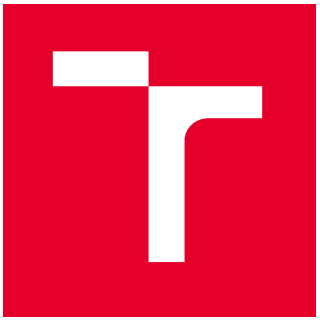


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH LABORATORNÍCH ÚLOH PRO PŘEDMĚT SLUŽBY TELEKOMUNIKAČNÍCH SÍTÍ

DESIGN OF LABORATORY ACTIVITIES FOR TELECOMMUNICATION NETWORK SERVICES COURSE

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — **Bc. Adrián Dúbravka**

AUTHOR

VEDOUCÍ PRÁCE — **Ing. Tomáš Horváth, Ph.D.**

SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Telekomunikační a informační technika**

Ústav telekomunikací

Student: Bc. Adrián Dúbravka ***ID:*** 220886

Ročník: 2 ***Akademický rok:*** 2023/24

NÁZEV TÉMATU:

Návrh laboratorních úloh pro předmět Služby telekomunikačních sítí

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je vytvořit tři laboratorní úlohy do předmětu služby telekomunikačních sítí. V teoretickém úvodu student vypracuje aktuální požadavky metalických/optických sítí a jejich přístupy k jednotlivým službám. Důraz bude kladen na síťový analyzátor IXIA. Teoretická část práce bude dále obsahovat detailní popis uvedeného nástroje s výhodami/nevýhodami a praktické využití s detailně vysvětlenou architekturou. V rámci praktické části student vytvoří tři laboratorní úlohy zapadající do koncepce předmětu. Úlohy musejí být na sobě. Každá laboratorní úloha bude obsahovat odpovídající teoretický úvod, praktickou část s postupem, samostatný úkol nad rámec praktické realizace a kontrolní otázky k problematice.

DOPORUČENÁ LITERATURA:

[1] BOCK, Lisa. Learn Wireshark: A definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark. 2nd. Velká Británie: Packt Publishing, 2022. ISBN 978-1803231679.

[2] CVIJETIC, Milorad. Optical Transmission Systems Engineering. 1. USA: Artech House Print on Demand, 2003. ISBN 978-1580536363.

Termín zadání: 5.2.2024 ***Termín odevzdání:*** 21.5.2024

Vedoucí práce: Ing. Tomáš Horváth, Ph.D.

prof. Ing. Jiří Mišurec, CSc.
předseda rady studijního programu

ABSTRAKT

Táto diplomová práca sa zameriava na návrh troch laboratórnych úloh pre predmet Služby telekomunikačných sietí. Cieľom tejto práce je rozvoj výuky v oblasti telekomunikačných sietí prostredníctvom praxe orientovaných úloh. Práca sa začína teoretickým úvodom, ktorý sa venuje súčasným požiadavkám na metalické a optické siete. Detailne sa rozoberajú jednotlivé služby a prístupy využívané v týchto sieťach. Teoretická časť sa špeciálne venuje sieťovému analyzátoru IXIA, ktorý je prezentovaný ako kľúčový nástroj pre analýzu a testovanie v laboratórnych podmienkach, vrátane jeho výhod a obmedzení. V praktickej časti práce je predstavený návrh troch laboratórnych úloh, ktoré sú integrované do predmetu. Tieto úlohy sú navrhnuté tak, aby zodpovedali realistickým sieťovým scenárom a poskytli študentom praktické zručnosti so zariadeniami a softvérom. Prvá úloha zahŕňa prácu so sieťovým generátorom IXIA, druhá úloha sa zameriava na simuláciu a testovanie s využitím softvéru GNS3 a tretia úloha podrobne analyzuje systém DOCSIS, jeho konfiguráciu a funkčnosť.

KĽÚČOVÉ SLOVÁ

DOCSIS, IXIA, latencia, metalická sieť, NAT, optická sieť, prepínač, QoS, smerovač

ABSTRACT

This master's thesis focuses on designing three laboratory tasks for the subject of Telecommunication Network Services. The aim of this work is to develop education in the field of telecommunication networks through practice-oriented tasks. The work begins with a theoretical introduction that addresses current requirements for metallic and optical networks. It thoroughly examines the various services and approaches used in these networks. The theoretical part specifically focuses on the IXIA network analyzer, which is presented as a key tool for analysis and testing in laboratory conditions, including its advantages and limitations. In the practical part of the work, the design of three laboratory tasks integrated into the course is presented. These tasks are designed to correspond to realistic network scenarios and provide students with practical skills with devices and software. The first task involves working with the IXIA network generator, the second task focuses on simulation and testing using the GNS3 software and the third task thoroughly analyzes the DOCSIS system, its configuration, and functionality.

KEYWORDS

DOCSIS, IXIA, latency, metallic network, NAT, optical network, QoS, router, switch

Vysadené pomocou balíčku `thesis` verzie 4.07; `http://latex.feec.vutbr.cz`

DÚBRAVKA, Adrián. *Návrh laboratorních úloh pro předmět Služby telekomunikačních sítí*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2024, 148 s. Diplomová práca. Vedúci práce: Ing. Tomáš Horváth, Ph.D.

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora:	Bc. Adrián Dúbravka
VUT ID autora:	220886
Typ práce:	Diplomová práca
Akademický rok:	2023/24
Téma závěrečnej práce:	Návrh laboratorních úloh pro předmět Služby telekomunikačních sítí

Vyhlasujem, že svoju záverečnú prácu som vypracoval samostatne pod vedením vedúcej/cého záverečnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej záverečnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto záverečnej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podpisuje iba v tlačenej verzii.

POĎAKOVANIE

Rád by som poďakoval vedúcemu diplomovej práce pánovi Ing.Tomáš Horváth, Ph.D. za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Ďalej by som chcel poďakovať svojej rodine za ich neustálu podporu a povzbudzovanie počas celého štúdia. Ich láska, porozumenie a obetavosť mi dodávali silu a motiváciu prekonávať všetky prekážky, ktoré som počas štúdia stretol. Ich rady a životné skúsenosti mi pomohli v momentoch, keď som sa cítil zneistený alebo stratený. Rodina je základom, na ktorom stojí každý môj úspech, a preto im patrí moje úprimné a hlboké poďakovanie za všetko, čo pre mňa urobili. Ich podpora pre mňa znamenala viac, než dokážu slová vyjadriť, a ich láska a obetavosť boli hnacou silou, ktorá ma posúvala vpred.

Veľká vďaka patrí aj mojim priateľom, ktorí ma podporovali a dodávali mi odvahu. Ich priateľstvo a podpora boli pre mňa neoceniteľné a veľmi si to vážim.

Vaša pomoc a podpora bola pre mňa nesmierne dôležitá a veľmi si ju cením.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Telekomunikačné služby tvoria základný pilier modernej komunikácie. S rozvojom nových technológií a rastúcim dopytom po vysokorýchlostnom pripojení sa svet telekomunikačných služieb rýchlo mení. Táto diplomová práca sa zameriava na návrh laboratórnych úloh pre predmet Služby telekomunikačných sietí, čo umožní študentom nadobudnúť praktické zručnosti potrebné na prácu v oblasti telekomunikácií. Laboratórne úlohy sú špeciálne navrhnuté tak, aby pokryli kľúčové aspekty, ako je konfigurácia sieťového hardvéru, analýza a správa sieťovej prevádzky. Dôraz je kladený na praktické zvládnutie techník riadenia a diagnostiky sieťových problémov, ktoré sú rozhodujúce pre zabezpečenie hladkej a bezpečnej komunikácie v rámci siete.

Prvá kapitola obsahuje základný opis modelov ISO/OSI (International Organization for Standardization / Open Systems Interconnection) a TCP/IP (Transmission Control Protocol over Internet Protocol). Tieto modely sú nevyhnutné pre správne pochopenie, ako sú dáta prenášané cez rôzne vrstvy siete a aké úlohy jednotlivé vrstvy plnia. Zároveň kapitola obsahuje aj zrovnanie a náväznosť vrstiev jednotlivých modelov. V druhej kapitole sa uvádzajú typy sietí, ako sú metalické a optické. Obsahom je aj popis základných komponentov sietí a ich funkcií, úvod do telekomunikačných služieb v sieťach ako je IPTV (Internet Protocol Television) a VoIP (Voice over Internet Protocol) a správa sieťového prenosu zameraná na metriky pre optimálny sieťový prenos. Tretia kapitola popisuje sieťový generátor IXIA, ktorý je neoceniteľným nástrojom na testovanie a analýzu sieťových zariadení a služieb. Primárne je zameraná na sieťový generátor Optixia XM2 nakoľko je tento model využitý na zostavenie laboratórnej úlohy. Taktiež sú súčasťou kapitoly typy modulov a softvérov. Štvrtá kapitola sa venuje systému DOCSIS (Data Over Cable Service Interface Specification), ktorý je štandardom pre prenos dát cez káblové televízne systémy. Opisuje rôzne verzie DOCSIS, ich vlastnosti, prínosy a využívané modulácie, ako aj konkrétnu implementáciu pomocou zariadenia DAH100. Piata kapitola obsahuje stručný popis návrhu laboratórnych úloh. Vytvorený je koncept troch laboratórnych úloh, ktoré sú odlišné a využívajú rôzne komponenty. Posledné tri kapitoly obsahujú vypracované laboratórne úlohy. Tieto úlohy sú navrhnuté tak, aby poskytovali praktický prístup k teoretickým konceptom. Prvá úloha sa zameriava na testovanie sieťových prepínačov pomocou sieťového generátora IXIA. Druhá úloha analyzuje vplyv NAT (Network address translation) na kvalitu IP televízie pomocou programu GNS3. Posledná tretia úloha sa zaoberá analýzou a konfiguráciou systému DOCSIS. Tieto úlohy sú navrhnuté tak, aby študentom poskytli praktické skúsenosti a pripravili ich na riešenie reálnych problémov v oblasti telekomunikačných sietí.

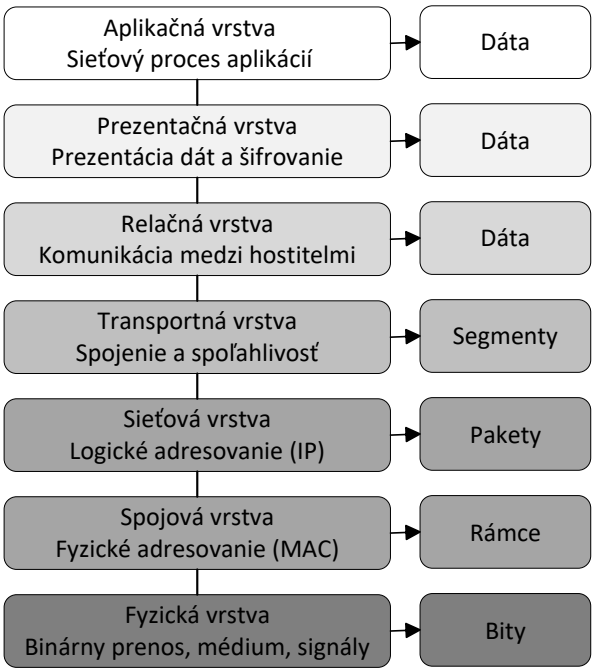
.

1 Model ISO/OSI a TCP/IP

Siete sú systémy, ktoré zabezpečujú prenos dát medzi zariadeniami. Sú dva typy sietí, optické a metalické. Na prenos dát po sieti sa využívajú dva modely a to ISO/OSI (International Organization for Standardization / Open Systems Interconnection) a TCP/IP (Transmission Control Protocol over Internet Protocol).

1.1 Model ISO/OSI

Referenčný model ISO/OSI popisuje, ako by mali jednotlivé systémy pracovať na sieti. Skladá sa zo siedmich vrstiev ako je možné vidieť na obr. 1.1.



Obr. 1.1: Model ISO/OSI [1]

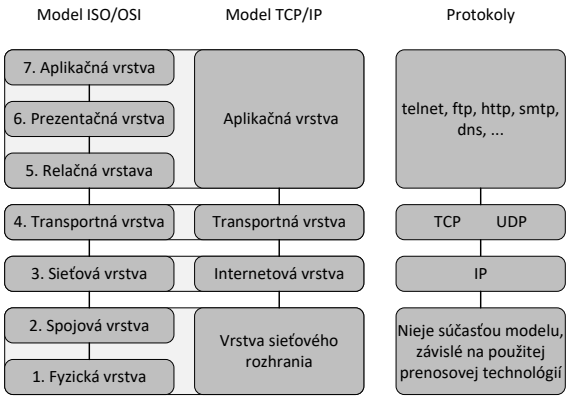
Jednotlivé vrstvy majú svoje špecifické úlohy, ktoré budú špecifikované v tejto kapitole. Tento model celkovo zabezpečuje správnosť prenosu dát od zdroja k cieľu cez sieť. Využívané sieťové prvky sú napríklad smerovače, opakovače, rozbočovače, prepínače, brány a iné. Na fyzickej vrstve pracujú opakovače a rozbočovače, na spojovej vrstve pracujú prepínače a na sieťovej vrstve pracujú smerovače.

1.2 Model TCP/IP a náväznosť na ISO/OSI

TCP/IP označuje celú sústavu protokolov a znázorňuje, ako by sa mali počítačové siete budovať a ako by mali fungovať. Tento model označuje ako by jednotlivé vrstvy mali plniť dané úlohy a akým spôsobom by ich mali plniť. Jedná sa teda o konkrétne protokoly na jednotlivých vrstvách a ich dané funkcie, ktoré by mali plniť. TCP/IP rovnako ako ISO/OSI predstavuje architektúru siete [1].

Hlavným rozdielom medzi týmito dvoma modelmi je, že ISO/OSI kladie dôraz na vlastnosti siete, ako je spojovaný a spoľahlivý charakter služieb. Taktiež pracuje s myšlienkou, že pripojené hostiteľské počítače v danej sieti budú mať relatívne jednoduchú úlohu. Za predpokladanú nevýhodu sa môže považovať, že vyššie vrstvy nemusia považovať sieť za dostatočne bezpečnú pre svoje potreby. Z toho dôvodu sa do určitej miery zaoberá každá vrstva referenčného modelu zaisťovaním spoľahlivosti. Naopak TCP/IP predpokladá, že zabezpečenie bezpečnosti je problém koncových užívateľov danej komunikácie. Bezpečnosť by mala byť teda riešená až na úrovni transportnej vrstvy. Týmto spôsobom komunikačná sieť nestráca časť svojej prenosovej kapacity na zabezpečovanie spoľahlivosti ale na plné využitie na vlastný dátový prenos [1, 2].

V sieťach môže dochádzať ku zahadzovaní a stratám paketov, ktoré sú cez danú sieť prenášané. Sieť by nemala bezdôvodne pakty zahadzovať ale mala by vyvíjať maximálnu snahu na doručenie. Zahadzovanie by malo nastať len v takom prípade ak dôjde k poškodeniu pri prenose, výpadku spojenia a iné. TCP/IP predstavuje jednoduchú a rýchlu sieť, ku ktorej sú pripojené inteligentné zariadenia (počítače). Taktiež tento model predpokladá nespojitý prenos v komunikačnej sieti a obsahuje len štyri vrstvy. Na obrázku nižšie je zobrazený model TCP/IP v porovnaní s referenčným modelom ISO/OSI s jednotlivými protokolmi.



Obr. 1.2: Model TCP/IP a jeho náväznosť na ISO/OSI [1]

1.2.1 Vrstva sieťového rozhrania

Najnižšie vrstvy modelu ISO/OSI, ktorými sú fyzická vrstva a spojová vrstva, majú kľúčovú rolu pri správe a zaistení konkrétneho prenosu dát a fyzického prepojenia v počítačovej sieti. Spájajú sa dohromady a v rámci modelu TCP/IP tvoria vrstvu sieťového rozhrania. Táto vrstva nie je v rámci modelu TCP/IP bližšie špecifikovaná, nakoľko jej funkcie sú závislé na konkrétnej prenosovej technológií. Medzi tieto technológie patrí napríklad Ethernet, Wi-Fi a Bluetooth, a každá z týchto technológií môže vyžadovať iné postupy a protokoly pre správu prenosu dát [1, 2].

1.2.2 Internetová vrstva

Jedná sa o vyššiu vrstvu, ktorá nie je závislá od použitej prenosovej technológie. Nazýva sa aj IP vrstva, nakoľko je implementovaná pomocou protokolu IP. Táto vrstva v modeli ISO/OSI odpovedá sieťovej vrstve. Úlohou tejto vrstvy je zaistenie prenosu paketov od odosielateľa až ku svojmu koncovému príjemcovi, obvykle pomocou medziľahlých smerovačov. Keďže TCP/IP poskytuje nespojitý prenos, je na tejto vrstve zaisťovaná jednoduchá datagramová služba. V úvahu musia byť brané aj rozdiely medzi rôznymi časťami siete ako napríklad rozdielny charakter adries, rozdielna maximálna veľkosť prenášaných paketov alebo rámcov a ich formát a taktiež aj odlišný charakter prenosových služieb, ktoré poskytujú nižšie úrovne [1, 2].

1.2.3 Transportná vrstva

Táto tretia vrstva je taktiež známa ako TCP vrstva nakoľko je v určitých prípadoch najčastejšie implementovaná pomocou protokolu TCP. Hlavnou úlohou tejto vrstvy je zabezpečovať prenos dát medzi dvoma koncovými užívateľmi. Môže tiež, v závislosti od potrieb alebo požiadaviek, riadiť toky dát a zaistiť spoľahlivý prenos dokonca aj transformovaním nespojitého charakteru na spojitý. Medzi ďalší používaný protokol patrí UDP protokol, ktorý nanrozdiel od TCP neposkytuje spoľahlivý prenos. UDP často využívajú aplikácie, ktoré nepotrebujú spoľahlivosť na úrovni transportnej vrstvy [1, 2].

1.2.4 Aplikačná vrstva

Najvyššia vrstva, ktorej subjektmi sú jednotlivé aplikačné programy, komunikuje priamo s transportnou vrstvou, na rozdiel od referenčného modelu ISO/OSI. V tomto modele nie sú k dispozícii prezentačná a relačná vrstva ako v modele ISO/OSI, ktoré by poskytovali špecifické služby. Aplikácie musia samostatne zaisťovať akékoľvek prezentačné alebo relačné funkcie. Pokiaľ aplikácia nepotrebuje ani jednu z týchto vrstiev, nevzniká zbytočné zaťaženie alebo réžia [1, 2].

2 Metalické a optické siete

Táto kapitola sa venuje dôležitosti metalických a optických sietí, ich základným princípom a aplikáciám. Každá podkapitola predstavuje, ako každá komponenta a služba prispieva k celkovej efektivite a bezpečnosti telekomunikačných sietí. Tieto dva druhy sietí predstavujú rozdielne prístupy k prenosu dát a unikátnymi vlastnosťami a aplikáciami.

Metalická sieť je taký typ telekomunikačnej siete, ktorá na prenos dát využíva metalické (kovové) káble. Existujú aj napríklad hliníkové káble ale najviac využívané, skrz výhodných vlastností, sú medené. Káble sa v metalických sieťach využívajú na prenos elektrických signálov medzi rôznymi typmi zariadení alebo uzlami v danej sieti. Požiadavky na tieto siete sú určované technologickými inováciami, predpismi, štandardmi a čoraz väčšími nárokmi na rýchlejší a spoľahlivejší prenos dát a samotný prístup k dátam. Metalické siete sú ideálne pre aplikácie v prostrediach, kde je prioritou nákladová efektívnosť a maximálne prenosové rýchlosti nie sú rozhodujúce.

Schopnosť metalických sietí je taktiež prenášať široké spektrum telekomunikačných služieb od internetu po VoIP. Súčasné technológie ako napríklad IPTV a pokročilé sieťové funkcie ako NAT (Network Address Translation) a QoS (Quality of Service) sú veľmi významné pre správu sieťového toku dát a kladú na metalické siete stále vyššie nároky.

Optická sieť je na druhej strane taký typ telekomunikačnej siete, ktorá pre prenos dát využíva svetelné signály prenášané pomocou optických vlákien. Medzi optické vlákna patria jednovidové, mnohovidové a gradientné vlákna, ktoré predstavujú rozdielny spôsob prenosu svetla optickým vláknom a taktiež zabezpečujú rozdielne charakteristiky prenosu. Tento spôsob prenosu predstavuje revolučnú kapacitu a rýchlosť prenosu dát. Vďaka ich vynikajúcej priepustnosti a nízkej latencií predstavujú vhodnejšiu voľbu pre backbonové siete a taktiež prispievajú k znižovaniu chybovosti paketov a jitteru, čím zlepšujú celkovú kvalitu sieťového prenosu.

Tieto siete musia taktiež dbať na bezpečnosť, čo je kľúčový aspekt v ochrne prenášaných dát. Či sa už jedná o ochranu pred DDoS útokmi (Distributed Denial of Service), neoprávnenými skenovaniami portov, alebo zabezpečení prostredníctvom firewallu a systémov IDS/IPS (Intrusion Detection Systems/Intrusion Prevention Systems). Tieto bezpečnostné mechanizmy sú dôležité pre ochranu infraštruktúry a dát, ktoré metalické a optické siete prenášajú.

2.1 Metalické a optické vedenie

Metalické a optické vedenia poskytujú základ pre prenos informácií v rôznych prostrediach, od domácností až po veľké podnikové siete. Táto podkapitola sa zameriava na rôzne druhy metalických káblov, ich štruktúru, vlastnosti a použitie v sieťových inštaláciách. Medzi niektoré z nich patria krútené káble, koaxiálne káble a optické káble.

Krútené káble

Krútené káble sa rozdeľujú podľa kategórie (Cat5E, Cat6, Cat6A...), podľa konštrukcie tienenia(UTP, FTP, STP...) a podľa vonkajšieho plášta(PVC, LSOH, PE, PEG...).

- **UTP (Unshield Twisted Pair)** káble sú jedným z najpoužívanejších typov káblov v sieťových inštaláciách. Tieto káble sú zložené z párov medených vodičov, ktoré sú vzájomne stočené, čo pomáha minimalizovať elektromagnetické rušenie (EMI) a presluchy (crosstalk). Majú nestienený krútený pár a nestienený krútený kábel. UTP káble sa najčastejšie používajú v rôznych aplikáciách, ako napríklad v počítačových sieťach, telefonických systémoch a domácich multimediálnych sieťach [3].
- **STP (Shielded Twisted Pair)** káble sú podobné UTP káblom, ale každý pár vodičov je navyše obalený kovovým tienením. Tienenie poskytuje lepšiu ochranu proti elektromagnetickému rušeniu a presluchom, čím zlepšuje kvalitu prenosu signálu [3].
- **FTP (Foil Shielded Twisted Pair)** káble kombinujú prvky UTP a STP káblov tým, že majú jednotlivé páry vodičov stočené do párov, ktoré sú obalené fóliovým tienením. Toto tienenie chráni kábel pred vonkajším elektromagnetickým rušením, čím zvyšuje celkovú kvalitu a spoľahlivosť prenosu signálu [3].

Koaxiálne káble

Koaxiálne káble sú typom metalického vedenia, ktoré sa široko používajú v televíznych a internetových pripojeniach. Tieto káble majú centrálny vodič obklopený izoláciou, ktorá je obalená kovovým tienením a vonkajším ochranným plášťom. Tento dizajn umožňuje koaxiálnym káblom prenášať elektronické signály s minimálnou interferenciou z externých zdrojov, nazývané ako EMI (Electromagnetic Interference). Koaxiálne káble sú používané na rozvod televízneho signálu v káblových televíziách. Taktiež mnohé formy širokopásmového internetu využívajú koaxiálne káble na prenos dát a v bezpečnostných systémoch sú často využívané na prenos video signálu

z bezpečnostných kamier.

Medzi jeden z najpoužívanejších typov koaxiálnych káblov je RG6. Vyznačuje sa svojimi špecifickými a elektrickými vlastnosťami, ktoré ho robia ideálnym pre aplikácie v oblasti televízneho vysielania a internetových pripojení. RG6 má hrubší stredový vodič, čo zabezpečuje nízky odpor a vysokú kvalitu signálu. Izolácia s pevného polyetylénu minimalizuje straty signálu a udržuje stabilitu signálu aj pri vysokých frekvenciách. Väčší počet tienenia zabezpečuje ochranu proti EMI a RFI (Radio-frequency Interference). RG6 káble majú štandardnú impedanciu 75 ohmov. Vďaka nižšiemu útlmu dokáže prenášať signál na väčšie vzdialenosti. Koaxiálny kábel dokáže efektívne prenášať signály na veľké vzdialenosti bez významnej straty signálu. Medzi hlavné výhody patrí [3]:

- **Odolnosť voči rušeniu**: Vďaka štruktúre je koaxiálny kábel viacej odolnejší voči rušeniu.
- **Vysoká šírka pásma**: Koaxiálne káble prenášajú veľké množstvo dát, pre televízne vysielanie, internet a iné komunikačné aplikácie.

Optické káble

Optické káble sú technológiou, ktorá umožňuje prenos dát pomocou svetelných impulzov cez optické vlákna. Tieto vlákna sú vyrobené z čistého skla alebo plastu a sú schopné prenášať dáta na veľmi dlhé vzdialenosti s minimálnymi stratami. Optické káble ponúkajú obrovskú šírku pásma a vysokú rýchlosť prenosu, čo ich robí ideálnymi pre moderné telekomunikačné a dátové siete. Veľkou výhodou optických káblov je ich odolnosť voči elektromagnetickému rušeniu, čo zabezpečuje spoľahlivý prenos dát. Základné delenie optických vlákien je [3]:

- **Jednovidové vlákna** Majú malý priemer jadra (8-10 µm) a umožňujú prenos iba jedného vidu elektromagnetickej vlny. Dosahujú nižšie hodnoty útlmu a väčšiu prenosovú šírku pásma. Využívajú sa na dlhšie vzdialenosti.
- **Mnohovidové vlákna** Majú väčšie jadro (50 až 100 µm), čo umožňuje, aby káblom prechádzalo viac vidov svetla naraz. Využitím viacerých vidov vzniká vidová disperzia, ktorá obmedzuje šírku pásma. Využívajú sa na kratšie vzdialenosti v porovnaní s jednovidovými.
- **Gradientné vlákna** Využívajú zmenu indexu lomu. Index lomu sa postupne mení, čo spôsobuje, že svetelné lúče sa ohýbajú a sú neustále zaostrované späť k osi vlákna, čím sa znižuje módová disperzia. Narozdiel od mnohovidových vlákien majú väčšiu šírku pásma a nižší útlm, čo umožňuje dlhšie prenosové vzdialenosti.

