České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra počítačových systémů

Diplomová práce

Nasazení IPTV do počítačové sítě

Bc. Jakub Láznička

Vedoucí práce: Ing. Alexandru Moucha, Ph. D.

7. května 2014

Poděkování

Chtěl bych poděkovat panu Ing. Alexandru Mouchovi, Ph.D. a Ing. Viktoru Černému za rady při realizaci této práce. Dále bych chtěl poděkovat aktivním členům ze sdružení JM-Net o.s., díky kterým se podařilo zajistit produkční prostředí pro nasazení televize v síti.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

V Praze dne 7. května 2014 .....

Odkaz na tuto práci

Láznička, Jakub. *Nasazení IPTV do počítačové sítě.* Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2014.

Abstrakt

Tato práce shrnuje problematiku výběru vhodného IPTV řešení až po jeho nasazení do středně velké počítačové sítě. Velkým tématem práce jsou sledovací sondy, které vícesměrový provoz monitorují a vyhodnocují chyby při přenosech v síti. Práce se v rámci nasazení zabývá problematikou klientských řešení.

Klíčová slova IPTV, multicast, unicast, IPTV řešení, sledování multicast provozu, OpenWRT iptv, MikroTik iptv

Abstract

This thesis summarizes the issues of selecting the proper IPTV solution till its deployment to a mid-size computer network. Main topic of this work describes tracking sensors, which are monitoring and evaluating errors during multicast transmission in the network. Separate topic concerns of deployment of client solutions.

Keywords IPTV, multicast, unicast, IPTV solutions, multicast monitoring, OpenWRT iptv, MikroTik iptv

Obsah

Úvod **1**

1 Představení IPTV **3**
1.1 Architektura 4
1.2 Hlavní funkce IPTV 4
1.3 IPTV platformy v České republice 8
1.4 Metody komprese při přenosu televizních kanálů 13
1.5 Možnosti přenosu datových proudů přes IP síť 14
1.6 Protokoly a prostředky využité pro přenos vícesměrového vysílání 15

2 Analýza způsobu nasazení IPTV **23**
2.1 Představení sítě 23
2.2 Vybrané referenční lokality 29
2.3 Možné metody šíření vícesměrového vysílání 33
2.4 Volba technologie 35

3 Nasazení IPTV **37**
3.1 Konfigurace páteřní sítě 37
3.2 Nastavení bezdrátových prvků 40
3.3 Místa nasazení IPTV 43
3.4 Klientská řešení 43

4 Monitoring vícesměrového vysílání **51**
4.1 Analýza způsobů monitorování 51
4.2 Monitorovací sondy 52
4.3 Problémy v síti 61
4.4 Referenční lokality 64

Závěr **67**

Literatura **69**

A Doplnění vybraných částí práce **77**
A.1 Podrobné informace o monitorovacím programu 77
A.2 Informace o klientských směrovačích TP-LINK se systémem OpenWRT 80
A.3 Konfigurace páteřních prvků 86

B Seznam použitých zkratek **91**

C Obsah přiloženého DVD **95**

Seznam obrázků

1.1 Architektura IPTV 5
1.2 Ukázka rozhraní uživatele platformy sledovanitv.cz 9
1.3 Ukázka rozhraní Nangu.TV 11
1.4 Ukázka rozhraní uživatelského prostředí platformy 4network.tv . . 11
1.5 Ukázka rozhraní Easytv 12
1.6 Nasazení „multicast protokolů“ v jednotlivých segmentech sítě . . 15
1.7 Představení jednoduché sítě s nasazenou funkcí MVR 16

2.1 Mapa páteřní sítě 24
2.2 Fotografie bezdrátového spoje Alcoma 26
2.3 Fotografie bezdrátového spoje Orcave 1S10 27
2.4 Fotografie bezdrátového spoje Ericsson Mini-Link 27
2.5 Fotografie bezdrátového spoje UBNT AirFiber 28
2.6 Fotografie bezdrátového spoje Siklu EtherHaul 29
2.7 Fotografie bezdrátové technologie UBNT řady M 30
2.8 Mapa sítě v Modleticích 31
2.9 Mapa sítě v Říčanech 32
2.10 Mapa sítě v Nupakách 32
2.11 Mapa sítě v pražské Libuši 33
2.12 Ukázka samostatných IPTV VLAN v síti 35

3.1 Ukázka propojení se sítí provozovatele IPTV platformy 38
3.2 Nastavení QoS u bezdrátového spoje Alcoma 41
3.3 Rozhraní bezdrátového spoje NEC iPasolink 42
3.4 Ilustrace funkce prvku, který odděluje IPTV od internetu u koncového uživatele 44
3.5 Schéma čipu AR7240 z pohledu síťového administrátora 45

4.1 Doporučené rozmístění sond v páteřní síti 53
4.2 Monitoring - běžný případ 55
4.3 Monitoring - případ, kdy horní mez přeteče 56

4.4 Monitoring - případ, kdy horní mez a čítač identifikátoru paketu přetečou 56
4.5 Graf chyb v příjmu jednotlivých paketů 60
4.6 Graf přijatého počtu paketů 61
4.7 Referenční lokality - výstup sond v páteřní síti 64
4.8 Referenční lokality - výstup sondy v Říčanech 65
4.9 Referenční lokality - výstup sondy v Nupakách 66

A.1 OpenWRT Luci přihlášení 81
A.2 OpenWRT Luci nastavení interního přepínače 82
A.3 OpenWRT Luci nastavení síťových mostů a adres 83
A.4 OpenWRT Luci nastavení bezdrátové sítě 84
A.5 Přihlašovací stránka přepínače HP V1900 90
A.6 Nastavení funkce IGMP-snooping v přepínači HP V1900 90

Seznam tabulek

3.1 Mapování portů u modelu TP-LINK WR741nd 48
3.2 Mapování portů u modelu TP-LINK WR1043nd 48
3.3 Mapování portů u modelu TP-LINK WDR4300 49

Úvod

Termín IPTV (*internet protocol television* - televize přes internetový protokol) je obecný pojem ukrývající v sobě mnoho funkcí a výhod spojených v jednu službu [29]. Zároveň je pro mnohé síťové správce velmi nenáviděným termínem. Zavedení televize do sítě je mnohdy velmi náročné jak na čas, tak i na peněženku majitele sítě. Je zároveň i velkou zatěžkávací zkouškou, ve které se projeví, jak kvalitně je síť postavena a jestli byl při výstavbě kladen důraz na kvalitu, nebo na kvantitu.

Po přechodu na digitální vysílaní a vypnutí posledních analogových vysílačů došlo k velkému boji mezi současnými poskytovateli a ostatními subjekty o zákazníka. Kdo dnes nenabízí nějakou formu televize, jako kdyby na trhu nebyl.

Největším konkurentem pro IPTV je standard digitálního kabelového vysílání DVB-C, digitálního satelitního vysílání DVB-S a digitálního pozemního vysílaní DVB-T [74]. Na rozdíl od jiných standardů má televize přes internetový protokol řadu úskalí, ale přináší i obrovskou škálu výhod, které se ostatních možností netýkají nebo týkají jen z části [29].

Tato práce tedy přináší ucelený přehled problematiky IPTV v reálném provozu a zároveň její monitoring.

Velkým tématem mé diplomové práce budou monitorovací sondy, kterým bude vyhrazena samostatná kapitola. Mnoho poskytovatelů IPTV nesleduje vícesměrové vysílání a reagují tak až na nespokojené podněty zákazníků. Ty mnohdy nejsou vyřešeny efektivně, jelikož poskytovatel nezjistí, kde se nachází jádro problému. Bude implementována efektivní možnost sledování sítě za účelem eliminace těchto problémů. Naměřená data budou použita k soupisu jednotlivých nalezených chyb při implementaci. Následně budou tyto chyby vyřešeny, případně bude navrhnuta cesta k řešení.

Teoretická část bude obsahovat představení služby IPTV včetně nutných komponent pro provoz. Zároveň bude uveden přehled nejvyužívanějších platforem v České republice. Součástí této kapitoly bude i přehled protokolů a forem

distribuce obsahu klientům.

V analytické části bude představena síť, do které bude IPTV implementována. Bude shrnuto několik způsobů, jak v této síti službu nasadit a následně bude jeden z nich vybrán.

V praktické části práce bude využito informací z teoretické a analytické části a budou provedeny změny, aby mohla IPTV fungovat. Součástí sítě bude také návrh vhodného řešení brány oddělující IPTV provoz od ostatních dat v síti u koncových klientů.

V závěru budou shrnuty výsledky této práce včetně praktických dopadů na síť, do které bude IPTV nasazena.

Kapitola 1

Představení IPTV

IPTV provozují telekomunikační operátoři ve svých datových sítích. Na rozdíl od běžného pozemního (DVB-T), satelitního (DVB-S) nebo kabelového (DVB-C) vysílání přináší tato technologie řadu výhod, které se u jiných technologií nevyskytují [30].

Televize přes internetový protokol podporuje řadu přidaných funkcí a přináší velkou míru interaktivity pro uživatele. V případě běžného vysílání se jedná o jednosměrnou komunikaci, vysílač vysílá a postrádá zpětnou vazbu od uživatelů, kteří jeho signál přijímají. V případě IPTV existuje zpětný kanál v podobě IP sítě, který mohou uživatelé využít pro zpětnou komunikaci.

Zpětný kanál dává IPTV i nesmírnou výhodu v optimalizaci jednotlivých přenosů a přidává interaktivitu. Díky omezené kapacitě přenosových technologií je nutné omezit kvalitu přenášeného obrazu (jedná se o běžný jev například u satelitního nebo pozemního vysílání). U IPTV v případě vícesměrového vysílání je tento problém vyřešen, jelikož je možné efektivněji využít přenosové kanály ke klientům. Díky zpětné vazbě je totiž možné zjistit, kdo který kanál sleduje. Kapacitu linek tak lze směrem k uživatelům vytěžovat efektivně pouze provozem, který v daném segmentu uživatel sleduje. Vše tak závisí na technologii a kapacitě přenosové sítě poskytovatele.

To vše je však možné pouze díky existenci pozemní vysokokapacitní sítě. Satelitní i kabeloví operátoři již dnes také nabízí možnost interaktivity, ale jen díky funkcím v přijímači, který se přes internet připojí k jejich službám (například dle serveru Digizone.cz [50] služba UPC Horizon [70] v Nizozemsku). Novou alternativou se v posledních letech začíná stávat tzv. hybridní vysílání HbbTV, které využívá také celosvětovou síť pro přidání interaktivních možností [27]. Základní aplikace a informace jsou ale zahrnuty v datových proudech jednotlivých kanálů a mohou tedy být vysílány i pomocí pozemních vysílačů. V České republice HbbTv spustila na všech programech například Česká televize [75].

1.1 Architektura

Aby mohla IPTV fungovat, musí existovat několik prvků v síti, které zajišťují provoz a přenos dat od televizního studia až k uživateli. Zároveň musí existovat prvky zajišťující činnost dalších nadstavbových služeb. Schéma základní architektury je na obrázku 1.1.

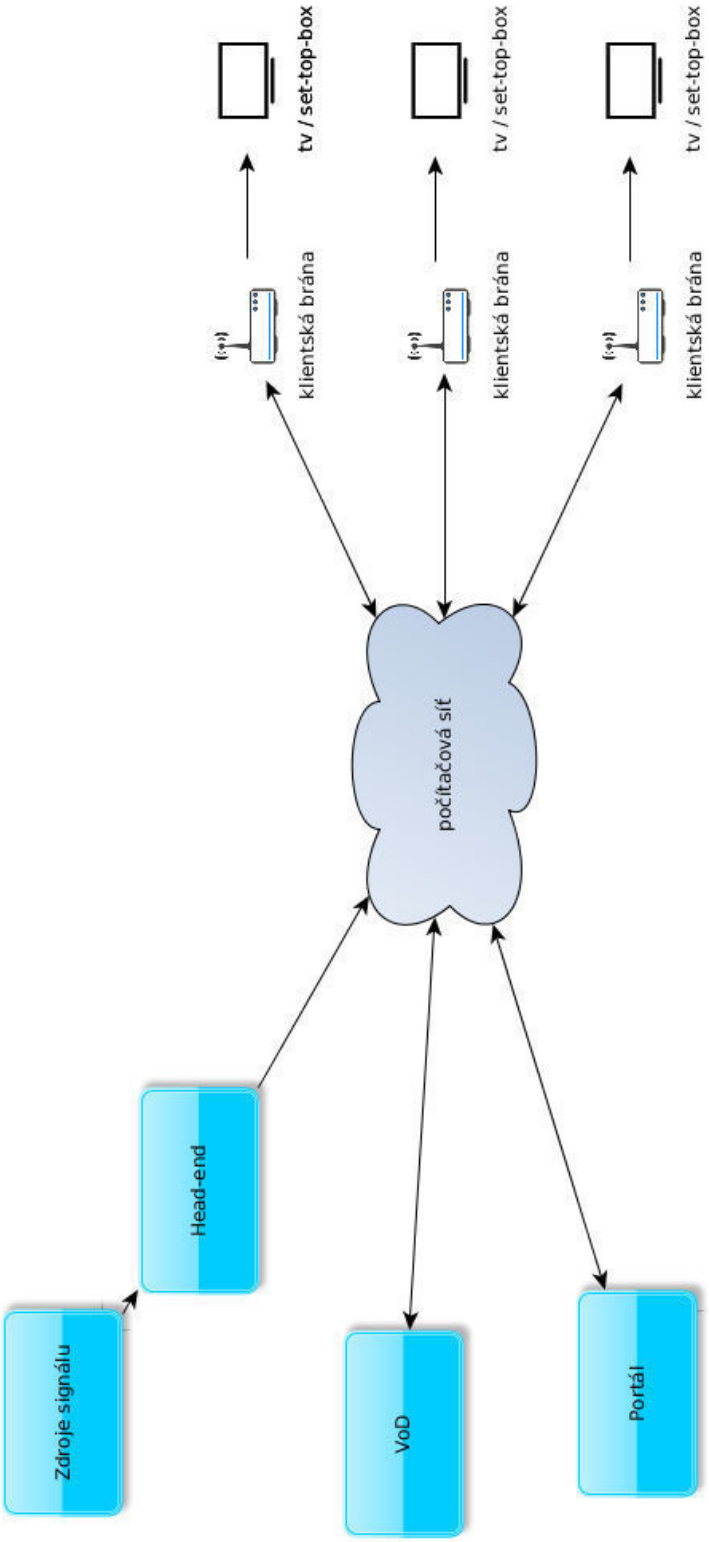
Základní prvky platformy tedy jsou [28]:

- TV head-end - jedná se o jedno nebo více zařízení, která fungují jako zdroje televizního signálu pro uživatele platformy (např. satelitní přijímač, který následně distribuuje kanály pomocí vícesměrového vysílání)
- VoD platforma - zde jsou prvky, které obsahují nahrané pořady, případně prémiový obsah (filmy, seriály) a na vyžádání uživatele jsou přenášeny ve formě jednosměrného vysílání. Vedle VoD může v platformě existovat i služba nPVR, která nahrává televizi a na vyžádání zákazníka jí přenáší
- Interaktivní portál - umožňuje uživateli procházet různé IPTV služby. Například je možné prohlížet katalog filmů
- Distribuční síť - síť pro výměnu IP paketů (unicast a multicast), kterou se šíří datové proudy od zdroje k cíli
- Vstupní síťové zařízení u uživatele - jedná se o prvek, který slouží jako brána přímo u uživatele a odděluje koncovou síť poskytovatele od domácí sítě
- IPTV přijímač - slouží k dekódování obsahu a dále zobrazuje obsah přímo na televizní obrazovku

Dále se v soustavě mohou nacházet zařízení pro překódování vysílaného obsahu tzv. enkodéry nebo například zařízení pro šifrování obsahu. Pokud je síť rozsáhlá, tak mohou být součástí architektury i místní vyrovnávací cache a další prvky podporující přidané služby IPTV pro rychlejší a efektivnější doručení k uživateli.

1.2 Hlavní funkce IPTV

U IPTV lze zmínit několik již dnes velmi využívaných funkcí [72]. Kromě živé televize lze využít tzv. nelineárních funkcí, které na platformě fungují právě díky obousměrné komunikaci.



Obrázek 1.1: Ilustrace základní architektury IPTV

1.2.1 Živá televize (Live-TV)

Jedná se o příjem televize podobný jiným technologiím. Uživatel může vybírat živý obsah pomocí přepínání kanálů. Přenos živé televize je v IPTV realizován obvykle pomocí vícesměrového vysílání, ale existují i implementace založené na jednosměrném vysílání.

1.2.2 Electronic program guide (EPG)

Klasický programový průvodce je běžnou součástí televizního vysílání. Každý uživatel tak může přijímat a prohlížet televizní program stanice. V případě IPTV lze ale průvodce rozšířit o různé interaktivní funkce jako jsou například ukázky pořadů, náhledy a další možnosti. EPG může byt součástí vysílání živé televize, nebo se načítá pomocí jednosměrného vysílání z IPTV platformy poskytovatele.

1.2.3 Pay per view (PPV)

U vybraných prémiových kanálů lze uživateli umožnit sledování jen v daný časový úsek. Tento model je využit hlavně u prémiového obsahu (erotika nebo filmy) pro občasné předplatitele. Obsah může být získán pomocí vícesměrového i jednosměrného vysílání.

1.2.4 Networked personal video recorder (nPVR)

Jedná se o centrální nahrávání pořadů na vzdálený disk. Uživatel místo nahrávání na svůj domácí disk odešle platformě požadavek a ta jej nahraje na své datové úložiště. Výhodou je úspora dat (více uživatelů chce nahrát stejný pořad, na společném disku bude umístěn pouze jednou). Nevýhodou je ale zvýšená zátěž pro síť v případě opakovaného přehrávání.

S touto funkcí souvisí další rozšíření. Příkladem je možnost spustit si od začátku pořad, přetáčet obraz v čase až několik hodin zpětně a další výhody. Přenos nahraných souborů probíhá ze vzdáleného disku pomocí jednosměrného vysílání.

1.2.5 Video on demand (VoD)

Video na vyžádání je jednou z klíčových výhod IPTV. Přináší uživatelům možnost přehrávat filmy v reálném čase (za poplatek nebo třeba i bez poplatku). Přehrávání probíhá pomocí jednosměrného vysílání ze zdroje v platformě, nebo ze vzdáleného zdroje (je možné získat nahrávky i prostřednictvím internetu). VoD je hojně využívanou nadstavbou, například v nabídce společnosti Telefónica Czech Republic, a.s. se tato služba nazývá O2 videotéka [63]. Ta aktuálně obsahuje více než 1000 filmů. Dalším příkladem je služba HBO On-Demand [33].

1.2.6 Výhody a nevýhody IPTV

V případě IPTV existují výhody, které může uživatel využít:

- Díky IP technologii lze službu IPTV provozovat na jednom médiu (jednom kabelu) společně s dalšími službami jako jsou například internet nebo telefon
- IPTV je ekonomicky výhodná služba. Díky doručování pouze vybraných dat, která uživatel požaduje, lze ve službě vysílat větší počet kanálů než prostřednictvím jiných technologií
- Služba podporuje velkou míru interaktivity díky přidaným funkcím

Největší nevýhody, které lze ve velké míře eliminovat investicemi do technologií, jsou:

- Velká náchylnost na ztrátu paketů. Každý problém na lince se projeví na kvalitě obrazu
- V případě nasazení společně s dalšími službami je nutné správně prioritizovat jednotlivé druhy provozu

1.2.7 Nároky na přístupovou síť

Nároky celé služby na přístupovou síť jsou velmi špatně odhadnutelné. U poskytovatelů vždy závisí na koncové technologii účastníka a někdy i na distribuční síti. Od ní se obvykle také odvíjí nabízené přidané služby a hlavně kvalita služeb.

V případě technologie xDSL, která se vyznačuje závislostí rychlosti přenosového kanálu k uživateli na délce kabelového vedení od ústředny [9], je nutné uvažovat o omezení datového toku televizních programů a dalších funkcí, aby byla služba na straně zákazníka funkční. Pokud bude chtít zákazník využít více přijímačů v domácnosti, pak se předpokládaný datový tok zvyšuje násobkem počtu televizních přijímačů. Běžným jevem na xDSL přípojkách je pokles rychlosti internetu v případě sledování televize.

U technologií FTTH nebo FTTB je problém s kapacitou vyřešen díky vyšší propustnosti celé technologie. U funkce živé televize lze predikovat využití sítě. Bohužel v kombinaci s dalšími funkcemi, které síť zatěžují pomocí jednosměrného vysílání může zátěž v případě stovek uživatelů vyrůst klidně přes 1 Gb/s. Pro ilustraci postačí příklad 500 klientů. 300 z nich sleduje živou televizi (dohromady 60 programů) a 200 klientů využívá nelineárních funkcí platformy (jednosměrné vysílání). Odhadem při zjednodušeném výpočtu datového toku 5 Mb/s na kanál se jedná o 1 300 Mb/s datového toku. V síti mohou existovat místa, která takovýto datový tok nemusí propustit a tak je nutné ze strany poskytovatele sledovat zátěž a reagovat postupným nahrazením technologií za rychlejší.

1.2.8 Budoucnost

Rozvoj vysokorychlostního internetu přinese další možnosti nasazení IPTV a umožní rozšířit objem služeb dodávaných skrz platformy. Některé technologie jako například xDSL přestanou časem kapacitně stačit při přenášení obrazu s velmi vysokým rozlišením a tak nebude na některých přípojkách možné nové výhody v budoucnu naplno využít. Nejrychlejší a nejefektivnější možnost pro doručení televizních proudů a doplňkových služeb je v současnosti technologie FTTH nebo FTTB (technologie optických vláken), která je prozatím nejrychlejší možností pro přenos dat na velké vzdálenosti.

Jako příklad služeb budoucnosti (nebo i současnosti) je možné uvést [36]:

- Více kanálů ve vysokém rozlišení (HD) a kanály s extrémně vysokým rozlišením (UHD)
- Více obsahu pro video na vyžádání (VoD)
- Výběr kamery při sportovním utkání
- Hlasování během pořadu
- U reklam možnost zobrazit si více informací o produktu

1.3 IPTV platformy v České republice

Aktuálně je v sítích českých poskytovatelů využito několik platforem od různých firem. Některé platformy se specializují na přenos dat po internetu podobně jako služba iVysílání České televize. Další jsou mnohem složitější, jelikož se v nich používá pro přenos živé televize vícesměrové vysílání a fungují jen v sítích jednotlivých poskytovatelů.

1.3.1 Platformy využívající jednosměrné vysílání

Jedná se o platformy, které pro přenos využívají internet (případně své lokální vyrovnávací cache přímo u poskytovatelů). Pro optimalizaci datových přenosů se ke komprimaci vysílaných kanálů používá standard MPEG4-AVC včetně omezení datového toku, takže spuštění a provozování služby není tolik závislé na kvalitě koncové sítě uživatelů. Mnohdy lze službu provozovat i přes bezdrátové přípojky s kolísající propustností. Uživatel nemusí poznat v obraze ani malou ztrátu paketů na přípojce.

1.3.1.1 Sledovanitv.cz

Sledovanitv.cz je možností, kterou dle stránek poskytovatele služby [57] nyní využívá více jak 65 lokálních poskytovatelů v České republice. Klienti mohou

Obrázek 1.2: Ukázka rozhraní uživatele platformy sledovanitv.cz

sledovat více jak 30 kanálů v omezené kvalitě. Kanály jsou komprimovány pomocí standardu MPEG-4 AVC s variabilním datovým tokem [58].

Aktuálně služby nelze odebírat přímo v televizním přijímači, klienti mohou využít akorát aplikace pro mobilní telefony se systémy iOS a Android, případně lze televizi sledovat i pomocí počítače (ukázka na obrázku 1.2).

Službu Sledovanitv.cz nemůže využít každý zákazník. Služba je poskytována pouze na velkoobchodní úrovni poskytovatelům i ostatním subjektům v České republice.

1.3.1.2 Onelinetv.cz

Onelinetv.cz provozuje společnost UPC Business s.r.o. Televizní obsah zahrnuje i prémiové kanály a různé balíčky včetně kanálů z rodiny HBO. Obsah lze sledovat pouze na vybraných televizních přijímačích od výrobce Panasonic.

Na prezentačních stránkách služby [69] je upřesněno tvrzení pro koho je služba určena. Televizní kanály prostřednictvím Onelinetv.cz lze objednat a sledovat pouze prostřednictvím sítí elektronických komunikací partnerů služby. Jedná se tedy o podobný model jako v případě služby sledovanitv.cz.

1.3.2 Platformy využívající pro přenos živé televize také vícesměrové vysílání

Jedná se o platformy, které využívají vícesměrového vysílání v sítích pro doručení živé televize. Ostatní (nelineární) služby fungují pomocí jednosměrného vysílání. Na rozdíl od výše uvedených služeb je nasazení tohoto druhu platforem do sítě mnohem komplikovanější a vyžaduje změny v síti.

1.3.2.1 Nangu.TV

Nangu.TV dnes využívá mnoho poskytovatelů v České republice, z těch největších je nutné zmínit nově společnost Telefónica Czech Republic, a.s. (během minulého roku společnost změnila dodavatele platformy z firmy Alcatel-Lucent právě na Nangu.TV [31]), dále SMART Comp a.s. prodávající své služby pod značkou NETBOX a jako posledního velkého hráče lze zmínit firmu RIO Media a.s. [26]. Řešení je vyvinuto společností Alnair a.s.

