráv o multicastu*
3	**Router(config)# snmp trap link-status permit duplicates**
Popis:	*Snmp zprávy, při změně stavu určité linky.*

Dále se na směrovači S3, byly nastaveny trap zprávy které jsou znázorněné v tab. 8.1. Nastavení směrovače se provádělo přes telnet připojení ke směrovači.

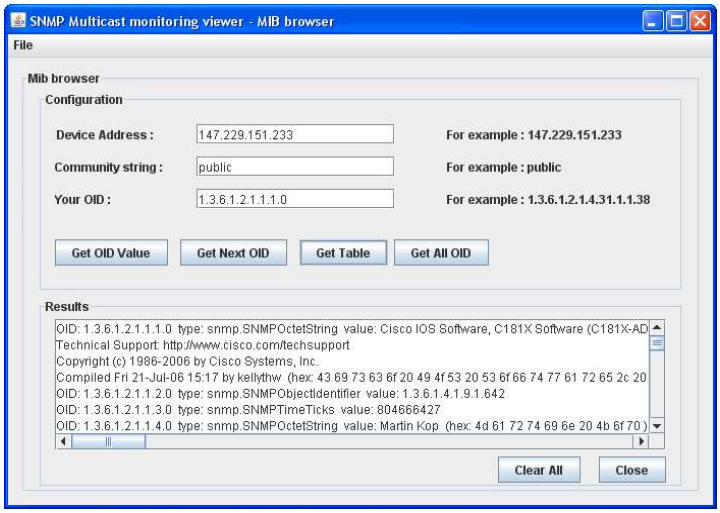
Na obr. 8.2 je znázorněn výpis některých zachycených SNMP trap zpráv, které jsou posílány například, při odpojení od některého funkčního portu směrovače. Položky jsou, verze trap zprav (Version trap), adresa ze které chodí trap zprávy (Agent address), poté skupina veřejná nebo privátní (Community), poté číslo objektu (Enterprise OID), trap o stavu zařízení (Generic Trap), systémový čas v sekundách (Systém uptime), specifikace trapu (Specific Trap) a také číslo trap zprávy v MIB databázi (Trap OID).



Obr. 8.2 – Trap agent

8.2. Použití MIB Browseru

V hlavním okně je také položka v nástrojové liště, která je pojmenovaná MIB. Po kliknutí na ikonku se otevře MIB browser, který je již popsaný v předcházejících kapitolách. Na názorném příkladu je znázorněn výpis celé tabulky od objektu z OID číslem 1.3.6.1.2.1.1.1.0 pomocí tlačítka Get Table. Výpis do tabulky je ze směrovače s označením S3 s ip adresou 147.229.151.233.

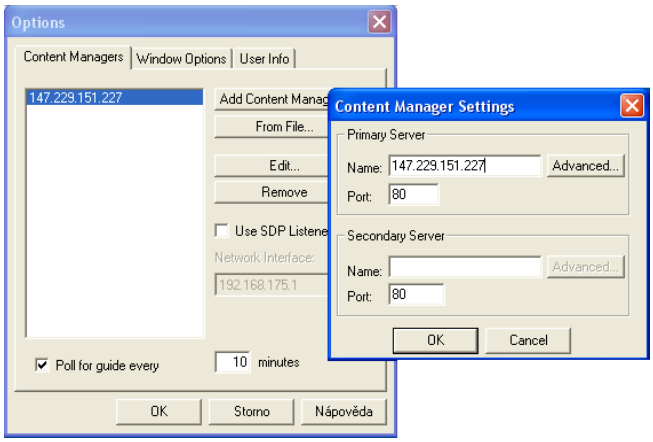


Obr. 8.3 – MIB browser použití

8.3. Generování multicástového provozu

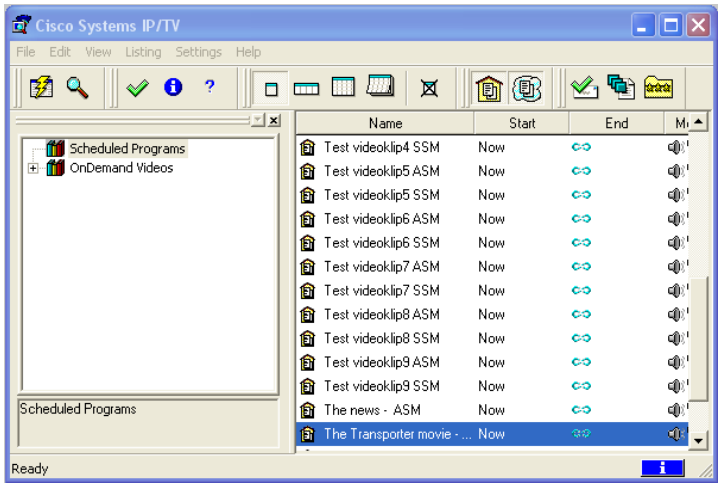
Jak již bylo zmíněno v předchozích kapitolách je zapotřebí generovat multicastový provoz do experimentální sítě. Aplikace je pak již schopna vypisovat dané multicastové veličiny. Po zapnutí Cisco Content Engine 566 v modu Program Manager a