2.2 Základné komponenty sietí

Základné komponenty sietí sú kľúčové pre efektívnu a spoľahlivú komunikáciu. Táto podkapitola sa venuje základným zariadeniam v počítačových sieťach a to konkrétne smerovačom (router) a prepínačom (switch).

Smerovače a prepínače sú základom pre správne fungovanie počítačových sietí. Kým smerovače zabezpečujú komunikáciu medzi rôznymi sieťami a efektívne smerovanie dát, prepínače zohrávajú kľúčovú úlohu v správe dátového toku vnútri lokálnych sietí. Spoločne tieto zariadenia umožňujú hladký a efektívny prenos dát, čo je základom pre všetky moderné komunikačné technológie.

2.2.1 Smerovač

Smerovače sú zariadenia, ktoré zohrávajú dôležitú rolu v prepájaní rôznych sietí. Tieto zariadenia pracujú na tretej vrstve referenčného modelu OSI, čo značí, že umožňujú smerovanie dát na základe IP adresy. Sú veľmi dôležité v širokých sieťových prostrediach, kde je dôležité efektívne riadiť toky dát medzi rôznymi LAN sieťami alebo medzi LAN a internetom. Najdôležitejšou funkciou smerovania je voľba optimálnej trasy pre dáta, čo môže byť najrýchlejšia, najspoľahlivejšia alebo najkratšia trasa z jedného bodu do druhého [1, 2].

Smerovače zaisťujú, že informácie využijú najefektívnejšiu cestu k cieľovému zariadeniu, čo je veľmi podstatné pre rýchlosť a efektivitu siete. Každý smerovač rozhoduje akou cestou bude paket ďalej smerovaný pokiaľ existuje viacero možností ciest. Tento rozhodovací faktor je založený na určitej znalosti globálnej topológie, čo ale zároveň predstavuje základný problém smerovania. Globálne topológie sú často zložité a rozsiahle a taktiež sa môžu dynamicky meniť v čase a informácie o nej môžu byť ťažko zaznamenávané [1, 2].

Pre úspešné plnenie smerovania je potrebné aby každý smerovač obsahoval nasledujúce informácie:

- IP adresu adresáta,
- možné cesty do všetkých vzdialených sietí,
- najlepšiu zvolenú trasu do cieľovej siete,
- susedné smerovače,
- metódu pre získavanie informácií o smerovaní.

Medzi kľúčovú funkciu smerovačov patrí aj preklad adries NAT (Network Address Translation) a QoS (Quality of Service), ktoré umožňujú efektívnejšiu a bezpečnejšiu prevádzku v sieťach. Nižšie sú tieto jednotlivé funkcionality bližšie špecifikované.

2.2.2 Prepínač

Na rozdiel od smerovačov, prepínače (switch) pracujú na druhej vrstve referenčného OSI modelu, známej ako dátová vrstva. Najčastejšie sa prepínače vyskytujú v Ethernetových sieťach. Základnou funkciou prepínača je, že na základe cieľovej MAC adresy rozhoduje, na ktorý port má byť rámec odoslaný, a na ktorý nie. Prepínače zodpovedajú za správu dátového toku vnútri jednej lokálnej siete. Ich hlavnou úlohou je prijímať dáta od jedného zariadenia a efektívne ich smerovať k určenému zariadeniu v rámci tej istej siete [1, 2].

Tieto zariadenia disponujú logikou, ktorá im umožňuje sledovať obsah rámcov a na základe nich rozhodovať, ako s danými rámcami naloží. Prepínače sú kľúčové pre minimalizovanie kolízií v sieti a optimalizáciu dátového toku, čo umožňuje viacerým zariadeniam komunikovať súčasne bez výrazného zníženia výkonu siete. Prepínače taktiež spolupracujú s fyzikou vrstvou, čo značí, že pracuje aj s kódovaním, moduláciami a pod. [1, 2].

2.3 Riadenie a optimalizácia sieťového prenosu

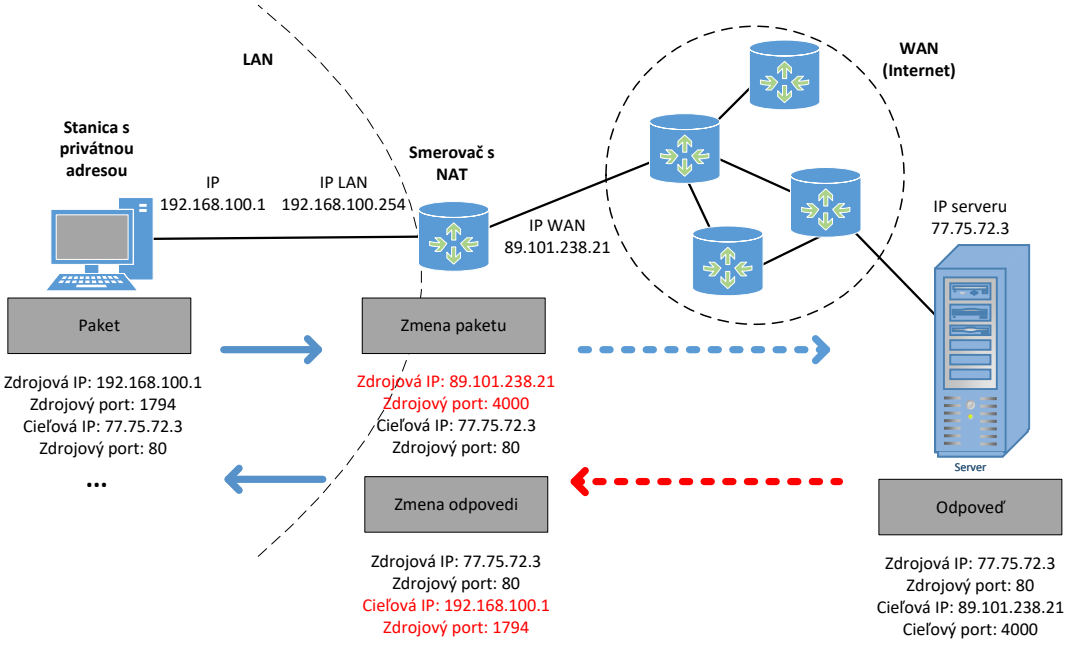
Efektívne riadenie a optimalizácia sieťového prenosu sú kľúčové pre zabezpečenie spoľahlivosti a kvality služieb v moderných sieťach. Medzi dve dôležité technológie patrí napríklad NAT (Network Address Translation) a QoS (Quality of Service). Hoci majú odlišné funkcie, často sa používajú spolu na optimalizáciu výkonu siete, zabezpečenie prioritizácie kritických aplikácií a ochranu proti preťaženiu. NAT poskytuje adresný priestor a bezpečnostné výhody tým, že skryje vnútornú sieť pred vonkajším svetom. QoS zabezpečuje, že aplikácie majú prístup k potrebným sieťovým zdrojom a prenosovej kapacite.

NAT (Network Address Translation)

Jedná sa o bežnú funkciu moderných smerovačov, ktorá zabezpečuje preklad (zmenu) IP adresy paketu, ktorá daným smerovačom prechádza. Zdrojová alebo cieľová IP adresa je prevádzaná medzi rôznymi rozsahmi. Umožňuje, aby počítače v lokálnej sieti komunikovali s internetom pod jednou verejnou IP adresou. Táto technika zabezpečuje efektívne oddelenie intranetu od internetu, čím prispieva k zvýšenej bezpečnosti siete, nakoľko skutočné IP adresy interných zariadení nie sú priamo vystavené vonkajším hrozbám [1]. Obrázok 2.1 znázorňuje techniku prekladu adries.

Smerovače s technikou NAT udržiavajú tabuľku prekladu adries, ktorá zabezpečuje rozlišovanie medzi dátovými tokmi jednotlivých staníc z vnútornej siete do internetu. Toto zabezpečuje aj v prípadoch, keď je pre celú sieť k dispozícii len

jedna verejná IP adresa, ktorá je pridelená k WAN (Wide Area Network) portu. Vďaka NAT je znížená potreba veľkého počtu verejných IP adries, čo je dôležité najmä z dôvodu nedostatku IPv4 adries. Taktiež umožňuje viacerým zariadeniam zdielať jednu verejnú IP adresu, čo znižuje potrebu veľkého počtu privátnych adries voči vonkajšiemu svetu. Smerovače vďaka NAT môžu rozlišovať a riadiť dátové toky medzi vonkajšími a vnútornými sieťami na základe komplexnejšieho systému, ktorý zahŕňa sieťové ale aj transportné adresy, čím zvyšuje efektivitu a bezpečnosť dátového prenosu [1].



Obr. 2.1: Znázornenie techniky prekladu adries [1]

V rôznych zdrojoch je možné nájsť rôzne spôsoby rozdelenia NAT. Medzi dva základné druhy prekladu adries patrí [1]:

- **SNAT (Source NAT)** – je technika, ktorá prekladá zdrojovú IP adresu vo všeobecnosti pri pripájaní zo súkromnej IP adresy na verejnú IP adresu. Je to najbežnejšia forma NAT, ktorá sa používa, keď interný hostiteľ potrebuje iniciovať reláciu s externým hostiteľom alebo verejným hostiteľom. Táto metóda umožňuje viacerým zariadeniam vo vnútornej sieti zdieľať jednu verejnú IP adresu. Je to praktické v prostrediach, kde je verejných IP adries obmedzené množstvo. SNAT mení zdrojovú adresu odchádzajúcich paketov z internej adresy na verejnú. Vďaka tomu môže interný hostiteľ komunikovať s externými servermi a službami bez toho, aby bolo potrebné prideliť každému zariadeniu

unikátnu verejnú IP adresu.

- **DNAT (Destination NAT)** – je technika, ktorá prekladá cieľovú IP adresu, najmä pri pripojení z verejnej IP adresy na súkromnú IP adresu. Používa sa najmä na presmerovanie paketov určených pre konkrétnu IP adresu alebo špecifický port na IP adrese. Tento presmerovaný paket sa zvyčajne smeruje na inú adresu, zvyčajne na inom hostiteľovi. Tento proces umožňuje, že vnútorné servery, ktoré bežne nie sú priamo dostupné z internetu, môžu byť sprístupnené externým používateľom, čo je často využívané pre web servery, FTP (File Transfer Protocol) servery alebo herné servery.

QoS (Quality of Service)

Kvality služby (QoS) je v smerovačoch dôležitý aspekt správy sieťovej prevádzky. QoS je nevyhnutné pre streamovanie hlasu a videa cez sieť ale aj pre podporu rozvíjajúceho sa IoT (Internet of Things). Niekedy sa v sieti nachádzajú aplikácie, ktoré sú citlivé na oneskorenie. Tieto aplikácie často používajú UDP protokol ktorý, na rozdiel od TCP, neopakuje prenos stratených paketov. V aplikáciach ako sú napríklad IP telefónne hovory, kde jedným z dôležitých faktorov je udržiavanie plynulého toku dát, môže byť strata alebo oneskorenie paketov veľkým problémom. Navyše, jitter, čo je zmena oneskorenia paketov, môže taktiež negatívne ovplyvňovať kvalitu aplikácií [4].

V určitých situáciách môže nastať preťaženie siete a smerovače začnú zahadzovať pakety, čo môže viesť k problému s kvalitou streamovacívh aplikácií. V tomto bode sa QoS stáva klúčovým faktorom, ktorý pomáha zabezpečiť, že dôležitá sieťová prevádzka, ako sú hlasové hovory, dostáva prednosť pred menej dôležitými údajmi. Týmto spôsobom sa znižuje riziko straty, oneskorenia alebo jitteru pre tieto citlivé aplikácie [4].

QoS pomáha riadiť stratu paketov, oneskorenie a jitter v sieťovej infraštruktúre a funguje v niekoľkých krokoch [4]:

- **Identifikácia Prioritných Aplikácií**
  Prvým krokom je určenie, ktoré aplikácie by mali mať prednosť v šírke pásma na sieti.
- **Označovanie Prevádzky**
  Rôzne metódy, ako je CoS (Class of Service) a DSCP (Differentiated Services Code Point), sa používajú na označenie prevádzky, čo umožňuje sieťovému zariadeniu kategorizovať dáta do rôznych skupín.

- **Kategorizácia Dátových Tokov a Implementácia Politiky**
  Po kategorizácii sa implementujú politiky na poskytnutie preferenčného zaobchádzania s určitými dátovými tokmi nad inými. To sa robí procesom zvaným frontovanie. Napríklad hlasovej prevádzke môže byť daná prednosť v šírke pásma, zatiaľ čo štandardné TCP dátové prenosové toky s nižšou prioritou môžu čakať alebo byť zahodené, ak sa fronty príliš naplnia.

Tento proces zabezpečuje prístup k nastaveniam smerovača, identifikáciu určitých typov prevádzky alebo aplikácií, ktoré je potrebné uprednostniť. Následne nastaveniu pravidiel alebo politík, ktoré určujú, ako daný smerovač zaobchádza s rôznymi typmi sieťovej prevádzky.

2.4 Testovanie sieťových zariadení

V dnešnej dobe sa sieťové a komunikačné technológie rýchlo vyvíjajú a stávajú sa neoddeliteľnou súčasťou každodenného života. Z toho dôvodu je dôležitejšie ako kedykoľvek predtým zabezpečiť, aby sieťové zariadenia poskytovali spoľahlivý a konzistentný výkon. V tejto súvislosti zohrávajú kľúčovú úlohu testovacie štandardy sieťovej infraštruktúry ako sú napríklad RFC 2544 a RFC 2889. Jedná sa o normy, ktoré poskytujú metológiu na objektívne a systematické hodnotenie výkonu sieťových komponentov. Tým umožňujú porovnávanie rôznych produktov a technológií na báze stanovených benchmarkov.

2.4.1 RFC 2544

RFC(Request for Comment) 2544 je metodika benchmarkingu vytvorená v roku 1999 na testovanie a meranie výkonu sieťových zariadení. Poskytuje štandardizované výsledky výkonu, ktoré umožňujú jednoducho porovnávať zariadenia od rôznych dodávateľov. RFC obsahuje niekoľko čiastkových testov, ktoré sú určené na vyhodnocovanie, ako bude zariadenie fungovať v reálnych scenároch. Tieto testy sa považujú za offline. To znamená, že skutočná sieťová prevádzka musí byť zastavená, aby tester generoval prevádzku so špecifickými charakteristikami [5, 6].

Ideálnym spôsobom implementácie týchto testov je použitie testovacej sady s vysielacími a prijímacími portami. Prevádzka sa posiela z testera do DUT (Device under test) a späť z DUT do testera. Zahrnutím sekvenčných čísel do prenášaných rámcov dokáže tester skontrolovať, či boli všetky pakety úspešne prenesené, a overiť, či boli prijaté aj správne pakety [5].

Aby sa zabezpečilo, že ethernetová sieť bude schopná podporovať rôzne služby ako napríklad VoIP, video atď., RFC 2544 podporuje sedem preddefinovaných veľkostí rámcov a to (64, 128, 256, 512, 1024, 1280 a 1518 bajtov) na simuláciu rôznych dopravných podmienkach. Malé veľkosti rámcov zvyšujú počet prenášaných rámcov, čím zaťažujú sieťové zariadenie [5].

Medzi najdôležitejšie patria definície testov na meranie priepustnosti, latencie, straty rámca, odolnosti systému a testovania rôznych pracovných zaťažení. Je tiež dôležité, aby sa výsledky prezentovali porovnateľným spôsobom a aby sa týkali bežných testovacích postupov. RFC 2544 zdôrazňuje potrebu komplexného testovania a podávania správ, aby sa zabezpečilo, že výsledky benchmarkov budú presné a relevantné pre používateľov. Pojmy ako sú priepustnosť, latencia, straty rámcov/paketov a jitter sú objasnené v podkapitole 2.4 [5].

2.4.2 RFC 2889

Rozširuje metodiku RFC 2544 a zameriava sa na metodiku testovania prepínačov v LAN sieťach. Toto doporučenie určuje v akom formáte majú byť reprezentované výsledky meraní. Rovnako ako doporučenie RFC 2544 taktiež podporuje sedem preddefinovaných veľkostí rámcov a to (64, 128, 256, 512, 1024, 1280 a 1518 bajtov) na simuláciu rôznych dopravných podmienok. RFC sa týka predovšetkým zariadení, ktoré prepínajú rámce na Media Access Control (MAC) vrstve. V nasledujúcom texte sú vybrané a popísané niektoré z testov [7].

Back Pressure

Jedná sa o metódu testovania, ktorá simuluje zaťaženie sieťového zariadenia v podmienkach preťaženia. Metóda testuje akým spôsobom zariadenie reaguje, keď prichádzajúci dátový tok presahuje jeho spracovateľskú kapacitu. Výsledkom testu môže byť napríklad spomalenie predchádzajúceho toku alebo odmietnutie nových rámcov. Test poskytuje informácie o výkonnosti a spoľahlivosti zariadenia v extrémnych podmienkach, čo je kritické pre návrh a prevádzku sieťovej infraštruktúry. Odhaľuje, či je zariadenie schopné zabezpečiť napríklad QoS aj počas vysokých zaťažení.

Broadcast Rate

Tento test určuje, ako rýchlo dokáže sieťové zariadenie (prepínač) spracovávať broadcastové rámce. Jedná sa o dôležitú schopnosť zariadenia efektívne distribuovať rámce, ktoré sú určené pre všetky zariadenia danej siete. Broadcast Rate dokáže pre zariadenie identifikovať výkon pri rozširovaní broadcastových správ. Taktiež môže

odhaliť obmedzenia v prenosovej rýchlosti alebo potencionálne problémy s preťažením siete, čo môže mať za následok stratovosť rámcov.

Frame error Filtering

Test Frame Error Filtering je používaný v sieťových zariadeniach na identifikáciu a filtrovanie poškodených rámcov, ktoré nespĺňajú štandardné podmienky veľkosti alebo majú chyby v kontrolnom súčte. CRC (Cyclic Redundancy Check) je metóda používaná na detekciu chýb v dátach. Pracuje tak, že z pôvodných dát vygeneruje kontrolný súčet, ktorý je potom priložený k dátovému bloku a odoslaný alebo uložený spolu s ním. Keď sú dáta na druhej strane prijaté alebo čítané, systém zopakuje výpočet CRC na overenie integrity dát. Ak sa novovypočítaný kontrolný súčet líši od toho, ktorý bol odoslaný, signalizuje to, že dáta boli počas prenosu alebo uloženia nejakým spôsobom zmenené, čo naznačuje potenciálnu chybu. Filtrovanie týchto chybných rámcov je dôležité pre udržanie integrity dát a efektívneho fungovania siete. Filtrovanie zabraňuje šíreniu poškodených alebo neplatných dát po sieti.

Fully Meshed

Fully Meshed sa podla RFC 2889 týka výkonnosti a spoľahlivosti prepínačov v plne prepojenej topológii. Test slúži na overenie, ako efektívne môže sieťové zariadenie spracovať sieťovú premávku medzi všetkými svojimi portmi naraz. Týmto spôsobom simuluje prostredie s vysokou mierou vzájomnej konektivity. Cieľom je identifikovať úzke miesta v spracovaní dát a overiť schopnosť zariadenia udržiavať konštantný výkon za situácií, keď sú všetky porty aktívne zapojené do prenosu.

Head of Line Blocking

V teste sú rámce smerované cez zariadenie v plnej prepojenej topológii. Test sleduje, ako zariadenie zvláda preťaženie na rozhraniach pri súčasnom prenose dát medzi viacerými portmi. Výsledkom sú informácie o schopnosti zariadenia spracovávať dátový tok a predchádzať blokovaniu, keď jeden port vysiela dáta súčasne na viacero prijímacích portov, čo simuluje reálnu sieťovú situáciu. Spracovanie jedného rámca na vstupe blokuje ďalšie rámce v rade čakajúce na spracovanie, aj keď môžu byť určené pre iné výstupné porty. Tento jav môže spôsobiť zvýšenie latencie a zníženie celkovej efektívnosti prenosu dát v sieťovom zariadení. Rámce, ktoré by inak mohli byť okamžite preposlané, musia čakať, kým sa nevyrieši blokovanie na čele radu.

2.5 Telekomunikačné služby v sieťach

V súčasnej dobe sú telekomunikačné služby kľúčovým prvkom, ktorý ľudom zabezpečuje komunikáciu na diaľku. S rozvojom digitálnych technológií a sieťových infraštruktúr sa objavuje stále viac inovatívnych spôsobov, ako využívať rozsiahle možnosti telekomunikácií. Táto podkapitola sa zameriava na niektoré základné a súčasne neoddeliteľné služby moderných telekomunikačných sietí, ako je IPTV (Internet Protocol Television) a VoIP (Voice over IP).

2.5.1 IPTV

Televízna distribúcia je jednou z najväčších technologických infraštruktúr, nasadených po telefónnych a elektrických sieťach. IPTV je jednou zo sľubných techník, ktoré spájajú telekomunikačné a digitálne televízne doručovacie služby.

Jednou z najnáročnejších telekomunikačných aplikácií ju robia požiadavky na šírku pásma prenosu videa. Prenos video streamu v štandardnom rozlíšení (SD) vyžaduje niekoľko Mbit/s, zatiaľ čo vysoké rozlíšenie (HD) dosahuje desiatky Mbit/s. To je oveľa viac, ako je potrebné na prenos hlasu (zvyčajne 32 až 64 Kbit/s) alebo dokonca na prehliadanie internetu [4].

Štruktúra IPTV systémov

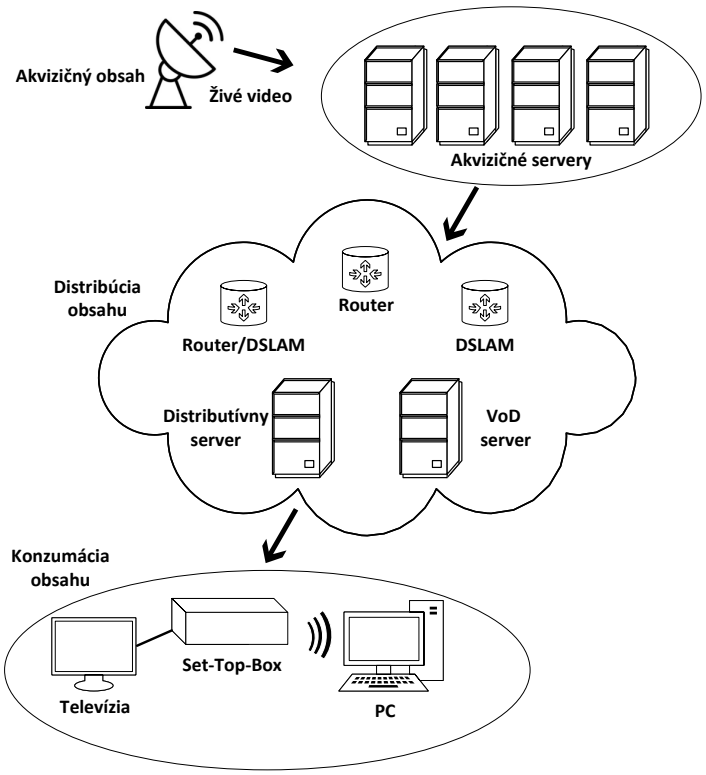
IPTV je založená na odosielaní video streamov zo zdroja, čiže streamovacieho zariadenia, odkiaľ je obsah distribuovaný, do terminálu. Na základe toho je možné prenos rozdeliť do dvoch kategórií a to vysielanie a video na požiadanie.

Prvá kategória vo všeobecnosti vyžaduje použitie viacsmerového vysielania IP na zníženie šírky pásma siete potrebnej na prenos video streamov zdieľaním medzi používateľmi. Naproti tomu druhá kategória, video na požiadanie, využíva jednoduché doručovanie Unicast (z bodu do bodu). Rýchlosť tohto doručovania možno zvýšiť implementáciou sietí na doručovanie obsahu. Na to, aby koncové zariadenie získalo prístup k video obsahu, či už ide o obsah na požiadanie alebo vysielanie, musí byť informované o jeho existencii a spôsobe, ako k nemu pristupovať [8]. Reťazec IPTV zahŕňa štyri domény:

- spotrebiteľská doména poskytujúca služby koncovému používateľovi,
- doména poskytovateľa siete umožňujúca spojenie medzi doménou spotrebiteľa a doménou poskytovateľa služieb,
- doména poskytovateľa služieb, ktorá je zodpovedná za poskytovanie služieb spotrebiteľom,
- doménu poskytovateľa obsahu, ktorá vlastní obsah alebo obsahové aktíva alebo má na ne licenciu.

Základná infraštruktúra pozostáva z troch hlavných stavebných blokov a tými sú získavanie obsahu, distribúcia obsahu a spotreba obsahu. Táto infraštruktúra je vybudovaných v hierarchii národného, regionálneho a lokálneho pokrytia až do priestorov zákazníka. Na obr. 2.2 je zobrazená základná architektúra IPTV opisujúca hlavné komponenty typického systému IPTV. Tieto komponenty zahŕňajú [4]:

- **Akvizičné servery (A-servery)**: Kódujú video a pridávajú metadáta DRM (Digital Rights Management).
- **Distribučné servery (D-servery)**: Poskytujú ukladanie do vyrovnávacej pamäte a riadenie QoS.
- **Tvorcovia a servery VoD (Video On Deman)**: Uchovávajú si knižnicu zakódovaného obsahu VoD na poskytovanie služieb VoD.
- **IP smerovače**: Smerujú IP pakety a poskytujú rýchle presmerovanie v prípade zlyhania smerovania.
- **Rezidenčné brány**: IP smerovače pre združené služby v domácnosti.
- **STB (Set-top box)**: Je zariadenie na strane zákazníka, ktoré je prepojené s užívateľským terminálom (napr. TV, PC, laptop a iné) pomocou DSL alebo káblového vedenia.



Obr. 2.2: Základná architektúra IPTV [4]

IPTV štandardy

IPTV je nasadená v rámci súkromných IP sietí a nespotrebováva zdielané zdroje ako je napríklad rádiové spektrum, čo značí, že nevzniká okamžitá potreba štandardizovať systémy a architektúry.

Jeden operátor môže nasadiť niekoľko IPTV systémov v tej istej sieti bez nepriaznivých účinkov, ak sú vylúčené celkové náklady, potreba vyhradeného set-top boxu a obsadenosť šírky pásma distribučnej siete niekoľkými paralelne fungujúcimi systémami [8].