Platforma podporuje všechny dnes velmi žádané funkce jako nahrávání na vzdálený disk (nPVR), zpětné přehrávání (TimeShift, Catch-Up), přehrávání od začátku (StartOver), elektronický programový průvodce (EPG), TV archiv a v rámci platformy jsou k dispozici i aplikace jako například HBO On-Demand [7]. Klientům je umožněno objednat si rozšířené balíčky televize přímo prostřednictvím samoobsluhy na televizní obrazovce [32]. Ukázka rozhraní je na obrázku 1.3.

Jelikož náklady na vybudování a spuštění IPTV platformy v síti jsou vysoké a pro středně velké operátory mnohdy nedosažitelné, umožňují velcí operátoři pronájem své infrastruktury (jedná se o tzv. virtualizovanou licenci). Příkladem je nabídka společnosti SMART Comp a.s. uvedená na stránce prezentující velkoobchodní služby společnosti [59]. Výhodou je dle uvedené stránky kompletní řešení na míru, kde menší síť nemusí řešit smlouvy s poskytovateli obsahu a ochrannými svazy, zároveň nemusí investovat do technologického zajištění platformy (vše zajišťuje vlastník platformy, tedy poskytovatel velkoobchodních služeb). Na operátora s virtualizovanou licencí tedy zbývá úkol implementovat jednotlivé protokoly a nastavit jednotlivé prvky tak, aby IPTV jeho vlastní sítí procházela až do koncových přípojek.

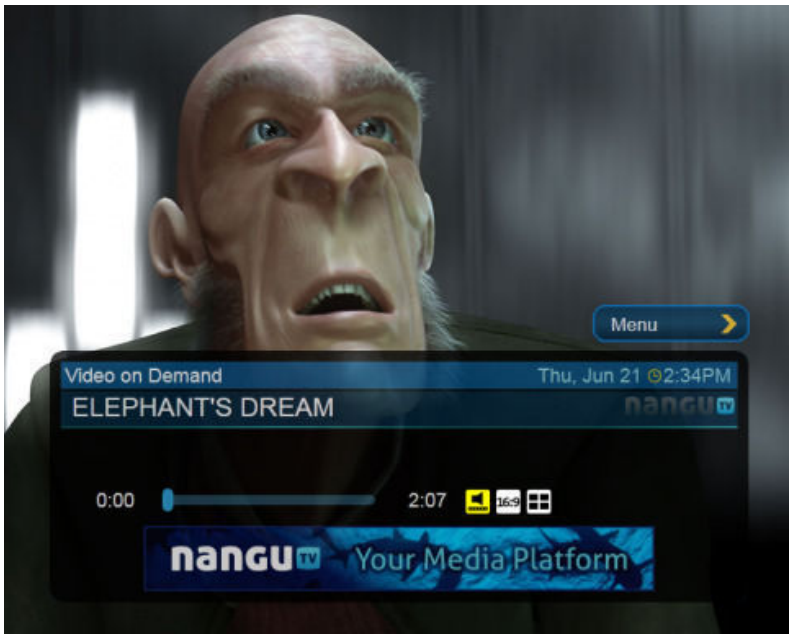
1.3.2.2 4network.tv

4network.tv je vyvíjena českou firmou NETFORMS s.r.o. Tuto platformu využívá několik poskytovatelů, dle prezentačních stránek platformy [45] například PODA a.s. nebo JON.CZ s.r.o. Základem této platformy je podpora všech přidaných funkcí podobně jako v případě platformy Nangu.tv. Sám dodavatel platformy dle svých stránek [43] nabízí poskytovatelům možnost virtualizovaného řešení. Moderní vzhled uživatelského prostředí je vidět na obrázku 1.4.

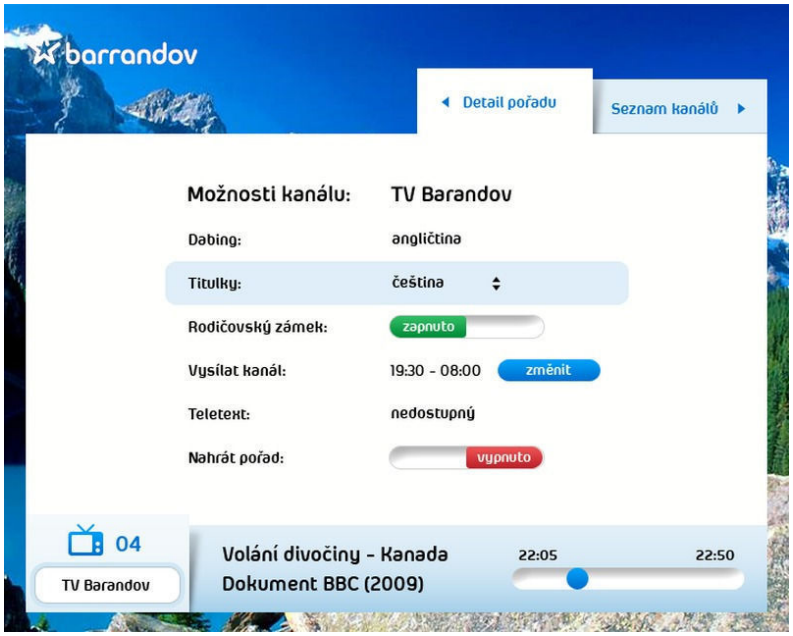
1.3.2.3 EasyTV

Platformu EasyTV vyvíjí česká společnost Allstar Group s.r.o. Podporuje veškeré základní funkce včetně zpětného přehrávání a v set-top-boxech je možné využít například i webový prohlížeč [4]. Referenčním poskytovatelem, který má tuto platformu nasazenu, je pražská společnost CentroNet a.s [5].

Ukázka rozhraní je viditelná na obrázku 1.5.



Obrázek 1.3: Ukázka rozhraní Nangu.TV [6]



Obrázek 1.4: Ukázka rozhraní uživatelského prostředí platformy 4network.tv [44]

Obrázek 1.5: Ukázka rozhraní Easytv [4]

1.3.2.4 Juice

Slovenský poskytovatel Antik Telecom (konkrétně jeho dceřiná firma ANTIK Technology s.r.o.) je dodavatelem platformy Juice, kterou v České republice využívá několik místních operátorů.

Tato platforma umí využít vícesměrového příjmu živé televize, podporuje ale i další žádané přidané funkce jako nPVR, EPG a další. Jako přijímače využívá platforma vlastní řešení pod značkou Juice [8].

1.3.3 Rozšíření IPTV

Dle poslední veřejně dostupné monitorovací zprávy ČTÚ o vývoji trhu elektronických komunikací se zaměřením na rok 2012 [74] vychází u počtu IPTV přípojek vzestupný trend.

Ve zprávě [74] je uvedeno: „Aktivní přípojky, na kterých je poskytována služba IPTV, dosáhly ke konci roku 2012 počtu 211 250. Počet přípojek meziročně vzrostl o 27 543, to znamená meziroční nárůst o 15,0 %. CAGR[1] činil ve sledovaném období (2008–2012) 14,1 %.“

Naopak kabelové přípojky (analogové i DVB-C) vykazují sestupný trend. Ve zprávě [74] je psáno: „Počet aktivních přípojek, na kterých je poskytována služba šíření kabelového televizního vysílání, dosáhl ke konci roku 2012 počtu 745 179. Počet přípojek meziročně poklesl o 4 264, to znamená meziroční pokles o 0,6 %. CAGR činil ve sledovaném období (2008–2012) -3,7 %“

[1]Compound Annual Growth Rate [35] neboli meziroční nárůst investice během specifického období.

Z uvedených údajů vyplývá, že zájem o televizní vysílání pomocí IP protokolu stoupá oproti dlouhodobému trendu klesajícího počtu placených TV přípojek.

1.4 Metody komprese při přenosu televizních kanálů

Pokud by bylo nutné bez komprimace přenášet televizní kanály skrz datovou síť, byla by výstavba celé sítě velmi drahá. Proto poskytovatelé i vysílatelé přistupují ke kompresi signálu, díky které lze ekonomicky využít prostředků k doručení signálu k zákazníkovi. Informace zmíněné v této části práce jsou čerpány z publikace pana Ing. Oujezdského Ph. D. [14].

Pokud daný provozovatel přistoupí na to, že chce šetřit datové kanály, je nutné zvolit vhodnou kompresi. U datových proudů je nutné ze začátku zmínit pojem kontejner. Ten se používá pro uložení videa a zvuku do jednoho souboru nebo datového proudu. Kromě toho je možné, aby jeden soubor nebo proud obsahoval i více zvukových stop, titulky a další možnosti, které může cílový konzument obsahu využít. Každý kontejner poté obsahuje informace, jakým kodekem byl každý datový proud kódován, nebo (pokud není kódován) v jakém formátu je datový proud uložen.

V případě televizního vysílání se nejčastěji používá kontejner MPEG-TS.

1.4.1 MPEG-2

MPEG-2 je ztrátový datový komprimační formát. Místo komprimace jednotlivých snímků se v tomto formátu pracuje se sekvencemi snímků. Tento formát je často využíván ve spojení s proměnlivým datovým tokem (VBR), který je více vhodný pro některé scény na rozdíl od konstantního datového toku. MPEG-2 pracuje s rozlišením 720x576 pixelů a datový tok se pohybuje mezi 2 - 9.8 Mb/s.

V televizním vysílání jsou ve standardu MPEG-2 obvykle kódovány tzv. SD kanály, tedy kanály ve standardním rozlišení.

1.4.2 MPEG-4

MPEG-4 je standard pro kódování multimediálního obsahu a je nástupcem standardu MPEG-2. Jedná se o sadu povinností, které musí splnit komprimační algoritmy založené na tomto standardu. Na rozdíl od MPEG-2 algoritmy založené na MPEG-4 nekomprimují obraz jako celek, ale rozdělují ho na pozadí a na jednotlivé objekty. Ty jsou dále rozděleny do zakódovaných vrstev.

Standard obsahuje mnoho profilů rozdělených dle úrovně kvality obrazu. V případě přenosu televizního vysílání je pro IPTV nejzajímavější profil MPEG-

4 AVC, který umožňuje nahradit normu MPEG-2 a dovoluje rozlišení obrazu dosahující až 4096x2048 pixelů.

1.4.3 H.264

Jedná se o kompresní formát založený na standardu MPEG-4 AVC. Využívá se v televizním vysílání pro šíření kanálů ve vysokém i ve standardním rozlišení. V případě standardního rozlišení oproti MPEG-2 umožňuje efektivnější kompresi a tím i menší zatížení přenosových tras. Většina televizních HD kanálů je vysílána právě pomocí tohoto kompresního formátu.

1.5 Možnosti přenosu datových proudů přes IP síť

Metod šíření proudů v IP sítích existuje mnoho, v případě omezení na třetí vrstvu ISO/OSI modelu existují tři nejznámější možnosti šíření paketů od zdroje k cíli. Jedná se o velmi známý a téměř u všech aplikací využívaný unicast neboli jednosměrné vysílání. Druhým příkladem, který zde ale není uveden přímo je broadcast, který je běžně využíván pro vysílání v rámci jedné domény. Třetím méně známým způsobem je multicast neboli vícesměrové vysílání.

1.5.1 Unicast

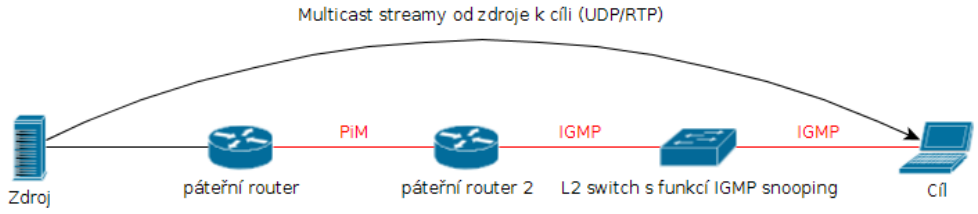
Jedná se o jednosměrné vysílání, které je naprosto běžné u většiny protokolů. Klient vždy naváže spojení se serverem a server odpovídá přímo jemu, klienta poté může rozpoznat například dle IP adresy a zdrojového portu. V případě přenosu televizního signálu tedy pro každého příjemce vysílač musí vyslat data odděleně. Z toho pramení velká zátěž pro síť i pro samotný vysílač.

1.5.2 Multicast

Multicast neboli vícesměrové vysílání je metoda posílání datagramů skrz počítačovou síť ke skupině více příjemců současně. Jednou linkou tedy vždy v ideálním případě prochází jeden datagram pro více příjemců. Současná verze internetového protokolu známá jako IPv4 vyhrazuje pro tento typ vysílání dle RFC 5771 [24] adresy typu D, tedy 224.0.0.0-239.255.255.255. Každou jednotlivou adresu z tohoto rozsahu je možné nazvat vícesměrovou skupinou.

Využívá se převážně k distribuci multimediálního obsahu, lze jej ale využít i například k rozeslání aktualizací a k dalším případům, kde se musí k více hostitelům dostat stejná data. Cílem zavedení této technologie je tedy snížit zátěž jak zdrojového uzlu, tak celé počítačové sítě. Pro přenos je využit protokol UDP.

Vybrané nejdůležitější rozsahy multicast IPv4 adres:



Obrázek 1.6: Nasazení „multicast protokolů“ v jednotlivých segmentech sítě

- Rezervovaný rozsah 224.0.0.0/24 je vyhrazen pouze pro lokální podsítě. Tyto adresy využívají i směrovací protokoly (OSPF, RIPv2)
- Administrativní rozsah 239.0.0.0/8 je vyhrazen pro vnitřní potřeby jednotlivých organizací. Příkladem je provoz IPTV v jednotlivých skupinách
- Veřejné adresy (Globally scoped adresses) jsou všechny zbývající. Jsou určeny pro provoz směrovaný napříč internetem. Například pro protokol NTP pracující v multicast režimu je vyhrazena adresa 224.0.1.1.

V IPv6 jsou definovány rozsahy pro tento typ vysílání také, nicméně tato diplomová práce se touto problematikou nezabývá.

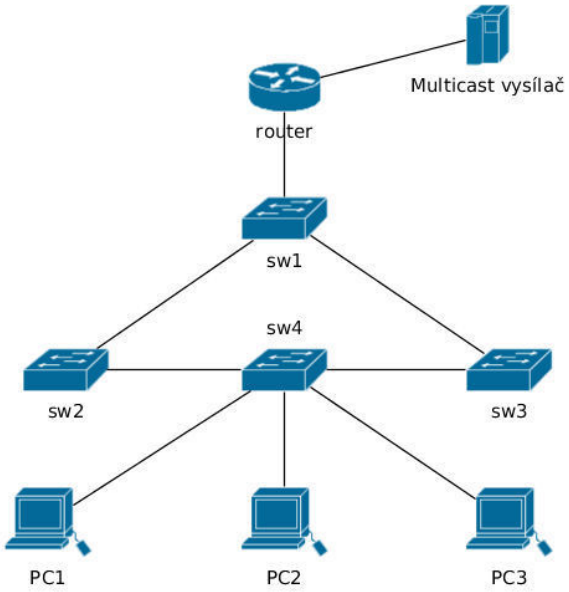
1.6 Protokoly a prostředky využité pro přenos vícesměrového vysílání

Ke správnému šíření vícesměrového vysílání lze využít mnoho protokolů, ty nejznámější jsou PiM a IGMP. Na obrázku 1.6 je možné vidět využití těchto protokolů v jednotlivých segmentech sítě.

1.6.1 MVR

Multicast VLAN registration (MVR) slouží především k úspoře a zabezpečení přenosů vícesměrového vysílání. Základem je dle [10] rozdělení stejného vícesměrového provozu do více VLAN. Díky tomuto protokolu je zavedena možnost existence členů jedné vícesměrové skupiny ve více VLAN. Místo nutnosti replikovat vícesměrový provoz do každé VLAN je tedy možné zasílat ten samý provoz pouze jednou.

Na obrázku 1.7 je mezi všemi přepínači aktivovaná funkce MVR se samostatnou VLAN určenou pro vícesměrový provoz. Zároveň jsou na SW4 připojené klientské počítače s vlastní VLAN. Pokud některý z počítačů odešle IGMP paket, SW4 tento paket přepošle pomocí multicast VLAN až k routeru. Následně router začne odesílat data, která switch přepošle z vícesměrové



Obrázek 1.7: Představení jednoduché sítě s nasazenou funkcí MVR

VLAN do klientské VLAN. Pokud by měl každý počítač vlastní VLAN a zároveň by se chtěl zaregistrovat do stejné vícesměrové skupiny, datový tok této skupiny by byl v multicast VLAN šířen jen jednou a switch by data přeposlal do každé soukromé VLAN.

V běžné situaci by router odesílal (pokud by měl každý počítač samostatnou VLAN) provoz skupiny do každé VLAN samostatně a odděleně.

1.6.2 PiM

Protokol Independent Multicast (PiM) je protokol pracující na třetí vrstvě ISO/OSI modelu. Je podobný protokolům OSPF nebo RIP, používá se ale ke směrování vícesměrového vysílání v IP sítích, tedy k distribuci datových toků od vysílače k jednotlivým přijímačům, nebo od mnoha vysílačů k mnoha přijímačům. Důležitou vlastností je nezávislost na jiných protokolech, které zajišťují směrování jiných typů provozu.

Každá vícesměrová skupina je pomocí PiM šířena a směrovače tak postupně získají cestu k šíření každé skupiny k příjemcům. Pro výměnu zpráv je použit všeobecně známý formát zpráv a komunikace mezi routery probíhá buď pomocí vícesměrového vysílání, nebo pomocí konkrétních adres využitých pro komunikaci.

Existují 4 režimy PiM, z nichž se nejčastěji využívá hustý režim nebo řídký režim.

1.6.2.1 Hustý režim (Dense Mode)

Protokol Independent Multicast-Dense Mode (PIM-DM) je popsán v RFC 3973 [20]. Preferuje šíření všech vícesměrových dat ve skupinách do částí sítě s tímto režimem. Pokud některá část danou multicast skupinu nepotřebuje, musí odeslat tzv. prune zprávu, díky které je následně posílání multicast paketů v dané skupině na nadřazeném routeru zastaveno. Dle [54] je režim vhodný pro pravidelný a konstantní datový proud dat na síti, kde jsou přijímače i vysílače blízko a je jich malý počet.

1.6.2.2 Řídký režim (Sparse Mode)

Protocol Independent Multicast-Sparse Mode (PIM-SM) je popsán v RFC 4601 [22]. Funguje opačným způsobem na rozdíl od PIM-DM. Obsahuje join a prune zprávy, díky kterým se nejdříve musí podřízený router k dané multicast skupině připojit (prune zprávou se zase od příjmu multicast skupiny odpojí). Aby vše fungovalo jak má, musí v síti existovat tzv. RP (*rendezvous point*), což je výchozí bod, který přijímá všechny možné dostupné skupiny. Z něho jsou poté k příjemcům jednotlivé skupiny posílány pomocí cest, které můžou být optimalizovány. Dle [54] je režim vhodný pro malý počet příjemců a vysílačů a pro nepravidelný datový tok.

1.6.2.3 Obousměrný režím (Bidirectional)

Protocol Independent Multicast-Bidirectional (PIM-Bidir) je specifikován v RFC 5015 [23]. Je velmi podobný řídkému režimu. Velký rozdíl je ale v možnosti vícesměrového vysílání mezi routery za RP, jelikož vytváří obousměrné stromy.

1.6.2.4 Režim specifický na zdroji (Source-specific multicast)

Protocol Independent Multicast - Source-Specific Multicast (PIM-SSM) je specifikován v RFC 3569 [19]. Vytváří strom, který začíná v jednom místě (zdroji). Přináší více zabezpečený a škálovatelný model pro omezené množství aplikací (hlavně pro vysílání obsahu). IP datagram je vyslán zdrojem S na koncovou adresu G. Přijímače můžou tento datagram přijímat pomocí přihlášení se do skupiny G s vynucením zdroje S.

1.6.3 IGMP

Internet group management Protocol (IGMP) je protokol rozšiřující možnosti protokolu IP o podporu některých funkcí sloužících vícesměrovému vysílání. Je použit k dynamickému přihlášení a odhlášení ze skupiny u směrovačů v lokální síti. Protokol umí od vyšších verzí vyřešit i situaci, kdy se v síti nachází více multicast vysílačů (v nižších verzích se počítá s pouze jedním směrovačem).

Existují 4 verze tohoto protokolu. V dnešní době se lze nejčastěji setkat s protokolem IGMP v2.

1.6.3.1 IGMP v0

IGMPv0 je definován v RFC 988 [25], tato verze se již dnes nepoužívá.

1.6.3.2 IGMP v1

IGMPv1 je definován v RFC 1112 [16].

Existují dva typy zpráv v IGMPv1:

- Host membership report - zpráva o členství ve skupině
- Host membership query - žádost o členství ve skupině

Router (*IGMP Querier*) předávající pakety vícesměrového vysílání slouží příjemci tak, že odesílá dotazy (*host membership query*) v pravidelných intervalech (ve výchozím nastavení každých 60 sekund) na již žádanou multicast skupinu. Hostitelé reagují na zprávu potvrzením, že danou skupinu odebírají (*host membership report*). Aby se předešlo velké záplavě zpráv, hostitelé odešlou informaci o odběru za náhodně vygenerovanou dobu (od 0 do 10 sekund). V případě, že v tomto intervalu zachytí jinou zprávu o členství ve stejné skupině, tak zprávu neodesílají.

Pomocí stejné zprávy se může hostitel přihlásit k odběru skupiny. V tomto případě zprávu odesílá hned a neprodleně. Veškeré zprávy o členství ve skupině probíhají přes vyhrazenou adresu 224.0.0.1, kterou přijímají všichni příjemci ve stejné podsíti.

IGMP v1 má několik omezení, která již dnes omezují jeho nasazení:

- Neexistuje zpráva, která by umožňovala příjemci opustit skupinu. To může způsobit velké vytížení sítě, pokud například účastník IP televize začne velmi rychle přepínat televizní kanály
- Definice protokolu neříká, jak je vybrán router posílající zprávy o členství ve skupině, pokud existuje více směrovačů vícesměrového vysílání v podsíti. Tyto zprávy odesílají všechny vícesměrové směrovače
- Žádosti o členství ve skupině směřují na všechny příjemce

1.6.3.3 IGMP v2

RFC 2236 [17] popisuje IGMP verzi 2. Přináší několik vylepšení:

- Žádosti o členství lze směřovat přímo na skupiny

- Definuje mechanismus volby směrovače vysílajícího zprávy o členství ve skupině
- Přidává maximální lhůtu pro odpověď na zprávy o členství ve skupině
- Přidává typ zprávy leave (možnost vynuceně opustit skupinu)

Žádosti o členství odeslané všem příjemcům ve skupině (*general membership query*) slouží ke zjištění všech multicast skupin, ve kterých jsou příjemci registrováni. Ta samá zpráva směřovaná na skupinu (*group-specific membership query*) slouží ke zjištění, jestli existuje příjemce dané skupiny.

Novinkou je zpráva o opuštění skupiny. Umožňuje mnohem rychlejší vyřazení příjemce ze skupiny a může tak ochránit část sítě před zahlcením. Zpráva je v tomto případě odeslána příjemcem na adresu 224.0.0.2 (všem směrovačům).

1.6.3.4 IGMP v3

Verze 3 je definovaná v RFC 3376 [18]. Nejdůležitějším vylepšením oproti verzi 2 je možnost žádat o členství ve skupině od konkrétního zdroje, nebo lze některé zdroje vyloučit. Nejen k tomu je určena variabilní délka IGMP paketu.

1.6.4 IGMP snooping

Jedná se o funkci nejčastěji podporovanou co do funkcí lépe vybavenými přepínači. Dle RFC4541 [21] funguje na principu odposlouchávání IGMP provozu mezi směrovačem a klientem. Díky tomu udržuje přepínač seznam portů, do kterých je potřeba doručit vybrané skupiny vícesměrového provozu.

Standardně se přepínač chová tak, že posílá vícesměrový provoz na všechny porty, kromě toho, ze kterého provoz přišel.
To může způsobit přetížení linky, případně přetížení zařízení zapojeného za linkou. IGMP snooping umožňuje tento provoz díky poslouchání protokolu IGMP doručovat přepínačem jen na rozhraní, na kterých je daná vícesměrová skupina žádána. IGMP snooping pracuje na druhé vrstvě, ale ke své funkci využívá informace z třetí vrstvy v hlavičce paketu.

Existují dva druhy implementací:

- Proxy zprávy (Proxy reporting)
- IGMP tazatel (IGMP querier)

1.6.4.1 Proxy reporting

Přepínač aktivně filtruje IGMP pakety za účelem snížení počtu dotazů na směrovač. Vytvoří tak pro směrovač zdání, že je směrem k němu pouze jeden příjemce, přestože jich může být i více. Pokud jsou za přepínačem dva přijímače a jeden se odhlásí, pak se směrovači neodesílá žádná informace. V následujícím dotazu směrovače na členství ve skupině přepínač propustí informaci od posledního zbylého přijímače ve skupině, že je členem dané skupiny, aby provoz nevypnul.

1.6.4.2 IGMP Querier

V tomto případě se přepínač chová přímo jako vícesměrový směrovač a agreguje tak veškerý IGMP provoz. IGMP provoz od přijímačů je přijat přepínačem a vyhodnocen. Ten si poté sám řídí komunikaci s multicast směrovačem (nefiltruje tak pakety, ale sám si je tvoří).

1.6.5 QoS

QoS (v překladu kvalita služeb) je dle [73] termín zahrnující řízení datových toků. Je podporován velkým množstvím síťových zařízení. Pokud je výstupní rozhraní těchto zařízení obsazeno a probíhá tedy skrz něj jiná komunikace, výstupní rámec se uloží do vyrovnávací fronty a přenos se tak zpozdí. Pokud je fronta plná, je rámec vyřazen nebo ztracen. Právě způsobem užití front se zabývají QoS mechanismy.