Cisco IP/TV server 3442 začne být generován provoz do celé multicastové sítě. Podmínkou pro odchycení multicast zpráv je použití IP/TV Viewer, který je potřeba nastavit podle obr. 8.4. V okně tohoto programu si uživatel zvolí například některou z vysílaných stanic. Poté se vytvoří multicastová skupina a již lze monitorovat multicastové relace v experimentální síti.



Obr. 8.4 – Nastavení IP/TV viewer

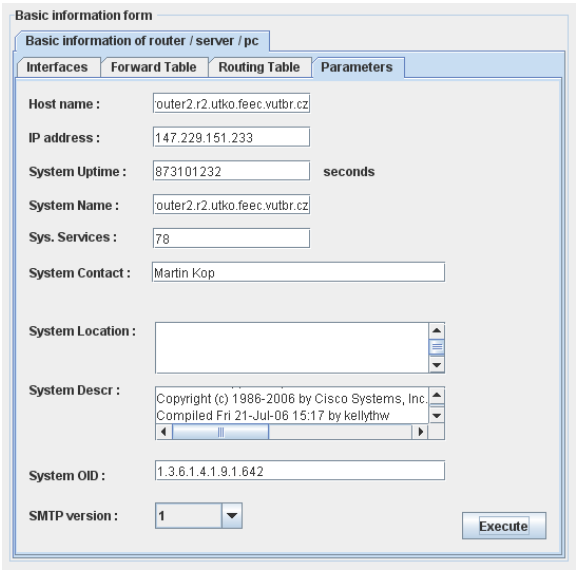
Na dalším obr. 8.5 je aplikace IP/TV viewer, tak s velice přehledným grafickým rozhraním. Stačí si z následujícího výběru zvolit některý s daných streamovaných programů.



Obr. 8.5 – Grafické rozhraní IP/TV viewer

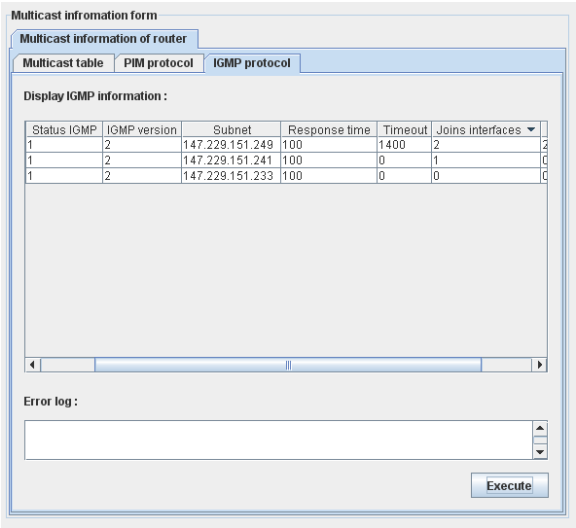
8.4. Výpis základních a multicast informací

Po připojení na směrovač s ip adresou 147.229.151.233 se zobrazí okno statistik. Poté již stačí pouze stisknout tlačítko Execute a v záložce parameters se zobrazí základní informace o daném síťovém zařízení, v tomto případě o směrovači S3.



Obr. 8.6 – Výpis základních informací ze směrovače

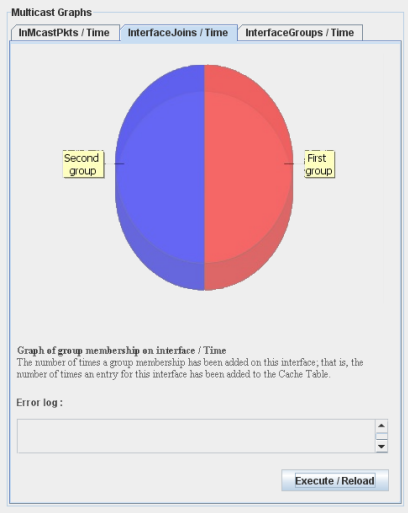
Po generování multicastového provozu v experimentální síti, lze vypsat například parametry IGMP protokolu na rozhraních směrovače S3. Položky již byly popsány v předchozích kapitolách.