Nízky počet obmedzení a nedostatok ľahko dostupného a uceleného štandardu IPTV vedú k rozvoju vlastných riešení. Tieto riešenia tvoria základ pre všetky systémy IPTV prevádzkované po celom svete. Na druhej strane tieto systémy vychádzajú z niekoľkých základných štandardov. Prvým je MPEG (Motion Picture Expert Group) pre kódovanie videa (MPEG-2, MPEG-4) a prenosové protokoly (MPEG TS). Kvôli nevyhnutnej úlohe IP je druhým určite IETF (Internet Engineering Task Force) pre svoje doručovacie a riadiace protokoly (RTP/RTCP, RTSP, SDP, SIP atď.) [8].

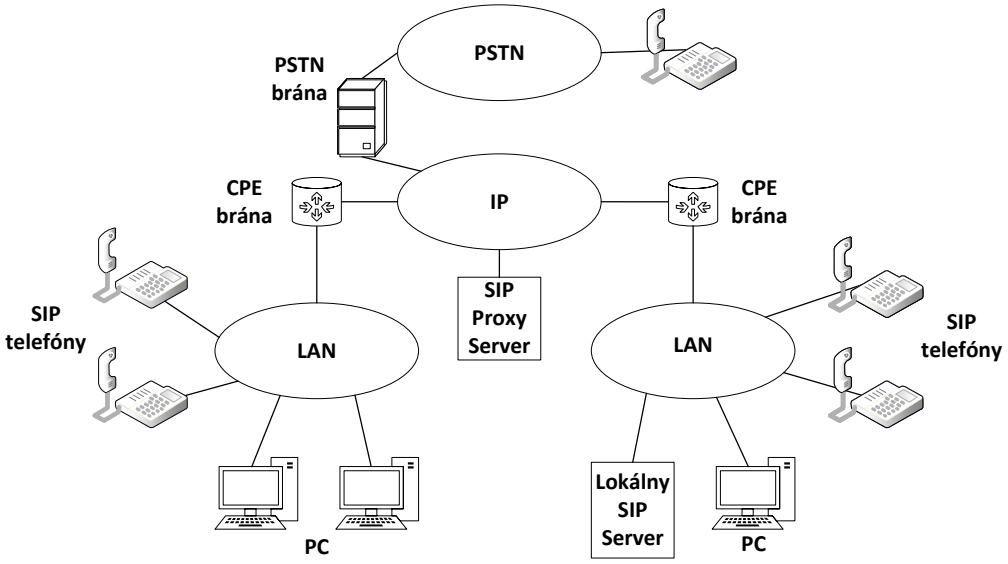
2.5.2 VoIP

Voice over IP zabezpečuje prenos hlasu ako paketov cez sieť a na to používa internetový protokol IP. Preto je možné aplikovať tento typ služby v akejkoľvek dátovej sieti, ktorá využíva IP, ako je internet, intranet a lokálne siete. Táto služba digitalizuje hlasový signál, komprimuje a konvertuje ho na IP pakety a následne dané pakety prenáša cez IP sieť. Signalizačné protokoly sa používajú na zostavovanie a zrušenie hovorov, prenášanie informácií potrebných na lokalizáciu používateľov a vyjednávanie možností. VoIP predstavuje skutočný spôsob prenosu hlasu cez IP sieť a popisuje telefónne zariadenia, ktoré používajú IP ako natívny prenos pre hlasovú a hovorovú signalizáciu [9, 10].

Pri vytváraní VoIP hovoru je potrebné brať do úvahy veľké množstvo faktorov. Medzi tieto faktory patrí kodek reči, paketizácia, strata paketov, oneskorenie, variácia oneskorenia a sieťová architektúra na zabezpečenie QoS. Medzi ďalšie faktory, ktoré sa podieľajú na úspešnom volaní VoIP, patrí signalizačný protokol nastavenia hovoru, kontrola prijatia hovoru, bezpečnostné problémy a schopnosť prechádzať NAT a firewall [10].

Obr. 2.3 zobrazuje zjednodušenú schému IP telefónneho systému pripojeného k rozsiahlej IP sieti a IP telefóny sú pripojené k LAN. Jednotlivé hlasové hovory je možné realizovať lokálne cez LAN. IP telefóny obsahujú kodeky, ktoré digitalizujú a kódujú (a tiež dekódujú) reč. IP telefóny tiež paketizujú a depaketizujú zakódovanú reč. Hovory medzi rôznymi lokalitami je možné uskutočňovať cez rozľahlú

IP sieť. Jednotlive proxy servery uskutočňujú registráciu IP telefónov a koordinujú signalizáciu hovorov, najmä medzi lokalitami. Pripojenie k PSTN (Public Switched Telephone Network) je možné realizovať cez VoIP brány [11].



Obr. 2.3: Zjednodušená schéma IP telefónneho systému pripojeného k rozsiahlej IP sieti [9]

Väčšina internetových aplikácií používa protokol TCP, zatiaľ čo VoIP používa UDP. TCP nie je vhodné pre komunikáciu v reálnom čase, ako je napríklad prenos reči nakoľko funkcia potvrdenia a opätovného prenosu by viedla k veľkým oneskoreniam. Na druhej strane, UDP poskytuje nespoľahlivú službu doručenia na prenos správ medzi koncovými bodmi na internete.

RTP, používané v spojení s UDP, poskytuje end-to-end prenosové funkcie pre aplikácie, ktoré prenášajú dáta v reálnom čase. Tými sú audio a video, cez unicast a multicast. RTP nerezervuje zdroje a nezaručuje kvalitu služieb. Sprievodný protokol RTCP umožňuje monitorovanie spojenia, avšak väčšina aplikácií VoIP ponúka nepretržitý tok paketov bez ohľadu na stratu paketov alebo oneskorenie pri dosiahnutí prijímača [10].

VoIP protokoly

V oblasti komunikácie VoIP je veľké množstvo protokolov, ktoré umožňujú prenos hlasu a videa cez internetové siete. Jedným z najrozšírenejších štandardov používaných v celosvetovej komunikácii je RTP, ktorý je zodpovedný za prenos multimediálnych paketov. Tento protokol je špecifikovaný IETF v dokumente RFC 3550

a podporuje rôzne audio a video kodeky, definované v RFC 3551 a ďalších technických dokumentoch ITU a IETF. RTP taktiež zabezpečuje správne usporiadanie dátových paketov a prostredníctvom sprievodného protokolu RTCP ponúka nástroje pre zvládanie oneskorení a jitteru v sieťovom prenose [11].

Ako další je napríklad protokol SIP (Session Initiation Protocol), ktorý sa využíva na správu signalizačnej vrstvy aplikácií a je nevyhnutný pre zriaďovanie, správu a ukončovanie multimediálnych relácií, vrátane VoIP a videokonferencií. SIP, ktorý vychádza z RFC 2543, je textový protokol integrovaný do internetovej infraštruktúry a je súčasťou multimediálnej architektúry IETF, ktorá zahŕňa aj ďalšie protokoly ako RSVP (Resource Reservation Protocol), RTTP (Real-Time Transport Protocol) a SDP (Session Description Protocol) [11].

2.6 Správa sieťového prenosu

Nakoľko sa počítačové siete neustále rozvíjajú, správa sieťového prenosu predstavuje základný pilier a je nevyhnutné zabezpečiť plynulú a efektívnu komunikáciu medzi zariadeniami. Medzi štyri základné metriky, ktoré spoločne definujú výkon a spoľahlivosť sieťovej infraštruktúry, patria priepustnosť, latencia, chybovosť paketov a jitter. Z toho dôvodu je dôležité porozumieť a korektne riadiť tieto aspekty, aby bol dosiahnutý optimálny sieťový prenos.

2.6.1 Priepustnosť

Priepustnosť (Throughput) je hlavným ukazovateľom sieťovej kapacity a je možné ju definovať ako množstvo dát, ktoré je sieť schopná úspešne preniesť z jedneho bodu do druhého v určitom časovom rozmedzí. Táto metrika je meraná v bitoch za sekundu (bit/s) a vyššie hodnoty priepustnosti signalizujú schopnosť siete prenášať viac dát. To je zásadné pre aplikácie vyžadujúce veľké prenosové rýchlosti, ako sú napríklad databázové aplikácie, prenášajúce veľké objemy dát, alebo pre streamovacie služby, kde kontinuálny a rýchly prenos videa zaisťuje plynulý zážitok bez zasekávania [12, 13].

2.6.2 Latencia

Latencia sa v sieti vzťahuje na časové zdržanie pri ceste dátového paketu z jedného sieťového uzlu do druhého. Obvykle sa meria ako oneskorenie spiatočnej cesty a ideálne by mala byť čo najbližšie k nule, pre dosiahnutie lepších výsledkov. Táto metrika je zvyčajne meraná v milisekundách (ms) a je dôležitá pre aplikácie, kde je dôležitá rýchla odozva, ako sú napríklad hlasové služby alebo online hry. Latencia

je ovplyvnená mnohými faktormi, vrátane fyzických vzdialeností medzi komunikujúcimi zariadeniami, kvality sieťového hardvéru, softvéru a aktuálneho preťaženia siete[14, 15].

2.6.3 Chybovosť paketov

Chybovosť paketov je situácia, keď sú dátové pakety počas prenosu stratené alebo poškodené, čo vedie k narušeniu prenosu dát a vyžaduje si ich opätovné odoslanie. Opätovné zasielanie zaťažuje sieť a znižuje jej celkový výkon. Chybovosť paketov môže byť spôsobená rôznymi faktormi, ako sú sieťové preťaženie, hardvérové zlyhanie, softvérové chyby alebo útoky typu packet drop. Jedná sa o kritický parameter pre aplikácie, ktoré vyžadujú vysokú spoľahlivosť, ako sú finančné transakcie alebo dôležité dátové zálohovania. Chybovosť paketov sa meria ako percentuálny podiel stratených paketov z celkového počtu odoslaných [16, 17, 18].

2.6.4 Jitter

Jitter, alebo variabilita latencie v sieti sa týka variácie v oneskoreniach príchodu paketov v sieti. Je to spôsobené mnohými faktormi vrátane sieťového preťaženia, kolízií a rušenia signálu. Vysoký jitter je problémom najmä v aplikáciách, kde je dôležitá konzistencia časovania, ako sú VoIP hovory alebo video konferencie. Ak je jitter príliš vysoký, používatelia môžu zažiť prerušované audio a video prenosy, čo môže výrazne ovplyvniť komunikačný zážitok. Jitter je dôležité sledovať a minimalizovať, aby sa zabezpečila spoľahlivosť a kvalita prenosu v reálnom čase. Jitter sa meria v milisekundách (ms) a opisuje sa ako narušenie v normálnej sekvencii odosielania dátových paketov [19, 20, 21].

3 Sieťový analyzátor IXIA

Táto kapitola sa venuje sieťovému generátoru IXIA s jeho rôznymi možnosťami využitia. Konkrétne sa táto kapitola zaoberá vybraným modelom IXIA XM2, nakoľko je tento model súčasťou prvej laboratórnej úlohy v kapitole číslo 6.

Systém IXIA je jeden z najkomplexnejších nástrojov na testovanie viacvrstvového 10/100 Mbit/s Ethernetu, Ethernet Gigabitu, 10 Gigabit Ethernetu, ATM a Packet over SONET prepínača, smerovača a siete. Testovací systém IXIA poskytuje komplexné riešenia v oblasti testovania výkonu, funkcionality a súladu sietí a sieťových aplikácií. Ide o testovaciu platformu, ktorá slúži na testovanie širokého spektra služieb ISO/OSI modelu od siedmej vrstvy až po druhú. Najväčšie zameranie generátora IXIA je na druhú a tretiu vrstvu modelu ISO/OSI. Poskytuje široké množstvo záťažových modulov a testovacích aplikácií. Taktiež prináša flexibilitu pri vykonávaní celého radu testovania sietí, zariadení, údajov, signalizácie, hlasu, videa, aplikácií a zabezpečenia [22, 23].

Rodina produktov IXIA zahŕňa šasi (rám), záťažové moduly, softvérový program IXIA IxExplorer a voliteľné TCl skripty a súvisiaci softvér. Šasi je možné nakonfigurovať s rôznymi kombináciami záťažových modulov a taktiež je možné prepojiť viacero šasi a zosynchronizovať ich tak, aby podporovali veľké a zložité testovacie prostredia.

Jednotku je možné priamo konfigurovať a ovládať prostredníctvom pripojenia klávesnice, myši a monitoru. Tiež je možné jednotku pripojiť k ethernetovej sieti a daný správca ju môže vzdialene monitorovať a ovládať pomocou softvérového programu IxExplore. Súčasne môže k danej jednotke pristupovať viacero užívateľov pričom každý užívateľ využíva iný port šasi a riadi činnosť a konfiguráciu všetkých portov a funkcií [22, 23].

Na prednom paneli sa nachádza aj displej, ktorý poskytuje okamžitú indikáciu stavu spojenia, prenosu alebo prijatia paketov a chybových stavov. IXIA vyrába niekoľko záťažových modulov, ktoré poskytujú prenos a príjem dát pre rôzne rýchlosti a technológie. Záťažové moduly sú umiestnené v šasi a poskytujú rôzne počty slotov a výkonov.

Každý model šasi disponuje samostatným počítačom so systémom Windows XP Professional. Obsahuje aj sieťové rozhranie 10/100/1000 Mbit/s a lokálny disk. Tieto modely môžu obsahovať disketovú jednotku, CD-ROM alebo DVD-ROM. Existuje niekoľko modelov IXIA šasi a tými sú napríklad [24, 25] :

- **XG12 Chassis** - jedná sa o novú generáciu vysokovýkonnej platformy, ktorá podporuje záťažové moduly novej generácie. Šasi obsahuje 12 slotov, ktoré poskytuje vyšší výkon s výhradami na vyšší výkon karty. Táto platforma taktiež umožňuje moduly s vyššou hustotou zaťaženia portov.

- **Optixia XM12 Chassis** - tento model dokáže využiť až 12 záťažových modulov IXIA a disponuje dodatočným napájaním a ventilátormi, ktoré sú potrebné pre vysokovýkonné záťažové moduly. Taktiež aj podporuje vyššiu hustotu portov.

- **Optixia XM2 Chassis** - dokáže využívať dva záťažové moduly IXIA. Je vybavený dodatočným napájaním a ventilátormi, ktoré sú vyžadované z dôvodu použitia niektorých vysokovýkonných záťažových modulov. Podporuje aj vyššiu hustotu portov.

- **Optixia XL10 Chassis** - jedná sa o model so schopnosťou pojať kombináciu IXIA s vysokou hustotou zaťažovacích modulov s 24 portami. Podporuje až 240 portov s rýchlosťami 10/100/1000 Mbit/s. Je taktiež vybavený redundantnými zdrojmi napájania.

3.1 IXIA MX2

Sieťový analyzátor Optixia XM2 patrí medzi ľahko prenosné zariadenia, ktorý poskytuje profesionálne riešenie analýzy siete. Uplatnenie má vo väčích firmách a je predovšetkým určená na optimalizáciu sieťovej infraštruktúry. Optixia XM2 disponuje dvoma slotmi pre podporu až dvoch samostatných záťažových modulov. Podporuje všetky záťažové moduly XM a mnoho štandardných záťažových modulov so zlepšeným napájaním a chladením systému. Dvoj-slotová platforma poskytuje moduly s vyššou hustotou zaťaženia portov. Tieto zásuvné moduly je možné osadiť do dvoch rozhraní, ktoré obsahuje. Na týchto moduloch sa nachádzajú rozhrania, ktoré slúžia na pripojenie meraných prvkov. Výhodou tohto sieťového analyzátora je, že moduly je možné vymeniť za behu zariadenia, čo neovplyvní meranie, ktoré prebieha na druhom slote [25, 26].

Šasi podporuje 32 GbE porty a 4-paketové porty SONET (POS) alebo štyri porty asynchrónneho prenosu (ATM). Tieto typy portov slúžia na zabezpečenie veľkého toku dát. Vysoký výkon zariadenia poskytuje sledovanie správania siete v hraničných podmienkach. Moduly poskytujú sieťové rozhrania a zdroje distribuovaného spracovania, ktoré sú potrebné na vykonanie testovania údajov pričom prevádzka

môže byť rôzneho typu. Napríklad testovanie obrazu, zvuku signalizácie, smerovania a aplikácií pre vrstvy 2-7 [25, 26].

Optixia XM2 obsahuje integrovanú riadiacu jednotku, ktorá slúži na manažment, kontrolu portov a štatistík. Na tejto riadiacej jednotke je spustený systém Windows XP Professional. Funkcia podpory pre viacerých užívateľov zabezpečuje, že rôzni administrátori môžu pracovať na analyzátore a vykonávať merania rôznych sieťových zariadení bez vzájomného ovplyvňovania. Týka sa to aj priradenia portov na analyzátore XM2, kde môže byť každému užívateľovi pridelený osobitný port, alebo naopak, porty z jednej karty môžu byť rozdelené medzi viacerými užívateľmi. Pomocou jednoduchého prihlásenia majú administrátori možnosť pripojiť sa zabezpečene alebo nezabezpečene, lokálne alebo diaľkovo, prostredníctvom klienta. Vďaka funkcií reťazenia je možné prepojiť až 256 zariadení a využiť ich ako celok na jedno konkrétne meranie [25, 26, 27].

Obr. 3.1: Sieťový analyzátor Optixia XM2 [26]

Medzi ďalšie výhody patrí:

- Veľmi vysoká hustota gigabitových a 10Gbit ethernetových portov a široká škála dostupných sieťových rozhraní, ktorá umožňuje flexibilné a multifunkčné nasadenie.
- Vysokovýkonná architektúra urýchľuje inicializáciu a spúšťanie testov.
- Integrovaný softvérový balík pre šasi a jednotlivé moduly rozhrania znižujú réžiu správy a zjednodušuje aktualizácie.

- Vzdialená správa umožňuje jednoduchý prístup k prostriedkom šasi cez sieť.
- Automatizované testovacie balíky, ktoré sú vopred zostavené, umožňujú jednoduché vykonávanie škálovateľných záťažových testov.
- Spätná kompatibilita hardvéru a softvéru s existujúcimi testovacími systémami IXIA umožňuje jednoduchý prechod z alebo integráciu s už existujúcimi inštaláciami.

Technické parametre

Tab. 3.1: Technické parametre Optixia XM2 [24]

Sloty	2 (kompatibilné so záťažovými modulami XM)
Napájanie	100-240V 60/50Hz 12-6A
Operačný systém	Windows XP Professional
CPU	Intel Pentium Mobile, 2.0 GHz
Pamäť	2 GB
Disk	250GB SATA Disk HD

Tab. 3.2: Konektory na prednom paneli [24]

USB	1 USB dual type A, 4-pin jack connector
Sync In	4-pin RJ11
Sync Out	4-pin RJ11

Tab. 3.3: Konektory na zadnom paneli [24]

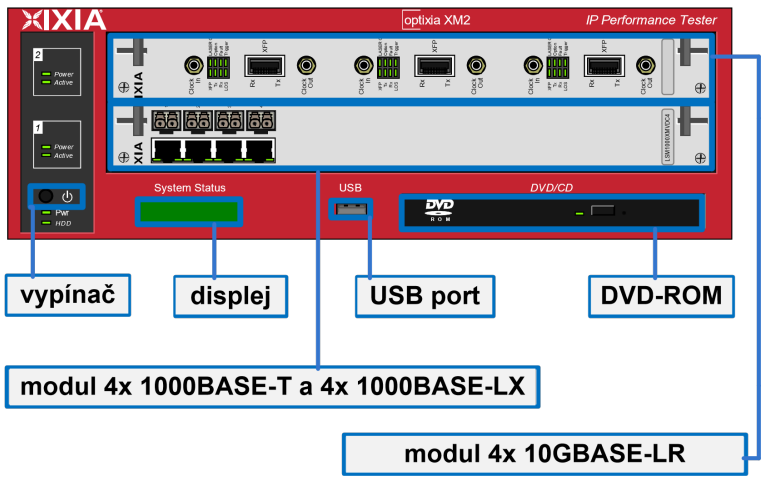
Myška	PS/2 6-pin DIN
Klávesnica	PS/2 6-pin DIN
Monitor	HD-DB15 Super VGA
Tlačiareň	Female DB25 parallel port
Ethernet	RJ-45 10/100/1000Mbit/s Gigabit Ethernet Management Port
Serial	1 male DB9 ports
USB	2 USB dual type A, 4-pin jack connectors

Moduly

Zoznam vybraných modulov s určitými funkciami, ktoré sú podporované na Optixia XM2, sú uvedené v tabuľke 3.4. V tabuľke sú uvedené aj moduly, ktoré sú využité v prvej laboratórnej úlohe.

Tab. 3.4: Vybrané moduly pre Optixia XM2 [24]

Modul	Funkcia
HSE40/100GETSP1-01	40 a 100 gigabitový Ethernet 1-port, 2-slotové rozhranie CFP (plná funkcia)
LSM1000XMVR4-01	4-portový Dual-PHY (RJ45 a SFP) 10/100/1000 Mbit/s Ethernet záťažový modul, znížený výkon
LSM10GXMR4S-01	Modul 10 Gigabit Ethernet so 4 portami, 400 MHz, 128 MB, jeden slot, znížená podpora L2/3 s obmedzeným smerovaním L3, Linux SDK a aplikácie L4-7
LSM1000XMSR12-01	Modul 10/100/1000 Ethernet 12 portov, redukovaná sada funkcií
LSM10GXM8-01	10 Gigabit Ethernet, 8 portov, jeden slot, plnohodnotný modul, 800 MHz, 512 MB. Plná podpora L2/7. Linux SDK a aplikácie L4-7



Obr. 3.2: Popis analyzátora Optixia XM2 s modulmi, ktoré sú využité v laboratórnych úlohách [27]

Software

Pomocou rôznych prostredí je možné toto zariadenie ovládať. Medzi tieto aplikácie patrí napríklad IxLoad, IxNetwork, IxExplorer a iné.

IxLoad

Táto aplikácia umožňuje testovanie konvergovanej služby, bezpečnostných prvkov a systémov so zameraním na testovanie sietí 4-7 vrstvy. IxLoad simuluje odberateľov dát, videa a zvuku, dátové zdroje a príslušné protokoly. Podporuje aj služby malware a DDoS (Distributed Denial of Service) pre simuláciu útokov na testovanie bezpečnosti siete. Umožňuje podporu pre dátové služby ako sú napríklad DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) a iné. Ďalej podporuje video služby ako RTSP (Real Time Streaming Protocol) a hlasové služby ako SIP (Session Initiation Protocol), VoIP (Voice over IP) [27].

IxNetwork

Aplikácia slúži na overenie sieťovej infraštruktúry, kapacity a konvergencie za pomoci emulačného protokolu. Zabezpečuje rýchlu identifikáciu sieťových problémov na 2 a 3 vrstve siete. IxNetwork umožňuje testovať prepínače a smerovače pomocou protokolov ako napríklad BGP (Border Gateway Protocol), OSPF (Open Shortest Path First), IP multicast a ďalších. Využitie má napríklad pri začleňovaní nových sieťových prvkov [27].

IxExplorer

Softvér IxExplorer je pred-inštalovaný na každom zariadení IXIA. Je zameraný na analýzu 1-4 vrstvy sieťového modelu ISO/OSI. Analýza prevádzky medzi 4–7 vrstvou je možná len ako nestavová. Taktiež je možné nainštalovať program na inom zariadení a pomocou vzdialeného prístupu ovládať a konfigurovať porty Chassis XM2 [25].

Program poskytuje detailné konfigurácie paketových a rámcových hlavičiek, s možnosťou nastavenia pre ToS/QoS (Type of Service / Quality of Service). IxExplorer dokáže generovať až 255 unikátnych tokov paketov s rôznymi prenosovými rýchlosťami. Pre jednotlive streamy je možné nastavovať veľkosti rámcov a ich vzor. Podrobnosti o vrstvách 2 a 3, vrátane VLAN a rôzne protokoly(IPv4, IPv6, ARP...). Ďalej simulácie chýb ako napríklad CRC (Cyclic Redundancy Check) chyby. Nastavenie streamov taktiež poskytuje nastavenie typu prevádzky (nepretržitý, jednorázový ...), počet opakovaní streamov a iné [25].

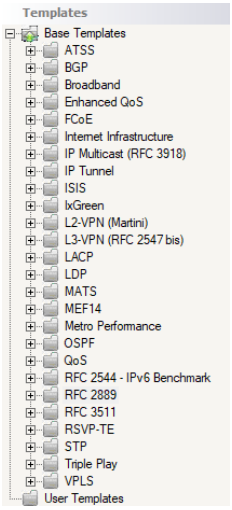
Po ukončení analýzy je možné pristupovať a prehliadať štatistiky meraní. Štatistiky je možné prehliadať individuálne pre každý port alebo skupinovo všetky toky

paketov. Tieto štatistiky obsahujú informácie ako počet odoslaných/prijatých rámcov alebo bytov a stratovosť. V štatistikách je možné aplikovať filtre pre ToS/QoS, veľkosť paketu, IP/MAC zdrojové a cieľové adresy [25].

IxAutomate

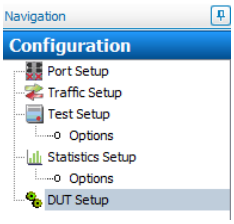
IxAutomate je program s grafickým užívateľským rozhraním na automatizované testovanie sieťových zariadení a sietí, ktorý obsahuje preddefinované testy podľa štandardov RFC. Tieto testy, ako napríklad RFC 2544 pre benchmarking IPv6 alebo RFC 2889 na prepínacie testy druhej vrstvy, umožňujú zistiť rýchlosť konvergencie protokolov, maximálny počet ciest pre každý protokol a ďalšie výkonnostné metriky. Napriek tomu, že pre každý test RFC je potrebná samostatná licencia, výhodou je rýchle a jednoduché testovanie bez potreby detailného nastavovania parametrov. Aplikácia Aptixia IxAutomate ponúka výkonný, prispôsobiteľný nástroj na automatizované vyhodnocovanie výkonu, škálovateľnosti a funkčnosti sieťových zariadení. IxAutomate poskytuje jednoduché grafické rozhranie na konfiguráciu vlastných automatizovaných testovacích scenárov a analýzu výsledkov testov. Využívaním možností hardvéru Ixia, ako sú generovanie premávky na maximálnej rýchlosti, filtrovanie, zachytávanie a zbieranie štatistík, IxAutomate ponúka bohatý súbor predpripravených testov založených na štandardoch RFC a požiadavkách zákazníkov. Výsledky testov sú zbierané a prezentované s flexibilným súborom funkcií, vrátane grafík v reálnom čase zobrazujúcich priebeh testovania, formátovaných správ pre detailnú analýzu po testovaní, farebných indikátorov úspechu alebo zlyhania testov a podrobných záznamov o vykonávaní testov. Ako testovacie prostredie IxAutomate ponúka architektúru zásuvných modulov navrhnutú na ľahké pridávanie vlastných testov do už rozsiahlej knižnice testov [28].