Typickými problémy při přenosu rámců jsou:

- Přeuspořádání - rámce dorazí v jiném pořadí, než byly vyslány
- Chyba při přenosu - nesouhlasí výsledný kontrolní součet některého rámce
- Zpoždění při přenosu - rámce dorazí pozdě
- Ztráta při přenosu - rámce nedorazí všechny
- Přetížený přenosový kanál - kanál nepojme všechny rámce

Pro přenos IPTV je v případě přenosu pomocí síťového protokolu UDP zásadním problémem ztráta paketů, přenosová rychlost, chyba při přenosu a přeuspořádání. Úkolem QoS je minimalizovat tyto problémy při přenosu. Protokol TCP se dokáže s omezeným počtem chyb vypořádat a přenos je tak mnohem méně náchylný na všechny neduhy UDP.

1.6.5.1 802.1p

Tato specifikace dle [15] umožňuje síťovým prvkům upřednostňovat některé typy paketů před jinými. Je implementována v druhé (MAC) vrstvě. Hlavička každého rámce obsahuje tříbitové pole pro priorizaci, která umožňuje rozdělit provoz do tříd. IEEE vydalo doporučení, do jaké třídy každý typ provozu spadá. Díky tříbitovému poli je možné rozdělit provoz na 8 stupňů priority. Nejvyšší priorita je 7, do které by měl spadat pro síť kritický provoz (například data protokolu RIP nebo OSPF). Hodnoty 5-6 jsou vyhrazeny pro provoz náchylný na zpoždění, tedy pro video a hlas. Hodnoty 1-4 jsou vyhrazeny pro protokoly, které se můžou se ztrátou některých dat vypořádat. Hodnota 0 je standardní a je využita, pokud žádná jiná hodnota není nastavena.

1.6.5.2 Odlišené služby (Differentiated services)

Rozdělené služby jsou dle [51] definovány v IP hlavičce paketu. Pole o šesti bitech je podobné u protokolu IPv4 i IPv6, v případě IPv4 se nazývá tzv. *DiffServ*, v případě IPv6 se nazývá třída dopravy (*Traffic Class*). U IPv6 jsou navíc přidány 2 bity (je tedy osmibitové), nicméně dva nejvýznamnější bity nejsou zatím využity. Lze tedy rozeznat až 64 (případně 256) různých typů provozu. Na základě obsahu těchto polí je možné řídit datové toky v síti.

Na vstupu do sítě prvek (případně rovnou vysílatel paketu) vyplní pole hodnotou (doporučené hodnoty polí jsou například popsány na stránkách tucny.com [64]). Všechny prvky v cestě s aktivovanou funkcí DSCP QoS poté v případě správného nastavení obsah tohoto pole přečtou a dle vlastního nastavení tyto pakety rozdělí do různých front. Fronty jsou poté dle nastavení odbaveny (odeslány dále k cíli). Některé přednostně, jiné se zpožděním.

Kapitola 2

Analýza způsobu nasazení IPTV

V této části bude představeno aktuální schéma sítě, ve které bude IPTV nasazena. Budou vybrány referenční lokality s důrazem na různorodost, aby bylo možné službu nasadit do různých prostředí na různá místa a aby byl provoz otestován přes různé technologie. Na konci kapitoly budou zváženy možnosti nasazení do popsané počítačové sítě a bude vybráno jedno z řešení.

2.1 Představení sítě

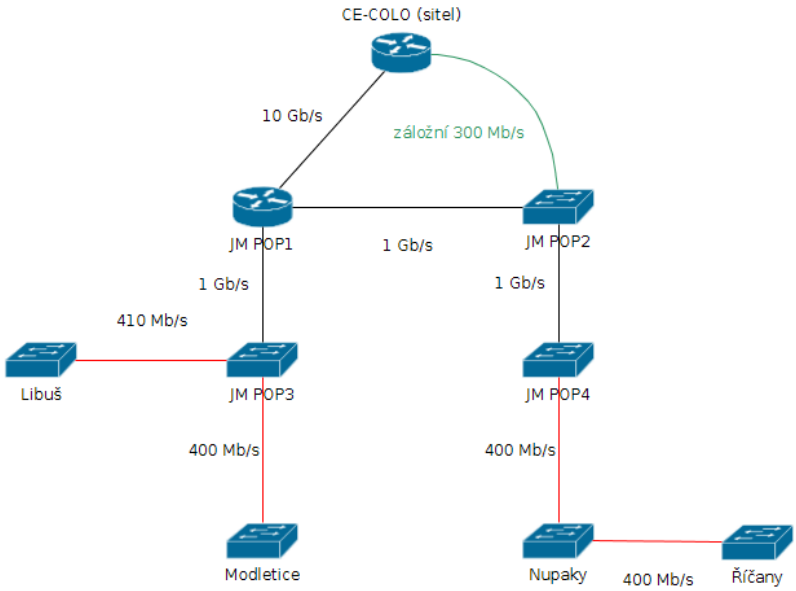
Počátek sítě, do které se řešení nasazuje, sahá až do roku 2002. Na začátku šlo o velmi malou síť spravovanou několika nadšenci. Jejich počet se ale každý měsíc zvyšoval a síť tak postupně rostla. Od počátku svého fungování nebylo využito žádného grantu ani finanční injekce ze strany státu nebo Evropské unie. Celkový rozvoj sítě byl financován výhradně z členských příspěvků postupně rostoucí členské základny.

Ke konci roku 2009 došlo k raketovému vzestupu počtu připojených členů převážně díky přechodu na optické okruhy a profesionální technologie. Od tohoto roku se počet členů každoročně zdvojnásobuje.

Síť byla původně stavěna jako čistě bezdrátová. V posledních dvou letech prošla organizace raketovým vývojem v oblasti kabelových LAN připojení. Jednotlivé koncové domy jsou v některých oblastech připojeny dokonce pomocí optických vláken, jinde pomocí profesionálních bezdrátových spojů.

Aktuální potenciál je veliký, je ale několik aspektů, které jej brzdí. Předně je to nedostatek kvalifikovaných osob. Vzhledem k velkému rozvoji kabelových sítí je ale nutné nabídnout i jiné možnosti než jen připojení k síti.

Pro mnoho současných připojených uživatelů je kabelová televize nutností a tak se krom běžných možností rozhodlo spustit možnost televize IPTV. Díky tomu bylo možné celé navrhované řešení v praxi vyzkoušet a přidat k této práci i praktickou část.



Obrázek 2.1: Mapa páteřní sítě

2.1.1 Páteřní síť

Páteřní síť se skládá z L3 přepínačů, v některých případech pouze L2 přepínačů a směrovačů. Prvky jsou propojené datovými okruhy, případně kabely založenými na technologii ethernet. Na obrázku 2.1 je vidět zjednodušené schéma sítě, červeně je vyznačena distribuční část sítě. Zelenou barvou je označen záložní okruh.

Jako L3 přepínače jsou v síti použity prvky od firmy Juniper Networks, konkrétně typy EX2200, EX3200 a EX3300. Podporují veškeré funkce potřebné pro přenos IPTV sítí.

V páteřní síti se nachází také přepínače pracující na druhé vrstvě, a to od výrobce Edge-Core Networks. Konkrétním zástupcem je Edge-Core ES4528V. Taktéž jako předchozí přepínače podporuje funkce potřebné pro přenos IPTV na druhé vrstvě.

V některých místech páteřní sítě jsou nasazeny i routery, a to buď počítače s operačním systémem GNU/Linux, nebo routery s označením Routerboard nebo Cloudcore router s operačním systémem MikroTik RouterOS. Tyto routery zastávají funkce směrovačů na místech, kdy je v páteřní síti k dispozici pouze L2 switch. Tento způsob je nasazen hlavně kvůli finanční optimalizaci, jelikož cenový rozdíl mezi L2 a L3 přepínači je znatelný.

2.1.2 Distribuční síť

Na každém distribučním bodě se nachází router se systémem GNU/Linux nebo MikroTik RouterOS v kombinaci s přepínačem Edge-Core ES3528M. Dále je distribuční síť tvořena bezdrátovými propoji o kapacitě až 660 Mb/s nebo optickými propoji o kapacitě 1 Gb/s. Tato část sítě může být problematická vzhledem k přenosu IPTV hlavně kvůli menší propustnosti a zároveň kvůli možným povětrnostním vlivům na bezdrátové spoje.

2.1.2.1 Bezdrátové spoje s plně duplexním přenosem

Dle [71] se jedná o spoje používající párové kanály (vysílací kanál je rozdílný od přijímacího).

2.1.2.2 Alcoma MPxx

Síť využívá několika FOD[2] spojů od renomovaného českého výrobce Alcoma a.s. Tento výrobce vyrábí zařízení do různých frekvenčních pásem [3], v síti nasazení jsou využity převážně spoje vysílající ve volných pásmech 10 GHz a 17 GHz. Nejnovější typy spojů plně podporují fronty a priorizaci vybraného provozu. Zajímavou vlastností je možnost rozdělit provoz do dvou kanálů o určených rychlostech (lze například pro IPTV vyhradit přenosový kanál o určené kapacitě) [1]. Fotografii antény je možné vidět na obrázku 2.2.

2.1.2.3 Orcave 1S10

Jedná se o spoj od českého výrobce Miracle Group, spol. s.r.o. operující ve volném pásmu 10 GHz o maximální kapacitě 200 Mb/s [42]. Tento spoj dle specifikací uvedených na stránkách výrobce [41] nepodporuje priorizaci provozu, takže v případě možných přenosů IPTV přes tento spoj se mohou vyskytnout problémy při společném provozu s běžnými daty. Fotografii spoje lze včetně antény od švédského výrobce Arkivator vidět na snímku 2.3 (jedná se o anténu vespod, která míří směrem doprava).

2.1.2.4 Ericsson Mini-Link

Spoje od firmy Ericsson [11] využívají ve velkém mobilní operátoři po celém světě [12]. V síti je nasazeno několik spojů operujících v licencovaných pásmech 11 GHz a 32 GHz jako IDU-ODU[3] řešení s vnitřní jednotkou Ericsson CN500. Tento spoj podporuje upřednostnění vybraného provozu (QoS). Maximální kapacita spoje v případě sítě nasazení je 400 Mb/s. Fotografii ODU části

[2] Full-outdoor spoje nemají vnitřní jednotku, spoj je připojen pouze datovým kabelem a napájením a je umístěn přímo na stožár.

[3] Zařízení je umístěné uvnitř (IDU), venku je obvykle pomocí koaxiálního kabelu zapojena venkovní (ODU) jednotka.

Obrázek 2.2: Bezdrátový spoj Alcoma MP600

spoje s anténou od firmy Andrew je možné najít na obrázku 2.4 (anténa dole na obrázku).

2.1.2.5 UBNT AirFiber

Jedná se o nový FOD produkt, který ke svojí funkci využívá volné pásmo 24 GHz. Výrobcem je Americká společnost Ubiquiti Networks. V síti je osazeno několik spojů do některých lokalit, ve kterých může být poptávka po televizi. Maximální kapacita spoje je při aktuální maximální modulaci 64QAM [53] až 700 Mb/s. Testy provedené sdružením Internet pro všechny [34] zavrhují možnost bezproblémového vícesměrového provozu přes tento spoj, v rámci práce ale bude provoz IPTV přes tento spoj vyzkoušen. Zařízení je možné vidět uprostřed obrázku 2.5. Zvláštností jsou dvě antény, kde výrobce využil jednu na příjem a druhou na vysílání.

Obrázek 2.3: Fotografie spoje Orcave 1S10

Obrázek 2.4: ODU část spoje Ericsson

Obrázek 2.5: Bezdrátový spoj UBNT AirFiber

2.1.2.6 Poloduplexní bezdrátové spoje

Dle [71] se jedná o spoje využívající pouze jeden vysílací kanál pro obousměrnou komunikaci.

2.1.2.7 Siklu EtherHaul 1200TL

FOD spoj Siklu EtherHaul vyrobený izraelskou společností Siklu Communication Ltd. operuje v pásmu 80 GHz [55]. Maximální přenosová rychlost je 700 Mb/s. Jedná se ale o agregovanou rychlost. Kapacita se tedy musí rozdělit mezi oba směry v různých poměrech (90:10, 75:25, 50:50, 25:75 nebo 90:10). Upřednostnění vybraného provozu je tímto spojem podporováno. Na obrázku 2.6 dole je možné vidět osazený spoj v provozu.

2.1.3 Koncová síť

Koncová síť se skládá z domovních rozvodů (ty můžou být připojeny bezdrátově), případně z klientů připojených na bezdrátový vysílač pomocí antény. Pouze na vybraných koncových bodech se nachází routery se systémem MikroTik RouterOS.

Pokud je uživatel napojen pomocí kabelu, jedná se zpravidla o strukturovanou kabeláž ve formě kroucené dvoulinky kategorie 5e nebo 6 technologie

Obrázek 2.6: Bezdrátový spoj Siklu EtherHaul 1200TL

ethernet. Další možností je optický kabel až do bytu, kde je zpravidla využit opticko-metalický převodník.

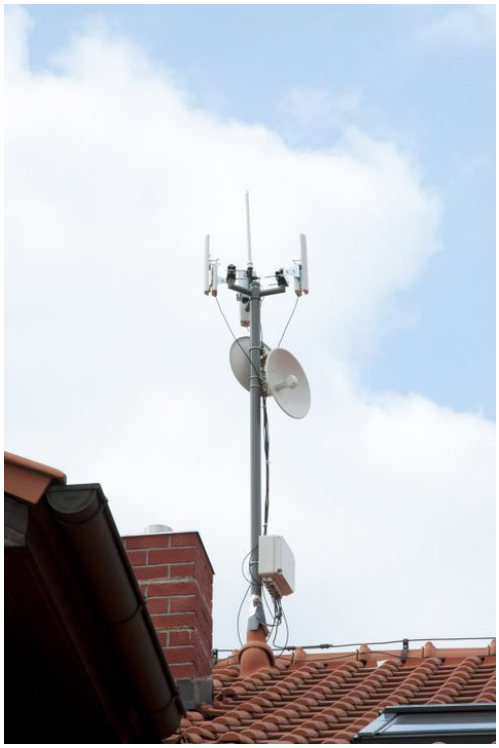
Jako koncové antény jsou využity prvky od firmy Ubiquiti Networks operující v pásmu 5 GHz s podporou uzavřeného protokolu AirMAX [68], který umožňuje spravedlivé rozdělení kapacity vysílače díky metodě přístupu k médiu TDMA.

Jednotlivá zařízení dokážou fungovat jako přístupový bod, nebo klient. Některé antény jsou určené pro přímý spoj bod-bod. Na fotografii 2.7 je možné vidět bezdrátový vysílací bod. Na vrchu stožáru jsou vidět tři sektorové antény se zařízením UBNT Rocket M5 (slouží spojení bod-více bodů). Dále jsou pod sektorovými anténami zařízení UBNT Nanobridge M5 pro spoje bod-bod.

Jako koncové přepínače jsou využity výroby od firmy Edge-Core Networks, a to převážně přepínače ES3528M. Dále jsou v síti nasazeny přepínače od firmy HP s označením HP V1900-8G. Nakonec jsou v některých domech umístěny také obyčejné prvky bez jakékoliv formy managementu, například výrobek ZyXEL ES-108A.

2.2 Vybrané referenční lokality

V síti byly vybrány některé referenční lokality, které jsou výjimečné z pohledu technologického řešení. Těmto lokalitám bude v dalších částech této práce věnován velký zřetel, neboť v každé z nich bude IPTV nasazena.



Obrázek 2.7: Bezdrátový vysílač s technologiemi UBNT řady M

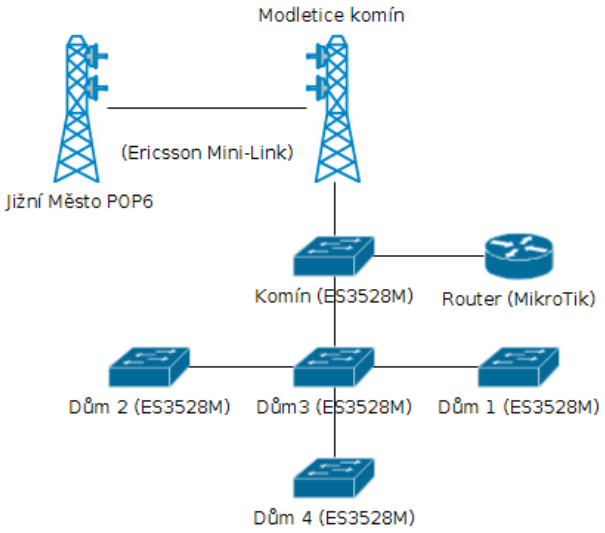
2.2.1 Modletice

V Modleticích je provozována optická síť mezi všemi panelovými domy v obci. Na komíně na obecním zámku se nachází páteřní spoj Ericsson Mini-Link, kterým je celá oblast propojena s jedním z hlavních bodů na Jižním Městě. V jednom z domů se nachází páteřní rozvaděč, ze kterého jsou napojené ostatní budovy pomocí optického vlákna. Dále se zájemci můžou připojit prostřednictvím bezdrátového vysílače, který je umístěn na komínu zámku a pokrývá široké okolí. V každém bodě je umístěn přepínač Edge-Core ES3528M s připojenými byty pomocí strukturované kabeláže. Směrování celé oblasti má na starost centrální prvek Routerboard s operačním systémem MikroTik RouterOS.

Na obrázku 2.8 je vyobrazena mapa sítě. Místním specifikem je optická síť FTTB za bezdrátovým spojem Mini-Link. Oblast nedisponuje kapacitní záložní linkou do optické sítě skrz jinou oblast.

2.2.2 Říčany

Říčany jsou nově napojenou lokalitou. V každém domě je umístěn switch Edge-Core ES3528M, do kterého je zapojena strukturovaná kabeláž vedoucí do bytů. Všechny linky jsou svedeny do hlavního bodu, ve kterém je zároveň umístěn



Obrázek 2.8: Mapa sítě v Modleticích

směrovač s operačním systémem MikroTik RouterOS. Hlavním specifikem oblasti je napojení na oblast Nupaky, která je zároveň také připojena bezdrátovým spojem. Připojení oblasti zajišťuje bezdrátový spoj UBNT AirFiber na vzdálenost 4 km díky retranslaci[4], což je zároveň další její specifikum. Posledním specifikem je i připojení jednoho domu prostřednictvím bezdrátového spoje UBNT řady M.

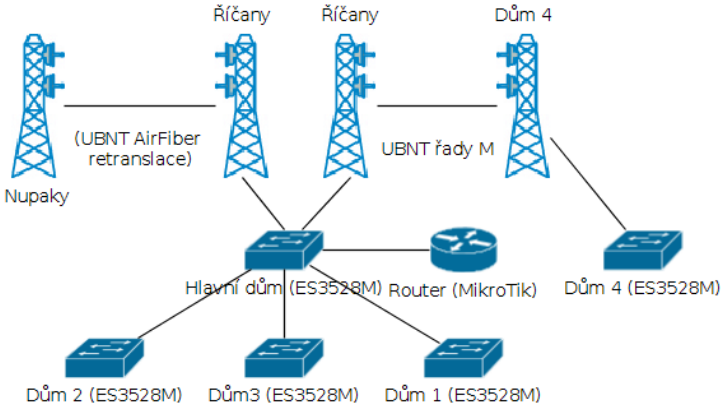
Mapa sítě je viditelná na obrázku 2.9. V plánu je umístění záložního bezdrátového spoje, který bude propojen přímo do páteřní sítě na Jižní Město pro utvoření kruhové topologie pro oblast Říčan a Nupak.

2.2.3 Nupaky

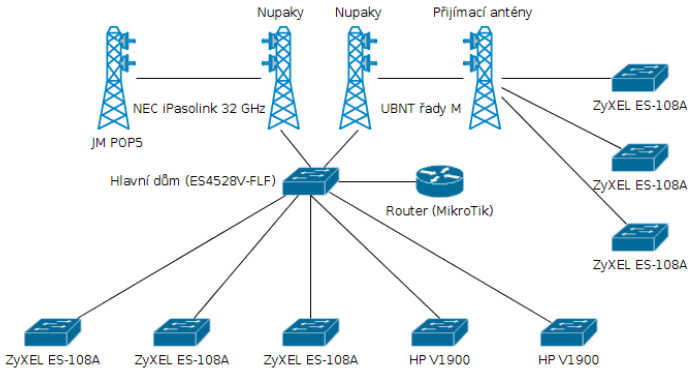
Nupaky jsou tranzitní oblastí pro další část sítě a zároveň oblastí koncovou. Síť v oblasti disponuje páteřním přepínačem Edge-Core ES4528V-FLF. V domech jsou umístěny přepínače HP V1900 a ZyXEL ES-108A z důvodu menšího počtu obyvatel domů. Domy jsou spojeny optickým kabelem nebo bezdrátovými spoji UBNT řady M.

Specifikem oblasti je použití přepínačů od firem HP a Zyxel a zároveň využití bezdrátového spoje NEC iPasolink. Mapu sítě je možné vidět na obrázku 2.10.

[4]Retranslace je využití dvou a více bezdrátových spojů v řadě za sebou za účelem překlenutí velké vzdálenosti nebo za účelem vyhnutí se překážce.



Obrázek 2.9: Mapa sítě v Říčanech



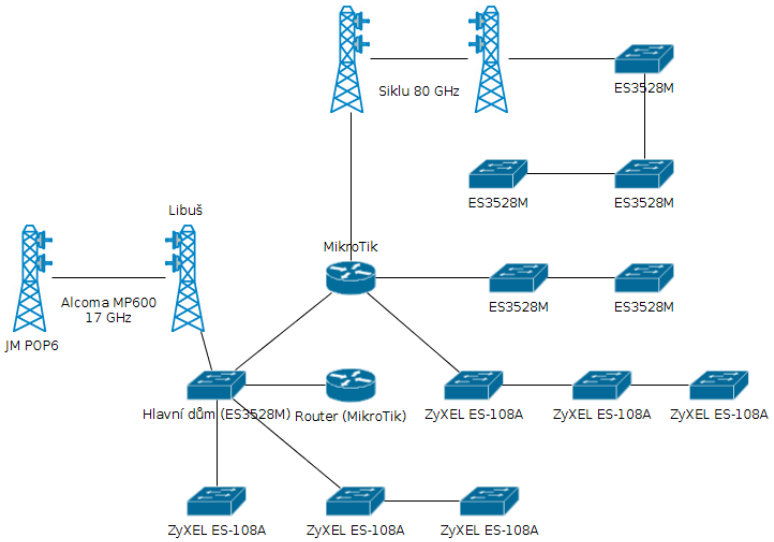
Obrázek 2.10: Mapa sítě v Nupakách

2.2.4 Praha 4 - Libuš

Celá lokalita Praha 4 - Libuš je připojena pomocí mikrovlnného spoje Alcoma MP600 v bezlicenčním pásmu 17 GHz s maximální rychlostí 410 Mb/s. V lokalitě se nachází několik optických propojů a také spoj Siklu.

V některých domech ještě není připravena strukturovaná kabeláž a je v jejich případě využito přepínačů bez vzdálené správy. Během psaní této diplomové práce probíhaly intenzivní práce na revitalizaci těchto rozvodů, aby mohla být IPTV dostupná i zde. Mapa sítě je na obrázku 2.11.

V již rekonstruovaných a nově budovaných koncových sítích v Libuši jsou umístěny přepínače Edge-Core ES3528M.



Obrázek 2.11: Mapa sítě v pražské Libuši

2.3 Možné metody šíření vícesměrového vysílání

V této části jsou popsány metody nasazení IPTV ze síťového hlediska. Jednotlivé metody lze vzájemně kombinovat (například v některém uzlu sítě lze využít MVR a dále, kde to již (například z technického hlediska) není možné již stačí využít samostatnou multicast VLAN. Zároveň je multicast routing obvykle využit při předání služby od velkoobchodního partnera, může ale být nasazen i přímo v síti.

2.3.1 Multicast routing

Základem této topologie je využití všech routerů pro přímé směrování multicast provozu sítí. Každý router musí tento typ provozu směrovat buď staticky, nebo dynamicky například pomocí protokolu PiM.

Výhody:

- Jednoduché nasazení (stačí rozšířit směrovací tabulky prvků)

Nevýhody:

- Velká zatěž směrovačů
- Menší bezpečnost v případě použití stejné VLAN pro internetový i televizní provoz
- Možné ovlivnění stability set-top-boxů

Druhou možností je pro vyšší zabezpečení možnost z každého routeru nakonfigurovat samostatnou VLAN do každé podsítě, znamenalo by to ale ohromné množství VLAN v síti.

2.3.2 Využití MVR a oddělených multicast VLAN

MVR je vhodné nasadit v případě rozdělení VLAN vyhrazené pro IPTV, pokud směrem od routeru budou rozdělené VLAN procházet některým rozhraním společně.

Výhody:

- Možné rozdělení IPTV sítě do více VLAN se stejnou zátěží linek jako v případě jedné velké VLAN. Z toho vyplývá větší úroveň zabezpečení

Nevýhody:

- Nutná podpora MVR u všech přepínačů v síti pro efektivní nasazení
- Větší složitost při nasazení (různá čísla VLAN v různých částech sítě)

Tuto metodu je vhodné využít na místech, kde není možné rozdělit IPTV VLAN do více VLAN z důvodu absence směrovače v některém z uzlů pomocí metody multicast routing.