Obr. 8.7 – Výpis multicast informací IGMP protokolu

8.5. Zpracování grafů

Při testování grafů je nejobtížnější časová synchronizace se síťovým zařízením. Čas, který se generuje osu X, je generován také pomocí SNMP dotazu do MIB tabulky a hodnota je přímo ze směrovače. Posléze si uživatel již může zobrazit graf například počet připojených uživatelů do skupiny. V testování byly vytvořené pouze dvě mutlicastové skupiny, jak je vidět na obrázku 8.8.



Obr. 8.8 – Počet uživatelů připojených do multicastové skupiny

9. ZÁVĚR

Cílem této práce bylo se seznámit se z problematikou multicastových relací v IP sítích a navrhnout aplikaci pro monitorování těchto mutlicastových relací. Pro návrh aplikace bylo nutné nastudovat možnosti nastavení pomocí příkazů Cisco IOS na síťových prvcích a možnosti SNMP protokolu. Poté navrhnout aplikaci s přehledným grafickým rozhraním, která bude monitorovat základní veličiny multicastu.

Tato práce teoreticky seznamuje s možnostmi monitorování multicastových relací v IP sítích. V úvodní části se pojednává o monitorování počítačových sítí a jejich významu, především z pohledu správců počítačových sítí. V této části je důležité pochopit, proč je monitorování počítačových sítí potřebné a k čemu je důležité. Je zde několik standardizovaných modelů, které zastřešují monitorování počítačových sítí. Protokoly, které se pro monitoring používají, zastávají také důležitou část práce. Pojednává se zde o funkčnosti a použití protokolu SNMP a také méně populárního protokolu RMON. Důležitý je především protokol SNMP, který je použit v aplikaci a tvoří její základ. Funkčnost protokolu je demonstrována na několika příkladech komunikace typu manager-agent. Zprávy protokolu jejich typy a především databáze MIB jsou zde rozebrány podrobněji a jsou nezbytnou částí, s kterou je potřeba se seznámit. MIB databáze je základem SNMP protokolu a díky této databázi můžeme sledovat mnoho parametrů v síťových prvcích experimentální počítačové sítě.

Další část práce pojednává především o multicast a multicastových relací v IP sítích. Jaké jsou možnosti z hlediska uplatnění několika technologií multicastu. Protokoly pro multicast, které využívá SNMP protokol a především názorný příklad jaké parametry v multicast relacích lze sledovat. V práci je navrhnuté schéma a jeho popis z hlediska správce sítě a postup pro zjištění informací pomocí navrhované aplikace v Java (JDK.1.6).

Následující část práce je rozdělena na dvě části. První z těchto částí se věnuje nastavování síťových prvků sítě pro multicast technologii pomocí příkazů Cisco IOS a také nastavení funkčnosti SNMP protokolu a jeho paramaterů. Také se jedná o zvolení správné topologie experimentální sítě a její adresní rozsah adres. Experimentální síť je tvořena z 5-ti směrovačů a 2 multimediálních serverů, které zajišťují provoz IP/TV v této síti. Druhá část pojednává o návrhu aplikace v modelu manager-client protokolu SNMP. Pro vývoj aplikace bylo použito vývojové prostředí NetBeans a aplikace, byla programována v jazyce Java, kvůli kompatibilitě a univerzálnosti.

Aplikaci tvoří několik dílčích částí. V každé z těchto částí si správce sítě zobrazí požadované parametry, které jsou přehledně zpracovány do tabulek a také grafů. Aplikace byla otestována na reálné mutlicastové síti v místnosti PA-249 v budově Purkyňova 118, Ústav Telekomunikací v Brně. Testování je poslední kapitolou této práce. V této práci jsou názorné příklady, jak otestovat aplikaci a naučit se s ní pracovat.

Jelikož v oblasti monitorování mutlicastových relací chybí software pro toto využití, byla vytvořená aplikace právě pro tyto účely. Aplikace je v anglickém jazyce, kvůli globálnějšímu použití a případné distribuci této aplikaci.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM POUŽITÝCH ZKRATEK