Rozhranie IxAutomate je prezentované v hierarchickom strome, čo umožňuje jednoduchú navigáciu medzi rôznymi testami ako je možné vidieť na obrázku 3.3. Šablóny je možné jednoducho prechádzať, pričom ich diagram a popis umožňujú používateľom ľahký výber testov. Po výbere sa testovacie šablóny skopírujú do používateľského testovacieho priestoru, kde sú následne nakonfigurované, prispôsobené a spustené [28].



Obr. 3.3: Hierarchický strom testov

Test Configuration je podporovaná štandardná štruktúra Aptixia s postupnou konfiguráciou pre všetky testy. Túto štruktúru je možné vidieť na obrázku 3.4.



Obr. 3.4: Konfigurácia testov

Jednotlivý popis častí konfigurácií pre testy [28]:

1. **Port Setup** menu umožňuje zobrazenie a konfiguráciu všetkých testovacích portov dostupných na testovanie. Tu sa konfigurujú vlastnosti fyzickej vrstvy.
2. **Traffic Setup** menu obsahuje informácie pre špecifikáciu premávky, ktorá sa má odoslať počas testu, vrátane parametrov, ako sú veľkosti rámca, mapovanie prevádzky medzi portami, adresovanie a obsahu.
3. **Test Setup** ponuka obsahuje informácie týkajúce sa trvania testu, počtu pokusov, iterácií a ďalších informácii špecifických pre vybraný test.
4. **Statistics Setup** sa používa na definovanie štatistík, ktoré budú graficky zobrazené programom StatViewer a konfigurácia SNMP pre monitorovanie DUT.
5. **DUT Setup** umožňuje používateľom zadávať príkazové súbory na konfiguráciu/monitorovanie zariadenia.

4 DOCSIS

DOCSISn (Data Over Cable Service Interface Specificatio) je medzinárodný telekomunikačný štandard, ktorý poskytuje obojsmerné širokopásmové dátové prenosy po existujúcich televíznych káblových rozvodoch.

Prvé širokopásmové káblové siete sa objavili už v 70. rokoch 20. storočia v oblastiach, kde bolo pokrytie pozemným vysielaním slabé [29]. Približne v polovici 80. rokov sa začali šíriť širokopásmové káblové siete využívajúce 75-ohmovú koaxiálnu technológiu na dodávanie analógových televíznych a rozhlasových programov.

Od 90. rokov 20. storočia sa budovali nové siete využívajúce technológiu optických vlákien, a optické vlákna sa používali aj v častiach existujúcich sietí. To umožnilo vznik pojmu HFC (Hybrid Fiber Coax), ktorý označuje hybridné použitie optických vlákien a koaxiálnych technológií. Posledná míľa do priestorov zákazníka sa v rámci nich väčšinou stále realizuje pomocou medených káblov.

Účelom DOCSIS bolo špecifikovať obojsmerné dátové spojenie medzi CM (Cable Modem) a CMTS (Cable Modem Termination System) tak, aby bolo možné poskytnúť prístup na internet. V Európe sa používa mierne upravená verzia systému „Euro-DOCSIS“, ktorá pre downstream kanál využíva DVB-C namiesto J83B, ktorý je využívaný v originálnom DOCSIS. DVB-C používa primárne 64QAM alebo 256QAM moduláciu. J83B využíva 64QAM alebo 256QAM, ale s inými parametrami systému a môže taktiež používať 32QAM. DVB-C používa frekvencie pre downstream približne od 50 do 865 MHz a pre upstream približne od 5MHz do 65MHz. J83B môže používať podobné frekvenčné rozsahy ale líši sa v podrobnostiach o symbolových rýchlostiach a modulačných schémach. Taktiež sú závislé aj na špecifikáciách poskytovateľov služieb.

DOCSIS definuje dve najnižšie vrstvy architektúry a to fyzickú a spojovú. Nad fyzickou vrstvou je podvrstva konvergencie, ktorá sa používa pre downstream. Tu sa dáta zapuzdrujú do rámca MPEG-2. Táto podvrstva taktiež podporuje digitálne televízne vysielanie v sieti HFC [29].

Architektúra DOCSIS zahŕňa dva základné komponenty, a to káblový modem umiestnený v priestoroch zákazníka a koncový systém káblového modemu (CMTS), ktorý je umiestnený v ústredni CATV (Cable Television). Počítač zákazníka a súvisiace periférne zariadenia sa označujú ako zariadenie CPE (Customer-premises Equipment) v priestoroch zákazníka. CPE sú pripojené ku káblovému modemu, ktorý je pripojený prostredníctvom HFC siete k CMTS. CMTS potom smeruje prevádzku medzi HFC a internetom. Pomocou systémov poskytovania a prostredníctvom CMTS vykonáva prevádzkovateľ káblovej siete kontrolu nad konfiguráciou káblového modemu.

4.1 Verzie štandardu DOCSIS

Verzie DOCSIS sa vyvíjali s cieľom zlepšiť prenosové rýchlosti, efektivitu a spoľahlivosť. Každá nová verzia priniesla významné vylepšenia, ktoré umožnili rýchlejší a efektívnejší prenos dát, lepšiu podporu pre moderné internetové aplikácie a zvýšenú kapacitu siete. V tabuľke 4.1 sú uvedené základné špecifikácie pre jednotlivé verzie DOCSIS. Medzi verzie DOCSIS patrí [30]:

- **DOCSIS 1.0:** Táto verzia obsahuje funkčné prvky pozostávajúce z predchádzajúcich proprietárnych káblových modemov.
- **DOCSIS 1.1:** Štandardizovala základné QoS (Quality of Services), ktoré neboli súčasťou DOCSIS 1.0.
- **DOCSIS 2.0:** Verzia poskytuje zvýšené prenosové rýchlosti dát na základe zvýšeného dopytu po symetrických službách ako je napríklad IP telefónia.
- **DOCSIS 3.0:** Táto verzia výrazne poskytla zvýšenie prenosových rýchlostí (pre upstream aj downstream) a priniesla aj podporu pre internetový protokol verzie 6 (IPv6).
- **DOCSIS 3.1:** Prináša pre downstream kapacitu až 10 Gbit/s a pre upstream 1 Gbit/s pomocou 4096QAM. Tieto nové špecifikácie eliminovali 6 MHz a 8 MHz široký kanálový odstup a namiesto toho používa užšie 25 alebo 50 kHz subnosné. Táto verzia taktiež poskytuje funkcie správy napájania, ktoré poskytujú zníženie energetickej spotreby a vďaka algoritmu DOCSIS-PIE znižuje aj bufferbloat (jedná sa o latenciu a jitter v sieťach s prepínaním paketov spôsobených nadmerným ukladaním paketov do vyrovnávacej pamäte a taktiež môže spôsobiť aj zmeny oneskorenia paketov a znížiť celkovú priepustnosť siete).
- **DOCSIS 4.0:** Zameriava sa na zvýšenie prenosovej rýchlosti dát s cieľom dosiahnuť rovnaké rýchlosti pre upstream a aj downstream a to až 10 Gbit/s. CableLabs predstavil celú špecifikáciu v Októbri 2017. Táto technológia, ktorá bola predtým označovaná ako DOCSIS 3.1 FullDuplex, bola premenovaná na súčasť DOCSIS 4.0. Naďalej je vo vývoji.

Tab. 4.1: Špecifikácie pre jednotlivé verzie DOCSIS [30]

Verzia	Prenosová rýchlosť Down-stream [Mb/s]	Prenosová rýchlosť Upstream [Mb/s]	Frekvenčný rozsah Down-stream [MHz]	Frekvenčný rozsah Upstream [MHz]	Šírka pásma Down stream [MHz]	Šírka pásma Upstream [MHz]
1.0	40	10	91-857	5-42	6	6,4
1.1	40	10	91-857	5-42	6	6,4
2.0	40	30	50-864	5-42	6	6,4
3.0	1 000	200	108-1002	5-85	8	6,4
3.1	10 000	1 000	258-1794	5-204	200	200
4.0	10 000	6 000	108-1794	5-684	1 800	679

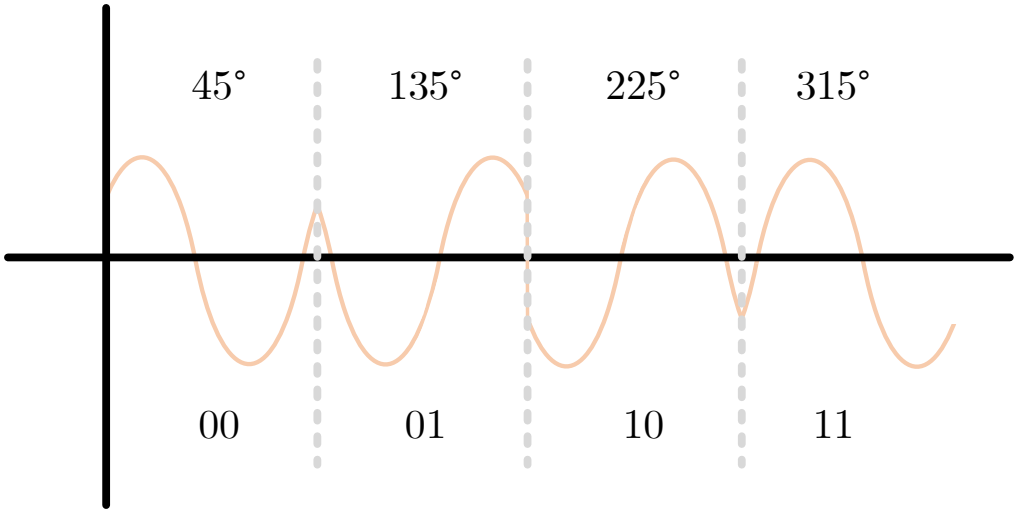
4.2 Modulácie v DOCSIS

V komunikácii prostredníctvom káblových a telekomunikačných sietí zohrávajú kľúčovú úlohu modulačné techniky. Modulácia je proces, počas ktorého sa modifikujú vlastnosti nosnej vlny (amplitúda, frekvencia alebo fáza) tak, aby mohla efektívne niesť informáciu cez komunikačný kanál. Modemové zariadenie ako napríklad DAH100 (DOCSIS Access Hub 100) využíva rôzne typy modulácií na prenos digitálnych dát cez analógové prenosové média, ako je koaxiálny kábel. V prípade DAH100 sú kľúčové modulačné techniky, ako je Quadrature Amplitude Modulation (QAM) a Quadrature Phase Shift Keying (QPSK). Novšie verzie (3.1 a 4.0) využívajú aj OFDM (Ortogonal Frequency-Division Multiplexing) a OFDMA (Ortogonal Frequency-Division Multiple Acces).

Vodafone v Českej republike používa pre svoje káblové internetové služby štandard DOCSIS 3.1. Tento štandard umožňuje využívať rýchlosti až do 1 Gbit/s pre downstream. DOCSIS 3.1 umožňuje využívanie OFDM, OFDMA a SC-QAM (Single-Carrier Quadrature Amplitude Modulation), ktoré zvyšujú kapacitu a efektivitu prenosu dát v porovnaní so staršími technológiami. Pre dosiahnutie prenosových rýchlostí 1 Gbit/s (downstream) sú využívané typy kanálov (24 kanálov) SC-QAM s moduláciou 256QAM a dva typy kanálov OFDM s moduláciou 4096QAM. Pre dosiahnutie prenosových rýchlostí 100 Mbit/s (upstream) sú využívané typy kanálov (5 kanálov) SC-QAM s moduláciou 64QAM a dva typy kanálov OFDM s moduláciou 1024QAM.

Quadrature Phase Shift Keying (QPSK)

Je modulačná technika často využívaná pre upstream, teda pre prenos dát od používateľa späť k centrálnej stanici. Jej robustnosť voči chybám z dôvodu šumu a iných prenosových problémov robí QPSK vhodnou pre situácie, kde je stabilita a spoľahlivosť prenosu dôležitejšia ako spektrálna efektívnosť. Napriek tomu, že QPSK neponúka takú vysokú spektrálnu efektívnosť ako QAM, je predsa len spoľahlivejšia v náročných podmienkach. QPSK pracuje s dvoma nosnými vlnami (sínus a kosínus), ktoré sú vzájomne ortogonálne. Tento typ modulácie používa štyri bodové pozície v konštelačnom diagrame, umožňujúce prenos dvoch bitov (00, 01, 10 a 11) na jeden symbol [31]. V QPSK sa nosná mení z hľadiska fázy, nie frekvencie, a existujú štyri možné fázové posuny. Tieto štyri body reprezentujú štyri rozličné fázové hodnoty posunuté o 90°, teda 45°, 135°, 225° a 315° (obrázok 4.1). Tieto uhly sa dajú jednoducho generovať pomocou I/Q (In-phase/quadrature) modulačných techník, pretože sčítanie I a Q signálov, ktoré sú buď invertované alebo neinvertované, vedie k týmto štyrom fázovým posunom. Tabuľka 4.2 obsahuje spôsob fázových posunov.



Obr. 4.1: Modulácia QPSK [31]

Použitie QPSK je predovšetkým rozšírené v vzostupnom smere, kde sa často kombinuje s 16QAM moduláciou, aby sa dosiahla lepšia efektívnosť v šumovom prostredí. Pridanie oboch nosných zložiek, sínus a kosínus, vedie k vytvoreniu výsledného signálu, ktorý je potom vysielaný z modemu do siete.

Tab. 4.2: I/Q modulačná technika [31]

I	Q	Fázový posun
Neinvertovaný	Neinvertovaný	45°
Invertovaný	Neinvertovaný	135°
Invertovaný	Invertovaný	225°
Neinvertovaný	Invertovaný	315°

Quadrature Amplitude Modulation (QAM)

Je obzvlášť užitočná v káblových a širokopásmových sieťach, kde vysoká spektrálna efektívnosť umožňuje prenos veľkého množstva dát na jednotku šírky pásma. DAH100 používa QAM pre downstream, teda prenos dát z centrálnej stanice k užívateľovi, kde rôzne úrovne modulácie, ako 64QAM alebo 256QAM, môžu byť implementované v závislosti od kvality prenosového kanálu a požiadaviek na prenosovú rýchlosť. Modulácia využíva amplitúdové kľúčovanie na dve vzájomne ortogonálne nosné vlny, ktoré sú nezávislé a využívajú funkcie sínus a kosínus. Tento typ modulácie spája amplitúdovú a fázovú moduláciu, pričom kapacitu kanálu určuje frekvencia nosnej a pomer signál/šum. V súlade so štandardom DOCSIS sa pre downstream najčastejšie využíva modulácia 256QAM pričom v najnovšej verzii štandardu je možné využiť až 4096QAM. Upstream obvykle využíva nižšie úrovne QAM kvôli väčšej náchylnosti použitého frekvenčného rozsahu k rušeniu.

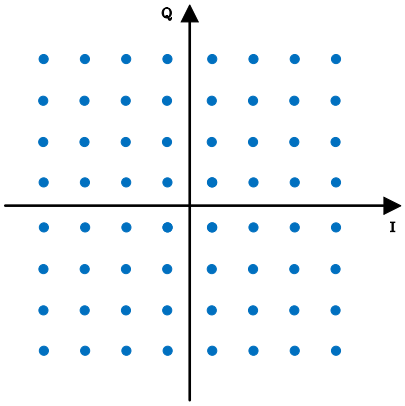
64QAM

Je jeden z typov kvadratúrnej modulácie (QAM), v ktorej nosná vlna s pevnou frekvenciou môže existovať v jednom zo šesťdesiatich štyroch rôznych diskrétnych a merateľných stavov v konštelačnej schéme. Konštelačný graf pozostáva z dvoch zložkových osí, a to z fázovej (os X) a kvadratúrnej (os Y). Tieto dve zložky sú navzájom ortogonálne alebo fázovo posunuté o 90°. Na obrázku 4.2 sa nachádza konštelačný diagram 64QAM. Každý symbol v 64QAM je stav konštelácie, ktorý obsahuje šesť bitov a každý symbol je jednou možnou kombináciou zo 64 rôznych stavov v rozsahu od **000 000** do **111 111** [32]. Pomocou 64QAM je možné modulovať amplitúdu aj fázu nosnej vlny a prenášať relatívne väčší počet bitov, čím sa dosiahne vyššia bitová rýchlosť v porovnaní s inými modulmi QAM nižšieho rádu.

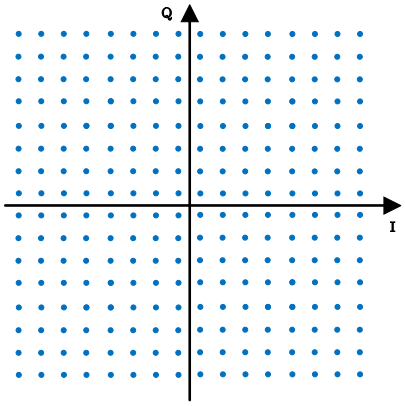
256QAM

Je ďalší z typov kvadratúrnej amplitúdovej modulácie (QAM), v ktorej môže nosná vlna konštantnej frekvencie existovať v jednom z 256 rôznych diskrétnych a merateľných stavov v konštelačnej schéme. Fázová aj kvadratúrna os modulovaného signálu

sú taktiež navzájom ortogonálne (fázovo posunuté o 90°). Na obrázku 4.3 sa nachádza konštelačný diagram 256QAM. Každý symbol v 256QAM je stav konštelácie, ktorý obsahuje osem bitov a každý symbol je jednou možnou kombináciou z 256 rôznych stavov v rozsahu od **0000 0000** do **1111 1111** [33]. Keďže táto modulačná schéma používa na prevádzku binárne dáta, celkový počet možných kombinácií pre 8 bitov je 256. Počet bitov možno vypočítať v zmysle logaritmickej hodnoty ako (1/6 bitovej rýchlosti). Pomocou 256QAM je možné modulovať amplitúdu aj fázu nosnej vlny a prenášať väčší počet bitov, čo vedie k vyššej bitovej rýchlosti v porovnaní s inými QAM nižšieho rádu, ako je napríklad 64QAM.



Obr. 4.2: Modulácia 64-QAM [32]

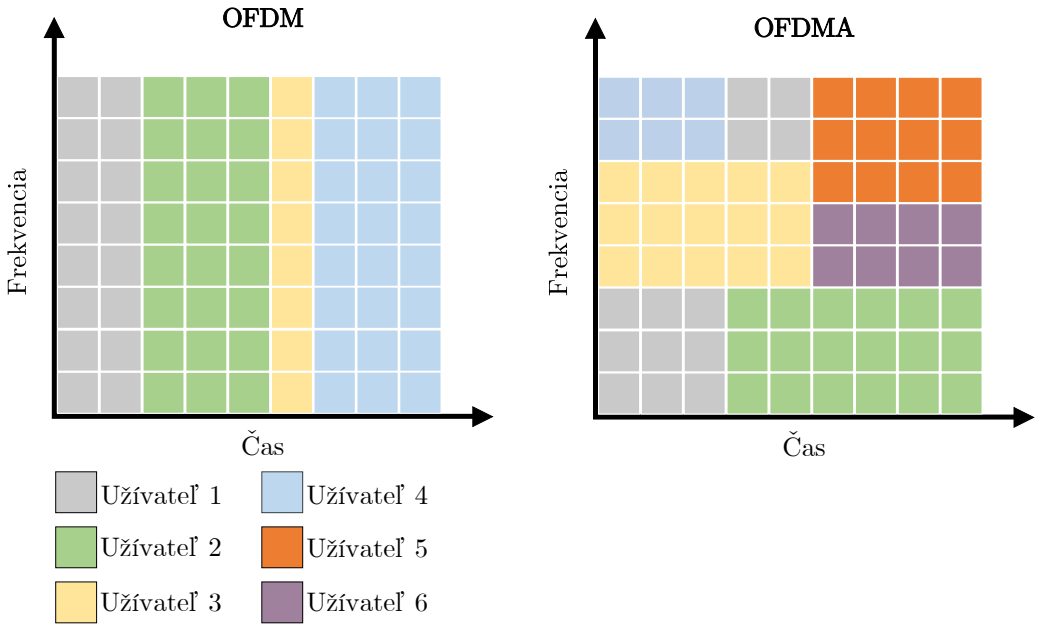


Obr. 4.3: Modulácia 64-QAM [33]

Ortogonal Frequency-Division Multiple Acces (OFDMA)

Je technika multiplexovania a prístupová metóda, ktorá umožňuje efektívne využitie spektra v bezdrôtových a káblových komunikačných systémoch. Je kľúčovou komponentnou v moderných komunikačných štandardoch ako je napríklad LTE (Long Term Evolution) a DOCSIS 3.1. Rozdeľuje dostupný kanál na menšie čiastkové pásma alebo čiastkové nosné frekvencie. Tieto čiastkové pásma sa označujú ako zdrojové jednotky (RU) a každá zdrojová jednotka je priradená individuálnemu užívateľovi klienta, čím sa umožňuje prístupovým bodom (AP) využívať RU na súčasné obsluhovanie viacerých užívateľov [34].

V OFDM, sa každý signál alebo dátový rámec od používateľa prenáša sekvenčne, takže ostatní používatelia musia čakať, kým aktuálny používateľ dokončí prenos všetkých OFDM symbolov. OFDMA umožňuje prístupovým bodom komunikovať s viacerými používateľmi ich optimálnym priradením ku konkrétnym RU v závislosti od potrebnej šírky pásma, veľkosti dát a stavu kanála. Rozdelením kanála a priradením týchto RU viacerým užívateľom sa môže súčasne prenášať viacero dátových rámcov. Podobne ako pri OFDM je dostupný kanál rozdelený na viacero čiastkových nosných, pričom každá čiastková nosná je navzájom ortogonálna. Princíp a rozdiel medzi OFDM a OFDMA je zobrazený na obrázku 2.4.



Obr. 4.4: Porovnanie OFDM a OFDMA [35]

OFDMA zabezpečuje, že používatelia môžu súčasne prenášať dátové rámce. Medzi rôznymi používateľmi vysielajúcimi na rôznych čiastkových nosných frekvenciách teda nedochádza k žiadnemu presluchu.

Typy modulácii pre jednotlivé verzie downstreamu

- Všetky verzie pred verziou 3.1 špecifikujú 64 alebo 256 úrovňovú QAM.
- DOCSIS 3.1 pridáva 16, 128, 512, 1024, 2048 a 4096QAM.
- DOSCIS 4.0 pokračuje v používaní modulácie QAM ako je 4096QAM a vyššie aby sa využila zvýšená šírka pásma a zlepšila sa tak celková prenosová rýchlosť dát.

Typy modulácii pre jednotlivé verzie upstreamu

- DOCSIS 1.x využíva modulácie QPSK alebo 16QAM.
- DOCSIS 2.0 a 3.0 využíva QPSK a 8, 16, 32, 64QAM.
- DOCSIS 2.0 a 3.0 podporuje mriežkovú kódovú moduláciu 128-QAM v režime S-CDMA.
- DOCSIS 3.1 podporuje modulácie od QPSK až po 1024-QAM, s voliteľnou podporou pre 2048 a 4096QAM.
- DOSCIS 4.0 bude podporovať pokročilejšie modulácie QAM ako je 4096QAM aby sa zlepšila celková prenosová rýchlosť dát. Dôležité to je pre full duplex operácie, ktoré umožňujú súčasne vysielanie a prijímanie dát.

4.3 Bezpečnosť DOCSIS

DOCSIS zahŕňa bezpečnostné služby vrstvy riadenia prístupu k médiám (MAC). DOCSIS 1.0 používal pôvodnú špecifikáciu BPI (Baseline Privacy Interface). BPI bol neskôr vylepšený vydaním špecifikácie BPI+ (Baseline Privacy Interface Plus), ktorú používa DOCSIS 1.1 a 2.0. Najnovšie bolo do základného rozhrania súkromia pridaných niekoľko vylepšení ako súčasť DOCSIS 3.0 a špecifikácia bola premenovaná na SEC (Security). Zámerom špecifikácií BPI/SEC je opísať bezpečnostné služby vrstvy MAC pre komunikáciu medzi CMTS a káblovým modemom DOCSIS. Bezpečnostné ciele BPI/SEC sú [29]:

- poskytnúť používateľom káblových modemov súkromie údajov v káblovej sieti,
- poskytnúť prevádzkovateľom káblových služieb ochranu služieb (t. j. zabrániť neoprávneným modemom a používateľom získať prístup k službám RF MAC siete).

BPI/SEC má zabrániť vzájomnému odpočúvaniu používateľov káblových modemov. Robí to šifrovaním dátových tokov medzi CMTS a káblovým modemom. BPI a BPI+ používajú 56-bitové šifrovanie DES (Data Encryption Standard), zatiaľ čo SEC pridáva podporu 128-bitového AES (Advanced Encryption Standard). Kľúč AES je však chránený iba 1024-bitovým kľúčom RSA (Rivest–Shamir–Adleman). BPI/SEC má umožniť prevádzkovateľom káblových služieb odmietnuť službu necertifikovaným káblovým modemom a neautorizovaným používateľom. BPI+ posilnil ochranu služieb pridaním overovania založeného na digitálnych certifikátoch do svojho protokolu na výmenu kľúčov pomocou PKI (Public Key Infrastructure), založenej na digitálnych CA (Certificate Authority) certifikačných testerov.

Prevádzkovateľ káblových služieb zvyčajne manuálne pridá adresu MAC káblového modemu do účtu zákazníka u prevádzkovateľa káblových služieb a sieť umožní prístup len káblovému modemu, ktorý môže potvrdiť túto adresu MAC pomocou platného certifikátu vydaného prostredníctvom PKI. Bezpečnosť v sieti DOCSIS sa výrazne zlepšila, keď je povolená len komunikácia kritická pre podnik a komunikácia koncového používateľa so sieťovou infraštruktúrou je zamietnutá. Úspešné útoky sa často vyskytujú, keď je CMTS nakonfigurovaný na spätnú kompatibilitu s prvými modemami pred štandardom DOCSIS 1.1. Tieto modemy boli softvérovo aktualizovateľné v teréne, ale neobsahovali platné koreňové certifikáty DOCSIS alebo EuroDOCSIS [29].