2.3.3 Samostatná multicast VLAN

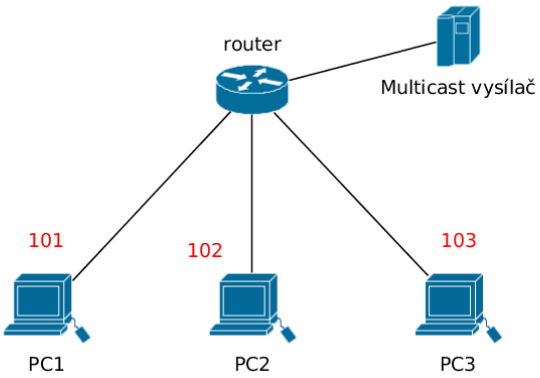
Tato metoda funguje na principu samostatné VLAN (případně více VLAN) šířených z některého místa sítě (zpravidla z některého hlavního páteřního bodu). Tento bod vykonává funkci směrovače, vysílá do koncové sítě DHCP pro jednotlivé klientské set-top-boxy a má zapnutou funkci IGMP. Tento bod zná cestu k jednotlivým multicast skupinám (zdrojům) například pomocí protokolu PiM. Pomocí protokolu IGMP poté jednotliví klienti žádají o příjem jednotlivých skupin.

Na obrázku 2.12 je možné vidět zjednodušenou síť. Jednotlivá PC nahrazují části sítí, ve kterých se každá samostatná VLAN šíří. Pro každou část sítě tedy bude existovat vlastní VLAN sloužící k přenosu IPTV (paralelně k ní bude existovat například VLAN s internetem).

Výhody:

- Velká škálovatelnost (VLAN lze rozdělit)
- Vhodné pro nasazení do středně velkých sítí, u velkých lze škálovat

Nevýhody:



Obrázek 2.12: Ukázka samostaných IPTV VLAN v síti

- V případě využití škálovatelnosti je nutný směrovač v každém uzlu, kde se provede rozdělení na více VLAN
- Menší bezpečnost sítě, v případě nedostatečného nastavení zabezpečení na přepínačích může problém v jedné VLAN ohrozit stabilitu celé sítě

2.4 Volba technologie

Jelikož většina platforem podporuje podobné funkce, bylo přihlédnuto k obchodnímu hledisku. Zároveň pro optimalizaci přenosových tras bylo zamítnuto řešení pomocí jednosměrného vysílání z důvodu možného přetížení sítě. Byla tedy vybrána k nasazení virtualizovaná platforma Nangu.TV od jednoho z předních českých poskytovatelů.

Jako metoda šíření IPTV sítí byla zvolena samostatná multicast VLAN s tím, že v páteřní části sítě může být využito směrování multicastového provozu. Tato metoda byla zvolena hlavně díky jednoduchému a přehlednému nasazení. Jelikož v síti nebude velké množství klientů (do 500 v prvních dvou letech), není nutné IPTV VLAN rozdělovat na více VLAN. Doporučením do budoucna je v případě rostoucího počtu IPTV klientů tuto VLAN rozdělit na prvcích postupně od zdroje.

Příkladem je možné ukončení IPTV místo v propojovacím centru (CE-COLO) až na bodu JM POP1 (viz. obrázek 2.1), kde lze na POP2 a POP4 VLAN rozdělit (mezi prvkem v CE-COLO a JM POP1 může být spuštěn protokol PiM). Díky funkci VLAN translation [38] v přepínači Juniper není potřeba rekonfigurace dalších prvků, jelikož lze skrz obě rozhraní posílat jinou VLAN se stejným číslem.

Výhodou je hlavně přehlednější nasazení (nebude nutné v každé oblasti konfigurovat jiné číslo VLAN pro IPTV). Dále také přehledná možnost zá-

lohy samostatné VLAN prostřednictvím protokolu spanning-tree skrz záložní okruh.

Kapitola 3

Nasazení IPTV

Praktická část nasazení IPTV obsahuje kompletní souhrn nasazení technologie včetně klientských směrovačů, kterým byl dán v této práci velký prostor vzhledem k implementaci vlastního cenově dostupného řešení.

3.1 Konfigurace páteřní sítě

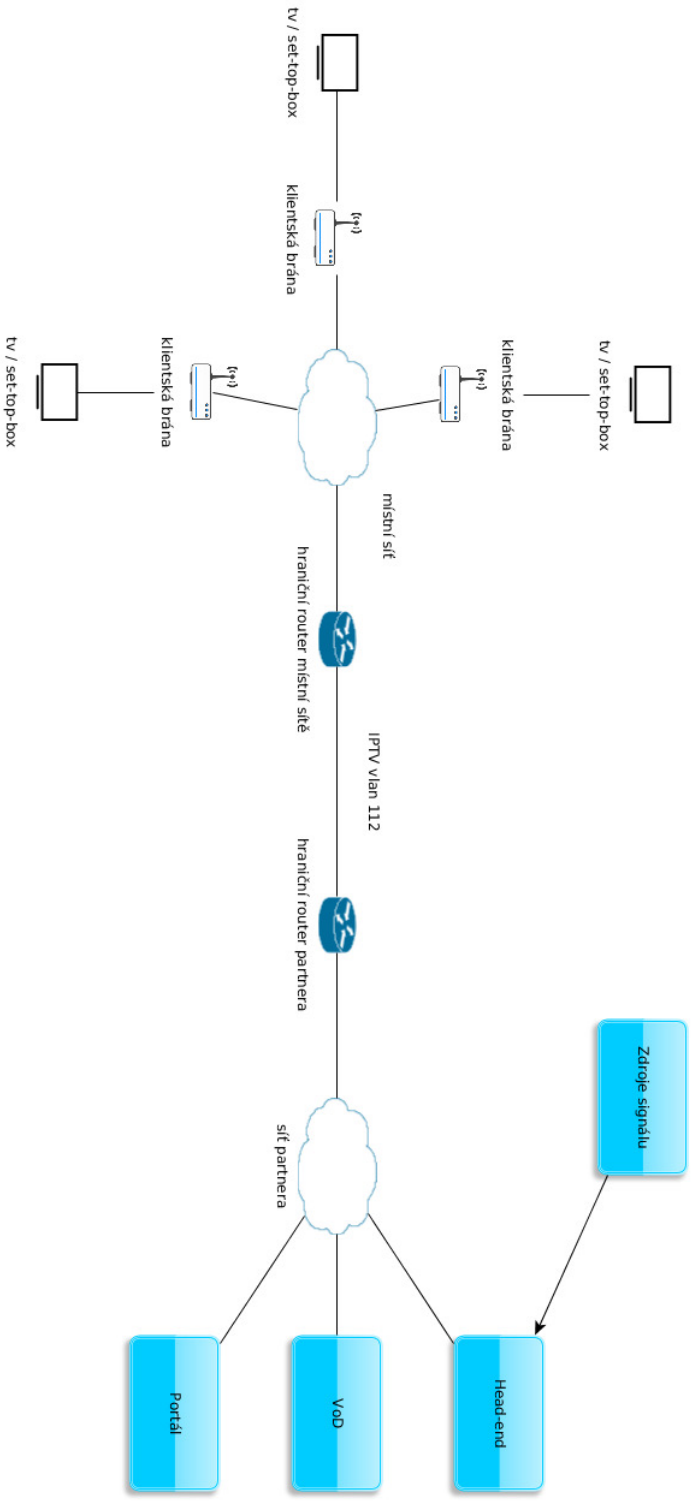
Pro nasazení IPTV bylo nutné nejdříve zřídit propojení mezi sítí provozovatele platformy a sítí nasazení. K tomuto účelu bylo vhodné zřídit propojení v některém z propojovacích center v České republice. Nutností bylo hledat takové centrum, ve kterém budou mít obě sítě vlastní technologie.

Došlo tedy k propojení sítí v jednom z kolokačních center v Praze ethernetovým kabelem s kapacitou 1 Gb/s. Propojení bylo zakončeno v přepínači, který byl umístěn přímo v propojovacím centru, vše je možné vidět na obrázku 3.1. Jsou zde vidět dva směrovače, které zajišťují komunikaci mezi sítěmi. Oba jsou umístěny v datovém centru.

Jelikož pro přenos všech poskytovaných datových proudů byla vyžadována kapacita větší než 1 Gb/s a zároveň na předávací části sítě byla využita metoda multicast směrování (viz. 2.3.1), bylo nutné využít na předávacím směrovači protokol PiM v hustém režimu (viz. 1.6.2.1). Směrovač si následně řídil vypnutí a zapnutí příjmu jednotlivých příchozích vícesměrových skupin pomocí protokolu IGMP.

3.1.1 Nastavení směrování vícesměrového vysílání na hraničním přepínači

Příjem IPTV a komunikace s poskytovatelem probíhá prostřednictvím samostatného rozhraní ge-0/0/1 na VLAN 112. V síti je pro uživatele IPTV využita VLAN 111.



Obrázek 3.1: Ukázka propojení se sítí provozovatele IPTV platformy

Byly tedy nakonfigurovány VLAN na jednotlivá rozhraní včetně nastavení IP adres pro komunikaci. Následně bylo provedeno nastavení protokolu PiM v režimu dense. Okomentovaný seznam příkazů je možné nalézt v příloze A.3.

Po aktivaci příkazů již prvek navázal komunikaci se směrovačem partnera pomocí protokolu PiM.

```
switch> show pim neighbors

B = Bidirectional Capable, G = Generation Identifier
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: PIM.master
Interface  IP V  Mode   Option  Uptime          Neighbor addr
vlan.112   4  2         HPLG    0d 00:10:11     172.1.1.1
vlan.112   4  2         HPLGT   0d 00:10:11     172.1.1.2
vlan.112   4  2         HPLGT   0d 00:10:11     172.1.1.3
```

Směrovací tabulka byla také pozměněna (jedná se jen o část tabulky).

```
switch>show route

inet.1: 238 destinations, 238 routes (238 active, 0 holddown,
0 hidden)
+ = Active Route, - = Last Active, * = Both
239.1.163.1,172.16.1.1/32*[PIM/105] 00:02:45
                        Multicast (IPv4) Composite
239.1.163.2,172.16.1.1/32*[PIM/105] 00:02:45
                        Multicast (IPv4) Composite
239.1.163.3,172.16.1.1/32*[PIM/105] 00:02:45
                        Multicast (IPv4) Composite
239.1.163.4,172.16.1.1/32*[PIM/105] 00:02:45
                        Multicast (IPv4) Composite
```

V tuto chvíli již byla vícesměrová komunikace funkční. K tomu, aby byla funkční i jednosměrná komunikace bylo nutné aktivovat statické směrovací pravidla do partnerské sítě, aby jednotlivé IPTV přijímače mohli komunikovat přímo s platformou.

3.1.2 Označení příchozího provozu pomocí vyplnění DSCP pole

Kvůli upřednostnění datových toků v síti bylo nutné na hraničním přepínači spustit přepisování DSCP pole. Díky této funkci bylo možné v síti oddělovat jeden typ provozu od druhého a zároveň IPTV provoz upřednostňovat. Funkci DSCP QoS poté podporuje většina přepínačů a bezdrátových spojů. Konkrétní nastavení přepínačů je uvedeno v příloze A.3.2.

3.1.3 Nastavení QoS na přepínačích

Díky označení na hraničním prvku lze postupně v síti upřednostnit vybraný provoz. V přepínačích Juniper nasazených na páteřních trasách toto opatření umožní v případě zahlcení linky dávat přednost IPTV provozu před jinými druhy provozu. Nastavení je uvedeno v příloze A.3.3.

3.2 Nastavení bezdrátových prvků

Jelikož bylo nutné nastavit pro upřednostnění provozu i bezdrátové spoje, jsou tato nastavení v práci také uvedena.

3.2.1 AirFiber

Tento bezdrátový spoj podporuje priorizaci provozu. Jednotlivá priorizační pravidla jsou již přednastavena dle tabulky uvedené na stránkách výrobce [65].

3.2.2 UBNT zařízení řady M

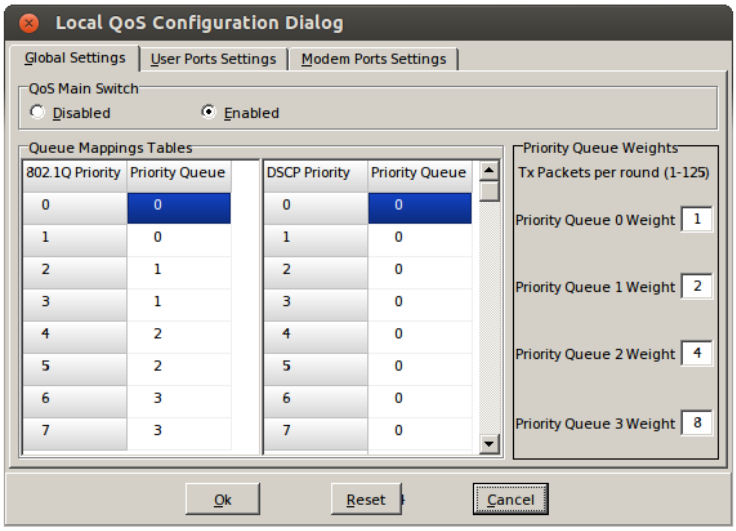
Ke konfiguraci spojů řady AirMAX je doporučeno webové rozhraní. Spoje mají od výrobce implementován QoS staticky dle stránky [66]. Zároveň je nutné dle dokumentu [67] pro umožnění průchodu vícesměrového vysílání ve spoji aktivovat na webu v záložce *advanced* položku *Multicast Data* a pro optimalizaci přenosů také *Multicast Enhancement*. Druhá zmiňovaná položka je využita pouze v případě, kdy jednotky fungují v režimu přístupového bodu a je přes ně připojeno více klientů do sítě. Funkce zařizuje, že jednotky simulují chování podobně jako IGMP snooping na přepínačích (provoz vícesměrových skupin je předáván pouze ke stanicím, které jej žádají).

3.2.3 Alcoma MPxx

K nastavení bezdrátových spojů Alcoma se využívá program ASD [2]. U těchto spojů je možné průchodu IPTV spojem dosáhnout dvěma způsoby, které lze i kombinovat.

Pokud je k dispozici svorkovnice s více rozhraními, lze rozhraní na obou stranách propojit, aby se z uživatelského pohledu tvářily jako více linek. Prostřednictvím systému *ASD client* lze mezi linky rozdělit kapacitu spoje.

Druhým způsobem je možnost aktivovat DSCP QoS, který spoj přímo podporuje. Po stisknutí tlačítka *set* v rozbalovacím menu je nutné vybrat záložku *QoS Properties*. V tomto menu, které je zobrazeno na obrázku 3.2, je nutné zapnout *QoS Main Switch*. Následně již jsou jednotlivé fronty předkonfigurovány.



Obrázek 3.2: Nastavení QoS u bezdrátového spoje Alcoma

3.2.4 Siklu

Spoje Siklu využívají k nastavení vlastní java aplikaci (případně CLI). Pro nastavení priorit bylo nutné dle příručky [55] nastavit striktní priority.

```
EH-1200L>set scheduler mode strict-priority
```

Dle modelu *strict-priority* spoj rozřazuje jednotlivé druhy provozu na základě hlavičky CoS, následně vždy odbavuje fronty od té s nejvyšším číslem k té s nejnižším.

3.2.5 NEC iPasolink

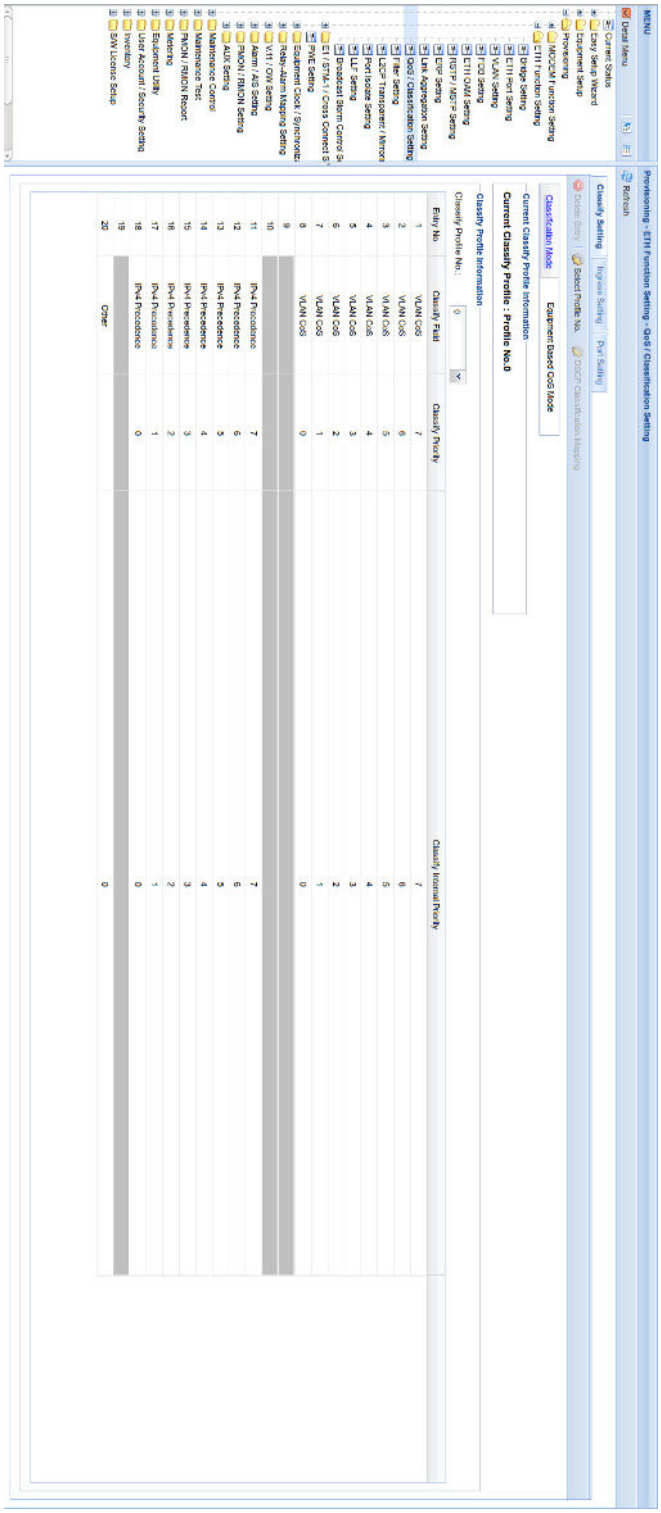
Bezdrátový spoj NEC iPasolink je spravován přes webové rozhraní. V levém menu se nachází záložka *Provisioning* a poté prostřednictvím záložky *ETH Function Setting* a odkazu *QoS / Classification Setting* lze otevřít nastavení upřednostnění provozu.

Jako klasifikační mód bylo nutné vybrat *Equipment Based QoS Mode*, kde jsou již jednotlivé fronty přednastaveny. Snímek konfigurační obrazovky je možné vidět na obrázku 3.3.

3.2.6 Ericsson Mini-Link

U bezdrátového spoje Ericsson Mini-Link se k nastavení využívá software MINI-LINK Craft [13]. Nastavení DSCP QoS je podobné jako u spoje Alcoma, nicméně se spoje liší v počtu front.

Do nastavení QoS lze vstoupit pomocí záložky *Ethernet* a v konfiguračním okně v záložce *Related Tasks* se nachází odkaz *Configure QoS*. U položky



Obrázek 3.3: Rozhraní bezdrátového spoje NEC iPasolink

Trusted Port bylo nutné nastavit *DSCP IPv4* a *Priority to TCP Mapping* na *802.1 Q Standard*.

V záložce *Configure Priority Mapping* byla následně DSCP ohodnocení 32 přiřazena fronta číslo 2, jelikož má spoj u této fronty největší vyrovnávací paměť.

3.3 Místa nasazení IPTV

Z důvodu nestability koncových bezdrátových technologií pro uživatele připojené bezdrátově bylo nasazení IPTV omezeno pouze na kabelové sítě připojené profesionálními bezdrátovými spoji nebo optickým kabelem. Později bylo uživatelům umožněno využít platformu sledovanitv.cz, nicméně její zavedení neznamenalo implementační problém, jelikož se jedná o službu poskytovanou přes internet.

V každé lokalitě bylo nastavení jednotek jiné, společné bylo pouze nastavení přepínačů. Bylo zde nutné nastavit shodné časovače u funkce IGMP snooping a procházející VLAN až ke klientům.

V Modleticích na bezdrátovém spoji Ericsson Mini-Link byla aktivována funkce DSCP QoS. Následně byly nakonfigurovány všechny prvky, aby mohla být IPTV aktivována jednotlivým zájemcům.

V Říčanech byla nakonfigurována IPTV, aby mohla protékat celou sítí. Bylo nutné nakonfigurovat i bezdrátový spoj UBNT řady M.

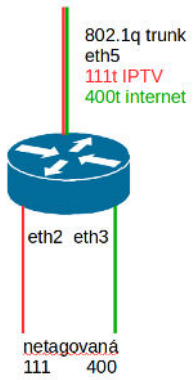
V Nupakách byly vyměněny přepínače Zyxel za přepínače HP V1900-8G. To umožnilo konfiguraci VLAN a dalších funkcí jako IGMP snooping. Zároveň byl nakonfigurován bezdrátový spoj NEC na upřednostnění IPTV provozu.

V pražské Libuši proběhlo nasazení na bezdrátovém spoji Alcoma MP600, kde byla aktivována funkce DSCP QoS. Ta samá funkce byla aktivována i u jednotek Siklu. Během přestavby byly vyměněny přepínače Zyxel za přepínače Edge-Core ES3528M. Zároveň byla linka do dalších částí sítě vedoucí přes směrovač se systémem MikroTik RouterOS přepojena přímo do přepínače. Díky tomu nemusel IPTV provoz téct přes směrovač.

3.4 Klientská řešení

Jelikož bylo v síti nasazeno řešení s oddělenou VLAN pro televizi, je nutné přímo k zájemcům umístit prvek, který oddělí IPTV od jiné VLAN, která slouží k přenosu běžných dat. Ideální možností je vést ke klientovi dva samostatné kabely pro připojení do sítě a pro televizi, je to však mnohdy nepraktické a jedno zařízení u klienta umožní to samé a může sloužit i jako bezdrátový a kabelový směrovač, který by klient stejně musel použít.

Příklad rozdělení je viditelný na obrázku 3.4. Do bytu přichází jedno médium, ve kterém jsou přenášeny různé VLAN. Dle obrázku dojde k rozdělení provozu na dvě rozhraní, IPTV směřuje na rozhraní eth2, data (internet)



Obrázek 3.4: Ilustrace funkce prvku, který odděluje IPTV od internetu u koncového uživatele

na rozhraní eth3. Na obou výstupních rozhraních se již přenášené pakety neoznačují.

3.4.1 Routerboard (MikroTik RouterOS)

Zařízení označené jako Routerboard jsou produktem litevské společnosti Mikrotikls Ltd. Většinou se jedná o výrobky přímo určené pro směrování provozu, které jsou založeny na vlastním operačním systému nazvaném MikroTik RouterOs.

3.4.1.1 Routerboard (MikroTik RouterOS) s využitím interního přepínače

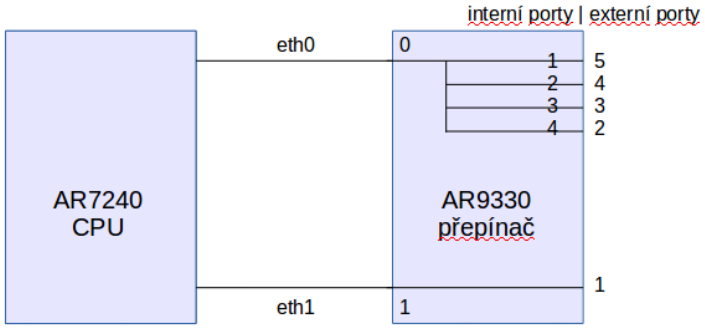
Některé verze výrobku Routerboard obsahují dle dokumentace [39] interní přepínač, konkrétně se jedná o výrobky s čipy AR8327, AR8316, AR8227, AR7240 a IC+175D. Díky této možnosti lze desku Routerboardu využít jako přepínač a tak bez zatížení CPU rozdělovat provoz na IPTV a na ostatní data (lze kombinovat i s NAT a Wi-Fi pro domácí síť).

Na obrázku 3.5 je vyobrazeno, kudy tečou data uvnitř prvku v případě čipu AR7240 z pohledu správce s přístupem do konfigurační části zařízení. V případě využití jednoho z portů 2-5 lze provoz IPTV odklonit do jiného portu na stejném přepínači a šetřit tak zátěž CPU.

Pro nastavení této funkce je nutné se připojit do příkazové řádky operačního systému MikroTik RouterOS. Veškerá nastavení jsou realizována na modelu Routerboard RB2011UiAS-2HnD.

Porty 2,3 a 5 musí fungovat jako přepínač.

```
/interface ethernet
set eth2 master-port=ether5
```



Obrázek 3.5: Schéma čipu AR7240 ze „síťového“ pohledu

```
set eth3 master-port=ether5
```

Je nutné nastavit porty 2 a 3 do režimu *access*[5]. Nastavení *always-strip* znamená, že po průchodu přepínačem každý rámec na výstupu portu ztratí VLAN hlavičku (bude neoznačený). V případě portu 5 je nutné nastavit, aby vždy hlavičku se správným číslem VLAN na výstupu prvek odesílal (jedná se o *trunk*[6] režim).

```
/interface ethernet switch port
set ether2 vlan-mode=secure vlan-header=always-strip\
default-vlan-id=111
set ether3 vlan-mode=secure vlan-header=always-strip\
default-vlan-id=400
set ether5 vlan-mode=secure vlan-header=add-if-missing
```

Nakonec je nutné všechny údaje promítnout i do tabulky se seznamem VLAN.

```
/interface ethernet switch vlan
add ports=ether2,ether5 vlan-id=111 switch=switch1
add ports=ether3,ether5 vlan-id=400 switch=switch1
```

Toto nastavení odpovídá obrázku 3.4. Pokud by bylo nutné místo rozdělení využít dalších možností výrobku (udělat z prvku směrovač) a pro uživatele tak využít NAT, je nutné VLAN 400 místo do portu eth3 nasměrovat na CPU (port 0).