ASCII	*American Standard Code for Information Interchange*
ASN.1	*Abstract Syntax Notation number*
CCIT	*International Telegraph and Telephone Consultative Committee*
CGI	*Common Gateway Interface*
CGMP	*Cisco Group Management Protocol*
CLI	*Command-line Interface (CLI)*
CMIP	*Common Management Information Protocol*
DES	*Data Encryption Standard*
DVMRP	*Distance Vector Multicast Routing Protocol*
GUI	*Graphical User Interface*
ICMP	*Internet Control Message Protocol*
IETF	*Internet Engineering Task Force*
IGMP	*Internet Group Management Protocol*
IP	*Internet Protocol*
IPX	*Internetwork Packet Exchange*
ISO	*International Organization for Standardization*
LAN	*Local Area Network*
MIB	*Management Information Base*
NMS	*Network Monitoring System*
OID	*Object Identifier*
PDU	*Protocol Data Unit*
PIM	*Protocol-Independent Multicast*
RMON	*The Remote Network MONitoring*
SNMP	*Simple Network Management Protocol*
TCP/IP	*Transmission Control Protocol / Internet Protocol*
TTL	*Time To Live*
UDP	*User Datagram Protocol*
WAN	*Wide Area Network*
WAN	*Wide Area Network*
WWW	*World Wide Web*

POUŽITÁ LITERATURA

[1] KLAŠKA,Luboš. *Smysl a přínosy správy sítí* [online]. Svět sítí [cit. 2000-06-06]. URL: < http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=24>.

[2] ROTT, Milan. *Správa a monitorování lokálních počítačových sítí* [online]. ComputerWorld [1999] URL:<http://archiv.cw.cz/cwarchiv.nsf/clanky/321B1D5406D95F13C12569B00055B852?OpenDocument>.

[3] International Organization for Standadization (ISO). Enhanced communications transport protocol: Specification of simplex multicast transport [online]. [cit. 2002-06-06]. URL:<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35679 >

[4] Protokol SNMP Simple Network Management Protocol. Problém správy a řízení sítí: Monitoring provozu v určitých uzlech sítě[online]. URL:<https://akela.mendelu.cz/~lidak/share/site-stare/20prednaska.ppt>

[5] Cisco Management Information Base (MIB) User Quick Reference: MIB User Quick Reference[online]. URL:<http://www.cisco.com/en/US/docs/ios/11_0/mib/quick/reference/mtext.html>.

[6] Simple Network Management Protocol (SNMP)[online]. [cit. 1996-04-04] URL:<http://www.cisco.com/warp/public/535/3.html>.

[7] WILIAMSON, Beau. *Developing IP Multicast Networks*. Indianapolis: Cisco Press, 2000.

[8] Multicast Quick Start Configuration Guide: Cisco Press [online]. Aktualizován [2005-09-30]. URL:<http://www.cisco.com/warp/public/105/48.html>.

[9] HUCABY, David – MCQUERRY, Steve. Konfigurace směrovačů Cisco, Autorizovaný výukový průvodce, překlad Jiří Veselský. ComputerPress, 2004, 632 stran. ISBN 80-7226-951-8.

[10] VELTE, Toby J. – ANTHONY, T. Velte. *Cisco: a beginner's guide.* Síťové technologie Cisco, Velký průvodce , překlad David Krásenský. ComputerPress, 2003, 759 stran. ISBN: 80-7226-857-0.

[11] SPORTACK, Mark A. *IP routing fundamentals*. Směrování v sítích IP, ComputerPress, 2004, 351 stran. ISBN: 80-251-0127-4.

[12] TEARE, Diane. Návrh a realizace sítí Cisco, Autorizovaný výukový průvodce. ComputerPress, 2003, 784 stran. ISBN: 80-251-0022-7

[13] WENSTROM, Michael. Zabezpečení sítí Cisco, Autorizovaný výukový průvodce. ComputerPress, 2003, 784 stran. ISBN: 80-7226-952-6

[14] Počítačové sítě IP multicasting. IP multicast – mechanismus pro skupinovou komunikaci v IP vrstvě. [online]. URL: https://akela.mendelu.cz/~lidak/site/slidy2008/11prednaska-2008.ppt

[15] Lekce 13 - GUI aplikace v NetBeans BlueJ. GUI aplikace v NetBeans BlueJ.[online]. URL:<http://www.boldar.cz/java/lekce13GUI.ppt>

[16] WRÓBLEWSKI Piotr, Algoritmy - Datové struktury a programovací techniky, Nakladatelství Computer Press, a.s.

[17] Maufer T. A.: Deploying IP Multicast in the Enterprise, Prentice-Hall Inc., ISBN: 0-13-89-897687-2.

SEZNAM PŘÍLOH

Příloha č.1 – OBSAH PŘILOŽENÉHO CD

Adresář	Obsah
\Text	-elektronická podoba diplomové práce a soubor s metadaty
\Program	-všechny soubory aplikace realizované v JAVA
\Obr	-obrázky použité v diplomové práci