4.4 Cable Modem Termination System (CMTS)

CMTS sa väčšinou nachádza v hlavnej stanici prevádzkovateľa CATV. Existuje viacero typov zariadení CMTS, ktoré disponujú jedným downstreamovým výstupom a jedným upstreamovým vstupom, ktoré sú určené pre pripojenie stoviek modemov. Existujú aj väčšie modulárne CMTS, ktoré sú určené pre pripojenie až desiatok tisíc modemov. Tieto väčšie CMTS možno osadiť rôznymi modulmi a sú navrhnuté tak, aby zvládli redundantné fungovanie v prípade poruchy niektorého z modulov. Hlavnou úlohou CMTS je modulácia signálu zo vstupného rozhrania (Ethernet) na výstupné (downstream) rozhranie reprezentované koaxiálnym výstupom. Upstream je opačný proces, pri ktorom dochádza k demodulácii signálu z koaxiálneho rozhrania a signál je ďalej odosielaný na Ethernet rozhranie.

Pre upstream a downstream je dôležité oddelene nastaviť útlmové pomery, keďže oba smerové signály využívajú rôzne frekvenčné pásma. Tieto signály sa následne zlučujú v zlučovači, kde sa spojený signál ďalej kombinuje s TV signálom (TV signál obyčajne zahŕňa 4 anténne vstupy pripojené do zlučovača, prijímané signály sú rôznych napäťových úrovní, preto sa zosilňujú v predzosilňovači). Tento kombinovaný

signál sa potom distribuuje prostredníctvom rozbočovača pre viacerých užívateľov. U užívateľa sa používa ďalší rozbočovač pre rozdelenie TV a internetového signálu.

Pre riadenie siete CMTS sa používa protokol SNMP (Simple Network Management Protocol) na správu siete [29]. Tento protokol prináša množstvo informácií o celkovej sieti. Každý modem má svoju unikátnu MAC adresu, podľa ktorej sú vedené údaje v CMTS a ak sa do siete pripojí modem, ktorý nie je registrovaný v CMTS, nemôže tento modem v sieti komunikovať. K nastaveniam CMTS sa dá pristupovať dvoma spôsobmi a to buď cez USB port pre pripojenie do konzoly a konfiguráciu zariadenia priamo v konzole, alebo druhým spôsobom, použitím WEB UI, graficky spracovaného rozhrania, ktoré umožňuje sledovať grafické zaťaženie kanálov. Pri základnej konfigurácii je dôležité dbať na typ modulácie, frekvenčné pásmo, registráciu modemov a nastavenie konfiguračného súboru pre modem.

4.4.1 DOCSIS ACCESS HUB

Teleste DAH100, známy tiež ako DOCSIS Access Hub, predstavuje mini-CMTS (Cable Modem Termination System) zariadenie navrhnuté na rozšírenie vysokorýchlostných širokopásmových pripojení a vysielania televíznych programov k zákazníkom prostredníctvom existujúcich dvojsmerných koaxiálnych sietí [36].

DAH100 ponúka riešenie pre širokopásmové pripojenie, ktoré je nielen nákladovo efektívne, ale aj rýchlo implementovateľné, využívajúc existujúce koaxiálne káble na doručovanie dátových, IPTV a OTT (Over The Top) služieb koncovým používateľom. Toto zariadenie je kompatibilné s DOCSIS 2.0 a 3.0 káblovými modemami a je schopné podporovať až 200 odberateľov. Typické využitie je v sieťach FTTB/C (Fiber To The Building/Curb) [36].

Na obrázku 4.5 sa nachádza DOCSIS Acces Hub 100 bez vrchného krytu a na obrázku 4.6 sa nachádza blokový diagram DAH100. Konfigurácia tohoto zariadenia je možná pomocou USB (Universal Seriál Bus) portu alebo predom nastaveným manažovatelným webovým rozhraním. DAH100 disponuje dvoma Ethernet portmi, ktoré slúžia k pripojeniu do internetu. Zariadenie obsahuje taktiež dva koaxiálne porty. Jeden je určený pre upstream a disponuje 4 kanálmi. Druhý je určený pre downstream a poskytuje až 16 kanálov [36]. Tabuľka 4.3 obsahuje základné špecifikácie DAH100.

Kľúčové funkcie a parametre

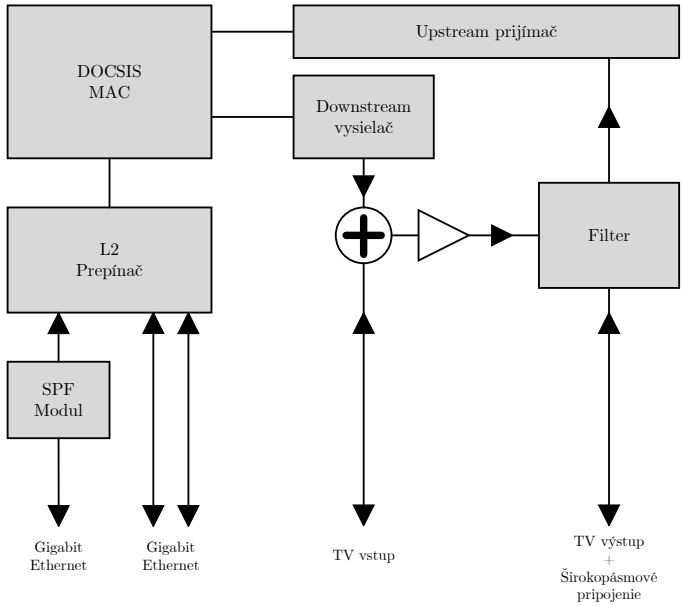
- **Integrovaný DHCP server**: DAH100 funguje ako samostatné zariadenie, ktoré nevyžaduje externý PC server na konfiguráciu káblových modemov. Táto funkcia zjednodušuje implementáciu a správu zariadenia.

- **Vysoká kapacita a modulácia**: Zariadenie podporuje 16 downstream a 4 upstream kanály s podporovanými downstream moduláciami 64, 256 a 1024QAM a upstream moduláciami QPSK a 16, 64 a 256QAM. To umožňuje kapacitu až 960 Mbit/s downstream a 160 Mbit/s upstream, čo zabezpečuje vysokorýchlostné pripojenie pre koncových používateľov.
- **Robustná a integrovaná konštrukcia**: DAH100 môže byť inštalovaný vonku v pouličných skriniach alebo vnútri budov, ako sú bytové domy. Jeho robustná konštrukcia spĺňa klasifikáciu IP54, čo znamená, že je vhodný aj pre náročné podmienky.
- **Úspora nákladov a rýchla implementácia**: Vďaka využitiu existujúcej koaxiálnej infraštruktúry umožňuje DAH100 poskytovateľom služieb rýchlo, a s výrazne nižšími nákladmi, rozšíriť širokopásmové služby. [36].

Obr. 4.5: DOCSIS Access Hub 100 [37]

Parameter	**Špecifikácia**
Downstream kanály	16 kanálov
Upstream kanály	4 kanály
Podporované downstream modulácie	QAM64, QAM256, QAM1024
Podporované upstream modulácie	QPSK, QAM16, QAM64, QAM256
Downstream kapacita	960 Mbit/s
Upstream kapacita	160 Mbit/s
Vzdialená konfigurácia	Podporovaná
Manažment	CLI cez SSH/Telnet, WEBUI HTTP
Downstream frekvenčný rozsah	54/85–1006 MHz
Zisk	42 dB
Výstupná frekvencia	108–1006 MHz
Výstupná úroveň	95–117 dBµV na kanál
Vstupná frekvencia	5–42 / 65 MHz
Nominálna vstupná úroveň	57–87 dBµV @ 5.12 Mbaud
Symbolová rýchlosť	1,28, 2,56, 5,12 Mbaud / kanál

Tab. 4.3: Kľúčové špecifikácie DAH100 [38]



Obr. 4.6: Blokový diagram DOCSIS Access Hub [39]

4.5 Cable Modem (CM)

Káblový modem je zariadenie, ktoré sa primárne stará o demoduláciu analógového signálu na digitálny a o moduláciu digitálneho signálu na analógový. Pracuje hlavne na prvej a druhej vrstve OSI modelu. Modem sa obvykle používa ako externé zariadenie, avšak existuje aj možnosť mať modem v podobe PCI karty. Smerom k počítaču sa využíva rozhranie Ethernet a smerom k CMTS koaxiálne rozhranie. Na konfiguráciu zariadenia je možné použiť USB rozhranie alebo Ethernet rozhranie.

4.5.1 Cisco Modem EPC3925

Domáca brána Cisco model DPC3925 predstavuje pokročilé riešenie pre používateľov hľadajúcich kombináciu vysoko rýchlostného internetového a kvalitného digitálneho telefónneho pripojenia. Kompatibilná s normami DOCSIS 3.0 a EuroPacketCable. Toto zariadenie poskytuje robustné širokopásmové pripojenie a podporuje súčasný prístup k dátovým a hlasovým službám bez potreby zásahu do domácej infraštruktúry [40].

Na obrázku 4.7 sa nachádza káblový modem Cisco EPC3925. Káblový modem disponuje integrovaným digitálnym hlasovým adaptérom a štyrmi ethernetovými portami 1000/100/10BASE-T pre pripojenie k lokálnej sieti. Ponúka aj bezdrôtové pripojenie vďaka štandardu 802.11n, čo umožňuje flexibilitu umiestnenia bez nutnosti káblovej inštalácie. Okrem toho modem zahŕňa funkcie WPS pre jednoduché a bezpečné nastavenie bezdrôtovej siete a pokročilé bezpečnostné prvky ako firewall, ktorý identifikuje a chráni domácu sieť pred neoprávneným prístupom [40].

Obr. 4.7: Cisco Modem EPC3925 [40]

4.6 Inicializácia a vzájomná závislosť systémov

V momente keď sa káblový modem prvý krát pripojí ku CMTS, tak medzi ním a jeho CMTS prebehne 8 krokov inicializácie. Modem nevie o prítomnosti iných modemov, vie len o CMTS ku ktorej je pripojený. Postupnosť inicializácie káblového modemu je nasledovná [41]:

- **Synchronizácia downstreamu**
  Káblový modem začne skenovať 6 MHz downstream video kanál pre signál CMTS. Ak bol modem už použitý tak sa po dočasnom zlyhaní (napríklad vypnutí) jednoducho reštartuje. Modem sa najprv pokúsi zablokovať signál CMTS na poslednom použitom downstreamovom kanáli. Pokračuje v skenovaní, kým nenájde signál, ktorý dokáže správne rozpoznať a synchronizovať.
- **Získanie upstream parametrov**
  CMTS pravidelne prenáša správy UCD (Upstream Channel Descriptors) na všetkých downstreamových kanáloch. UCD popisujú správne parametre, ktoré musí modem použiť na prenos na rôznych upstream kanáloch. Keď modem prijme UCD s parametrami pre kanál, ktorý môže použiť, uloží tieto informácie a použije ich na určenie vysielacích parametrov pre budúce upstream prenosy. Rovnako ako UCD, CMTS pravidelne vysiela správy SYNC. Tieto správy umožňujú modemu správnu synchronizáciu s CMTS a ostatnými modemami v sieti. Na obrázku 4.8 je skrátený výpis UCD správy.
  Popis základných parametrov
  - **MAC LEN (DÍžka MAC rámca)**: Udáva veľkosť správy v hexadecimálnom formáte.
  - **Upstream Channel ID (ID upstream kanálu)**: Identifikuje konkrétny upstream kanál.
  - **Config. Change Count (Počet zmien konfigurácie)**: Indikuje, koľkokrát bola konfigurácia zmenená.
  - **Mini-Slot Size (Veľkosť mini-slotu)**: Používa sa na časovanie prenosov.
  - **Downstream Channel ID (ID downstream kanálu)**: Identifikuje konkrétny downstream kanál.
  - **Symbol Rate (Symbolová rýchlosť)**: Počet symbolov prenesených za sekundu.
  - **Upstream Frequency (Upstream frekvencia**): Frekvencia upstream kanálu v hertzoch.
  - **Preamble Pattern (Vzor preambuly)**: Používa sa na synchronizáciu prenosov.
  - **Burst Descriptor (Typ burstu)**: Definuje konfiguráciu burstu pre pre-

nosové okno.

- **Modulation Type (Modulácia)**: Určuje typ modulácie pre prenos (napr. QPSK, 16QAM).
- **Scrambler**: Indikuje, či je scrambler zapnutý.

```
Downstream MAC type = UCD
MAC FC (HEX) = C2
MAC LEN (HEX) = 016A
Upstream Channel ID (HEX) = 01
Config. Change Count = 3
Mini-Slot Size = 64
Downstream Channel ID (HEX) = 0B
Symbol Rate = 160000 symbols/sec
Upstream Frequency = 26750000 Hz
Preamble Pattern = CC CC CC CC CC CC 0D 0D
Burst Descriptor = Request
IUC = 1
Modulation Type = 16QAM
Scrambler = ON
Burst Descriptor = Initial Maintenance
IUC = 3
Modulation Type = QPSK
Preamble Pattern = CC CC CC CC CC CC 0D 0D
Burst Descriptor = Station Maintenance
IUC = 4
Modulation Type = QPSK
Preamble Pattern = CC CC CC CC CC CC 0D 0D
Burst Descriptor = Short Data Grant
IUC = 5
Modulation Type = 16QAM
Preamble Pattern = F3 F3 F3 F3 33 F7
Burst Descriptor = Long Data Grant
IUC = 6
Modulation Type = 16QAM
Preamble Pattern = F3 F3 F3 F3 F3 33 F7
```

Obr. 4.8: Zjednodušený výpis správy UDC [42]

- **Synchronizácia a riadenie časovania v DOCSIS sieťach**
  V rámci káblových sietí DOCSIS, CM a CMTS musia efektívne spolupracovať, aby bola zabezpečená správna komunikácia a distribúcia dát. Každý modem si musí udržiavať synchronizáciu nielen s hodinami CMTS, ale aj s prenosovým oneskorením, aby sa predišlo prekrývaniu dátových prenosov. CMTS pridelením časových intervalov, tzv. minislotov, riadi, kedy môže ktorý modem vysielať, čím znižuje možnosť kolízie dát na linke. Konfliktné a nekonfliktné minisloty umožňujú efektívne riadenie prenosov podľa aktuálnej sieťovej záťaže. Periodické merania a úpravy prevádzkových parametrov, ako sú vysielací výkon alebo frekvencia, zabezpečujú, že všetky modemy na linke zostanú správne zarovnané a efektívne fungujúce.
- **Vytvorenie IP pripojenia**
  V momente keď sú parametre prenosu správne nastavené, CM by mal byť schopný správne komunikovať s CMTS. Teraz sa odošle požiadavka na „objavenie“ protokolu DHCP. Ako odpoveď DHCP server poskytne modemu pridelenú

IP adresu, ako aj adresu iného DHCP servera, ktorý môže poskytnúť modemu viac parametrov. Počiatočná odpoveď DHCP obsahuje aj názov súboru, ktorý obsahuje ďalšie konfiguračné parametre špecifické pre sieť pre CM.

- **Synchronizácia času dňa**
  CM a CMTS musia zdieľať spoločnú predstavu o približnom čase dňa, ktorý možno použiť na zaznamenávanie abnormálnych udalostí.
- **Prenos prevádzkových parametrov**
  CM stiahne konfiguračný súbor, ktorého názov poskytol pôvodný server DHCP. Toto sťahovanie používa protokol TFTP (Trivial File Transfer Protocol). Tento jednoduchý protokol je používaný na prenos súborov medzi klientom a serverom v sieti. TFTP je jednoduchší a má menej funkcií než protokol FTP (File Transfer Protocol). Prevádzkové parametre prepisujú všetky predvolené hodnoty nakonfigurované v modeme počas výroby. V konfiguračnom súbore môže byť prítomný veľký počet parametrov, ako sú frekvencie a prenosové rýchlosti kanálov upstream a downstream, ako aj adresy rôznych sieťových serverov, hodnoty časovačov atď.
- **Registrácia**
  Keď modem získa a spracuje konfiguračný súbor, informuje svoj CMTS o hodnotách svojich prevádzkových parametrov v správe so žiadosťou o registráciu.
- **Inicializácia Baseline Privacy Plus**
  Je to jedna z dôležitých požiadaviek na káblovú prístupovú sieť, pretože existuje aspoň teoretická možnosť, že sused môže odpočúvať komunikáciu medzi CM a CMTS. Aby sa vytvorilo bezpečnostné priradenie, modem teraz inicializuje svoju konfiguráciu Baseline Privacy Plus (BPI+), ktorá efektívne zabezpečuje spojenie pred náhodnými odpočúvaním. Po správnej inicializácii BPI+ je modem súčasťou siete.

5 Príprava laboratórnych úloh

Táto kapitola sa zameriava na tvorbu konceptu laboratórnych úloh pre predmet Služby telekomunikačných sietí. Primárnym cieľom úloh je rozvinúť výuku v oblasti telekomunikačných sietí a poskytnúť študentom praktické skúsenosti s telekomunikačnými sieťami. Na vytvorenie konceptu laboratórnych úloh boli využité poznatky z predchádzajúcich kapitol. Prvá úloha využíva IXIA XM2 ako nástroj na generovanie sieťovej prevádzky, čím poskytuje realistické prostredie na testovanie a štúdium telekomunikačných sietí. Toto zariadenie umožňuje študentom pochopiť a prakticky aplikovať teoretické koncepty v oblasti telekomunikačných sietí.

Každá laboratórna úloha bude špecificky zameraná na odlišné aspekty telekomunikačných sietí, ako sú sieťová infraštruktúra, protokoly a služby. Úlohy sa budú skladať z teoretického úvodu, ktorý študentom poskytne základné informácie s danou problematikou a kontext na pochopenie problematiky. Ďalej bude obsahom úloh podrobný postup praktických cvičení, ktoré študentom pomôžu získať praktické zručnosti a aplikovať teoretické vedomosti. Na záver každej úlohy bude aj časť venovaná samostatnej práci, ktorú dokáže študent vypracovať po dôkladnom splnení jednotlivých úloh postupu. V samostatnej práci študenti aplikujú získané vedomosti na vypracovanie, čo im poskytne priestor pre hlbšie pochopenie a kreatívny prístup k riešeniu problémov.

Po splnení samostatnej práce budú študentom položené kontrolné otázky, ktoré testujú ich porozumenie a schopnosť aplikovať teoretické koncepty v praktickej situácii. Na tieto kontrolné otázky by mal byť študent schopný odpovedať po prečítaní teoretického úvodu a dôkladnom pozorovaní pri vypracovávaní laboratórnej úlohy. Súčasťou laboratórnej úlohy bude aj zoznam odporúčanej literatúry v prípade, ak má študent záujem sa bližšie oboznámiť s danou problematikou. Na záver úlohy študenti vypracujú prehľadnú správu, v ktorej sumarizujú svoje zistenia a prednesú ju vyučujúcemu, čo im poskytne príležitosť na prezentovanie svojej práce a získanie cenných pripomienok.

Maximálny čas vypracovania každej laboratórnej úlohy by nemal presiahnuť 100 minút, aby sa zabezpečilo, že študenti majú dostatočný čas na pochopenie teoretického úvodu, dôkladné prevedenie praktických krokov a vypracovanie samostatnej práce. Predpokladaná dĺžka vypracovania laboratórnej úlohy je približne 90 minút. V tomto čase je zahrnuté úvodné predstavenie úlohy vyučujúcim a postupné riešenie jednotlivých bodov zadania. Tento čas je navrhnutý tak, aby bol študentom poskytnutý primeraný priestor pre pochopenie a aplikáciu teoretických konceptov.

5.1 Laboratórna úloha 1 - Výkonnostné parametre prepínača a QoS na linkovej vrstve.

5.1.1 Cieľ Úlohy

Cieľom úlohy je zmerať výkonnostné charakteristiky sieťového prepínača (switch) pod rôznymi záťažami a zoznámenie sa s konfiguráciou sieťového generátora IXIA XM2. Taktiež druhou časťou laboratórnej úlohy je oboznámenie sa s QoS (Quality of Service) na sieťovej vrstve pre rôzne dátové služby.

5.1.2 Potrebné Zariadenia

- IXIA XM2
- Sieťový prepínač (D-Link DES-108)
- Počítač s programami IxAutomate a IxExplorer (vzdialený prístup)

5.1.3 Pracovný postup

Táto laboratórna úloha sa skladá z dvoch častí a to z :

- Výkonnostne parametre prepínača
- Test služby QoS na linkovej vrstve

Výkonnostne parametre prepínača
V tejto časti sa študenti budú venovať záťažovým testom na prepínači D-Link DES-108 podľa dokumentácie RFC 2544 a RFC 2889 pomocou softwaru IxAutomate. Pomocou tohoto programu sa študenti pripoja pomocou vzdialeného prístupu na Chassis IXIA XM2. V tomto programe budú pomocou testov, ktoré program obsahuje testovať parametre prepínača. Medzi tieto testy patrí Throughput (Priepustnosť), Fully Meshed, Back Pressure, Broadcast Rate, Frame Error Filtering a Head of Line Blocking.

Test služby QoS na linkovej vrstve
Táto časť laboratórnej úlohy sa zaoberá testovaním kvality služieb (QoS) na druhej vrstve (linková vrstva). Pre rôzne streamy, ktoré reprezentujú rôzne dátové služby, bude nastavená rozdielna hodnota CoS (Class of Service). Tieto streamy sú generované pomocou programu IxExplorer.

Táto laboratórna úloha poskytuje študentom praktické skúsenosti s testovaním hardvéru, ako aj porozumenie dôležitých aspektov výberu a konfigurácie sieťových prepínačov. Taktiež študentom priblíži problematiku spojenú s prioritizáciou prenosu pri QoS.

5.2 Laboratórna úloha 2 - Vplyv prekladu adries (NAT) na kvalitu služieb.

5.2.1 Cieľ Úlohy

Cieľom laboratórnej úlohy je oboznámiť študentov s pojmom NAT (Network Address Translation) a jeho vplyvom na sieťovú prevádzku. Taktiež je cieľom úlohy predstavenie základnej konfigurácie sieťových zariadení (prepínačov).

5.2.2 Potrebné Zariadenia

- Počítač obsahujúci program GNS3

5.2.3 Pracovný postup

Konfigurácia NAT na jednom smerovači
V programe GNS3 študenti vykonajú zapojenie podľa predom stanovenej schémy. Toto zapojenie obsahuje jeden smerovač na ktorom študenti nakonfigurujú preklad adries (NAT). Taktiež bude potrebné nakonfigurovať zariadenia so správnou adresáciou. Následne študenti analyzujú ako sieťové zariadenie ovplyvňuje prenosovú latenciu.

Konfigurácia NAT na dvoch smerovačoch
Študenti opäť vykonajú zapojenie predom stanovenej schémy. Táto schéma obsahuje dva smerovače na ktorom študenti vykonajú základnú konfiguráciu ako je nastavenie adresácie a prekladu adries. Výsledkom zapojenia a konfigurácie je latencia, ktorú študenti zanalyzujú.

Analýza výsledkov
Získané výsledky latencie z prvého a druhého merania študenti porovnajú a zhodnotia aký vplyv má NAT a dvojitý NAT na sieťovú prevádzku.

Táto laboratórna úloha pomôže študentom pochopiť problematiku spojenú s NAT v telekomunikačných sieťach a ich vplyv na multimediálne služby. Taktiež sa študenti v tejto úlohe oboznámia so základnou konfiguráciou sieťových zariadení, ktoré taktiež zohrávajú dôležitú úlohu v multimediálnych službách.

5.3 Laboratórna úloha 3 - Analýza a konfigurácia systému DOCSIS.

5.3.1 Cieľ Úlohy

Cieľom laboratórnej úlohy je zoznámenie sa s medzinárodným štandardom DOCSIS (Data Over Cable Service Interface Specification), ktorý umožňuje vysoko rýchlostný prenos dát cez káblové televízne systémy. Taktiež je cieľom konfigurácia zariadení DAH100 (DOCSIS Acces Hub) a káblového modemu vrátane konfigurácie downstreamu a upstreamu.

5.3.2 Potrebné Zariadenia

- CMTS DAH100
- Cisco modem EPC3925
- PC (využité pre webové rozhranie na konfiguráciu DAH100 a následnom teste úspešného pripojenia na internet)
- Rozbočovač FV 9
- Koaxiálny kábel RG-6
- UTP kábel

5.3.3 Pracovný postup

Konfigurácia DAH100 a káblového modemu
V tejto časti sa študenti budú venovať základnej konfigurácií systému DOCSIS. Konkrétne nastaveniu prístrojov DAH100 a Cisco EPC3925, ktoré sprostredkovávajú prístup na internet cez koaxiálne káble.

Konfigurácia súboru káblového modemu
Táto časť laboratórnej úlohy sa zaoberá konfiguráciou súboru káblového modemu pomocou programu Excentis.

Samostatná úloha
V samostatnej úlohe študenti aplikujú získané vedomosti z predchádzajúcich úloh na konfiguráciu týchto dvoch zariadení. Študenti otestujú rôzne konfigurácie systému DOCSIS a ich vplyv na prenosové rýchlosti dátovej komunikácie.

Táto laboratórna úloha poskytuje študentom praktické skúsenosti s konfiguráciou systému DOCSIS, ako aj porozumenie dôležitých aspektov koaxiálnych spojov a modulácií.

6 Výkonnostné parametre prepínača a QoS na linkovej vrstve

6.1 Ciele a úlohy

6.1.1 Ciele

Cieľom úlohy je zmerať výkonnostné charakteristiky sieťového prepínača (switch) pod rôznymi záťažami a zoznámenie sa s konfiguráciou sieťového generátora IXIA XM2. Taktiež druhou časťou laboratórnej úlohy je oboznámenie sa s QoS (Quality of Service) na sieťovej vrstve pre rôzne dátové služby.

6.1.2 Úlohy

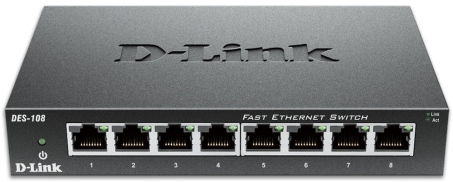
1. Za pomoci softwaru IxAutomate zmerajte základne parametre prepínača pomocou testov : Troughput, Fully meshed, Back pressure, Broadcast rate, Frame error filtering a Head of line blocking.
2. Pomocou softwaru IxExplorer nastavte rôzne hodnoty CoS (Class of Service) pre rôzne toky rámcov.