Pro nastavení směrování s využitím CPU (IPTV VLAN pořád funguje přes přepínač) je nutné si zvolit náhodně některé současně nevyužité číslo VLAN pro místní LAN (v našem případě 401). Poté stačí nastavit tuto VLAN na jednotlivé porty.

[5]Režim access znamená, že na daném rozhraní je přítomna pouze jedna neoznačená VLAN.

[6]Trunk režim umožňuje na jednom rozhraní komunikaci více VLAN, které musí být označené. U některých prvků tento režim umožňuje zároveň přenos tzv. nativní VLAN. To je VLAN, která je neoznačená.

```
/interface ethernet switch vlan
add ports=ether5,switch1_cpu vlan-id 400 switch=switch1
add ports=ether2,switch1_cpu vlan-id 401 switch=switch1
```

Je nutné změnit přístupovou VLAN na portu eth3, zároveň zařídit označení směrem k CPU.

```
/interface ethernet switch
set eth3 vlan-mode=secure vlan-header=always-strip\
default-vlan-id=401
set switch1_cpu vlan-mode=secure vlan-header=add-if-missing
```

Nakonec stačí nastavit rozhraní na směrovači. Dále lze již na rozhraní přidávat IP adresy nebo třeba nastavit DHCP server. Pro aktivaci funkce NAT je ještě nutné přidat pravidlo do NAT tabulky.

```
/interface vlan add interface=ether5 name=wan vlan-id=400
/interface vlan add interface=ether5 name=lan vlan-id=401
```

3.4.2 Routerboard (MikroTik RouterOS) s využitím CPU

V tomto případě prvek pracuje podobně jako směrovač s operačním systémem GNU/Linux. Nejprve je nutné vytvořit jednotlivé VLAN na rozhraní směrem do sítě poskytovatele.

```
/interface vlan
add name=eth5.400-internet vlan-id=400 interface=eth5
add name=eth5.111-iptv vlan-id=111 interface=eth5
```

Poté je nutné vytvořit most mezi rozhraními pro provoz IPTV.

```
/interface bridge
add name=br0-IPTV
/interface bridge port
add interface=eth5.111-iptv bridge=br0-IPTV
add interface=eth3 bridge=br0-IPTV
```

Ostatní nastavení (jestli bude internet dále procházet, nebo bude v režimu NAT) již závisí na dalším nastavení v systému MikroTik RouterOS.

Z testů provedených na prvku RB2011UiAS-2HnD vyplývá, že v případě plného vytížení (dva televizní přijímače a vytížení internetové přípojky na 50 Mb/s) se zatížení CPU u zařízení pohybuje mezi 50 - 60%.

3.4.3 OpenWRT

OpenWRT je další z linuxových distribucí, je ale určena výhradně pro síťové prvky. Jako ostatní distribuce nabízí balíčkovací systém, který umožňuje instalovat programy z repozitáře. Přináší do podporovaných směrovačů více funkcí,

než běžně dodávaný firmware od výrobců. Příkladem dalších funkcí je například SSH server, omezení rychlosti, IPv6 a pro cíl této diplomové práce velmi důležité nastavení VLAN [47].

Pro vývojáře nabízí OpenWRT balíček buildroot [48], díky kterému si může každý vytvořit firmware pro svůj vlastní směrovač na míru. Z kompilačního skriptu po dokončení přípravy vlastního firmware zůstanou pouze jednotlivé binární soubory (pro každý typ a revizi routeru jiné), které lze přímo nahrát do směrovačů.

Jako příklad byly vybrány 3 směrovače podporované distribucí OpenWRT rozdělené do cenových hladin od co nejlevnějšího modelu až k lépe vybavenému. Pro každý model byl vytvořen firmware pro přívod internetu a IPTV v označené VLAN (vstupní port v režimu trunk). Dále u vybraných modelů byla využita možnost přívodu internetu v neoznačené VLAN a IPTV v označené VLAN (trunk s nativní VLAN pro internet). Druhá možnost je výhodná hlavně pro jednodušší nastavení v koncových LAN sítích, kde jsou mnohdy čísla VLAN určené pro LAN rozdílná.

Byly vybrány směrovače od společnosti TP-LINK Technologies CO., LTD., konkrétně typy WR741nd, WR1043nd a WDR4300. Pro každý model byla k dispozici verze dle vydané revize a firmware je součástí přiloženého DVD se základním nastavením včetně podpory protokolu IPv6. Dále DVD obsahuje nastavení směrovačů pro IPTV na jednom a na dvou rozhraních (jeden a dva televizní přijímače v domácnosti). Jako verze OpenWRT byla použita v době psaní práce nejnovější revize s označením Barrier Breaker r39792.

Pro vyznačení vnitřní struktury propojení byla pro přehlednost uvedena místo diagramu tabulka. Každý z modelů vypadá podobně jako diagram Routerboardu. Je zde vždy hardwarový přepínač napojený na CPU, navíc může obsahovat další rozhraní, které je přímo napojeno na CPU. Ceny byly platné k 1. dubnu 2014 a jako cena je uváděna nejlevnější nabídka dle serveru heureka.cz [61].

Podrobné informace jak směrovače fungují a jak vypadá rozhraní pro nastavení a umístění konfiguračních souborů lze nalézt v příloze A.2.

3.4.3.1 WR741nd

Router se vyznačuje velice nízkou cenou 395 Kč. Byl vybrán jako nejlevnější model určený pro IPTV. Podporuje standard 802.11n. Interně je možné využít přepínače mezi 4 porty určenými v původním firmware pro LAN. Modrý (WAN) port je vyveden do CPU samostatně.

Spojení externí - interní port pro revizi 4.21 je uvedeno v tabulce 3.1

V případě implementace IPTV do tohoto zařízení je možné využít přepínač. Je tedy nutné jako výstupní port k poskytovateli využít jeden z portů přímo v přepínači. Dále interní přepínač u tohoto modelu podporuje na portu buď pouze označené rámce, nebo neoznačené. Počítá se tedy na straně poskytovatele se značením všech rámců, které směřují k uživateli.

Tabulka 3.1: Mapování portů u modelu TP-LINK WR741nd

Externí port	Interní port
1	switch eth0, port 4
2	switch eth0, port 1
3	switch eth0, port 2
4	switch eth0, port 3
WAN	eth1 samostatný
CPU	switch eth0, port 0

Tabulka 3.2: Mapování portů u modelu TP-LINK WR1043nd

Externí port	Interní port
1	switch switch0, port 4
2	switch switch0, port 3
3	switch switch0, port 2
4	switch switch0, port 1
WAN	switch switch0, port 5
CPU	switch switch0, porty 0 a 6

Je ale také možné využít přímo WAN rozhraní a pomocí mostů uvnitř zařízení přes CPU přeposílat rámce určené pro IPTV. Při měření pomocí generování 80 Mb/s UDP provozu směrem do jednoho z portů v domácí síti a paralelním sledování IPTV nedocházelo u televize k výpadku rámců (tento test počítal s nastavením upřednostnění provozu na přepínači u poskytovatele).

3.4.3.2 WR1043nd

Cena tohoto typu je 1192 Kč. Na rozdíl od nejlevnějšího modelu jsou k dispozici gigabitové porty a také jedno 2,4 GHz bezdrátové rozhraní s podporou 2x2 MIMO.

Revize 2.1 má vnitřní propojení dle tabulky 3.2.

CPU na portu 0 a 6 je pravděpodobně využito pro plně duplexní gigabitový přenos. Pro plnohodnotný provoz jsou tedy využity porty 2, jeden je v základním nastavení propojen s WAN rozhraním a druhý s LAN rozhraním. Interní přepínač plně podporuje označenou i neoznačenou VLAN na jednom rozhraní. IPTV tedy nemusí procházet přes CPU.

3.4.3.3 WDR4300

Router TP-LINK TL-WDR4300 je nejdražším modelem k implementaci s cenou 1699 Kč. Disponuje gigabitovými porty a dvěmi bezdrátovými 3x3 MIMO rozhraními pro 2,4 GHz a 5 GHz pokrytí (je tedy dvoupásmový). Kromě běž-

Tabulka 3.3: Mapování portů u modelu TP-LINK WDR4300

Externí port	Interní port
1	switch switch0, port 4
2	switch switch0, port 3
3	switch switch0, port 2
4	switch switch0, port 1
WAN	switch switch0, port 5
CPU	switch switch0, port 0

ných funkcí je ve firmware od výrobce podporována i akcelerace NAT na vnitřním přepínači [60].

Rozmístění portů u revize 1.6 lze najít v tabulce 3.3.

V případě využití s OpenWRT bohužel prozatím nelze akceleraci NAT využít (prozatím není specifikace této možnosti kompletně zveřejněna [60]). V používané revizi OpenWRT také nelze na přepínači využít port v režimu trunk s nativní VLAN. K opravení tohoto nedostatku byla vydána oprava komunitou [46] a je zahrnuta ve vydaném referenčním firmware v příloze na DVD.

Jelikož se podařilo díky opravě umožnit průchod nativní VLAN v trunk režimu, nebylo nutné využít CPU routeru pro přeposílání IPTV provozu. Stačí mezi jedním z portů a WAN portem nastavit přepínač tak, aby správně jednotlivé rámce přeposílal (na WAN bude rámec označen, na rozhraní k televiznímu přijímači rámec označen nebude). Zátěž CPU tedy nebude mít žádný vliv na provoz televize.

Kapitola 4

Monitoring vícesměrového vysílání

V tuto chvíli je již IPTV v síti nasazena a je funkční od zdroje až do jednotlivých televizních přijímačů. Každý datový rámec urazí dlouhou cestu mezi všemi částmi sítě. Bohužel, v každém průchodu se můžou vyskytnout problémy, které je mnohdy velmi těžké odhalit. V případě živé televize a vícesměrového vysílání zdroj vysílá data do některého ze svých rozhraní. Nemá ale zprávu, jestli byla data řádně přijata od klientů, pro které jsou určena.

Ke zjištění stavu tedy musí klienti dávat informace, jestli se v jejich příjmu nevyskytuje nějaká chyba. K těmto účelům by bylo vhodné využít přímo klientské přijímače, ale ty by posílaly jen ta data, na která se klienti přímo dívají a diagnostika by tak byla velmi složitá. Lepší variantou je rozmístit do různých oblastí sítě prvky, které budou vybranou množinu kanálů sledovat permanentně a budou o případných chybách informovat hned když nastanou.

4.1 Analýza způsobů monitorování

V případě monitorování IPTV, tedy hlavně vícesměrového provozu, je možné využít dvou metod.

První metodou je přímé sledování rámců posílaných do sítě. Dojde tedy k přihlášení se ke skupině vícesměrového vysílání a k sledování provozu v ní. Je nutné tento provoz oddělit od jiných typů provozu (například od protokolu IGMP). K tomu může sloužit ToS hlavička, která je vždy na vstupu do sítě přepsána.

Následně je nutné sledovat v provozu ID každého paketu v hlavičce a počítat, jestli dorazily všechny pakety správně (ID se inkrementuje). Pokud dojde k vyřazení paketu na některém prvku směrem k monitorovací sondě, sledování hned zaznamená, že daný paket nedošel díky chybějícímu číslu paketu v řadě.

Tím samým způsobem lze vyřešit i problém přeuspořádání, kdy na sledo-

vací prvek přijde paket s nižším ID než paket s ID, který sonda přijala jako poslední nebo který očekává.

Provoz vypsaný pomocí programu tcpdump je vidět v ukázce 4.1. Číslo paketu je v hlavičce přímo reprezentováno.

```
22:20:32.219348 IP (tos 0x20,CE, ttl 61, id 3519, offset 0,\
flags [none], proto UDP (17), length 1344)
172.16.1.2.37266 > 239.1.2.1.1111: [no cksum] UDP, length 1316
22:20:32.219362 IP (tos 0x20,CE, ttl 61, id 3520, offset 0,\
flags [none], proto UDP (17), length 1344)
172.16.1.2.37266 > 239.1.2.1.1111: [no cksum] UDP, length 1316
```

Ukázka 4.1: Část zachyceného IPTV provozu

Druhou možností je přímé sledování televizního kanálu (například pomocí programu vlc, konkrétně konzolovou verzí cvlc). Oproti první možnosti lze tímto způsobem detekovat nejen problémy v síti, ale i u vysílatele nebo v head-endu. To lze ale pouze v případě, když kanály v IPTV platformě nejsou při přenosu sítí šifrovány. V komerčních nasazeních IPTV je šifrování při přenosu sítí nutné a je poskytovateli implementováno. Další nevýhodou je mnohem vyšší zátěž pro monitorovací zařízení.

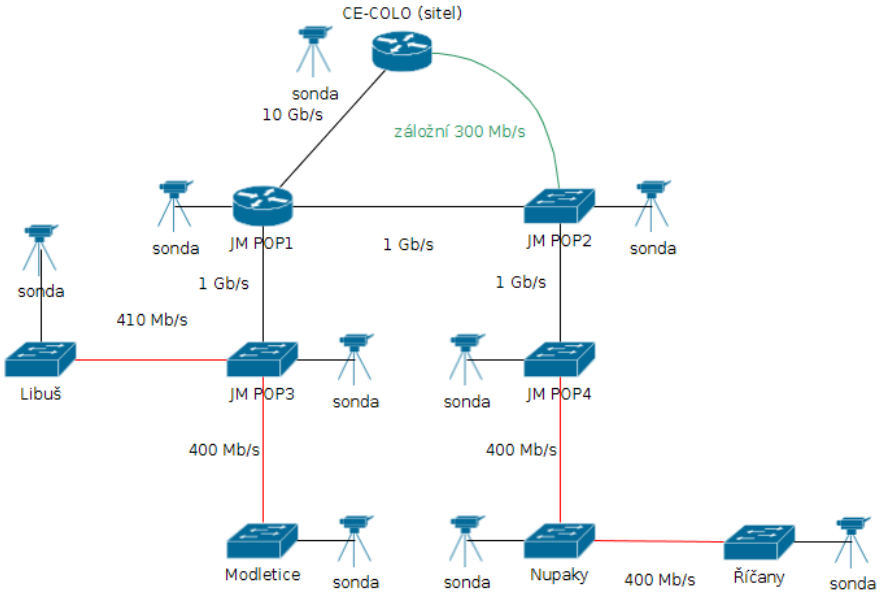
V případě implementace této diplomové práce bude počítáno s tím, že sledování chyb přicházejících od provozovatelů televizního vysílání (případně z head-endu) bude hlídáno společností provozující head-end v platformě. Pro hlídání chyb v síti je první řešení efektivní a dostatečné.

V obou případech monitorování se jedná o aktivní sledování. Je tedy nutné počítat se zvýšenou zátěží sítě kvůli sledování. Toto tvrzení neplatí pouze ve chvíli, kdy do stejného přepínače sdíleného se sondou bude zapojen klient, který právě v danou chvíli přijímá některý ze sledovaných kanálů. Naštěstí ale není nutné sledovat naprosto všechny kanály. Vybraná množina dvou až čtyř kanálů k monitorování stačí. Jedná se tedy o nadměrný provoz v řádu desítek megabitů.

4.2 Monitorovací sondy

Jako sondu lze využít libovolný počítač s dostatečným výkonem pro spuštění operačního systému GNU/Linux a sledovacích programů. S ohledem na rozmístění v kolokačních centrech a rozvodných skříních po síti je vhodné uvažovat s co do velikosti malým zařízením s malou spotřebou elektrické energie.

Pro tyto účely se jako vhodné zařízení jeví dnes velmi oblíbené Raspberry PI, které disponuje pro sondu dostatečným výkonem, síťovým portem a hlavně velmi nízkou spotřebou a malou velikostí. Sledovat datové toky jednotlivých vícesměrových skupin lze například i pomocí směrovačů a dalších prvků, které jsou již v síti rozmístěny.



Obrázek 4.1: Doporučené rozmístění sond v páteřní síti

4.2.1 Rozmístění sond v síti

Jednotlivé sondy byly rozmístěny do většiny oblastí. Ke sledování byly vybrány dva kanály. Jeden ve standardním rozlišení MPEG-2 a druhý ve vysokém rozlišení a normě MPEG-4. Kromě rozmístění do cílových oblastí bylo důležité sondy umístit i na vybrané body páteřní sítě. Nejdůležitějším místem je přímo předávací uzel kvůli efektivnímu porovnání chyb již přicházejících do sítě oproti těm, které se teprve v síti vyskytnou.

V jednotlivých oblastech i na páteřní síti bylo nutné sondy umístit přímo k ostatním technologiím do rozvodných skříní a spojit je ethernetovým kabelem s přepínači. Popis připojení jednotlivých sond v páteřní síti je možné vidět na obrázku 4.1. Během psaní diplomové práce se podařilo umístit sondy na téměř všechna navrhovaná umístění, chyběla pouze sonda na bodu JM POP2.

Kromě rozmístění fyzických zařízení byly využity již umístěné prvky s operačním systémem GNU/Linux (na předchozím obrázku též značeny jako sondy). Bylo nutné přidat VLAN, správně nastavit směrovací pravidlo ve směrovací tabulce a následně spustit program. Během testování se vyskytl problém s nefunkčním příjmem vícesměrového vysílání. Následně bylo zjištěno, že problém způsoboval zapnutý *reverse path filter*, který zakazoval příjem vícesměrového provozu na rozhraní [56]. Pomocí příkazu v ukázce 4.2 byl na daném rozhraní filtr vypnut.

```
echo 0 > /proc/sys/net/ipv4/conf/eth0.111/rp_filter
```

Ukázka 4.2: Zakázání *reverse path filtru* na rozhraní eth0 a VLAN 111

4.2.2 Program

Program pro sledování je psán v jazyce Python, součástí je i IGMP klient, který je implementován ve stejném jazyce. V programu jsou využity vybrané moduly určené převážně pro získání a vyhodnocení síťového provozu.

4.2.2.1 Scapy

Scapy je komunitním rozšířením jazyku Python o interaktivní program umožňující manipulaci s pakety [52]. Umožňuje vytvářet a dekódovat pakety řady protokolů a následně je opět odesílat nebo zachycovat na vybraném rozhraní.

U této práce je rozšíření Scapy využito pro dekódování a vytváření IGMP provozu pro korektní přihlášení programu k vícesměrové skupině. Simuluje tedy IGMP klienta (televizní přijímač), který žádá o příjem televizního kanálu.

4.2.2.2 Pcapy

Pcapy je komunitním rozšířením jazyku Python o možnost zachytit provoz na vybraném rozhraní. V programu pro sledování je modul Pcapy využit na sledování provozu v jednotlivých vícesměrových skupinách.

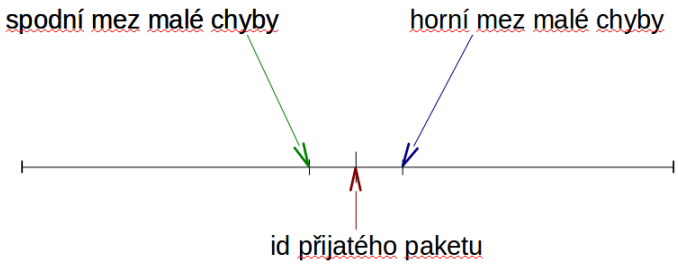
4.2.2.3 Munin

Munin je monitorovací systém zaměřený na analýzu trendů a problémů. Dle článku na serveru linuxsoft.cz [49] lze munin popsat jako flexibilní nástroj pro vytváření grafů. Na jednotlivých serverech je spuštěn sběrač dat (munin-node), ze kterého jsou data předávána dle požadavků hlavního serveru, kde jsou vytvářeny také grafy. Veškeré vizualizace jsou kresleny pomocí nástroje RRDtool.

V síti nasazení je systém munin použit pro sledování trendů u většiny síťových prvků. Tento systém tedy bude zobrazovat i jednotlivé informace získané IPTV sondami pro možné porovnání sledovaných dat s ostatními výstupy (například s vytížením linek nebo chybami na jednotlivých rozhraních přepínačů). Na koncových sondách bude spuštěna pouze odlehčená verze systému nazvaná munin-node, které se dotazuje hlavní sledovací server v síti.

4.2.3 Metodika měření

Díky zvolené metodě sledování vycházející z analýzy je možné popsat metodiku měření. Zdroj kanálů (head-end) vysílá do sítě pakety, které cílí na vícesměrovou skupinu. Každý paket je označen šestnáctibitovým identifikátorem,



Obrázek 4.2: Běžný případ

který se postupně inkrementuje. Jakmile se postupnou inkrementací dostane identifikátor na maximální hodnotu, tak u další inkrementace čítač přeteče a identifikátor se vynuluje.

Tohoto čítače identifikátoru využívá program, který postupně kontroluje souvislosti tohoto ID mezi navazujícími pakety. Program si vždy udržuje aktuální hodnotu identifikátoru (z ní je schopen odvodit i identifikátor očekávaného paketu, který má hodnotu příští inkrementace). Na základě porovnání identifikátorů očekávaného paketu a opravdu přijatého paketu může program odvodit, zda u přijatých dat došlo k chybě.

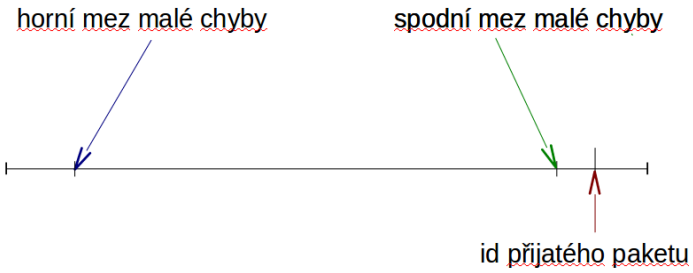
Je tedy možné detekovat problémy díky nesouvislostem mezi postupně přijatými pakety. Problémy lze dále rozdělit na dva případy:

- Chybně přijatý paket z budoucnosti (dorazil paket s ID větším, než bylo očekáváno)
- Chybně přijatý paket z minulosti (dorazil paket s menším ID, než bylo očekáváno)

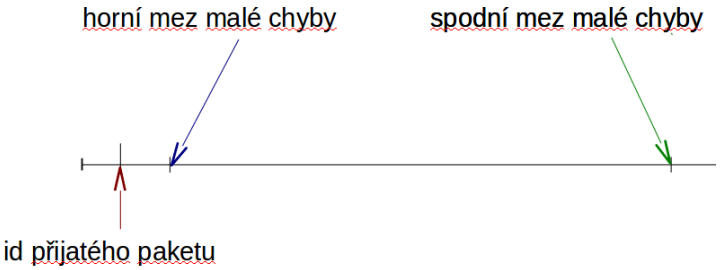
Tyto dva problémy se můžou zdát jako podobné, ale není tomu tak. Zatímco pokud dorazí paket s vyšším ID (první případ), znamená to, že někde v síti dochází ke ztrátám. V druhém případě dochází někde v síti k přeskupení, což je mnohem závažnější problém. Vyhodnocením těchto problémů včetně identifikace možných příčin se zabývá následující část 4.2.4.

Pokud jsme schopni rozlišit tyto dva druhy chyb, je nutné uvažovat i případ, kdy přijmeme paket s hodnotou identifikátoru, kterou není možné zařadit ani do jedné z těchto skupin (očekávám paket s ID 1, přijmu paket s ID 30000). Z popisu tohoto případu vyplývá, že je nutné určit interval „povolených hodnot“ identifikátoru přijatého paketu. V případě přijetí paketu s hodnotou identifikátoru ležící mimo povolený interval je nutné s chybou zacházet odlišně. Pokud se tento případ objeví, můžeme jej nazvat *velkou chybou*.

Díky všem poznatkům se vyhodnocovací fáze programu rozdělí na tři případy. U prvního případu 4.2 je vidět interval časovače (od 0 do 65535). Interval „povolených hodnot“ leží mezi dolní a horní mezí intervalu. V druhém případě



Obrázek 4.3: Případ, kdy horní mez přeteče



Obrázek 4.4: Případ, kdy horní mez a čítač identifikátoru paketu přetečou

4.3 už interval leží mezi hodnotami původní spodní meze a maximem čítače a dále mezi minimem čítače a původní horní mezí. Tento interval je shodný v druhém i třetím případě 4.4, ale z důvodu rozdělení malé chyby na dva případy se liší vyhodnocení chyb (rozdělení na chybný paket z minulosti a budoucnosti).

Může ale existovat případ, kdy díky omezené velikosti čítače dojde k chybnému přijetí paketů, ale výše uvedená detekce chyb nic nezachytí. Jedná se o ojedinělou možnost, kdy bude přijat paket s očekávaným identifikátorem. Tento paket ale bude součástí jedné z příštích inkrementací čítače a tedy do přijetí očekávaného paketu dojde k přetečení. V tomto případě dojde k opravdu velké chybě, kdy se může v síti najednou ztratit 65536 paketů i více). Tuto chybu lze detekovat pomocí vlastního čítače, který inkrementuje počet všech aktuálně přijatých paketů.

Dojde-li k zanesení všech naměřených hodnot do grafů (všechny chyby se budou vyhodnocovat za konstantní dobu), bude možné veškeré naměřené chyby včetně trendů pozorovat přehledně v čase.

4.2.4 Popis sledovaných chyb

Díky velkému počtu sond rozmístěných v síti lze v případě porovnání jednotlivých výstupních grafů najít téměř přesně místo, kde síť chybuje.

V případě správně fungující sítě by neměl čítač ztracených paketů v síti přesáhnout u kanálu s datovým tokem 25 Mb/s hodnotu 10 během 5 minut. Čítač přeskupení by měl být vždy nulový. Zároveň by se v žádném případě neměla vyskytnout v síti velká chyba.