6.2 Teoretický úvod

6.2.1 Prepínače

Prepínače (switche) pracujú na druhej vrstve referenčného OSI modelu, známej ako linková vrstva. Najčastejšie sa switche vyskytujú v Ethernetových sieťach. Základnou funkciou switchu je, že na základe cieľovej MAC adresy rozhoduje, na ktorý port má byť rámec odoslaný, a na ktorý nie. Switche zodpovedajú za správu dátového toku vnútri jednej lokálnej siete (LAN). Ich hlavnou úlohou je prijímať dáta od jedného zariadenia a efektívne ich prepínať k určenému zariadeniu v rámci tej istej siete.

Tieto zariadenia disponujú logikou, ktorá im umožňuje sledovať obsah rámcov a na základe nich rozhodovať, ako s danými rámcami naloží. Prepínače sú kľúčové pre minimalizovanie kolízií v sieti a optimalizáciu dátového toku, čo umožňuje viacerým zariadeniam komunikovať súčasne bez výrazného zníženia výkonu siete. Prepínače taktiež spolupracujú s fyzikou vrstvou, čo značí, že pracuje aj s kódovaním, moduláciami a pod.. Výber, konfigurácia a správne fungovanie prepínačov sú kľúčové pre zabezpečenie vysokého výkonu, spoľahlivosti a bezpečnosti siete [1, 2].



Obr. 6.1: Prepínač D-Link DES-108 [43]

6.2.2 RFC 2544

Request for comment (RFC) 2544 je metodika benchmarkingu vytvorená v roku 1999 na testovanie a meranie výkonu sieťových zariadení. Poskytuje štandardizované výsledky výkonu, ktoré umožňujú jednoducho porovnávať zariadenia od rôznych dodávateľov. RFC obsahuje niekoľko testov, ktoré sú určené na vyhodnocovanie, ako bude zariadenie fungovať v reálnych scenároch. Tieto testy sa považujú za offline. To znamená, že skutočná sieťová prevádzka musí byť zastavená, aby tester generoval prevádzku so špecifickými charakteristikami [5, 6].

Ideálnym spôsobom implementácie týchto testov je použitie testovacej sady s vysielacími a prijímacími portami. Prevádzka sa posiela z testera do DUT (Device under test) a späť z DUT do testera. Zahrnutím sekvenčných čísel do prenášaných rámcov dokáže tester skontrolovať, či boli všetky pakety úspešne prenesené, a overiť, či boli prijaté aj správne pakety [6].

Aby sa zabezpečilo, že ethernetová sieť bude schopná podporovať rôzne služby ako napríklad VoIP, video atď., RFC 2544 podporuje sedem preddefinovaných veľkostí rámcov a to (64, 128, 256, 512, 1024, 1280 a 1518 bajtov) na simuláciu rôznych dopravných podmienkach. Malé veľkosti rámcov zvyšujú počet prenášaných rámcov, čím zaťažujú sieťové zariadenie [5, 6].

Medzi najdôležitejšie patria definície testov na meranie priepustnosti, latencie, straty rámca, odolnosti systému a testovania rôznych pracovných zaťažení. Je tiež dôležité, aby sa výsledky prezentovali porovnateľným spôsobom a aby sa týkali bežných testovacích postupov. RFC 2544 zdôrazňuje potrebu komplexného testovania a podávania správ, aby sa zabezpečilo, že výsledky benchmarkov budú presné a relevantné pre používateľov. Pojmy ako sú priepustnosť, latencia, straty rámcov/paketov a jitter sú objasnené v texte nižšie [5, 6].

6.2.3 RFC 2889

Rozširuje metodiku RFC 2544 a zameriava sa na metodiku testovania prepínačov v LAN sieťach. Toto doporučenie určuje v akom formáte majú byť reprezentované výsledky meraní. Rovnako ako doporučenie RFC 2544 taktiež podporuje sedem preddefinovaných veľkostí rámcov a to (64, 128, 256, 512, 1024, 1280 a 1518 bajtov) na simuláciu rôznych dopravných podmienok. RFC sa týka predovšetkým zariadení, ktoré prepínajú rámce na Media Access Control (MAC) vrstve. V nasledujúcom texte sú vybrané a popísané niektoré z testov. [7]

Back Pressure

Jedná sa o metódu testovania, ktorá simuluje zaťaženie sieťového zariadenia (DUT) v podmienkach preťaženia. Metóda testuje akým spôsobom zariadenie reaguje, keď prichádzajúci dátový tok presahuje jeho spracovateľskú kapacitu. Výsledkom testu môže byť napríklad spomalenie predchádzajúceho toku alebo odmietnutie nových rámcov. Test poskytuje informácie o výkonnosti a spoľahlivosti zariadenia v extrémnych podmienkach, čo je kritické pre návrh a prevádzku sieťovej infraštruktúry.

Broadcast Rate

Tento test určuje, ako rýchlo dokáže sieťové zariadenie (prepínač) spracovávať broadcastové rámce. Jedná sa o dôležitú schopnosť zariadenia efektívne distribuovať rámce, ktoré sú určené pre všetky zariadenia danej siete. Broadcast Rate dokáže pre zariadenie identifikovať výkon pri rozširovaní broadcastových správ.

Frame error Filtering

Test Frame Error Filtering je používaný v sieťových zariadeniach na identifikáciu a filtrovanie poškodených rámcov, ktoré nespĺňajú štandardné podmienky veľkosti alebo majú chyby v kontrolnom súčte (CRC). Filtrovanie týchto chybných rámcov je dôležité pre udržanie integrity dát a efektívneho fungovania siete. Filtrovanie zabraňuje šíreniu poškodených alebo neplatných dát po sieti.

Fully Meshed

Fully Meshed sa podľa RFC 2889 týka výkonnosti a spoľahlivosti prepínačov v plne prepojenej topológii. Test slúži na overenie, ako efektívne môže sieťové zariadenie spracovať sieťovú premávku medzi všetkými svojimi portmi naraz. Týmto spôsobom simuluje prostredie s vysokou mierou vzájomnej konektivity. Cieľom je identifikovať úzke miesta v spracovaní dát a overiť schopnosť zariadenia udržiavať konštantný výkon za situácií, keď sú všetky porty aktívne zapojené do prenosu.

Head of Line Blocking

V teste sú rámce smerované cez zariadenie v plnej prepojenej topológii. Test sleduje, ako zariadenie zvláda preťaženie na rozhraniach pri súčasnom prenose dát medzi viacerými portmi. Výsledkom sú informácie o schopnosti zariadenia spracovávať dátový tok a predchádzať blokovaniu, keď jeden port vysiela dáta súčasne na viacero prijímacích portov, čo simuluje reálnu sieťovú situáciu. Spracovanie jedného rámca na vstupe blokuje ďalšie rámce v rade čakajúce na spracovanie, aj keď môžu byť určené pre iné výstupné porty. Tento jav môže spôsobiť zvýšenie latencie a zníženie celkovej efektívnosti prenosu dát v sieťovom zariadení. Rámce, ktoré by inak mohli byť okamžite preposlané, musia čakať, kým sa nevyrieši blokovanie na čele radu.

6.2.4 Priepustnosť

Priepustnosť (Throughput) je hlavným ukazovateľom sieťovej kapacity a je možné ju definovať ako množstvo dát, ktoré je sieť schopná úspešne preniesť z jedného bodu do druhého v určitom časovom rozmedzí [12]. Táto metrika je meraná v bitoch za

sekundu (bit/s) a vyššie hodnoty priepustnosti signalizujú schopnosť siete prenášať viac dát. To je zásadné pre aplikácie vyžadujúce veľké prenosové rýchlosti, ako sú napríklad databázové aplikácie, prenášajúce veľké objemy dát, alebo pre streamovacie služby, kde kontinuálny a rýchly prenos videa zaisťuje plynulý zážitok bez zasekávania. Výpočet priepustnosti definuje nasledujúci vzťah :

$$Priepustnosť = \frac{FramesPerSecond(fps) * FrameSize(bytes) * 8}{1000000} \tag{6.1}$$

6.2.5 Latencia

Latencia sa v sieti vzťahuje na časové zdržanie pri ceste dátového paketu z jedného sieťového uzlu do druhého. Obvykle sa meria ako oneskorenie spiatočnej cesty a ideálne by mala byť čo najbližšie k nule, pre dosiahnutie lepších výsledkov. Táto metrika je zvyčajne meraná v milisekundách (ms) a je dôležitá pre aplikácie, kde je dôležitá rýchla odozva, ako sú napríklad hlasové služby alebo online hry. Latencia je ovplyvnená mnohými faktormi vrátane fyzických vzdialeností medzi komunikujúcimi zariadeniami, kvality sieťového hardvéru, a softvéru a aktuálneho preťaženia siete [14].

6.2.6 QoS (Quality of Service)

Kvalita služby (QoS) je v prepínačoch dôležitý aspekt správy sieťovej prevádzky. V prostredí, kde rôzne služby a aplikácie, ako sú napríklad VoIP (hlas cez IP), streamovanie videa a rozvíjajúci sa internet vecí (IoT), zdieľajú rovnakú sieťovú infraštruktúru, je QoS nevyhnutná na zabezpečenie spoľahlivého a vysokokvalitného prenosu dát. Prepínače používajú QoS na rozlišovanie medzi rôznymi typmi prevádzky a priradenie vyššej priority citlivým aplikáciám, ktoré vyžadujú konzistentné časové charakteristiky pre nízku latenciu a minimálny jitter. Napríklad, hlasové a video aplikácie často používajú UDP protokol, ktorý na rozdiel od TCP nezabezpečuje opätovné posielanie stratených paketov, a preto je závislý na QoS mechanizmoch implementovaných v prepínači, aby sa zabezpečila plynulosť dát a aby sa predišlo stratám [4].

V situáciách, keď dôjde k preťaženiu siete, prepínače využívajú politiky QoS na zabezpečenie toho, aby dôležité služby ako hlasové hovory majú prednosť a sú chránené pred stratou a oneskorením, zatiaľ čo menej dôležitá sieťová prevádzka môže byť oddialená alebo zahodená. Tým sa znižuje riziko vplyvu jitteru na citlivé aplikácie. S QoS môžu byť prepínače konfigurované tak, aby efektívne rozdeľovali dostupné zdroje podľa priority a dôležitosti jednotlivých typov prevádzky.

6.2.7 Sieťový generátor IXIA XM2

Systém IXIA je jeden z najkomplexnejších nástrojov na testovanie viacvrstvového 10/100 Mbit/s Ethernetu, Ethernet Gigabitu, 10 Gigabit Ethernetu, ATM a Packet over SONET prepínača, smerovača a siete. Testovací systém IXIA poskytuje komplexné riešenia v oblasti testovania výkonu, funkcionality a súlad sietí a sieťových aplikácií. Ide o testovaciu platformu, ktorá slúži na testovanie širokého spektra služieb ISO/OSI modelu od siedmej vrstvy až po druhú. Najväčšie zameranie generátora IXIA je na druhú a tretiu vrstvu modelu ISO/OSI. Poskytuje široké množstvo záťažových modulov a testovacích aplikácií. Taktiež prináša flexibilitu pri vykonávaní celého radu testovania sietí, zariadení, údajov, signalizácie, hlasu, videa, aplikácií a zabezpečenia [25, 26, 27]. Na obrázku 6.2 sa nachádza IXIA XM2, ktorá je použitá v laboratórnej úlohe.

Obr. 6.2: Sieťový generátor IXIA XM2 [26]

IxExplorer

Jedná sa o program, ktorý slúži na programovanie hardwaru Ixia generátora a následným testovaním sietí a zariadení. IxExplorer je sofistikovaný nástroj, ktorý poskytujeSTore grafické užívateľské rozhranie pre nastavovanie a spúšťanie sieťových testov na rôznych vrstvách OSI modelu, od fyzickej až po transportnú vrstvu. Každá vrstva má nezávislý generátor, ktorý zvlášť generuje a analyzuje sieťovú prevádzku bez ovplyvnenia iných vrstiev. S týmto nástrojom je možné generovať až 255 rozličných prevádzkových tokov, pričom na jednom rozhraní generuje prevádzku a na druhom vykonáva analýzu.

Program poskytuje detailné konfigurácie paketových a rámcových hlavičiek, s možnosťou nastavenia pre ToS/QoS. IxExplorer dokáže generovať až 255 unikátnych tokov paketov s rôznymi prenosovými rýchlosťami. Pre jednotlivé streamy je možné nastavovať veľkosti rámcov a ich vzor. Podrobnosti o vrstvách 2 a 3, vrátane

VLAN a rôzne protokoly (IPv4, IPv6, ARP...). Ďalej simulácie chyb ako napríklad CRC (Cyclic redundancy check) chyby. Nastavenie streamov taktiež poskytuje nastavenie typu prevádzky (nepretržitý, jednorazový ...), počet opakovaní streamov a iné.

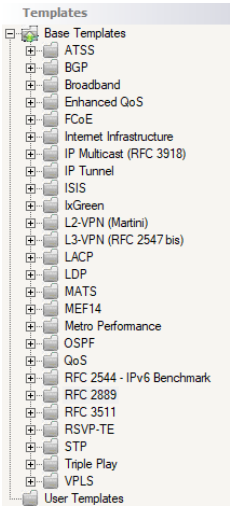
Po ukončení analýzy je možné pristupovať a prehliadať štatistiky meraní. Štatistiky je možné prehliadať individuálne pre každý port alebo skupinovo všetky toky paketov. Tieto štatistiky obsahujú informácie ako počet odoslaných/ prijatých rámcov alebo bytov a stratovosť. V štatistikách je možné aplikovať filtre pre ToS/QoS, veľkosť paketu, IP/MAC zdrojové a cieľové adresy [25].

IxAutomate

IxAutomate je program s grafickým užívateľským rozhraním na automatizované testovanie sieťových zariadení a sietí, ktorý obsahuje preddefinované testy podľa štandardov RFC. Tieto testy, ako napríklad RFC 2544 pre benchmarking IPv6 alebo RFC 2889 na prepínacie testy druhej vrstvy, umožňujú zistiť rýchlosť konvergencie protokolov, maximálny počet ciest pre každý protokol a ďalšie výkonnostné metriky. Napriek tomu, že pre každý test RFC je potrebná samostatná licencia, výhodou je rýchle a jednoduché testovanie bez potreby detailného nastavovania parametrov.

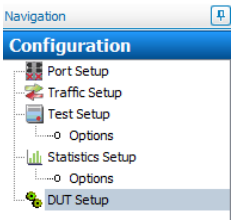
IxAutomate poskytuje jednoduché grafické rozhranie na konfiguráciu vlastných automatizovaných testovacích scenárov a analýzu výsledkov testov. Využívaním možností hardvéru Ixia, ako sú generovanie premávky na maximálnej rýchlosti, filtrovanie, zachytávanie a zbieranie štatistík, IxAutomate ponúka bohatý súbor predpripravených testov založených na štandardoch RFC a požiadavkách zákazníkov. Výsledky testov sú zbierané a prezentované s flexibilným súborom funkcií, vrátane grafík v reálnom čase zobrazujúcich priebeh testovania, formátovaných správ pre detailnú analýzu po testovaní, farebných indikátorov úspechu alebo zlyhania testov a podrobných záznamov o vykonávaní testov. Ako testovacie prostredie IxAutomate ponúka architektúru zásuvných modulov navrhnutú na ľahké pridávanie vlastných testov do už rozsiahlej knižnice testov.

Rozhranie IxAutomate je prezentované v hierarchickom strome, čo umožňuje jednoduchú navigáciu medzi rôznymi testami ako je možné vidieť na obrázku 6.3. Všetky testy sú ale licencované a jednotlivé licencie je potrebné zakúpiť. K dispozícii sú dva testy a to RFC 2544 a RFC 2889. Šablóny je možné jednoducho prechádzať, pričom ich diagram a popis umožňujú používateľom ľahký výber testov. Po výbere sa testovacie šablóny skopírujú do používateľského testovacieho priestoru, kde sú následne nakonfigurované, prispôsobené a spustené [28].



Obr. 6.3: Hierarchický strom testov

Test Configuration je podporovaná štandardná štruktúra Aptixia s postupnou konfiguráciou pre všetky testy. Túto štruktúru je možné vidieť na obrázku 6.4.



Obr. 6.4: Konfigurácie pre jednotlivé testy

Jednotlivý popis častí konfigurácií pre testy:

1. **Port Setup** menu umožňuje zobrazenie a konfiguráciu všetkých testovacích portov dostupných na testovanie. Tu sa konfigurujú vlastnosti fyzickej vrstvy.
2. **Traffic Setup** menu obsahuje informácie pre špecifikáciu premávky, ktorá sa má odoslať počas testu, vrátane parametrov, ako sú veľkosti rámca, mapovanie prevádzky medzi portami, adresovanie a obsahu.
3. **Test Setup** ponuka obsahuje informácie týkajúce sa trvania testu, počtu pokusov, iterácií a ďalších informácii špecifických pre vybraný test.
4. **Statistics Setup** sa používa na definovanie štatistík, ktoré budú graficky zobrazené programom StatViewer a konfigurácia SNMP pre monitorovanie DUT.
5. **DUT Setup** umožňuje používateľom zadávať príkazové súbory na konfiguráciu/monitorovanie zariadenia

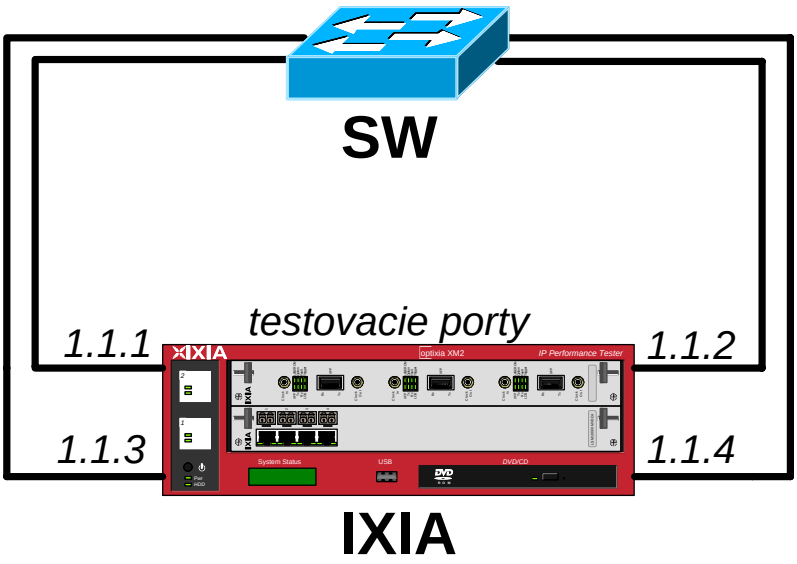
6.3 Pracovný postup

6.3.1 Vybavenie pracoviska

- IXIA-XM2
- Sieťový prepínač (D-Link DES-108)
- Počítač s programami IxAutomate a IxExplorer (vzdialený prístup)

6.3.2 Schéma zapojenia

Zapojené sú všetky metalické rozhrania analyzátoru (4 porty) do štyroch portov testovaného prepínača. Porty 1 až 4 na chassis sú označené ako 1.1.1 až 1.1.4. Na chassis IXIA XM2 sa pripája pomocou vzdialeného prístupu na počítači v laboratóriu. Tento počítač obsahuje nainštalované programy IxAutomate a IxNetwork. Zapojenie sieťového analyzátora s testovaným prepínačom je možné vidieť na obr. 6.5.



Obr. 6.5: Schéma zapojenia analyzátora s testovaným prepínačom [44]

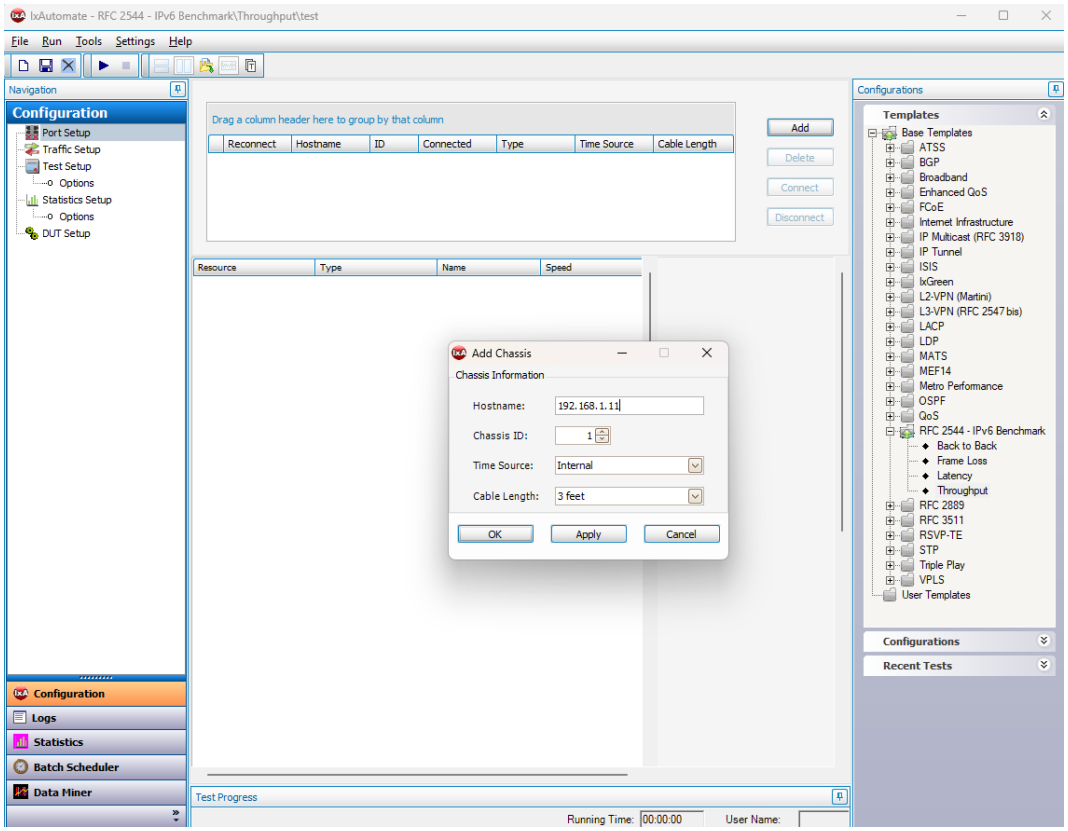
6.3.3 Výkonnostné parametre prepínača

Táto časť sa venuje záťažovým testom na prepínači D-Link DES-108 podľa dokumentácie RFC 2544 a RFC 2889 pomocou softwaru IxAutomate. Štyri porty testovaného prepínača sú pripojené na sieťový generátor/analyzátor podľa obr. 6.5.

Pred spustením samotných programov je potrebné skontrolovať pripojenie na virtuálnu privátnu sieť (VPN). Táto VPN slúži ako bezpečnostný most, ktorý umožňuje komunikáciu so chassis, ktorá je integrovaná do siete. Absencia takéhoto VPN tunelu by viedla k obmedzeniu prístupu k chassis a k ďalším sieťovým zdrojom, ktoré sú cez VPN dostupné. Prejdite do **Windows-> Nastavenia-> Sieť a internet -> VPN.** Pripojte sa na VPN s názvom **IXIA-XM2**. Ak je pripojenie na VPN úspešné môžete pokračovať v návode.

Throughput (Priepustnosť)

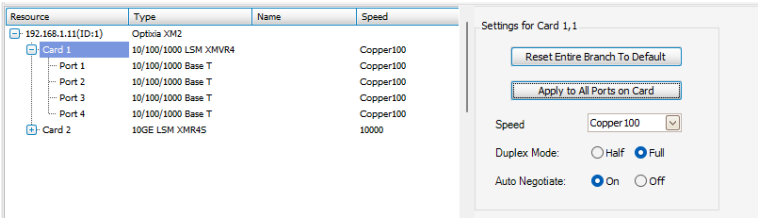
Spustite program IxAutomate, ktorý sa nachádza na ploche PC. V hlavnom okne programu v záložke **Configurations->Templates-RFC 2544** kliknite pravým tlačidlom myši na **Throughput** a zvoľte **New Test**. Názov testu pomenujte podľa svojho ID. Pri každom teste je potrebné vložiť danú Chassis pomocou ktorej budú vykonávané testy. Kliknite na **Add** a do políčka **Hostname** vložte IP adresu zariadenia na, ktoré sa pripojíte (v tomto prípade 192.168.1.11). Dĺžku káblov ponechajte pretože táto hodnota približne zodpovedá skutočnej dĺžke káblov. Ostatné parametre ponechajte a klikneme **Apply** a **OK** ako je na obrázku 6.6.



Obr. 6.6: Pridanie Chassis

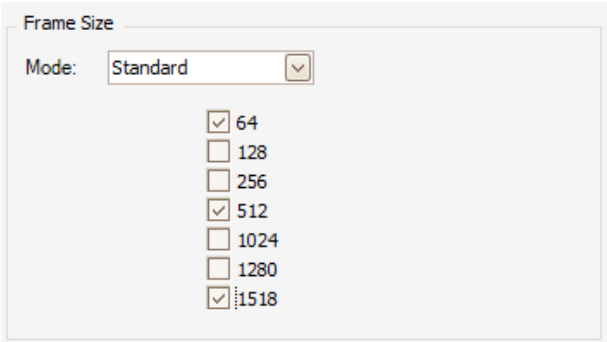
Dôležité je nastaviť ešte položku Speed. Kliknite na **Card 1** a v **Settings for Card 1,1** nastavte **Speed** na **Copper 100**. Následne kliknite na **Apply to All Ports on Card**. Tento krok je dôležitý z dôvodu, že je testovaný switch so 100 Mbit/s portmi. Správne nastavenie je zobrazené na obrázku 6.7.

V prípade, že nebude nastavená hodnota **Speed** na **Copper 100,** program bude automaticky vykonávať testy pre **Copper 1000.** To môže mať za následok zlyhanie testu (test nebude vykonaný) a možnú potrebu reštartovania Chassis serveru. V prípade, že nastane tento problém kontaktujte vyučujúceho.

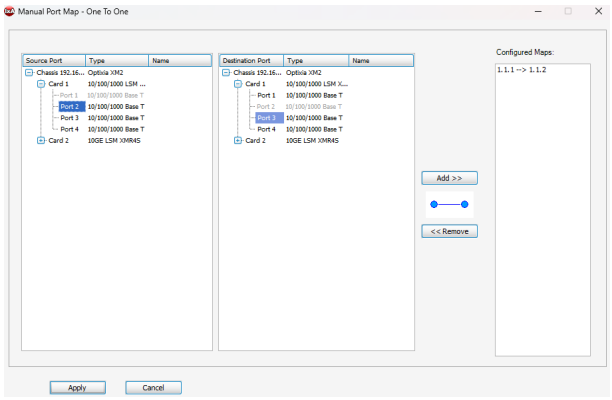


Obr. 6.7: Nastavenie rýchlosti pre jednotlivé porty chassis

Presuňte sa do **Configuration->Traffic Setup** a v časti **Frame Size** zvoľte veľkosť rámcov 64, 512 a 1518 bajtov (obrázok 6.8). Tieto hodnoty sú volené z toho dôvodu, že pre test stačí zmerať hodnoty pre maximálnu, strednú a minimálnu veľkosť rámcov, ktoré sú pre test k dispozícii. Pri týchto hodnotách je dostatočne vidieť závislosť priepustnosti na veľkosti rámcov. Rovnaké veľkosti rámcov sú volené aj v iných testoch. V časti **Traffic Map** zvoľte **Mode->Manual-> Configure.** Tu zvoľte **Port 1** v **Card 1** (Source Port) a **Port 2** v **Card 1** (Destination Port). Zvoľte **Add** a následne **Apply** ako je možné vidieť na obrázku 6.9. Následne sa presuňte do **Configuration->Test Setup** a nastavte **Duration** na 10 sekúnd.



Obr. 6.8: Výber veľkosti rámcov



Obr. 6.9: Nastavenie smeru tokov pre test Throughput

Test spustite trojuholníkom, ktorý sa nachádza v hornej ľavej časti okna (obrázok 6.10) alebo klávesovým tlačidlom F5. Výsledky sa zobrazujú v Záložke **Logs** ako je vidieť na obrázku 6.11. Test skončí výpisom **Test Complete**.

Obr. 6.10: Spustenie testu v IxAutomate

Ako môžete z testu vidieť pri veľkosti rámca 1518 B je hodnota **Agg Tput** 98.7 Mbit/s. Táto hodnota značí priepustnosť, ktorá je blízka hodnote 100 Mbit/s, čo naznačuje, že je výsledok testu v poriadku. Táto hodnota je veľmi blízka teoretickému maximu prepínača. Taktiež môžete vidieť, že nebol zaznamenaný žiaden stratený rámec (Frame Loss), čo značí 100% úspešnosť prenosu. Do tabuľky 6.1 poznamenajte namerané hodnoty priepustnosti. Test následne vykonajte aj pre opačný smer (Source Port - Port2), (Destination Port – Port 1) a výsledky poznamenajte do tabuľky 6.1

Tab. 6.1: Výsledky priepustnosti pre test Throughput

Veľkosť rámca [B]	**Priepustnosť [Mb/s] Smer testu 1.1.1 → 1.1.2**	**Priepustnosť [Mb/s] Smer testu 1.1.2 → 1.1.1**
64		
512		
1518		

```
======> FRAME SIZE 1518 STARTED Sat Apr 06 16:03:58
---> BINARY ITERATION 1, trial: 1, framesize: 1518, RFC 2544 Throughput Test - Per Port Binary Search
Configuring 1.1.1 -> 1.1.2
Transmitting frames for 10 seconds
Done after 10 seconds.

Waiting for Residual frames to settle down for 2 seconds
Waited for 1 of 2 seconds
Waited for 2 of 2 seconds
Collecting transmit statistics ...
1.1.1: Total frames transmitted: 81270
Collecting receive statistics ...
1.1.2: Total frames received: 81270

Iteration Metrics
******************
Trial: 1 Frame Size: 1518 Iteration: 1

Tx Port     Rx Port     Tx Count (frames)     Tput (fps)  Tput (% Line Rate)     Rx Count (frames)     Rx Rate (bps)          Frame Loss (frames)     Frame Loss (% Line rate)
*****************************************************************************************************************************************************************************
1.1.1       1.1.2       81270                 8127.440    100.000                81270 9               8695.631               0                       0.000

Result Metrics
***************
Trial: 1 Frame Size: 1518
******************
Tx Port     Rx Port     No Drop Rate (% Line Rate)          Throughput (fps)       Tx Rate (bps)          Rx Rate (bps)
*************************************************************************************************************************
1.1.1       1.1.2 1     00.000                              8127.440               98695.631              98695.631

Aggregate Metrics
*****************
Trial: 1 Frame Size: 1518

Agg Tput (fps)          Max Tput (fps)          Agg Tput (Mbps)       Max Tx Rate(bps)       Agg Rx Rate(bps)       Max Rx Tput(bps)       Agg Tput (% Line rate)
*************************************************************************************************************************************************************************
8127.440                8127.440                98.700                98695.631              98695.631              98695.631              100.000
======> FRAME SIZE 1518 COMPLETED Sat Apr 06 16:04:19
```

Obr. 6.11: Výsledok testu Throughput

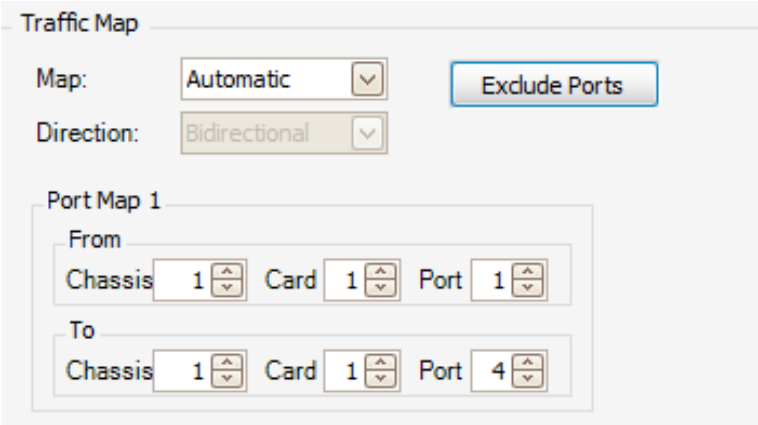
Priepustnosť v sieťových testoch závisí na veľkosti rámca, pretože spracovávanie hlavičiek zaberá čas bez ohľadu na to aké veľké sú dáta v rámci. Pri veľkosti rámca 64 B musia sieťové zariadenia spracovať väčší počet rámcov za sekundu aby dosiahli rovnaké množstvo prenesených dát. Nakoľko každý rámec musí byť spracovaný samostatne, viac času sa strávi spracovaním hlavičiek a menej času reálnymi dátami, čo znižuje efektivitu.

Fully Meshed

V hlavnom okne programu v záložke **Configurations->Templates->RFC 2889** kliknite pravým tlačidlom myši na **Fully Meshed** a zvoľte **New Test**. Názov testu pomenujte podľa svojho ID. Následne klikneme na **Add** a do políčka **Hostname** vložte IP adresu zariadenia na, ktoré sa pripojíte (v našom prípade 192.168.1.11). Ostatné parametre ponecháme a klikneme **Apply** a **OK**. Kliknite na **Card 1** a v **Settings for Card 1,1** nastavte **Speed** na **Copper 100**. Následne kliknite na **Apply to All Ports on Card**.

Presuňte sa do **Configuration->Traffic Setup** a v časti **Frame Size** zvoľte všetky veľkosti rámcov. Časť **Traffic Map** nastavíme podľa obrázka 6.12. Toto nastavenie určuje, že každý z portov bude vysielať na všetky ďalšie porty.

Následne sa presuňte do **Configuration->Test Setup** a nastavte **Duration** na 10 sekúnd. Zakliknite políčko **Calculate Latency** a Latency Type zvoľte **Store And Forward**. Test následne spusťte a počkajte kým test neprebehne.



Obr. 6.12: Nastavenie smeru tokov pre test Fully Meshed

Do tabuľky 6.2 poznamenajte nemerné hodnoty priepustnosti (Agg RxTput) a latencie (Agg Avg Latency).

Tab. 6.2: Výsledky priepustnosti a latencie pre test Fully Meshed

Veľkosťrámca [B]	**Celková priepustnosť [Mb/s]**	**Priepustnosť jedného portu [Mb/s]**	**Priemerná latencia [ns]**
64			
128			
256			
512			
1024			
1280			
1518			

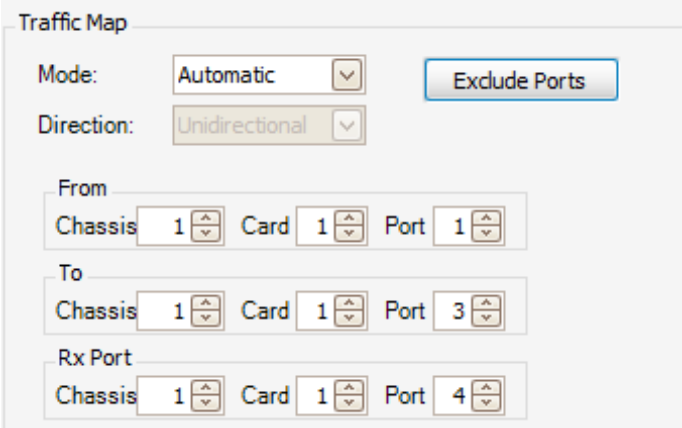
Na základe nameraných hodnôt vidieť, že sa priepustnosť približuje hodnote 100 Mbit/s, čo naznačuje, že je výsledok testu v poriadku. Táto hodnota je veľmi blízka teoretickému maximu prepínača. Taktiež môžeme vidieť, že nebol zaznamenaný žiaden stratený rámec (Frame Loss), čo značí 100% úspešnosť prenosu. Latencia má veľmi nízke hodnoty, čo značí, že zariadenie dokáže prenášať rámce s nízkym oneskorením. Je to výhodné pre výkon a rýchlosť siete.

Back Pressure

V hlavnom okne programu v záložke **Configurations->Templates->RFC 2889** kliknite pravým tlačidlom myši na **Back Pressure** a zvoľte **New Test**. Názov testu pomenujte podľa svojho ID. Následne klikneme na **Add** a do políčka **Hostname** vložte IP adresu zariadenia na, ktoré sa pripojíte (v našom prípade 192.168.1.11). Ostatné parametre ponecháme a klikneme **Apply** a **OK**.

Kliknite na **Card 1** a v **Settings for Card 1,1** nastavte Speed na Copper 100. Následne kliknite na **Apply to All Ports on Card**.

Presuňte sa do **Configuration->Traffic Setup** a v časti **Frame Size** zvoľte veľkosť rámcov 64, 512 a 1518. Časť **Traffic Map** nastavte podľa obrázka 6.13. Toto nastavenie určuje, že porty 1-3 budú vysielať na port 4.



Obr. 6.13: Nastavenie smeru tokov pre test Back Pressure

Následne sa presuňte do **Configuration->Test Setup** a nastavte **Duration** na 10 sekúnd. Test následne spustite a počkajte kým test neprebehne. Podobný výsledok testu môžete vidieť na obrázku 6.14.

Z výpisov testov pre 64, 512 a 1518 B je zrejmé, že došlo k vysokej miere strát približne 50% (Fremes Loss %). Tento výsledok naznačuje, že zariadenie má problém s riadením zápchy v sieti. Je teda možné konštatovať, že riadenie tokov prepínača nie je funkčné. Aby zariadenie mohlo efektívnejšie zvládať tento typ záťaže je dôležité, aby zariadenie malo dostatočnú výpočetnú kapacitu. Stratovosť je možné pri takomto zaťažení len minimalizovať nie odstrániť.

```
***** TRIAL 1, framesize: 1518 - RFC 2889 Congestion Control/Backpressure Test *****
Configuring 1.1.1 -> 1.1.4
Configuring 1.1.2 -> 1.1.4
Configuring 1.1.3 -> 1.1.4
Transmitting frames for 10 seconds
Done after 10 seconds.

Waiting for Residual frames to settle down for 2 seconds
Waited for 1 of 2 seconds
Waited for 2 of 2 seconds
Collecting transmit statistics ...
1.1.1: Total frames transmitted: 54180
1.1.2: Total frames transmitted: 54180
1.1.3: Total frames transmitted: 54180
Collecting receive statistics ...
1.1.4: Total frames received: 81280
Collecting collisions statistics ...
Collecting flowControlFrames statistics ...
Saving results for Framesize 1518 ...

RFC 2889 Congestion Control/Backpressure Test - MAC(Ethernet Type 08 00) --> Framesize: 1518

many2one
TX      RX      ILoad(fps)      Collisions      FlowCtrlFrames  Loss(%)
********************************************************************************
1.1.1   1.1.4   16254           0               NA              49.989
1.1.2   1.1.4   0               0               NA              49.989
1.1.3   1.1.4   0               0               NA              49.989
********************************************************************************
TotalTxFrames   = 162540
TotalRxFrames   = 81280
TotalLoss(%)    = 49.989
OLOAD           = 200
Backpressure    = NONE
```

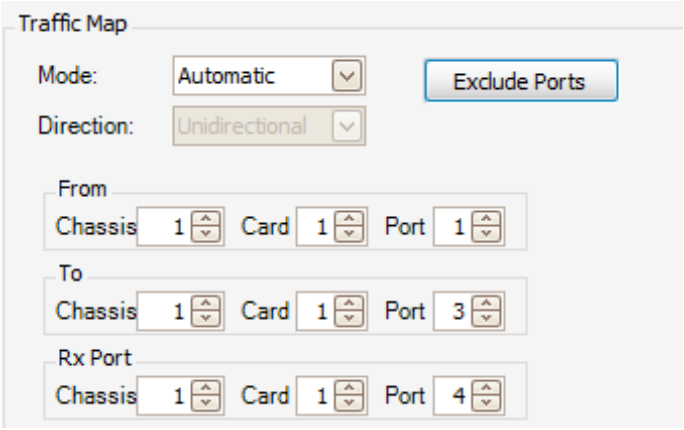
Obr. 6.14: Výsledok testu Back Pressure

Broadcast Rate

V hlavnom okne programu v záložke **Configurations->Templates->RFC 2889** kliknite pravým tlačidlom myši na **Broadcast Rate** a zvoľte **New Test**. Názov testu pomenujte podľa svojho ID. Následne klikneme na **Add** a do políčka **Hostname** vložte IP adresu zariadenia na, ktoré sa pripojíte (v našom prípade 192.168.1.11). Ostatné parametre ponecháme a klikneme **Apply** a **OK**.

Kliknite na **Card 1** a v **Settings for Card 1,1** nastavte **Speed** na **Copper 100**. Následne kliknite na **Apply to All Ports on Card**.

Presuňte sa do **Configuration->Traffic Setup** a v časti **Frame Size** zvoľte veľkosť rámcov 64, 512 a 1518. Časť **Traffic Map** nastavte podľa obrázka 6.15. Toto nastavenie určuje, že port 1 bude vysielať na pory 2-4.



Obr. 6.15: Nastavenie smeru tokov pre test Broadcast Rate

Následne sa presuňte do **Configuration->Test Setup** a nastavte **Duration** na 10 sekúnd. Test následne spustite a počkajte kým test neprebehne. Podobný výsledok testu môžete vidieť na obrázku 6.16.

```
******* TRIAL 1 - RFC 2889 Broadcast Frame Forwarding Test - Per Port Binary Search *******
Configuring 1.1.1 -> 1.1.2
Configuring 1.1.1 -> 1.1.3
Configuring 1.1.1 -> 1.1.4
Configuring RX port mode to portPacketGroup
Configuring RX port mode to acceptBroadcastPacketGroup
Checking link states on ports...
Lines on all ports are up.

----> BINARY ITERATION 1, trial 1, framesize: 64, RFC 2889 Broadcast Frame Forwarding Test - Per Port Binary Search
Transmitting frames for 10 seconds
Done transmitting for 10 seconds...

Waiting for Residual frames to settle down for 2 seconds
Waited for 1 of 2 seconds
Waited for 2 of 2 seconds
Collecting transmit statistics ...
1.1.1: Total frames transmitted: 744050
Collecting receive statistics ...
1.1.2: Total frames received : 744050
1.1.3: Total frames received : 744050
1.1.4: Total frames received : 744050

Configured Transmit Rates used for iteration 1
* Note: DUT Flow Control or Collisions may cause actual TX rate to be lower than Offered Rate
TX      RX          OLoad(fps)          MaxTxRate          AvgTxRunRate    AvgRxRunRate    Min Latency (ns)    Max Latency (ns)    Avg Latency (ns)
*************************************************************************************************************************************************************
1.1.1   1.1.2       74405               50.0000            74405           74405           8140                8660                8440
1.1.1   1.1.3       74405                                  74405           8180            8700                8476
1.1.1   1.1.4       74405                                  74405           8240            8740                8525

************************
Saving results for Trial 1 ...
************************

RFC 2889 Broadcast Frame Forwarding Test - Per Port Binary Search - MAC(Ethernet Type 08 00) --> Framesize: 64
TX      RX          TX (fps)            Min Throughput     MinLatency (ns)     MaxLatency (ns)     AvgLatency (ns)
*************************************************************************************************************************
1.1.1   1.1.2       74405               50.00              8140                8660                8440
1.1.1   1.1.3       74405               50.00              8180                8700                8476
1.1.1   1.1.4       74405               50.00              8240                8740                8525

AvgRate (fps)     = 74405
TotalTxCbs (s)    = 0
AvgLatency (ns)   = 8477
```

Obr. 6.16: Výsledok testu Broadcast Rate

Z vykonaných testov je vidieť, že sieťové zariadenie efektívne spracováva broadcastovú prevádzku bez straty rámcov pre rámce s veľkosťami 64, 512 a 1518 B. Priepustnosť je taktiež vysoká a hodnoty latencie pre každú veľkosť rámca boli nízke. To naznačuje, že zariadenie je schopné udržať stabilný výkon aj pri zvýšenej sieťovej záťaži.

Frame Error Filtering

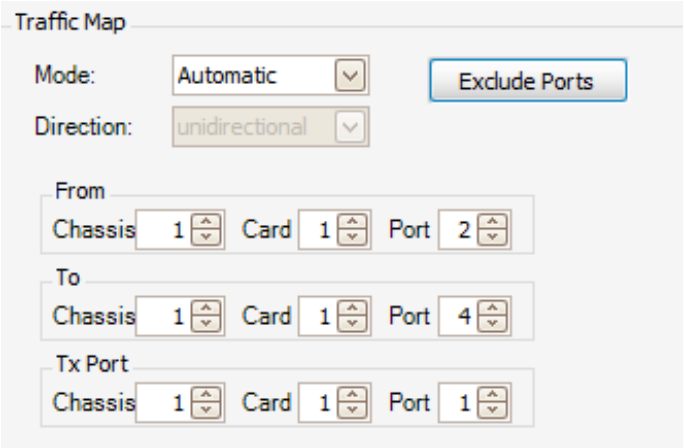
V hlavnom okne programu v záložke **Configurations->Templates->RFC 2889** kliknite pravým tlačidlom myši na **Frame Error Filtering** a zvoľte **New Test**. Názov testu pomenujte podľa svojho ID. Následne klikneme na **Add** a do políčka **Hostname** vložte IP adresu zariadenia na, ktoré sa pripojíte (v našom prípade 192.168.1.11). Ostatné parametre ponecháme a klikneme **Apply** a **OK**.

Kliknite na **Card 1** a v **Settings for Card 1,1** nastavte Speed na Copper 100. Následne kliknite na **Apply to All Ports on Card**.

Presuňte sa do **Configuration->Traffic Setup** a v časti **Frame Size** zvoľte veľkosť rámcov 64, 512 a 1518. Zvoľte iba **Undersize** a **Bad CRC**. Bad CRC bude vykonávať pre nami zvolené veľkosti rámcov. CRC (Cyclic Redundancy Check) je metóda používaná na detekciu chýb v dátach. Pracuje tak, že z pôvodných dát vygeneruje kontrolný súčet, ktorý je potom priložený k dátovému bloku a odoslaný alebo uložený spolu s ním. Keď sú dáta na druhej strane prijaté alebo čítané, systém zopakuje výpočet CRC na overenie integrity dát. Ak sa novo vypočítaný kontrolný súčet líši od toho, ktorý bol odoslaný, signalizuje to, že dáta boli počas prenosu alebo uloženia nejakým spôsobom zmenené, čo naznačuje potenciálnu chybu. Časť **Traffic Map** nastavte podľa obrázka 6.17. Toto nastavenie určuje, že port 1 bude vysielať na porty 2-4.

Následne sa presuňte do **Configuration->Test Setup** a nastavte **Duration** na 10 sekúnd. Test následne spustite a počkajte kým test neprebehne. Podobný výsledok testu môžete vidieť na obrázku 6.18.

Ako môžete vidieť pre typ Undersize boli zasielané rámce o veľkostiach 26, 32 a 63 B. Výsledky ukazujú, že ani jeden rámec nebol prijatý (RX Frames). Status Pass znamená, že funkcionalita filtrovania chybných rámcov pracuje korektne. Pri teste Bad CRC taktiež môžeme vidieť, že nebol prijatý ani jeden rámec a test teda prešiel (Pass).



Obr. 6.17: Nastavenie smeru tokov pre test Frame Error Filtering

RFC 2889 Eroded Frame Filtering Test - Error:undersize --> Framesize: 26

Mirror	TX Port	RX Port	Tx Frames	Rx Frames	Error Frames	Status
undersize	1.1.1	1.1.2	2717390	0	0	pass
	1.1.1	1.1.3	2717390	0	0	pass
	1.1.1	1.1.4	2717390	0	0	pass

Obr. 6.18: Výsledok testu Frame Error Filtering

Head of Line Blocking

V hlavnom okne programu v záložke **Configurations->Templates->RFC 2889** kliknite pravým tlačidlom myši na **Head of Line Blocking** a zvoľte **New Test**. Názov testu pomenujte podľa svojho ID. Následne klikneme na **Add** a do políčka **Hostname** vložte IP adresu zariadenia na, ktoré sa pripojíte (v našom prípade 192.168.1.11). Ostatné parametre ponecháme a klikneme **Apply** a **OK**.

Kliknite na **Card 1** a v **Settings for Card 1,1** nastavte Speed na Copper 100. Následne kliknite na **Apply to All Ports on Card**.

Presuňte sa do **Configuration->Traffic Setup** a v časti **Frame Size** zvoľte veľkosť rámcov 64, 512 a 1518. V časti **Traffic Map** zvoľte **Mode->Manual -> Configure.** Nastavte, že port 1 bude vysielať na porty 3-4 a port 2 na port 4. Toto nastavenie portov vykonajte pre Card 1.

Následne sa presunieme do **Configuration->Test Setup** a nastavíme **Duration** na 10 sekúnd. Test následne spustíme a počkáme kým test neprebehne. Do tabuľky 6.3 zaznamenajte hodnoty stratovosti pre jednotlivé veľkosti rámcov. Podobný výsledok testu môžete vidieť na obrázku 6.19.

V teste vidno, že pri porte 1.1.4 (Congested) nastalo preťaženie. V časti Head of Line, pri porte 1.1.3 vidieť hodnotu NO. Pri porte 1.1.4 táto hodnota nie je a to z toho dôvodu, že spracovanie rámca na začiatku fronty blokuje vysielanie ďalších rámcov tej istej fronte. Na tomto porte teda došlo k strate rámcov. Test teda naznačuje, že zariadenie má problémy s riadením fronty v prípade zvýšenej alebo rôznorodej sieťovej prevádzky.

Result Metrics
****
Trial: 1 Frame Size: 64

Group ID	Tx Port	Load (%)	Rx Port	ILoad (bps / Tx Port)	OLoad (bps)	Tx Frames	Rx Frames	Frame Loss	Head of Line
Test_Group_0	1.1.1 (TX1)	100	1.1.4 (Uncongested)	76190474.240	38095360	744050	744050	0	NO
Test_Group_0			1.1.4 (Congested)		38163302	744050	748298	1152	NO
Test_Group_0	1.1.2 (TX2)	100	1.1.4 (Congested)	76190474.240	38163302	1488100	745377	742723	NO

Aggregate Metrics
****
Trial: 1 Frame Size: 64

Group ID	Load (%)	Avg OLoad (bps)	Total Tx Frames	Total Rx Frames	Total Frame Loss	Total Frame Loss (%)
Test_Group_0	100	1142953093	2976200	2332325	247958	16.689

Obr. 6.19: Výsledok testu Head of Line Blocking

Tab. 6.3: Výsledky stratovosti pre test Head of Line Blocking

Veľkosť rámca [B]	**Total Frame Loss [%]**
64	
512	
1518	

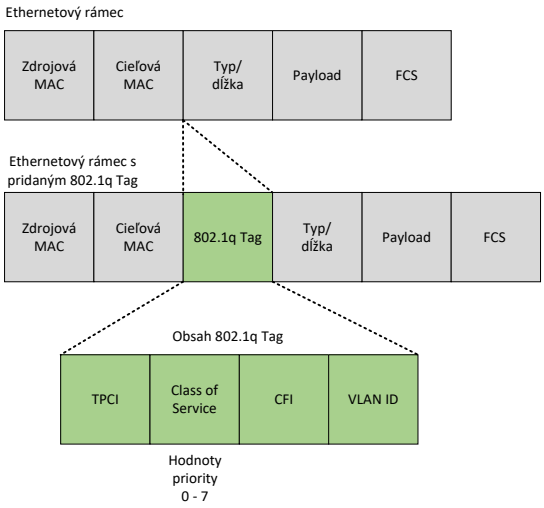
6.3.4 Test služby QoS na linkovej vrstve

Táto časť laboratórnej úlohy sa zaoberá testovaním kvality služieb (QoS) na druhej vrstve (linková vrstva). Pre rôzne streamy, ktoré reprezentujú rôzne dátové služby, bude nastavená rozdielna hodnota CoS (Class of Service). Tieto streamy sú generované pomocou programu IxExplorer. Prepínač je rovnaký ako v predchádzajúcej časti laboratórnej úlohy. Tento prepínač podporuje IEEE 802.1p QoS. To znamená, že podporuje priority, ktoré nadobúdajú hodnôt 0-7. Jednotlivé popisy týchto hodnôt môžete vidieť v tabuľke 6.4. Zapojenie je rovnaké ako z prechádzajúcej úlohy.

Tab. 6.4: Klasifikácia prevádzky pri QoS [45]

Priorita	**Akronym**	**Typ prevádzky**
0	BK	Background
1	BE	Best effort
2	EE	Excellent effort
3	CA	Critical applications
4	VI	Video, < 100 ms latency
5	VO	Voice, < 10 ms latency
6	IC	Internetwork control
7	NC	Network control

Políčko TAG sa vkladá do rámca za hodnotu DA MAC. V tomto políčku sú vyhradené 3 bity na určenie priority viz obrázok 6.20.