Pokud bude detekováno opravdu velké množství chyb, není řeba všechny případy zanášet do grafů. Pro výsledek, že IPTV funguje bez chyby je důležité nepřekročit hodnoty pro správně fungující síť. Není tedy důležité, jestli bylo v síti ztraceno 100 nebo 1000 paketů. Určujícím faktorem je skutečnost, že k takovéto velké ztrátě vůbec došlo.

Pokud se stanovená mez překročí, je nutné analyzovat každou chybu nebo každý souhrn chyb. Díky této analýze lze například objevit chyby v síti, které jsou pravidelné (například špatně fungující IGMP-snooping na některém z přepínačů).

Pokud nelze říct, že se problémy opakují pravidelně v nějakém intervalu, může být hledání těžší. Pokud sonda detekuje ztracené pakety, může se jednat o přetíženou linku. V případě kabelu lze přetížení zjistit pomocí čítačů v přepínačích, které obsahují počet vyřazených paketů. Tento problém se dá do jisté míry eliminovat nasazením QoS a prioritních front.

Pokud se ztráty objevují na bezdrátových zařízeních, může se jednat o zarušení pásma, slabý signál nebo o vadný typ jednotky. Vždy je dobré v tomto případě vstoupit do řídícího rozhraní bezdrátové jednotky a zkontrolovat jednotlivé parametry signálu a případné alarmy.

Horší je případ přeuspořádaných paketů. Tento problém by se v žádném případě neměl v síti objevit, jelikož se s největší pravděpodobností jedná o špatně fungující prvek (špatně implementované fronty v přepínačích nebo v bezdrátových spojích).

Větší výpadky je možné sledovat díky vyhodnocení trendu počtu přijatých paketů. Tyto údaje obvykle detekují přerušení kabelu, výpadek elektrického proudu nebo jiné problémy, které nejsou běžné. S chybovostí sítě pro nasazení IPTV ale nemusí mít spojitost.

4.2.5 Popis programu

Program je rozdělen na dvě části, které na sobě nezávisle pracují. Zároveň je celá práce mezi oběma programy rozdělena mezi více vláken.

První částí je samostatný IGMP klient, který se stará o registraci žádosti na příjem vícesměrové skupiny. Sleduje příchozí IGMP pakety a případně na ně reaguje (pokud přijde IGMP dotaz, klient na něj odpoví). Zároveň každých 180 sekund kontroluje, jestli přichází provoz a pokud ne, odešle žádost o zařazení do skupiny. Program tedy obnoví členství ve skupině při delším výpadku sítě.

Druhou částí je samostatný program, který je rozdělen na vlákno sloužící k zachytávání a vyhodnocení dat. Následně je v programu využito ještě druhé vlákno, které (v případě potřeby) slouží k exportu získaných krátkodobých výsledků pro další zpracování monitorovacímu systému munin.

Problém rozlišuje dva druhy chyb při přenosu. V případě korektního přijímání paketů se žádný čítač neinkrementuje. V případě přijetí paketu z budoucnosti (s ID vyšším než je očekáváno) došlo pravděpodobně ke ztrátě a k čítači s těmito chybami *futureErr* se přičtě počet pravděpodobně ztracených paketů. V případě přijetí paketu s nižším ID než je ID očekávaného se inkrementuje čítač *historyErr*.

Jelikož čítač vždy po ID 65535 přeteče a dorazí opět paket s ID 0, bylo nutné rozlišit v případě porušení souvislosti o jakou chybu se jedná. Dorazí-li paket, u kterého se ID liší od ID očekávaného o více jak 1000, jedná se o velkou chybu *bigErr* (příznak velké chyby se nastaví na 1).

Kvůli přehlednosti výsledků zanesených v grafech bylo nutné při exportování naměřených dat do systému munin čítače chyb omezit na maximální hodnotu 100 kvůli přehlednosti grafů. Po exportu se všechny čítače chyb obnoví na hodnotu 0. Velká chyba je ve výsledných grafech reprezentována oběma čítači chyb, které jsou nastaveny na maximální hodnotu. Interval doby jednotlivých měření je v základním nastavení systému munin pět minut.

Normální případ vyhodnocení chyb, kdy se neočekává přetečení čítače, je popsán pomocí pseudokódu.

```
if (id_prijateho_paketu != id_ocekavaneho_paketu) {
 spodni_mez = id_ocekavaneho_paketu-1000
 horni_mez = id_ocekavaneho_paketu+1000
 if (id_prijateho_paketu > spodni_mez) &&
    (id_prijateho_paketu < id_ocekavaneho_paketu) {
        historyErr++
        }
 elif (id_prijateho_paketu < horni_mez) &&
      (id_prijateho_paketu > id_ocekavaneho_paketu) {
        pocet_ztracenych_paketu = id_prijateho_paketu -
                                  id_ocekavaneho_paketu
        futureErr += pocet_ztracenych_paketu
        }
 else   {
        bigErr = 1
        }
}
```

Program již vyhodnotil, že nastala chyba (ID přijatého paketu nesouhlasí s ID očekávaného paketu). Rozdělí si tedy interval na tři případy a vyhodnotí, o jaký problém se jedná.

4.2.6 Parametry programu

Seznam parametrů pro spuštění programu je možné zobrazit prostřednictvím parametru „-h“.

```
Usage: multicast_monitor.py [options]

Options:
```

```
--version             show program's version number and exit
-h, --help            show this help message and exit
-i INTERFACE, --interface=INTERFACE
                      Monitoring interface
-g GROUP, --group=GROUP
                      Multicast group address
-l LEVEL, --level=LEVEL
                      Debug level 1 or 2
-e, --export          Export measured data to munin
-r, --run-igmpclient  Run igmp client
-d, --debug           Print debug information
```

V základním nastavení bez uvedení parametrů program sleduje provoz na rozhraní eth0 u skupiny s IP adresou 239.250.1.1, zároveň vypisuje veškeré informace o příchozích paketech včetně správně doručených. Více informací o programu je možné najít v příloze A.1.

4.2.7 Výstupy programu

V případě zapnutí ladění (parametr „-d“) je možné zvolit dva stupně výpisu. V případě volby stupně 1 jsou uživateli na obrazovku vypisovány pouze detekované chyby. Tato možnost je velmi užitečná pro případ testování linek na aktuální ztrátu paketů při přenosu v závislosti na aktuálním zatížení.

Následující ukázka výpisu ukazuje dvě detekované chyby, kde se na lince ztratily čtyři pakety.

```
FUTUREERR    futureErr/historyErr:2/0     arrived pcktid 5158\
expected pcktid 5156
FUTUREERR    futureErr/historyErr:4/0     arrived pcktid 29728\
expected pcktid 29726
```

Druhý stupeň zobrazuje naprosto všechny informace, tedy nejen chybné, ale i správně přijaté pakety. Tuto možnost je dobré využít v případě testu, jestli vůbec vícesměrové vysílání do sondy přichází.

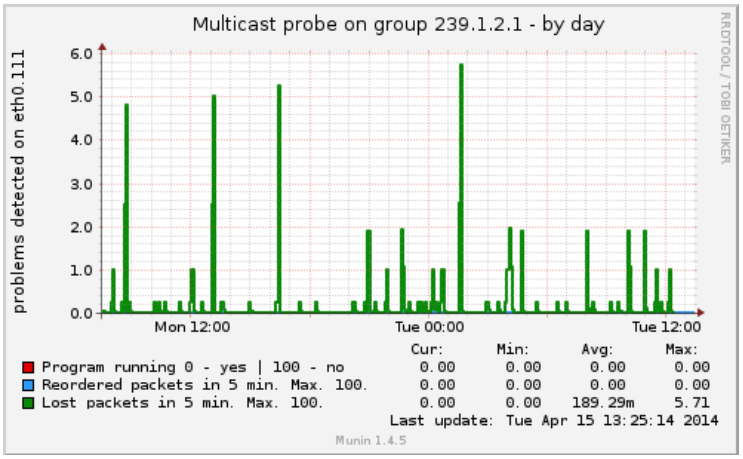
V tomto případě se tedy zobrazují všechny pakety, oba dva v následujícím výstupu jsou korektně přijaty.

```
OK      futureErr/historyErr:0/0        arrived pcktid 52625\
expected pcktid 52625
OK      futureErr/historyErr:0/0        arrived pcktid 52626\
expected pcktid 52626
```

V případě využití přepínače pro export „-e“ se spustí komunikační socket, přes který může systém munin získat aktuální monitorovaná data. Vždy po vybrání dat jsou jednotlivé čítače vynulovány.

4.2.8 Export do monitorovacího programu munin

V systému munin se vždy pro přidání monitorovací možnosti musí vytvořit vlastní skript, který samotný program spouští. V případě sledování IPTV se



Obrázek 4.5: Příklad výstupu monitorovacího systému - graf chyb v příjmu jednotlivých paketů

jedná o dva skripty, *mcast-probe* a *mcast-pkts*. První ze jmenovaných slouží k zpracování chyb, druhý k zpracování počtu přijatých paketů.

Monitorovací program vytvoří každé sledované vícesměrové skupině jeden socket v souborovém systému se jménem ve tvaru munin-[rozhraní]-[adresa_skupiny]. Prostřednictvím tohoto socketu dále vybírá monitorovací systém munin naměřená data. Pokud chce munin vybrat informace o čítačích, odešle přes socket požadavek „lost“. Pokud chce zjistit počet aktuálně přijatých paketů, odešle přes socket požadavek „pcktnum“. Výběr dat je vidět na ukázkách 4.3 a 4.4.

Pokud se spojení s monitorovacím programem přes socket nepodaří, munin vyhodnotí sledování jako nefunkční (v grafu se u položky „running“ objeví hodnota 100) a ostatní čítače budou v grafech nastaveny na nulu.

```
historyErr.value 0
futureErr.value 0
running.value 0
```

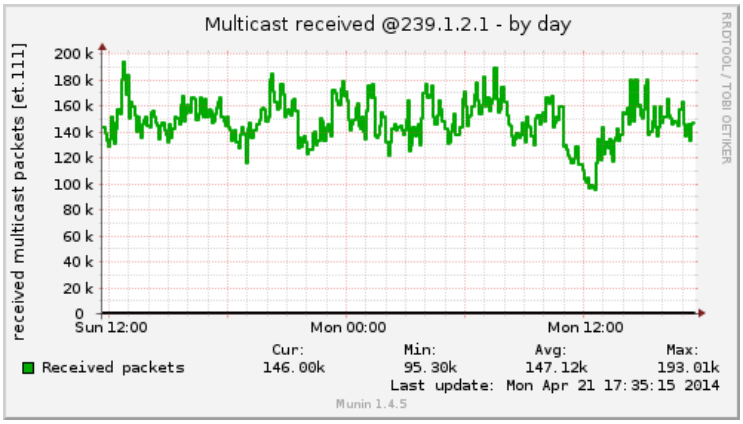
Ukázka 4.3: Odpověď monitorovacího skriptu na požadavek „lost“ přes socket

```
pcktCount.value 111604
```

Ukázka 4.4: Odpověď monitorovacího skriptu na požadavek „pcktnum“ přes socket

4.2.9 Výsledky

Obsah je dále zpracován skripty v systému munin a následně jsou vygenerovány grafy (ukázka na obrázcích 4.5 a 4.6).



Obrázek 4.6: Příklad výstupu monitorovacího systému - graf přijatého počtu paketů

V případě prvního grafu se jedná o detekci chyb, kde jsou vidět malé problémy na lince v náhodných intervalech.

U druhého grafu je vidět počet přijatých paketů, kde monitorovaným programem byl kanál ČT1. Na grafu je vidět variabilní datový tok tohoto kanálu.

V grafech jsou jednotlivé hodnoty normalizované v čase. Díky tomu nejsou jednotlivé čítače během 5 minut naprosto přesně zaneseny do grafů. To je způsobeno tím, že munin hodnoty nevybírá v přesně daných intervalech (vždy dojde alespoň k minimálnímu zpoždění při výběru dat přes síť). Pro lepší přesnost munin výsledky čítačů chyb přepočítá do stejných časových úseků [62].

4.3 Problémy v síti

Při nasazení vícesměrového provozu bylo zjištěno mnoho problémů, které ale pramenily pouze z několika chyb v síti. V této části jsou uvedeny problémy, na které se během zkušebního provozu IPTV v síti přišlo.

Zároveň byl stanoven proces pro řešení problémů přímo u klientů. Díky velké hustotě sond po celé síti nebylo nutné čekat na stížnost uživatele kvůli nefunkční televizi. Přesto bylo stanoveno, že v případě zaznamenaného problému, který nelze jednoznačně identifikovat pomocí stávající sítě sond, bude síť rozšířena o sondu buď přímo u koncového uživatele, nebo v rozvaděči domu, kde uživatel bydlí.

4.3.1 MikroTik neighbor discovery

U směrovačů Routerboard, které byly nasazeny u klientů pro IPTV byly detekovány rámce vycházející z jednotlivých zařízení do každé VLAN (pravidelně

1 paket během několika sekund). Vzhledem k implementaci v případě vyššího počtu zařízení v síti by tento provoz mohl být velký.

Tyto pakety byly identifikovány jako součást *neighbor discovery protokolu* implementovaného v systému MikroTik RouterOS [40]. Tato funkce slouží k rozpoznání konfigurace systému a slouží k jednoduchému a rychlému připojení do managementu směrovačů. Tato funkce není potřebná k provozu IPTV. Zbytečně tak zatěžuje síť. Byla provedena deaktivace této funkce pro IPTV VLAN pomocí příkazu 4.5. Nejdříve bylo nutné vypsat jednotlivé rozhraní a k nim přiřazená čísla. Následně bylo nutné dle těchto čísel funkci díky znalosti čísla rozhraní vypnout.

```
/ip neighbor discovery print
/ip neighbor discovery set 4 disabled=yes
```

Ukázka 4.5: Vypnutí funkce neighbor discovery v IPTV VLAN

4.3.2 Problém přetíženého okruhu

U propojení jednotlivých páteřních bodů v distribuční síti došlo k přetížení okruhu o kapacitě 1 Gb/s. Okruh byl vytížen tokem dosahujícím hodnot 800 Mb/s a přepínač odesílající data do okruhu musel některé pakety vyřazovat. Po porovnání s průtokem se tento jev objevoval nahodile u průměrného zatížení, které přesahovalo 800 Mb/s. Problémem je, že se dané zatížení velmi špatně detekuje, jelikož v souhrnných grafech datového provozu se jedná o agregované pětiminutové statistiky. Na eliminaci tohoto přetížení neměl vliv ani aktivovaný QoS na obou stranách linky (ani při zvýšení velikosti front). Výpis informací z přepínače je vidět na ukázce číslo 4.6. V ní je viditelné velké množství vyřazených paketů u všech tříd provozu, což svědčí o přetížení rozhraní.

```
switch# run show interfaces ge-0/1/3 detail | find egress
Egress queues: 8 supported, 5 in use
Queue counters: Queued packets  Transmitted packets     Dropped\
                                                        packets
0 best-effort   0               341799766793            690642
1 assured-forw  0               0                       0
4 iptv          0               363631362               25296
5 expedited-fo  0               0                       0
7 network-cont  0               128761517               395224
```

Ukázka 4.6: Výpis statistik v přepínači

Bylo doporučeno zvýšit kapacitu okruhu alespoň na 2 Gb/s. Nakonec došlo ke zvýšení kapacity linky na 10 Gb/s podobně jako u hlavních linek a problém byl odstraněn. Zároveň bylo doporučeno mnohem více sledovat čítače vyřazených paketů na jednotlivých prvcích v síti v monitorovacím systému.

4.3.3 Využití záložního okruhu v případě výpadku hlavního

Díky výpadku hlavního okruhu byla IPTV nedostupná v celé síti. Díky záložnímu okruhu bylo možné zálohovat IPTV VLAN v případě výpadku hlavního optického okruhu. Na přepínačích byl nakonfigurován protokol VSTP a poté byla vytvořena smyčka, kterou protokol přerušil.

```
switch> set protocols vstp vlan IPTV_Sit
```

Zároveň bylo nutné přidat na prvek přepisovací pravidlo pro označení procházejících paketů pro druhý (záložní) okruh.

```
switch# edit class-of-service
switch# set interfaces ge-0/0/0 unit 0 rewrite-rules\
dscp iptv_dscp
```

Díky automatickému výpočtu ceny dle rychlosti jednotlivých rozhraní bylo rovnou zajištěno zablokování VLAN přes záložní okruh.

```
switch> show spanning-tree interface

Interface     Port ID     Designated       Designated          Port\
State  Role
                           port ID          bridge ID           Cost

ge-0/0/0.0    128:561       128:561   33278.0881f4ab8741      30000\
BLK    DESG
ge-0/0/1.0   128:529       128:529   33278.0881f4ab8741      30000\
FWD    DESG
xe-0/1/2.0    128:563       128:563   33278.0881f4ab8741       2000\
FWD    DESG
```

Záložní okruh byl tedy díky této konfiguraci využit i pro IPTV v případě výpadku hlavního okruhu.

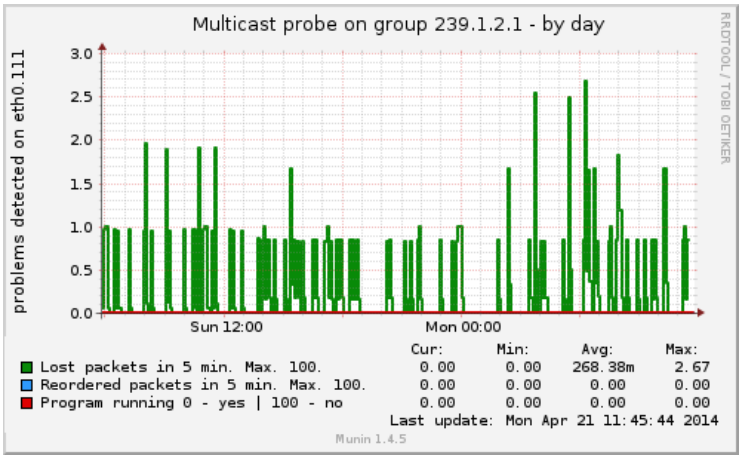
4.3.4 Flow control

Některé bezdrátové spoje se i přes aktivovanou funkci DSCP QoS a omezení datového průtoku potýkaly se ztrátami při přenosu. Byla aktivována funkce *flow-control* v přepínačích před spoji i přímo v nastaveních spojů, díky které došlo k menšímu zahlcení vnitřní jednotky bezdrátového pojítka.

Tato funkce umožňuje komunikaci mezi zařízeními pomocí druhé vrstvy ISO/OSI protokolu. Prvek, který je zahlcen, může poslat přímo propojenému prvku tzv. rámec pro dočasné přerušení vysílání [37].

4.3.5 Problémy na bezdrátovém spoji AirFiber

Ihned po nasazení sondy za první spoj AirFiber byly detekovány výpadky provozu. Vždy šlo o velké výpadky trvající několik desítek sekund. Na spoji byl nasazen nejnovější oficiální firmware v1.5. Po nasazení nejnovější vývojové verze



Obrázek 4.7: Výstup sond v páteřní síti

v2.0 beta-1 výpadky zmizely. Dle seznamu změn vydaných firmou Ubiquiti networks pro nejnovější beta firmware nebylo zřejmé, jestli došlo k opravě či ke zlepšení průchodnosti paketů skrz spoj. Po zaslání dotazu na neveřejné „beta fórum“ firmy Ubiquiti Networks bylo specifikováno, že ke změně došlo. U starých verzí docházelo k zahlcení CPU spoje vícesměrovými pakety. Verze 2.0 beta-1 přinesla možnost filtru, aby se tento provoz do CPU nedostal. Zároveň u staršího firmware existovalo řešení díky vypnutí funkce *in-band management*.

4.4 Referenční lokality

4.4.1 Okruhy na páteřní síti

Monitorovací sondy vykazovaly (až na případ přetíženého okruhu, který byl vyřešen) podobné výsledky. Okruhy tedy fungovaly bezchybně a od vstupní sondy se žádné pakety při přenosu sítí neztratily.

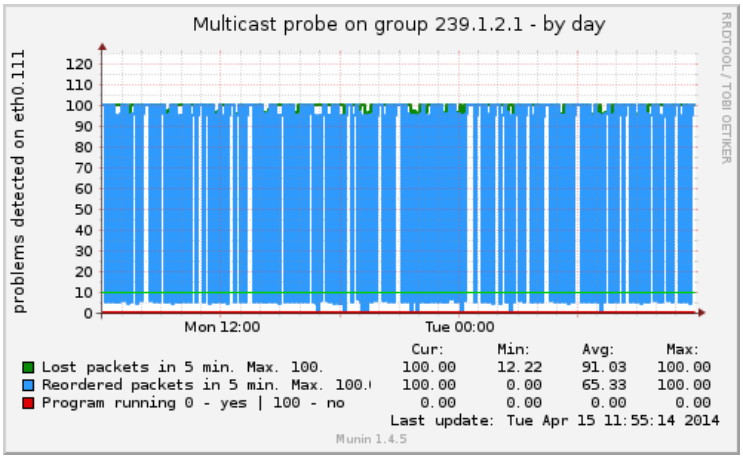
Výstup z monitorovacích sond je vidět na obrázku 4.7. Malé výpadky v řádu jednotek paketů nejsou na televizním obrazu znát.

4.4.2 Modletice

V Modleticích byla sonda umístěna do jednoho z panelových domů a byla zapojena do jednoho z přepínačů. Sonda nedetekovala výraznější chyby oproti sondám v optické síti.

4.4.3 Říčany

V Říčanech sonda detekovala velké problémy u vícesměrového vysílání. Její výstup je možné vidět na obrázku 4.8. Byla zapojena přímo do hlavního pře-



Obrázek 4.8: Výstup sondy v Říčanech

pínače v hlavním domě. Za viníka v kontrastu se stavem v Nupakách bylo možné označit bezdrátový spoj AirFiber, který v této oblasti fungoval ve zkušebním režimu. Signál datového spoje byl v tomto případě „na hraně“ a sonda tuto skutečnost ihned odhalila. Na jiném místě, které není referenční lokalitou, spoj AirFiber fungoval bez problému. Délka spoje však byla pouze 400 metrů.

Bylo doporučeno vyměnit spoj na Říčany za jiný operující v pásmech vhodných pro spoje na větší vzdálenosti.

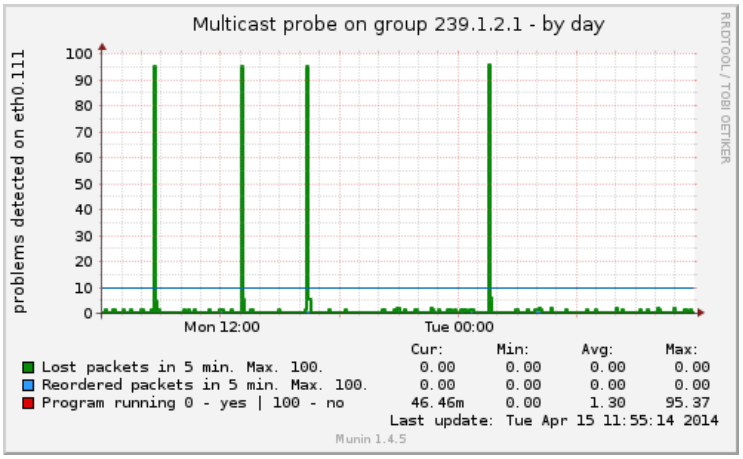
4.4.4 Nupaky

V Nupakách sondy naměřily větší odchylky v chybovosti od sond v páteřní síti. Jedna sonda byla umístěna přímo za přepínačem v domě s páteřním spojem, druhá za bezdrátovým spojem v pásmu 5 GHz. Vždy nárazově ve vybraném čase bylo naměřeno o něco více chyb (výpadek několika set paketů najednou). Tyto chyby se na přijímačích projevovaly rozpadáváním obrazu. Jelikož chyby nenastávaly často, bylo možné IPTV spustit. Výstup ze sondy je možné vidět na obrázku 4.9.

Jako zdroj chyb byly teoreticky identifikovány prvky ležící mezi páteřní sítí a přepínačem v Nupakách, tedy bezdrátový spoj NEC nebo jeden z přepínačů. Problém se ke dni odevzdání této práce nepodařilo vyřešit.

4.4.5 Praha 4 - Libuš

Výsledné naměřené hodnoty v oblasti nebyly rozdílné oproti těm, které naměřila sonda v optické síti. Trasa směrem do této oblasti tedy byla v pořádku a IPTV bylo možné oficiálně spustit.



Obrázek 4.9: Výstup sondy v Nupakách

Závěr

V práci se podařilo kompletně zmapovat problematiku nasazení IPTV řešení. Byly shrnuty nejčastěji využité platformy v sítích, z nichž byla jedna vybrána a posléze nasazena v reálném prostředí. Zároveň byly shrnuty možné způsoby nasazení služby IPTV s vícesměrovým vysíláním.

Bylo vytvořeno řešení založené na systému OpenWRT pro klientská zařízení, která oddělují IPTV od ostatních dat směřujících z koncových částí sítě do domácností uživatelů. Zároveň byla popsána možnost nastavení směrovače s operačním systémem MikroTik RouterOS. V obou případech byly popsány možnosti, které co nejméně zatěžovaly CPU jednotlivých zařízení.

Velkým přínosem této práce je monitorovací řešení, které již v rámci nasazení odhalilo chyby a umožnilo vidět problémy ve zkušební fázi před nasazením IPTV u koncových uživatelů. Díky nenáročnému běhu umožní řešení sond administrátorům efektivní dohled nad infrastrukturou, prostřednictvím které je vícesměrové vysílání šířeno. Jednotlivé poznatky a výstupy byly sepsány díky praktickému nasazení a tak se podařilo ověřit, že řešení funguje v praxi a dokáže odhalit chyby v síti.

Díky analýze chyb při průtoku vícesměrového vysílání se podařilo nejen najít problematická místa v síti, ale podařilo se také vyřešit problémy, které způsobovaly různé chyby při přenosu ostatních dat. Tyto problémy by bylo velmi těžké odhalit hlavně díky způsobu běžných přenosů pomocí protokolu TCP. Vícesměrový provoz se tedy ukázal jako výborný zatěžkávací test pro síť a po napsání všech částí této práce lze prohlásit, že pouze opravdu dobře postavená síť se vyznačuje bezproblémovým průchodem vícesměrového vysílání. Všechny cíle se tedy podařilo splnit.

Výsledkem celé implementace bylo oficiální spuštění IPTV do „ostrého“ provozu pro koncové uživatele. To znamenalo mnoho práce s odladěním všech prvků v síti (síť nasazení obsahovala velké množství různých druhů zařízení od různých výrobců). Ke dni odevzdání této práce již televizi přijímalo více než 50 uživatelů. Autor této práce dosud nezná žádnou podobnou práci v České republice, která by se s takovým zaměřením zabývala podobným tématem a

vzniklo by díky ní takto ucelené řešení mapující problematiku doručení vícesměrového provozu k uživatelům.

Možné pokračování této práce vidí autor v případě monitorovacích sond ve vývoji komplexnějšího monitorovacího systému, který by umožnil přímé porovnání trendů naměřených v různých částech sítě. To by umožnilo administrátorům velkých sítí mnohem rychleji lokalizovat a vyřešit detekovaný problém.

Klientské směrovače je možné dále rozšířit přidáním nových funkcí. Pro uživatele by byla vhodná vzdálená správa. V ní by měl každý uživatel možnost spravovat vzdáleně svůj vlastní domácí router prostřednictvím zjednodušených stránek (nastavení by například mohlo probíhat prostřednictvím zákaznického portálu poskytovatele).

Literatura

[1] Alcoma a.s.: *| Mikrovlnné spoje – pojítka a antény nejen k WiFi sítím | Alcoma a.s. [online].* [cit. 2014-02-15]. Dostupné z: `http://www.alcoma.cz/cz/katalog/free+bands/all+outdoor/al17f+mp600/`

[2] Alcoma a.s.: *Dohledový systém ASD | Mikrovlnné spoje - pojítka a antény nejen k WIFI sítím | Alcoma a.s. [online].* [cit. 2014-03-01]. Dostupné z: `http://www.alcoma.cz/cz/sekce/dohledovy+system+asd/`

[3] Alcoma a.s.: *Katalog produktů | řešení FULL OUTDOOR | Mikrovlnné spoje – pojítka a antény nejen k WiFi sítím | Alcoma a.s. [online].* [cit. 2014-02-15]. Dostupné z: `http://www.alcoma.cz/cz/katalog/all+outdoor/`

[4] Allstar Group s.r.o.: *EasyTV IPTV Middleware | EasyTV - IPTV pro ISP, hotely a nemocnice [online].* [cit. 2014-02-01]. Dostupné z: `http://www.easytv.cz/easy-iptv-middleware/`

[5] Allstar Group s.r.o.: *Hlavní reference | EasyTV - IPTV pro ISP, hotely a nemocnice [online].* [cit. 2014-02-01]. Dostupné z: `http://www.easytv.cz/reference/`

[6] Alnair a.s.: *Multibitrate and Storage Solved, Part III of VI | nangu.TV [online].* [cit. 2014-02-15]. Dostupné z: `http://nangu.tv/blog/2012-06/multibitrate-and-storage-solved-part-iii-vi`

[7] Alnair a.s.: *Nangu.tv [online].* [cit. 2014-02-01]. Dostupné z: `http://nangu.tv/overview`

[8] ANTIK Technology s.r.o.: *Juice Middleware /// Antik Technology [online].* [cit. 2014-02-01]. Dostupné z: `http://www.antiktech.com/software-iptv-solutions/juice-set-top-box-middleware`

[9] ASPA, a.s.: *Jak na IPTV | DSL.cz [online].* [cit. 2014-03-04]. Dostupné z: http://www.dsl.cz/jak-na-to/4-sluzby-k-pripojeni/33-jak-na-iptv

[10] Cisco Systems, Inc.: *Multicast VLAN Registration (MVR) [online].* [cit. 2014-03-18]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-0SY/configuration/guide/15_0_sy_swcg/ipv4_mvr.pdf

[11] CLARYSTONE s.r.o.: *MINI-LINK - Ericsson [online].* [cit. 2014-02-15]. Dostupné z: http://www.mini-link.cz/obchod.mini-link-cn-500.aspx

[12] CLARYSTONE s.r.o.: *MINI-LINK - Ericsson [online].* [cit. 2014-02-15]. Dostupné z: http://www.mini-link.cz/reference.aspx

[13] CLARYSTONE s.r.o.: *MINI-LINK - Ericsson [online].* [cit. 2014-03-01]. Dostupné z: http://www.mini-link.cz/mini-link.dohledovy-system.aspx

[14] D., I. A. O. P.: *DIGITÁLNÍ VIDEO Metodická příručka.* 2011. Dostupné z: http://www.person.vsb.cz/cz/kurzy/Digitalni%20video.pdf

[15] Ek, N.: *IEEE 802.1 P,Q - QoS on the MAC level [online].* Department of Electrical Engineering Helsinki University of Technology, 1999. Dostupné z: http://www.tml.tkk.fi/Opinnot/Tik-110.551/1999/papers/08IEEE802.1QosInMAC/qos.html

[16] IETF: *RFC 1112 - Host extensions for IP multicasting [online].* [cit. 2014-03-03]. Dostupné z: https://tools.ietf.org/html/rfc1112

[17] IETF: *RFC 2236 - Internet Group Management Protocol, Version 2 [online].* [cit. 2014-03-03]. Dostupné z: http://tools.ietf.org/html/rfc2236

[18] IETF: *RFC 3376 - Internet Group Management Protocol, Version 3 [online].* [cit. 2014-03-03]. Dostupné z: https://tools.ietf.org/html/rfc3376

[19] IETF: *RFC 3569 - An Overview of Source-Specific Multicast (SSM)[online].* [cit. 2014-03-03]. Dostupné z: https://tools.ietf.org/html/rfc3569

[20] IETF: *RFC 3973 - Protocol Independent Multicast - Dense Mode (PIM-DM) [online].* [cit. 2014-03-03]. Dostupné z: https://tools.ietf.org/html/rfc3973

[21] IETF: *RFC 4541 - Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches [online].* [cit. 2014-03-18]. Dostupné z: `https://tools.ietf.org/html/rfc4541`

[22] IETF: *RFC 4601 - Protocol Independent Multicast - Sparse Mode (PIM-SM) [online].* [cit. 2014-03-03]. Dostupné z: `https://tools.ietf.org/html/rfc4601`

[23] IETF: *RFC 5015 - Bidirectional Protocol Independent Multicast (BIDIR-PIM) [online].* [cit. 2014-03-03]. Dostupné z: `https://tools.ietf.org/html/rfc5015`

[24] IETF: *RFC 5771 - IANA Guidelines for IPv4 Multicast Address Assignments [online].* [cit. 2014-03-18]. Dostupné z: `https://tools.ietf.org/html/rfc5771`

[25] IETF: *RFC 988 - Host extensions for IP multicasting [online].* [cit. 2014-03-03]. Dostupné z: `https://tools.ietf.org/html/rfc988`

[26] Internet Info, s.r.o.: *Budoucnost kabelovek je v propojení DVB-C a IPTV, říká Antonín Král z nangu.TV - DigiZone.cz [online].* [cit. 2014-02-01]. Dostupné z: `http://www.digizone.cz/clanky/budoucnost-kabelovek-je-v-propojeni-dvb-c-a-iptv-mini-antonin-kral-z-nangu-tv/`

[27] Internet Info, s.r.o.: *Co je to hybridní televize HbbTV a jak tato platforma funguje? - DigiZone.cz [online].* [cit. 2014-03-15]. Dostupné z: `http://www.digizone.cz/clanky/co-je-hybridni-televize-hbbtv-a-jak-funguje/`

[28] Internet Info, s.r.o.: *IPTV v České republice - Architektura IPTV - Lupa.cz [online].* [cit. 2014-03-02]. Dostupné z: `http://www.lupa.cz/specialy/iptv/architektura-iptv/`

[29] Internet Info, s.r.o.: *IPTV v České republice - Co je IPTV a v čem se liší od kabelové televize - DigiZone.cz [online].* [cit. 2014-03-15]. Dostupné z: `http://www.digizone.cz/specialy/iptv/co-je-iptv-a-v-cem-se-lisi-od-kabelove-televize/`

[30] Internet Info, s.r.o.: *Jak funguje IPTV? - Lupa.cz [online].* [cit. 2014-03-15]. Dostupné z: `http://www.lupa.cz/clanky/jak-funguje-iptv/`

[31] Internet Info, s.r.o.: *O2TV se radikálně promění, opustí řešení od Alcatel-Lucent a přejde na nangu.TV - DigiZone.cz [online].* [cit. 2014-30-01]. Dostupné z: `http://www.digizone.cz/clanky/o2tv-se-radikalne-promeni-opusti-reseni-od-alcatel-lucent-a-prejde-na-nangu-tv/`

[32] Internet Info, s.r.o.: *Průvodce světem IPTV: největší poskytovatelé IP televize v České republice - DigiZone.cz [online].* [cit. 2014-02-01]. Dostupné z: http://www.digizone.cz/clanky/pruvodce-svetem-iptv-nejvetsi-poskytovatele-ip-televize-v-ceske-republice/

[33] Internet Info, s.r.o.: *Průvodce světem IPTV: Zpětný kanál a nejčastější způsoby jeho využití - DigiZone.cz [online].* [cit. 2014-03-04]. Dostupné z: http://www.digizone.cz/clanky/pruvodce-svetem-iptv-zpetny-kanal-a-nejcastejsi-zpusoby-jeho-vyuziti/

[34] Internet pro všechny, o.s.: *Spoj airFiber pro 24 GHz od Ubiquiti Networks – první doteky. Marketing versus skutečnost. [online].* [cit. 2014-02-15]. Dostupné z: http://www.internetprovsechny.cz/spoj-airfiber-pro-24-ghz-od-ubiquiti-networks-prvni-doteky-marketing-versus-skutecnost/

[35] Investopedia US, A Division of IAC.: *Compound Annual Growth Rate (CAGR) Definition | Investopedia [online].* [cit. 2014-03-01]. Dostupné z: http://www.investopedia.com/terms/c/cagr.asp

[36] ITU: *IPTV [online].* [cit. 2014-03-04]. Dostupné z: http://academy.itu.int/index.php/topics/item/328-iptv

[37] Jiří Peterka: *Jiří Peterka: flow control [online].* [cit. 2014-04-08]. Dostupné z: http://www.earchiv.cz/a95/a527k130.php3

[38] Juniper Networks, Inc.: *Example: Configuring VLAN Translation with a VLAN ID List - Technical Documentation - Support - Juniper Networks [online].* [cit. 2014-02-15]. Dostupné z: http://www.juniper.net/techpubs/en_US/junos13.3/topics/example/layer-2-bulk-configuration-example-vlan-translation-with-lists-example-mx-solutions.htmls

[39] Mikrotik: *Manual:Switch Chip Features - MikroTik Wiki [online].* [cit. 2014-02-15]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:Switch_Chip_Features

[40] Mikrotikls Ltd: *Manual:IP/Neighbor discovery - MikroTik Wiki [online].* [cit. 2014-02-30]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:IP/Neighbor_discovery

[41] Miracle Group, spol. s.r.o.: *1s10 [online].* [cit. 2014-02-15]. Dostupné z: https://www.orcave.com/orcave1s10

[42] Miracle Group, spol. s.r.o.: *Orcave [online].* [cit. 2014-02-15]. Dostupné z: https://www.orcave.com/

[43] NETFORMS s.r.o.: *Nasazení platformy :: 4network.tv [online]*. [cit. 2014-02-15]. Dostupné z: http://www.4network.tv/nasazeni-platformy

[44] NETFORMS s.r.o.: *Produkty :: NETFORMS s.r.o. [online]*. [cit. 2014-02-15]. Dostupné z: http://www.netforms.cz/produkty.html

[45] NETFORMS s.r.o.: *Reference :: 4network.tv [online]*. [cit. 2014-02-15]. Dostupné z: http://www.4network.tv/reference

[46] OpenWrt.org: *#12181 (VLAN tagging of TP-Link WDR4300 v1.1) - OpenWrt [online]*. [cit. 2014-02-01]. Dostupné z: https://dev.openwrt.org/ticket/12181

[47] OpenWrt.org: *About OpenWrt - OpenWrt Wiki [online]*. [cit. 2014-04-01]. Dostupné z: http://wiki.openwrt.org/about/start

[48] OpenWrt.org: *OpenWrt Buildroot – Usage - OpenWrt Wiki [online]*. [cit. 2014-02-15]. Dostupné z: http://wiki.openwrt.org/doc/howto/build

[49] Pavel Kysilka: *Munin - monitorování serverů -Linux software [online]*. [cit. 2014-03-01]. Dostupné z: http://www.linuxsoft.cz/article.php?id_article=1203

[50] Potůček, J.: *UPC začala nabízet kabelovku do počítače, tabletu a smartphonu. Zatím v Holandsku - DigiZone.cz [online]*.

[51] Samuraj: *Cisco QoS 1 - úvod do Quality of Service a Diffserv [online]*. [cit. 2014-03-18]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-qos-1-uvod-do-quality-of-service-a-diffserv/

[52] secdev.org: *Scapy*. [cit. 2014-03-01]. Dostupné z: http://www.secdev.org/projects/scapy/

[53] Sehnal, M.: *AirFIBER datasheet*. Dostupné z: http://dl.ubnt.com/datasheets/airfiber/airFiber_DS.pdf

[54] Sehnal, M.: *Sledování provozu protokolu PIM pro směrování multicastů [online]*. [cit. 2014-02-30]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/projekty0405/PIM_seh016.pdf

[55] Siklu: *EtherHaul 1200*. 2012. Dostupné z: http://gigabitradio.ru/wp-content/uploads/2013/09/Siklu-EH-1200-Install-User-Manual-EH-INSTL-02_Issue3-June-2012.pdf

[56] Slashroot.in: *Linux kernel rp_filter settings (Reverse path filtering) [online]*. [cit. 2014-03-18]. Dostupné z: http://www.slashroot.in/linux-kernel-rpfilter-settings-reverse-path-filtering

[57] Sledovanitv.cz s.r.o.: *Partneři sledovanitv.cz | sledovanitv.cz [online]*. [cit. 2014-20-01]. Dostupné z: http://www.sledovanitv.cz/info/partneri/

[58] Sledovanitv.cz s.r.o.: *sledovani.tv | sledovanitv.cz [online]*. [cit. 2014-20-01]. Dostupné z: http://www.sledovanitv.cz/

[59] SMART Comp a.s.: *Virtualizovaná IPTV [online]*. [cit. 2014-30-01]. Dostupné z: http://www.sc.cz/nase-sluzby/virtualizovana-iptv/

[60] *#11779 (WDR4300 - hardware nat feature) – OpenWrt [online]*. [cit. 2014-03-01]. Dostupné z: https://dev.openwrt.org/ticket/11779

[61] *Heureka.cz - Porovnání cen a srovnání produktů z internetových obchodů [online]*. [cit. 2014-01-30]. Dostupné z: https://http://www.heureka.cz/

[62] *RRDtool - Rates, normalizing and consolidating [online]*. [cit. 2014-03-01]. Dostupné z: http://www.vandenbogaerdt.nl/rrdtool/process.php/

[63] Telefónica Czech Republic, a.s.: *O2 | Videotéka [online]*. [cit. 2014-03-04]. Dostupné z: https://www.o2.cz/osobni/320906-videoteka/

[64] Tucny, D.: *DSCP TOS - tucny [online]*. [cit. 2014-03-01]. Dostupné z: http://www.tucny.com/Home/dscp-tos

[65] Ubiquiti Networks: *airFiber - How does airFiber handle QoS and frame priorization? - Ubiquiti Networks Community [online]*. [cit. 2014-03-15]. Dostupné z: http://community.ubnt.com/t5/airFiber-Frequently-Asked/airFiber-How-does-airFiber-handle-QoS-and-frame-prioritization/ta-p/456975

[66] Ubiquiti Networks: *AirMax - QoS DSCP/TOS Mappings - Ubiquiti Wiki [online]*. [cit. 2014-03-01]. Dostupné z: http://wiki.ubnt.com/AirMax_-_QoS_DSCP/TOS_Mappings

[67] Ubiquiti Networks: *Operating System for Ubiquiti M Series Products*. 2012-2013. Dostupné z: http://dl.ubnt.com/guides/airOS/airOS_UG.pdf

[68] Ubiquiti Networks, Inc.: *airMAX | Ubiquiti Networks, Inc. [online]*. [cit. 2014-02-15]. Dostupné z: http://www.ubnt.com/airmax#airMaxHardware

[69] UPC Business s.r.o.: *OneLine TV Vítejte [online]*. [cit. 2014-03-01]. Dostupné z: http://www.onelinetv.cz/

[70] UPC Netherlands: *Horizon - Televisie - UPC Nederland [online]*. [cit. 2014-03-01]. Dostupné z: http://www.upc.nl/televisie/horizon/

[71] Wikimedia Foundation, Inc.: *Duplex (telecommunications) - Wikipedia, the free encyclopedia [online]*. [cit. 2014-02-15]. Dostupné z: `http://en.wikipedia.org/wiki/Duplex_(telecommunications)`

[72] Wikimedia Foundation, Inc.: *IPTV - Wikipedia, the free encyclopedia [online]*. [cit. 2014-02-15]. Dostupné z: `http://en.wikipedia.org/wiki/IPTV`

[73] Wikimedia Foundation, Inc.: *Quality of Service - Wikipedia, the free encyclopedia [online]*. [cit. 2014-02-01]. Dostupné z: `http://cs.wikipedia.org/wiki/Quality_of_Service`

[74] Český telekomunikační úřad: *ZPRÁVA O VÝVOJI TRHU ELEKTRONICKÝCH KOMUNIKACÍ SE ZAMĚŘENÍM NA ROK 2012*. 2013. Dostupné z: `http://www.ctu.cz/cs/download/statisticke_udaje/rok_2013/zprava_vyvoj_trhu_ek_2012.pdf`

[75] Česká televize: *HbbTV aplikace České televize [online]*. [cit. 2014-03-01]. Dostupné z: `http://www.ceskatelevize.cz/hbbtv/`

Příloha A

Doplnění vybraných částí práce

A.1 Podrobné informace o monitorovacím programu

Tato část přílohy se zabývá podrobnějším vysvětlením funkce monitorovacího programu a zároveň obsahuje návod na spuštění tohoto programu.

A.1.1 Potřebné vybavení pro spuštění

Na sledovací sondě musí být:

- Operační systém GNU/Linux nainstalovaný na sledovacím zařízení včetně balíčků běžně přítomných na serverech
- Přítomna VLAN s vícesměrovým provozem (včetně její konfigurace v systému)
- Balíčky python, python-pcapy a python-scapy
- Sledovací agent munin-node

Na hlavním sledovacím serveru, který vybírá informace z jednotlivých sond musí být:

- Monitorovací program munin včetně korektního nastavení spouštění pomocí plánovače (cronu)
- Webový server
- RRDTool a další nástroje, které využívá systém munin k provozu

A.1.2 Spuštění sondy

Spustit sondu lze manuálně (v tomto případě je doporučeno spouštět IGMP klienta i sondu dohromady pomocí parametru „-r“).

Pro automatizované spuštění je připraven skript ve složce */etc/init.d*. Je nutné pozměnit cesty k programům přímo ve spouštěcím skriptu. Proměnná *DAEMON* značí cestu k monitorovacímu programu, proměnná *DAEMON2* cestu k programu *igmp_client*.

A.1.3 Zkušební spuštění programu

Pro ověření správné funkce sondy a správné konfigurace multicast VLAN je možné spustit monitorovací program v režimu plného ladění.

```
./multicast_monitor.py -i eth0.510 -g 239.250.1.1 -l 2 -d -r
```

Program poté začne vypisovat každý přijaty vícesměrový paket společně s informací, jestli dorazil korektně.

```
OK futureErr/historyErr:0/0 arrived pcktid 1 expected pcktid 1
OK futureErr/historyErr:0/0 arrived pcktid 2 expected pcktid 2
OK futureErr/historyErr:0/0 arrived pcktid 3 expected pcktid 3
OK futureErr/historyErr:0/0 arrived pcktid 4 expected pcktid 4
OK futureErr/historyErr:0/0 arrived pcktid 5 expected pcktid 5
```

Pokud v této fázi program nic nevypisuje, příjem vícesměrového vysílání v dané skupině není na sondě funkční.

Pro „živé“ zachytávání chyb je vhodné spustit monitorovací program v režimu ladění s potlačením informací o korektním provozu. Lze tak sledovat problémy v reálném čase.

```
./multicast_monitor.py -i eth0.510 -g 239.250.1.1 -l 1 -d -r
```

Ve výpisu se poté zobrazí tři druhy problémů:

- Chybně přijatý paket z budoucnosti *futureErr*
- Chybně přijatý paket z minulosti *historyErr*
- Velká chyba značí přijatý paket, který se se svým ID liší o více jak 1000 od ID očekávaného *bigErr*

Pokud nastane velká chyba, jsou oba čítače (chyb z budoucnosti i minulosti) při exportu shodně nastaveny na maximální hodnotu, tedy na 100. Dále v tomto režimu program informuje o resetování čítačů chyb pomocí hlášky o exportu (*EXPORTING*), která je vyvolána výběrem dat do programu munin.

A.1.4 Konfigurace agenta munin-node

Konfigurační soubor se nachází ve složce */etc/munin*, nazývá se *munin-node.conf*. Pro nastavení je nutné povolit IP adresu serveru, který se lokálního agenta bude dotazovat. V našem případě je adresa serveru 10.38.16.1.

```
...
allow ^10\.38\.16\.1$
...
```

Dále je nutné nastavit identifikátor agenta. V identifikátoru nesmí být velká písmena.

```
...
host_name sonda1-nupaky.iptv.sit.czf
...
```

Ke čtení jednotlivých informací ze sledovacích programů slouží dva skripty, které munin spouští. Nazývají se *mcast-probe* a *mcast-pkts*. Ty je nutné nakopírovat do složky */usr/share/munin/plugins*. Následně je nutné vytvořit symbolický odkaz ve složce */etc/munin/plugins* pro tyto skripty.

```
ln -s /usr/share/munin/plugins/mcast-probe\
/etc/munin/plugins/mcast-probe
ln -s /usr/share/munin/plugins/mcast-pkts\
/etc/munin/plugins/mcast-pkts
```

Po provedení příkazů bude čtení z monitorovacích skriptů aktivováno. Pro jistotu lze vše ověřit pomocí příkazu.

```
munin-node-configure | grep mcast

mcast-probe     | yes  |
mcast-pkts      | yes  |
```

A.1.5 Konfigurace monitorovacího programu munin

Munin funguje na hlavním monitorovacím serveru díky spuštění programu munin-cron a díky souboru s nastavením, který se nachází v souborovém systému v */etc/munin/munin.conf*. V tomto souboru je možné nastavit různé parametry od cesty k souborům pro ladění až po umístění webových stránek v souborovém systému, které jsou výstupem celého monitorovacího systému.

Pro sběr dat je nutné přidat na hlavním serveru řádku s adresou sondy včetně jejího názvu.

```
...
[sonda-nupaky.iptv.sit.cz]
    address 10.38.166.231
    use_node_name yes
...
```

Během pěti minut by mělo dojít k vygenerování grafů s prvními hodnotami.

A.1.6 Problémy

Pokud čtení pomocí systému munin nefunguje správně, existují dvě metody diagnostiky problému. Obvykle se chyba nachází přímo v sondě, případně v konfiguračním souboru systému munin.

Lokálně lze vyloučit problém na sondě pomocí spuštění programu *munin-run*. Ten spustí daný skript agenta a ukáže hodnoty. Skripty systému munin využívají parametru *config* pro zjištění podrobností o generovaných grafech, případně se spouští i bez parametru pro výběr aktuálních hodnot. Pokud program vypíše chybu, skript nefunguje správně nebo je špatně realizováno jeho nastavení v systému munin.

Druhou možností je problém v síti. Agent monitorovacího programu munin na každé sondě poslouchá na portu 4949. Funkčnost spojení lze ověřit z povolených IP adres (z hlavního monitorovacího serveru) pomocí programu telnet. Příkazem *fetch mcast_probe* lze získat aktuální naměřená data. Dále je možné například pomocí příkazu *list* zjistit aktuálně povolené monitorovací služby.

A.2 Informace o klientských směrovačích TP-LINK se systémem OpenWRT

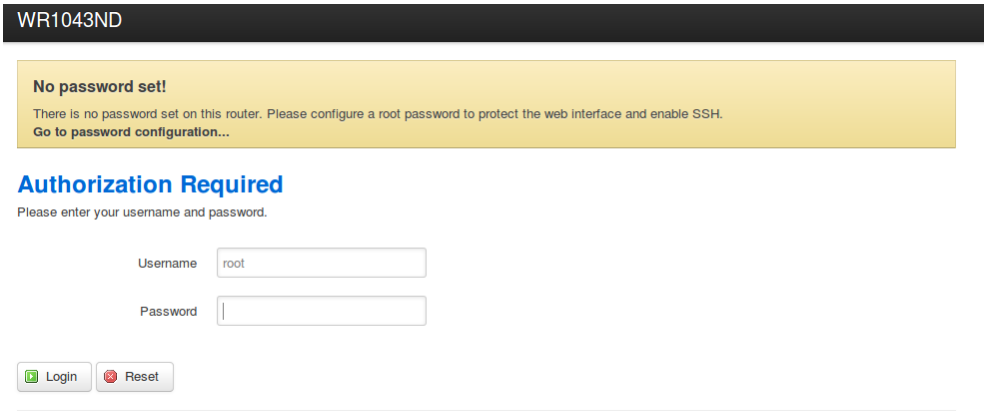
Systém OpenWRT je využit v práci pro klientské řešení oddělení IPTV provozu od internetu. Tato zařízení mají koncoví uživatelé přímo doma a tak lze místo kombinace více zařízení využít směrovače TP-LINK jako domácí brány i jako oddělovače IPTV provozu. K tomu slouží realizace sítě, kdy je využit NAT u provozu procházejícího WAN portem. U modelu TP-LINK WR1043nd lze využít i bezdrátovou část.

V této části přílohy bude zmíněno referenční nastavení routeru WR1043nd včetně NAT a Wi-Fi pro použití zařízení jako kompletní domácí brány pro IPTV provoz.

Administrační rozhraní je možné vidět na obrázku A.1. Jedná se o administrační systém Luci, který existuje jako balíček systému OpenWRT a přidává možnost jednoduché správy přes webové rozhraní.

Jak je uvedeno v nastavení na obrázku A.2, přepínač je v případě využití funkce NAT nastaven tak, že VLAN s označením 2 probíhá mezi jedním z CPU portů (portem číslo 6) a WAN portem číslo 5 bez označení. Tento CPU port je poté v systému reprezentován jako eth0.

Přes port eth1 (na obrázku A.2 port CPU nebo v případě nastavení port 0) poté probíhá komunikace vnitřní sítě, která funguje bez označení na portech 2-4. Nastavení je vidět na obrázku A.3. Na port 1 je svedena přímo z WAN portu VLAN pro IPTV, kde je na WAN portu označena a na portu 1 neoznačena. Systém podporuje protokol IPv6, který funguje díky *router-advertisement* a *router-solicitation* zprávám a umožňuje klientům na LAN části využít IPv6

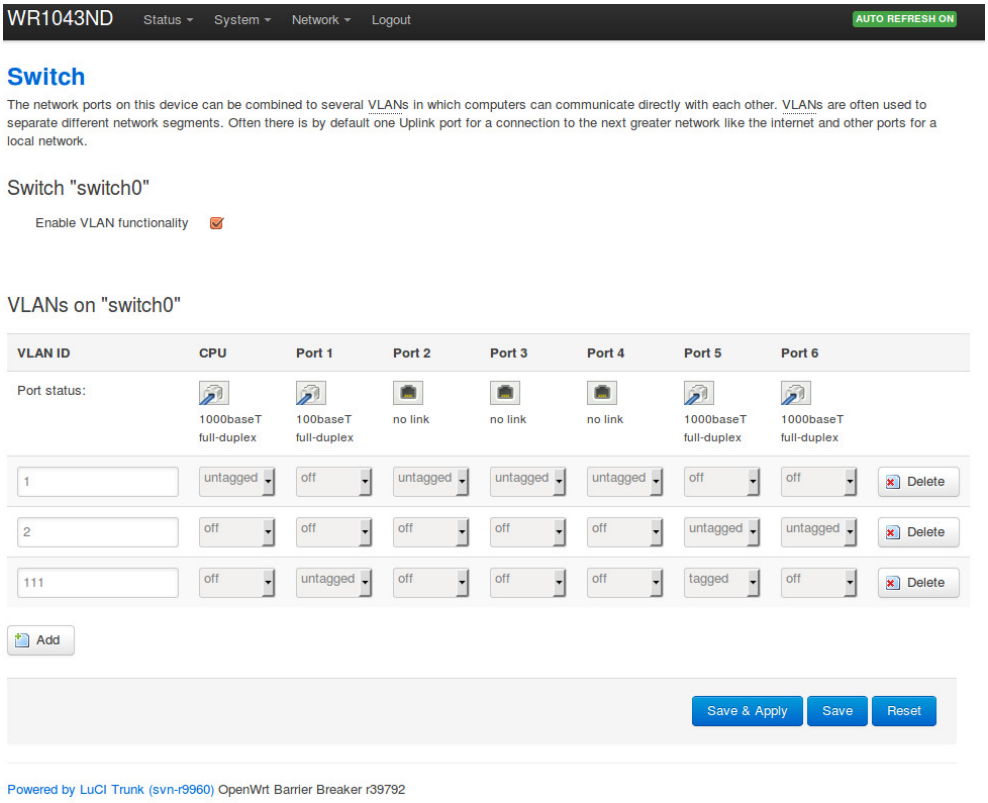


Obrázek A.1: Přihlašovácí stránka administračního rozhraní Luci (systém OpenWRT)

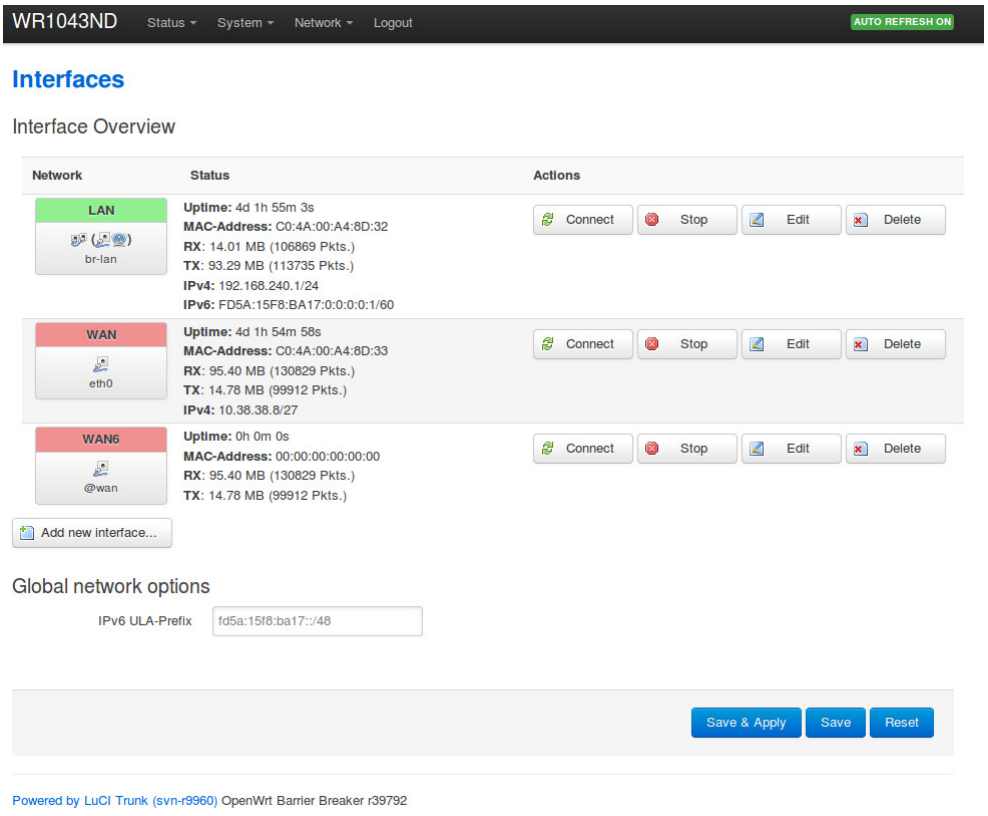
protokol od poskytovatele připojení. Nastavení Wi-Fi je možné vidět na obrázku A.4

V systému existují konfigurační soubory, které systém Luci vytváří nebo edituje. Nacházejí se v souborovém systému ve složce */etc/config*. Nejdůležitějším souborem pro nastavení síťového provozu je soubor network. Pro nastavení bezdrátové části je nutné se zaměřit na soubor wireless.

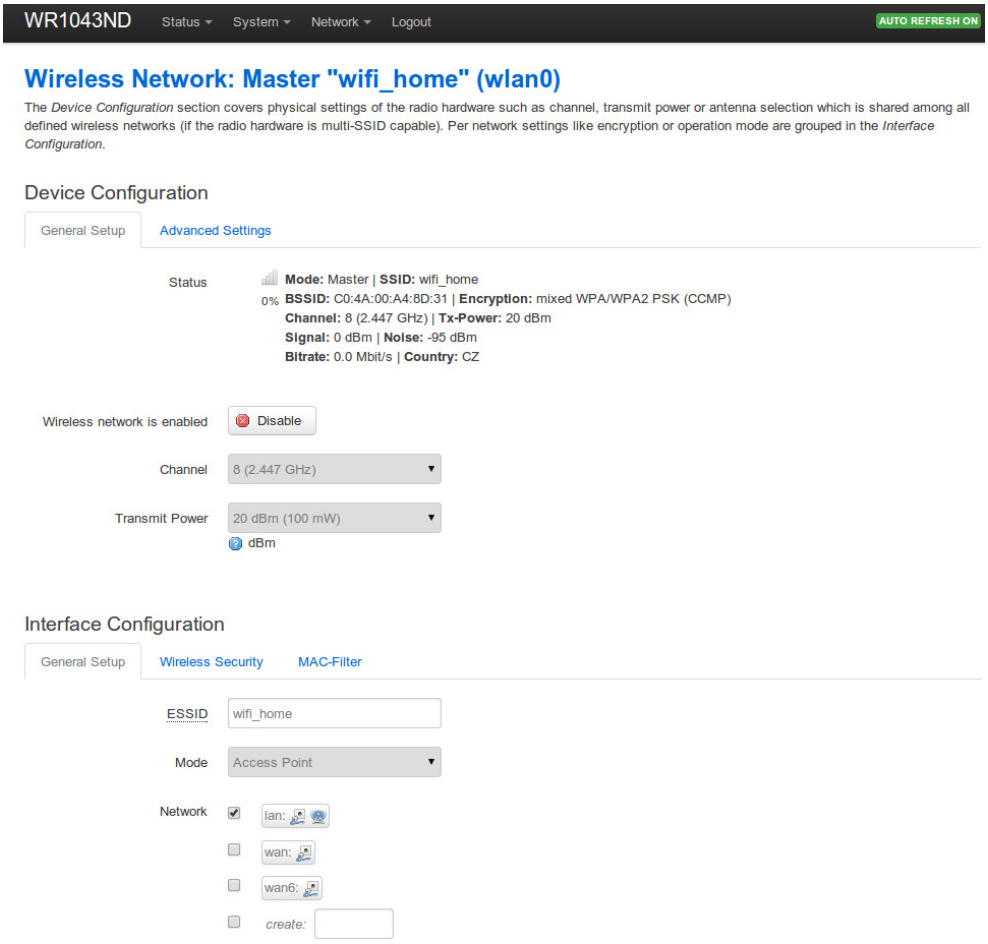
Ke směrovači je možné se také připojit pomocí programu telnet (pokud není nastaveno administrátorské heslo), případně pomocí protokolu SSH (pokud heslo nastavené je). K dispozici je pak běžná příkazová řádka skriptovacího jazyku BASH, prostřednictvím kterého lze spouštět programy pro přímou editaci konfiguračních souborů. Jako programy pro změnu nastavení lze využít příkazový systém Uci nebo libovolný textový editor. Již vytvořený soubor network pro provoz IPTV je vidět na ukázce A.1.



Obrázek A.2: OpenWRT Luci nastavení interního přepínače



Obrázek A.3: OpenWRT Luci nastavení síťových mostů a adres



Obrázek A.4: OpenWRT Luci nastavení bezdrátové sítě

```
 root@WR1043ND:~# cat /etc/config/network

config interface 'loopback'
        option ifname 'lo'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'

config globals 'globals'
        option ula_prefix 'fd5a:15f8:ba17::/48'

config interface 'lan'
        option ifname 'eth1'
        option type 'bridge'
        option proto 'static'
        option netmask '255.255.255.0'
        option ip6assign '60'
        option ipaddr '192.168.240.1'

config interface 'wan'
        option ifname 'eth0'
        option proto 'dhcp'

config interface 'wan6'
        option ifname '@wan'
        option proto 'dhcpv6'

config switch
        option name 'switch0'
        option reset '1'
        option enable_vlan '1'

config switch_vlan
        option device 'switch0'
        option vlan '1'
        option vid '1'
        option ports '0 2 3 4'

config switch_vlan
        option device 'switch0'
        option vlan '2'
        option ports '5 6'
        option vid '2'

config switch_vlan
        option device 'switch0'
        option vlan '3'
        option vid '510'
        option ports '1 5t'
```

Ukázka A.1: Konfigurační soubor *network* systému OpenWRT pro IPTV

A.3 Konfigurace páteřních prvků

V této části budou vypsány postupy pro nastavení jednotlivých přepínačů a směrovačů v síti pro průchod IPTV.

A.3.1 Nastavení páteřního přepínače, který směruje provoz od provozovatele platformy

VLAN 112 slouží pro komunikaci s partnerem, kdežto VLAN 111 slouží pro uživatele lokální sítě a jejich set-top-boxy.

```
switch# set vlans IPTV_Prijem vlan-id 112
switch# set vlans IPTV_Prijem l3-interface vlan.112
switch# set interface ge-0/0/1 unit 0 family ethernet-switching\
port-mode trunk
switch# set interface ge-0/0/1 unit 0 family ethernet-switching\
vlan members IPTV_Prijem
switch# set vlans IPTV_Sit vlan-id 111
switch# set vlans IPTV_Sit l3-interface vlan.111
```

Na jednotlivá rozhraní bylo nutné přidat IP adresy.

```
switch# set interfaces vlan unit 112 family inet address\
172.16.4.218/29
switch# set interfaces vlan unit 111 family inet address\
172.16.253.1/23
```

V případě interní VLAN sloužící klientům sítě bylo nutné nakonfigurovat DHCP relay pro získání adres od provozovatele platformy.

```
switch# set forwarding-options helpers bootp interface vlan.111\
server 172.1.2.3
```

Pro případnou kontrolu protokolu PiM je možné přidat soubor pro ladění. Soubor je poté možné vypsat například pomocí příkazu „cat“ v konzolovém řežimu. Soubor se po uložení nastavení nachází v souborovém systému v umístění */var/log/pim.log*.

```
switch# set protocols pim traceoptions file pim.log
switch# set protocols pim traceoptions flag normal
```

Na rozhraní směrem k poskytovateli bylo nutné zvolit mód dense.

```
switch# set interface vlan.112 mode dense
switch# set interface vlan.112 hello-interval 105
switch# set interface vlan.112 override-interval 2500
```

A.3.2 Nastavení jednotného označení DSCP pole na vstupu do sítě na přepínačích Juniper

Jelikož bylo nutné IPTV provoz v síti poznat a aplikovat na něj pravidla, která jej zvýhodní, bylo nutné na hraničním přepínači Juniper označit veškerý

provoz směrovaný od provozovatele IPTV. Jednalo se tedy o nastavení části nazvané *class-of-service* v přepínači.

```
switch# edit class-of-service
```

Ve skupině iptv_entry bylo nutné označit všechny pakety s DSCP poli s hodnotami v binárním kódu 000111 000000 000001 111000 (provozovatel platformy používá různá značení u různých kanálů). Ty byly následně změněny na jednotnou hodnotu 100000 v binárním kódu.

```
switch# set classifiers dscp iptv_dscp forwarding-class\
video loss-proority low code-points [ 000111 000000 000001 111000]
```

Jelikož byla fronta číslo 5 volná, využila se k účelu priorizace.

```
switch# set forwarding-classes class video queue-num 5
```

Bylo nutné přepsat obsah DSCP polí u všech paketů, které spadaly do skupiny *iptv_entry* na obsah 100000 binárně.

```
switch# set rewrite-rules dscp iptv_dscp forwarding-class video\
loss-priority low code-point 100000
```

Zároveň bylo nutné propojit plánovače mezi sebou. Vše co spadalo do třídy *video* muselo být párováno na plánovač *iptv_entry*.

```
switch# set scheduler-maps iptv_dscp forwarding-class video\
scheduler iptv_dscp
switch# set schedulers iptv_dscp priority low
```

Nakonec bylo nutné přiřadit nastavení k jednotlivým portům. Vstupní port ge-0/0/1 (propojení k IPTV provozovateli) byl klasifikován. Na port xe-0/1/0 (hlavní okruh) bylo přiřazeno přepisovací pravidlo.

```
switch# set interfaces xe-0/1/0 unit 0 rewrite-rules\
dscp iptv_dscp
switch# set interfaces ge-0/0/17 unit 0 classifiers dscp jmnet
```

Díky této konfiguraci tedy všechen provoz přicházející od IPTV operátora a vycházející portem do sítě splňující obsah DSCP polí dle konfigurace měl nastavenu hodnotu DSCP pole binárně na 100000. To umožňovalo dále v síti upřednostňovat tento typ provozu (jednotlivé prvky věděly, že provoz s tímto označením je IPTV).

A.3.3 Nastavení upřednostnění IPTV paketů dle hodnoty DSCP pole na přepínačích Juniper

Byla nastavena část zvaná class-of-service.

```
switch#edit class-of-service
```

Bylo nutné nutné importovat standardní nastavení DSCP, následně bylo nutné zvlášť priorizovat pakety s hodnotou DSCP pole 100000 (dle přeznačení paketů na hlavním prvku).

```
switch#set classifiers dscp net_classifiers import default
switch#set classifiers dscp net_classifiers forwarding class\
iptv loss-priority low code-points 100000
```

Televiznímu provozu od zdroje byla přirazena volná fronta s číslem 4.

```
set forwarding-classess class iptv queue-num 4
```

Byly nastaveny parametry jednotlivých front. Pro „best-effort“ provoz, tedy provoz, který se neoznačil jinak, byl vyhrazen zbytek vyrovnávací paměti.

```
switch# set schedulers nc_scheduler buffer-size percent 5
switch# set schedulers video_scheduler buffer-size percent 50
switch# set schedulers video_scheduler priority low
switch# set schedulers be_scheduler transmit-rate remainder
switch# set schedulers be_scheduler buffer-size remainder
switch# set schedulers be_scheduler priority low
```

Bylo nutné párovat jednotlivé třídy provozu rozdělené pomocí klasifikátorů s jednotlivými frontami (plánovači).

```
switch# set scheduler-maps net_scheduler forwarding class\
network-control scheduler nc_scheduler
switch# set scheduler-maps net_scheduler forwarding class\
iptv scheduler video_scheduler
switch# set scheduler-maps net_scheduler forwarding class\
best-effort scheduler be_scheduler
```

Následně bylo dané nastavení front přiřazeno na port s příchozím IPTV provozem. Příklad ukazuje nastavení 10 Gb/s portu xe-0/1/1, případně agregovaného portu ae0 s aktivovanou funkci LACP s kapacitou 2 Gb/s.

```
switch# set interfaces xe-0/1/1 scheduler-map net_scheduler\
unit 0 classifiers dscp net_classifiers
switch# set interfaces ae0 scheduler-map net_scheduler unit 0\
classifiers dscp net_classifiers
```

Do jaké třídy provoz spadá bylo možné zjistit pomocí následujícího příkazu. Výpis je omezen a je z něj vybrána pouze důležitá část.

```
switch# run show interfaces ge-0/1/2 detail | find egress
Egress queues: 8 supported, 5 in use
Queue counters: Queued packets  Transmitted packets     Dropped\
                                                        packets
0 best-effort   0               338932364411            2790
1 assured-forw  0               0                       0
4 iptv          0               19422335                0
5 expedited-fo  0               0                       0
7 network-cont  0               124796471               0
```

V tomto případě bylo zřejmé, že některá data již prochází frontou IPTV. Důležité bylo, aby přepínač žádné pakety nevyřazoval, což bylo v daném příkladě v pořádku.

A.3.4 Nastavení přepínačů pro průchod IPTV

A.3.4.1 Juniper EX

V případě přepínačů Juniper a přednastavených VLAN bylo nutné nastavit na každém přepínači interval opakování *IGMP Query* zprávy. Dále bylo nutné také přířadit VLAN, ve které bude IGMP-snooping zapnut.

```
switch# set protocols igmp query-inteval 125
switch# set protocols igmp-snooping vlan IPTV_Sit
```

A.3.5 Edge-Core ES3528M

V případě prvku ES3528M je IGMP-snooping již přednastaven pro každou VLAN a je naopak nutné tuto funkci deaktivovat tam, kde není potřeba.

Pro nastavení DSCP není třeba konfigurovat jednotlivé fronty, jelikož přepínač má priority přednastaveny. Je proto nutné pouze aktivovat funkci DSCP QoS.

```
Vty-0(config)# no map ip precedence
Vty-0(config)# map ip dscp
```

A.3.5.1 Edge-Core ES4528V

Přepínač ES4528V disponuje konzolí i webovým administračním rozhraním. Pomocí konzole byl nakonfigurován protokol IGMP.

```
IGMP Mode enable
IGMP State 111 enable
IGMP Querier 111 disable
```

V případě DSCP QoS bylo nutné v přepínači nastavit vyšší frontu pro IPTV pakety.

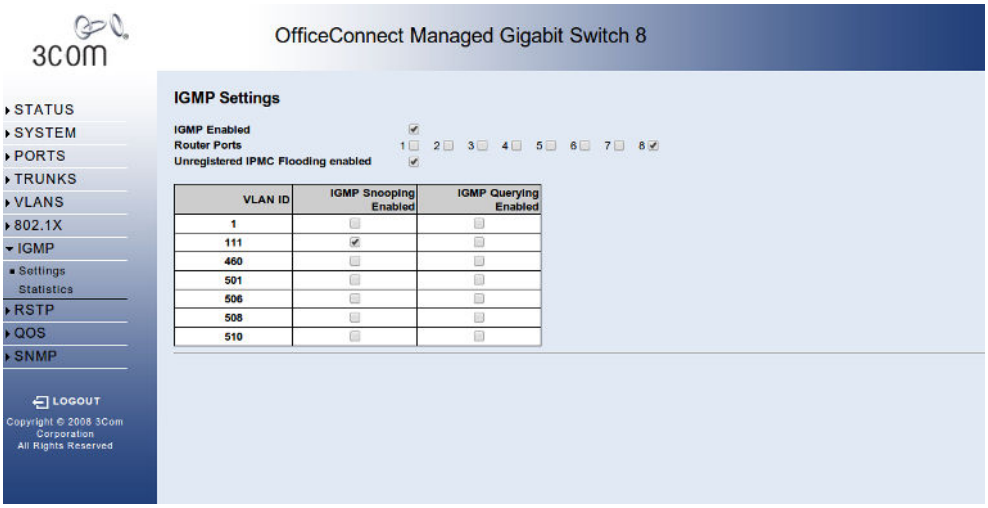
```
QoS QCL Add dscp 32 medium
```

A.3.5.2 HP V1900-8G

Přepínač HP V1900-8G disponuje webovým rozhraním pro veškerá nastavení. Po přihlášení (vyobrazeno na obrázku A.5 se v menu IGMP a v záložce settings objeví nastavení. Pro každou nově přidanou VLAN přepínač aktivuje IGMP-snooping včetně funkce IGMP-querying, což je nežádoucí.

Doporučovanou konfigurací bylo aktivovat IGMP a zároveň jako *router-port* vybrat rozhraní, kterým je přepínač připojen do sítě. Dále bylo nutné

Obrázek A.5: Přihlašovací stránka přepínače HP V1900



Obrázek A.6: Nastavení funkce IGMP-snooping v přepínači HP V1900

nakonfigurovat prvek tak, aby byl IGMP-snooping aktivován pouze v IPTV VLAN a zároveň bylo dotazování (*querying*) vypnuto, viz. obrázek A.6.

Při pokusu o aktivaci DSCP QoS v rozhraní přepínače se nastavení neukládá, tato funkce tedy není podporována.

Příloha **B**

Seznam použitých zkratek

IPTV Internet protocol television

DVB-S Digital video broadcasting - satellite

DVB-C Digital video broadcasting - cable

DVB-T Digital video broadcasting - terrestrial

RFC Request for comments

HbbTv Hybrid broadcast broadband television

nPVR Networked personal video recorder

VoD Video on demand

HBO Home box office

DSL Digital subscriber line

FTTH Fiber to the home

FTTB Fiber to the building

HD High definition

UHD Ultra high definition

MPEG Moving picture expert group

AVC Advanced video coding

EPG Electronic program guide

CAGR Compound annual growth rate

LED Light emitting diode

LCD Liquid crystal display

MPEG-TS Moving picture expert group - transport stream

VBR Variable bit-rate

IP Internet protocol

DVD Digital video disc

UDP User datagram protocol

TCP Transmission control protocol

MVR Multicast VLAN registration

VLAN Virtual local area network

PIM Protocol independent multicast

IGMP Internet group management protocol

QoS Quality of services

IEEE Institute of electrical and electronics engineers

RIP routing information protocol

OSPF Open shortest parth first

MAC Media access control

TOS Type of service

COS Class of service

LAN Local area network

GNU GNU is not UNIX

QAM Quadrature amplitude modulation

NIX Neutral internet exchange

DHCP Dynamic host configuration protocol

ETH Ethernet

CPU Central processing unit

WAN Wide area network

DSCP Differentiated services code point

DVMRP Distance vector multicast protocol

BASH Bourne-again shell

Příloha C

Obsah přiloženého DVD

- `readme.txt` ..... stručný popis obsahu DVD
- `monitoring` .... adresář se zdrojovými soubory monitorovacích programů
- `wrt` ..... adresář s firmware pro jednotlivé routery včetně konfiguračních souborů
- `raspi` ..... adresář s obrazem disku sondy Raspberry PI
- `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF
  - `thesis.ps` ..... text práce ve formátu PS