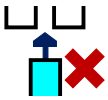


Obr. 6.20: Ethernet rámec s prioritou CoS [46]

Zatvorte program IxAutomate a na Ploche počítača otvorte program IxExplorer. Po otvorení programu je potrebné zadať IP adresu Chassis na ktorú sa chceme pripojiť. Zadajte IP adresu 192.168.1.11 a stlačte **OK**. V **Resources** rozbaľte všetky porty pre Card 1. Pravým tlačidlom kliknite na Card 1 a zvoľte možnosť **Reset Factory Defaults**. Tento krok je podstatný z dôvodu, aby nezostali na portoch konfigurácie z predošlých testov vykonávaných pomocou IxAutomate. Pravým tlačidlom kliknite na Port 1 a otvorte **Properties->OAM->Enable** (MAC adresu ponechajte (00 00 AB BA DE AD) a následne **Použiť** a **OK**. Rovnaké nastavenie

vykonajte aj pri ostatných portoch ale je potrebné na týchto portoch nastaviť odlišnú MAC adresu (Port 2 - 00 00 AB BA DE A2), (Port 3 - 00 00 AB BA DE A3) a (Port4 - 00 00 AB BA DE A4).

Teraz je potrebné pripraviť prehľadnejšie tabuľky a záložky streamu. Kliknite na **Port 01 -> Packet Streams** a kliknite na 6.21. Pridajte do **Visible Fields : Control, Frame Data, Vlan** a potvrďte.



Obr. 6.21: Tlačidlo Add/Remove field from table

Kliknite na **Packet Stream** v zložke **Port 1**. Na portoch sa streamy vytvárajú kliknutím pravým tlačidlom na **Packet stream->New Stream**. Vytvorte 3 streamy a nastavte ich ako je zobrazené na obrázku 6.22. Každý stream predstavuje inú dátovú službu. Prvý stream predstavuje Dáta, ktorý ma veľkosť rámcov 512 B. Druhý stream predstavuje Video, ktorý ma veľkosť rámcov 1300 B. Tretí stream predstavuje Voice, ktorý má veľkosť rámcov 64 B. **VLan ID** určuje, že všetky streamy patria do rovnakej VLan (10). **VLan User Priority** predstavuje prioritu na základe typu prevádzky (CoS). Rovnaké nastavenie vykonajte aj pre porty 2 a 3. Na porte 4 nenastavujte generovanie streamov nakoľko tento port bude dátové toky len prijímať.

	Name	Enable	Control	Flow	Loop Count	Suspend	Frame Size	Data Pattern Type	VLan	VLan ID	VLan ID Count	Repeat Count	VLan User Priority	VLan Canonical
1	Data	☑	Advance	↓	1	☐	512	Inc Byte	☑	10	Idle	10	0	Reset
2	Video	☑	Advance	↓	1	☐	1,300	Inc Byte	☑	10	Idle	10	4	Reset
3	Voice	☑	Return to ID	↩	1	☐	64	Inc Byte	☑	10	Idle	10	5	Reset

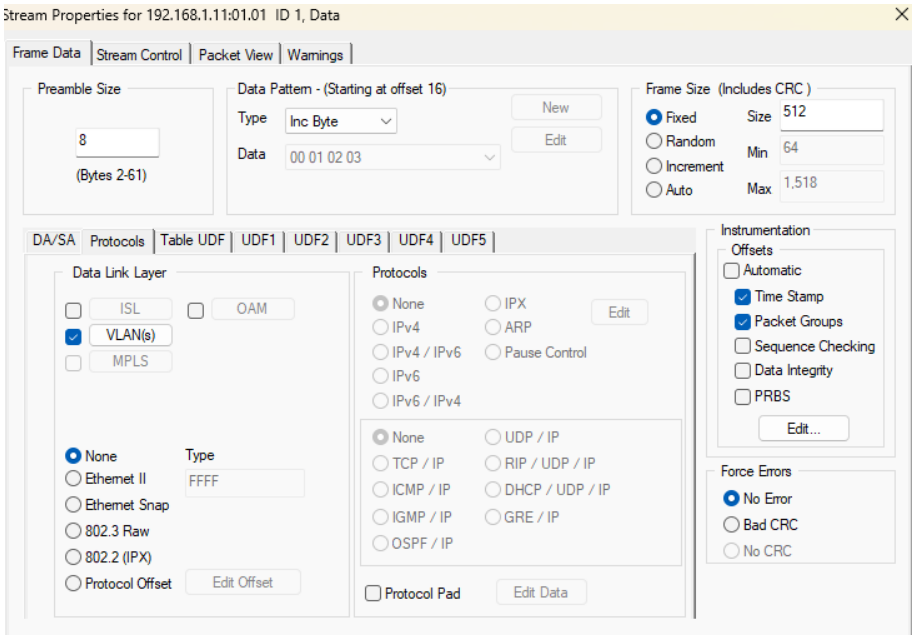
Obr. 6.22: Nastavenie streamov v IxExplorer

V záložke **DA/SA Data** nastavte **SA Value** MAC adresu príslušného portu a na **DA Value** nastavte MAC adresu portu 4. Nastavenie týchto MAC adries vykonajte pre každý stream na portoch 1 až 3. Pozor si treba dať na cieľovú MAC adresu pri nastavovaní streamov na portoch 2 a 3. Je potrebné pre všetky streamy na každom porte (1 až 3) nastaviť **DA Value** (MAC adresu portu 4). Nastavenie MAC adries pre port 1 je znázornené na obrázku 6.23. V záložke **Gap/Rate Control** nastavte pre každý stream **Desire % Line Rate** hodnotu 50. Toto nastavenie vykonajte pre porty 1 až 3. Táto hodnota reprezentuje percentuálnu rýchlosť linky z maximálnej možnej.

	DA Mode	DA Value	DA Count	SA Mode	SA Value	SA Count
1	Fixed	00 00 AB BA DE A4	16	Fixed	00 00 AB BA DE AD	16
2	Fixed	00 00 AB BA DE A4	16	Fixed	00 00 AB BA DE AD	16
3	Fixed	00 00 AB BA DE A4	16	Fixed	00 00 AB BA DE AD	16

Obr. 6.23: Nastavenie MAC adries v IxExplorer

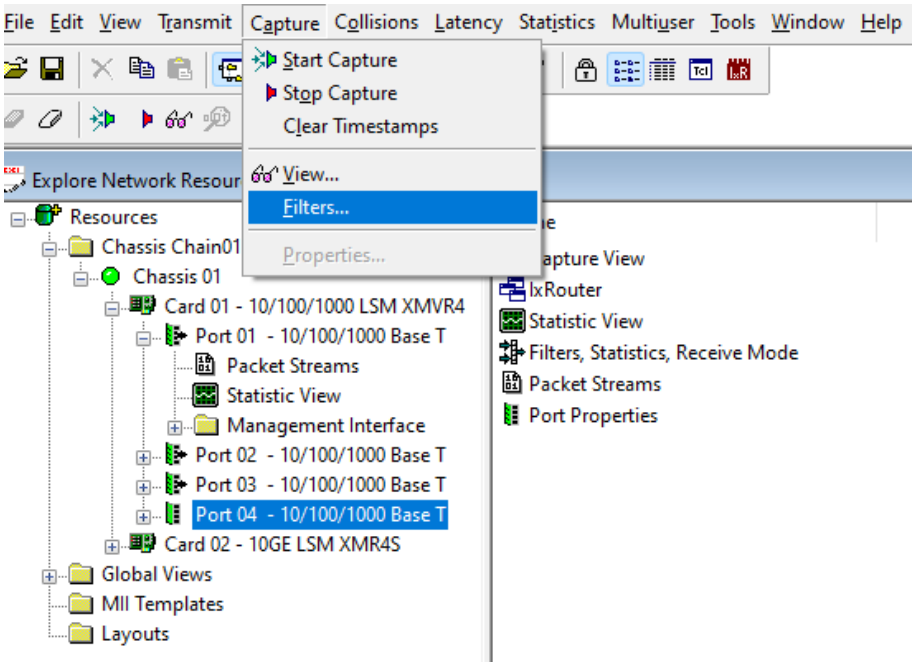
Na každom porte sú momentálne vytvorené tri streamy (Data, Video a Voice). Dvojklikom na daný stream napríklad **Data** otvoríte okno **Stream Properties** (obrázok 6.24). V časti **Instrumentation** zakliknite **Time Stamp** a **Packet Groups**. Zakliknutím políčka **Packet Groups** sú priradené rovnaké streamy do jednej skupiny. Táto skupina bude následne spolu analyzovaná. Toto nastavenie vykonajte pre všetky streamy **Data**, **Voice** a **Video** na portoch 1 až 3.



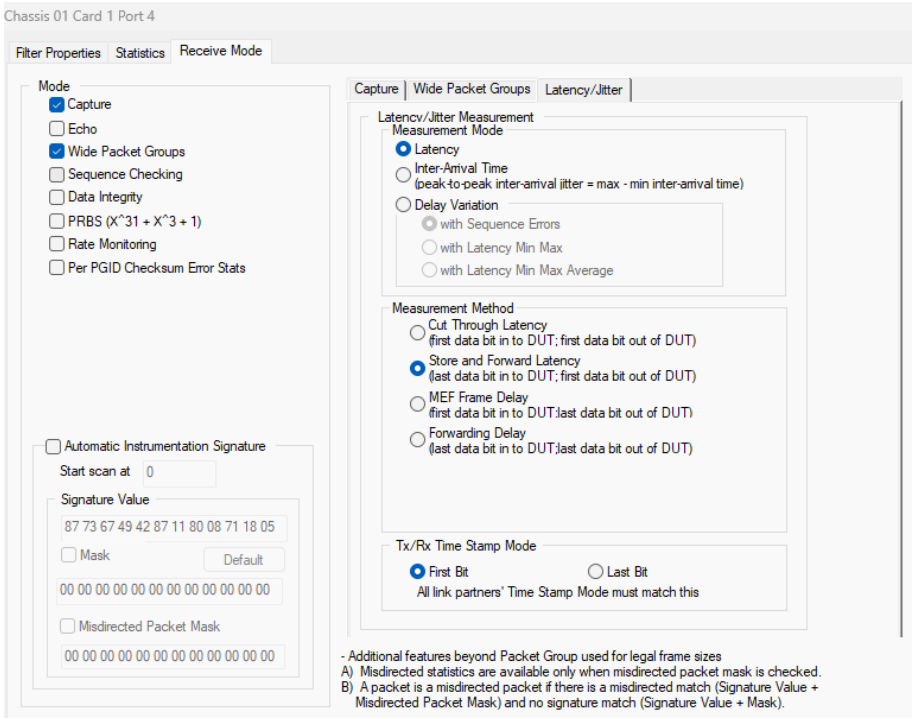
Obr. 6.24: Nastavenie streamov

Nakoľko sú teraz nastavené streamy na portoch 1-3, je potrebné nastaviť na porte 4 filtrovanie rámcov. Kliknite na port 4 a v hornej časti okna kliknite **Capture ->Filters** (obrázok 6.25). V záložke **Statistics** zakliknite **QoS** a v záložke **Receive Mode ->Mode** pridajte **Wide Packet Groups**. V záložke **Wide Packet Groups** nastavte **Signature->Offset** na 48 a **PGID->Offset** 52. V záložke **Latency/Jitter** zakliknite **Latency** a **Store and Forward Latency** (obrázok 6.26). Dôležité je potvrdiť nastavenia **Použiť- OK**. Je možné, že pri zaklikutí **Reset Factory Defaults** vznikol stream v záložke **Port 04-> Packet Streams**.

Pomocou **Enable** vypnete vysielanie streamu na tomto porte.

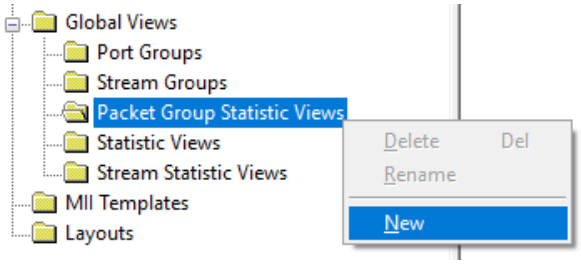


Obr. 6.25: Nastavenie filtrov pre port 4

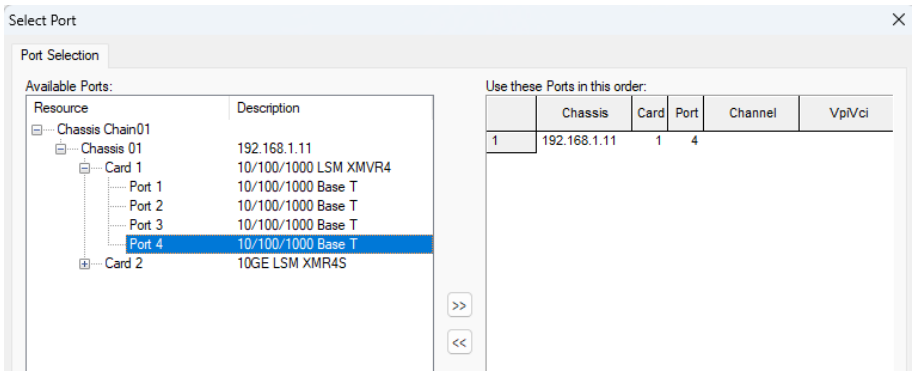


Obr. 6.26: Nastavenie filtru pre latenciu

V ľavej časti okna otvorte zložku **Global Views->Packet Groups Statistic Views** (obrázok 6.27). Pravým tlačidlom na túto zložku vytvorte **New** záznam. V **Select Port** vyberte port 4 z Card 1 ako je možné vidieť na obrázku 6.28. Novo vytvorený záznam nezatvárajte.

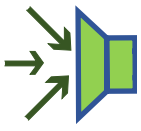


Obr. 6.27: Otvorenie zložky Packet Groups Statistic Views



Obr. 6.28: Výber portov pre generovanie streamov s QoS

Po všetkých nastaveniach je potrebné spustiť test. Kliknite pravým tlačidlom na **Card 1->Clear all Statistics.** Kliknite pravým tlačidlom na port 4 a stlačte **Start Capture**. Kliknite pravým tlačidlom na **Card 1->Start Transmit.** Otvorte vami vytvorenú štatistiku v **Packet Groups Statistic Views** a zapnite zachytávanie pomocou **Start Collecting Metrics** (obrázok 6.29).



Obr. 6.29: Tlačidlo Start Collecting Metrics

Ak všetko prebehlo úspešne tak vo vami vytvorenej štatistike uvidíte výsledné latencie a bitový tok ako je zobrazené na obrázku 7.26. test nechajte bežať pár sekúnd a výsledky priemernej latencie (**Latenca Store Forvard Avg**) poznamenajte do tabuľky 6.30.

PGID	Total # Frames	Latency Store Forward Min (µs)	Latency Store Forward Max (µs)	Latency Store Forward Max-Min (µs)	Latency Store Forward Avg (µs)	Bit Rate (/sec)	Byte Count	First Timestamp	Last Timestamp
1	574,488	208.14	22,754.58	22,546.44	1,556.15	27,057,283	294,137,856	00:00:00.000000000	00:01:28.200906060
2	574,353	61.58	1,139.50	1,077.92	583.51	66,382,379	735,171,840	00:00:00.000000000	00:01:28.216916920
3	574,300	30.54	647.74	617.20	83.19	3,542,026	39,052,400	00:00:00.000000000	00:01:28.188932540

Obr. 6.30: Výsledná latencia a bitový tok pre test s rôznymi hodnotami CoS

PGID 1 odpovedá prenosu dát pri ktorom bola nastavená hodnota CoS 0, čiže najnižšia priorita. Tu môžeme vidieť, že latencia dosahuje najvyšších hodnôt. PGID 2 predstavuje prenos videa a hodnota CoS bola nastavená na 4. Vidieť, že sa latencia výrazne znížila. Posledné PGID 3 prestavuje prenos hlasu/zvuku a pri tomto prenose bola nastavená hodnota CoS 5. Hodnota latencie tu dosahuje najnižšie hodnoty vďaka najvyššej priorite. Všetky latencie sú nízke a teda v rámci normy štandardu pre vysokokvalitne prenosy.

6.4 Samostatná úloha

1. Otestujte pomocou programu IxEplorer ako hodnoty CoS (0, 4 a 5) vplývajú na latenciu pri veľkosti rámcov 1518 a 64 B. Namerané hodnoty poznamenajte do tabuľky 6.5 a 6.6.

Tab. 6.5: Výsledky testu pre streamy s veľkosťou 1518 B s rôznymi hodnotami CoS

Veľkosť rámca [B]	**PGID**	**CoS**	**Latency SoreForward Avg [ms]**
1518	1	0	
1518	2	4	
1518	3	5	

Tab. 6.6: Výsledky testu pre streamy s veľkosťou 64 B s rôznymi hodnotami CoS

Veľkosť rámca [B]	**PGID**	**CoS**	**Latency SoreForward Avg [ms]**
64	1	0	
64	2	4	
64	3	5	

2. Otestujte aké hodnoty latencie nadobúdajú streamy v prípade ak majú rovnakú hodnotu priority CoS (0). Namerané hodnoty poznamenajte do tabuľky 6.7.

Tab. 6.7: Výsledky testu pre streamy s veľkosťou 64 B s hodnotou CoS (0)

Veľkosť rámca [B]	**PGID**	**CoS**	**Latency SoreForward Avg [ms]**
64	1	0	
64	2	0	
64	3	0	

6.5 Kontrolné otázky

1. Ako vplýva veľkosť rámcov na priepustnosť sieťového prepínača a prečo?
2. Aké sú hlavné rozdiely medzi metodikami testovania RFC 2544 a RFC 2889 a prečo sú obe dôležité?
3. Aké zariadenie preposiela rámce na linkovej vrstve a s akými adresami pracuje.
4. Vysvetlite pojmy Frame Error Filtering a Head of Line Blocking.
5. Čo je to CRC?
6. Vysvetlite, ako QoS na linkovej vrstve ovplyvňuje prioritizáciu sieťovej prevádzky.
7. Ako môže hodnota CoS ovplyvniť latenciu pri rôznych typoch sieťovej prevádzky?
8. Aká je latencia pri rovnakej prioritizácií?

7 Vplyv prekladu adries (NAT) na kvalitu služieb.

7.1 Ciele a úlohy

7.1.1 Ciele

Cieľom laboratórnej úlohy je oboznámenie s pojmom NAT (Network Address Translation) a jeho vplyvom na sieťovú prevádzku. Taktiež je cieľom úlohy predstavenie základnej konfigurácie sieťových zariadení (smerovačov).

7.1.2 Úlohy

1. Prvou časťou laboratórnej úlohy je základná konfigurácia jedného smerovača a následná konfigurácia NAT.
2. Druhou časťou laboratórnej úlohy je samostatná úloha, kde študenti na základe získaných poznatkov z prvej časti nakonfigurujú dva smerovače s NAT.

7.2 Teoretický úvod

7.2.1 Smerovač

Smerovače sú zariadenia, ktoré zohrávajú dôležitú rolu v prepájaní rôznych sietí. Tieto zariadenia pracujú na tretej vrstve referenčného modelu OSI (Open Systems Interconnection), čo značí, že umožňujú smerovanie dát na základe IP (Internet Protocol) adresy. Sú veľmi dôležité v širokých sieťových prostrediach, kde je dôležité efektívne riadiť toky dát medzi rôznymi LAN (Local Area Network) alebo medzi LAN a internetom. Najdôležitejšou funkciou smerovania je voľba optimálnej trasy pre dáta, čo môže byť najrýchlejšia, najspoľahlivejšia alebo najkratšia trasa z jedného bodu do druhého. Smerovače zaisťujú, že informácie využijú najefektívnejšiu cestu k cieľovému zariadeniu, čo je veľmi podstatné pre rýchlosť a efektivitu siete. Každý smerovač rozhoduje akou cestou bude paket ďalej smerovaný pokiaľ existuje viacero možností ciest. Tento rozhodovací faktor je založený na určitej znalosti globálnej topológie, čo ale zároveň predstavuje základný problém smerovania. Globálne topológie sú často zložité a rozsiahle a taktiež sa môžu dynamicky meniť v čase a informácie o nej môžu byť ťažko zaznamenávané. Medzi kľúčovú funkciu smerovačov patrí aj preklad adries NAT (Network Address Translation) Pre úspešné plnenie smerovania je potrebné aby každý smerovač obsahoval na sledujúce informácie [1, 2]:

- IP adresu adresáta,
- možné cesty do všetkých vzdialených sietí,
- najlepšiu zvolenú trasu do cieľovej siete,
- susedné smerovače,
- metódu pre získavanie informácií o smerovaní.

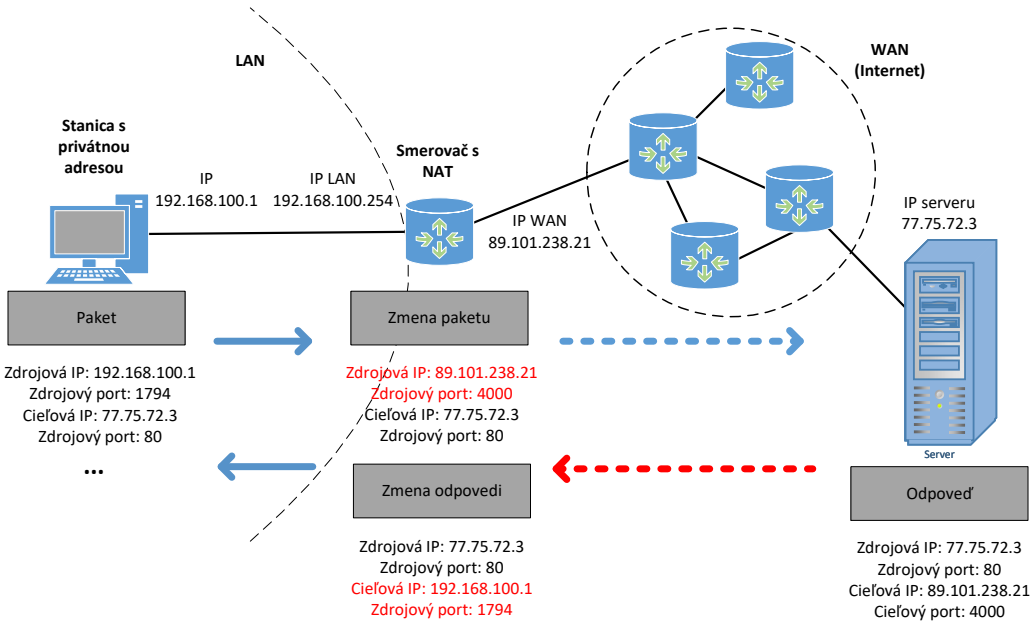
Jednou zo základných metrík, ktorá definuje výkon a spoľahlivosť sieťovej infraštruktúry je latencia. Latencia, ktorá sa v sieti vyskytuje najmä vďaka časovému zdržaniu pri prechode dátového paketu z jedného sieťového uzla do druhého, je priamo ovplyvnená práve smerovaním. Obvykle sa meria ako oneskorenie spiatočnej cesty a ideálne by mala byť čo najbližšie k nule, pre dosiahnutie lepších výsledkov. Táto metrika je zvyčajne meraná v milisekundách (ms). Vysoká latencia môže vzniknúť, ak smerovače nedokážu efektívne spracovať a presmerovať pakety, čo je často dôsledkom preťaženia, chýb v konfigurácii alebo nedostatočnej výkonnosti hardvéru. Efektívnosť smerovania paketov je teda kritická pre udržanie nízkej latencie, najmä v aplikáciách, kde je dôležitá rýchla odozva, ako sú hlasové služby alebo streamovanie videa. V tabuľke číslo 7.1 sú zobrazené priemerné hodnoty latencie s klasifikáciou.

Tab. 7.1: Doporučené hodnoty latencie a ich klasifikácia [47]

Latencia (ms)	**Vplyv na Služby**	**Typické Aplikácie**
0 až 150	Vynikajúca odozva, bez pozorovateľného zdržania užívateľom.	VoIP, real-time gaming, live video streaming
150 až 250	Dobrá odozva, mierny vplyv na komunikáciu bez výrazného negatívneho efektu.	VoIP, video hovory, online hry
250 až 400	Oznámené oneskorenia, ktoré môžu znížiť kvalitu interaktívnych hovorov.	Interaktívne videokonferencie, niektoré typy online hier
Nad 400	Výrazné oneskorenia, ktoré môžu spôsobiť prerušenia a problémy s komunikáciou.	VoIP v extrémnych podmienkach, interaktívne aplikácie vyžadujúce rýchlu odozvu

7.2.2 NAT (Network Address Translation)

Jedná sa o bežnú funkciu moderných smerovačov, ktorá zabezpečuje preklad (zmenu) IP adresy paketu, ktorá daným smerovačom prechádza. Zdrojová alebo cieľová IP adresa je prevádzaná medzi rôznymi rozsahmi. Umožňuje, aby počítače v lokálnej sieti (LAN) komunuikovali s internetom pod jednou verejnou IP adresou. Táto technika zabezpečuje efektívne oddelenie intranetu od internetu, čím prispieva k zvýšenej bezpečnosti siete, nakoľko skutočné IP adresy interných zariadení nie sú priamo vystavené vonkajším hrozbám. Smerovače s technikou NAT udržiavajú tabuľku prekladu adries, ktorá zabezpečuje rozlišovanie medzi dátovými tokmi jednotlivých staníc z vnútornej siete do internetu. Toto zabezpečuje aj v prípadoch, keď je pre celú sieť k dispozícií len jedna verejná IP adresa, ktorá je pridelená k WAN portu. Vďaka NAT je znížená potreba veľkého počtu verejných IP adries, čo je dôležité najmä z dôvodu nedostatku IPv4 adries. Taktiež umožňuje viacerým zariadeniam zdielať jednu verejnú IP adresu, čo znižuje potrebu veľkého počtu privátnych adries voči vonkajšiemu svetu. Smerovače vďaka NAT môžu rozlišovať a riadiť dátové toky medzi vonkajšími a vnútornými sieťami na základe komplexnejšieho systému, ktorý zahŕňa sieťové ale aj transportné adresy, čím zvyšuje efektivitu a bezpečnosť dátového prenosu [1]. Obrázok 7.1 popisuje princíp prekladu adries.



Obr. 7.1: Princíp prekladu adries [1]

V rôznych zdrojoch je možné nájsť rôzne spôsoby rozdelenia NAT. Medzi dva základné druhy prekladu adries patrí [1]:

- **SNAT (Source NAT)** – je technika, ktorá prekladá zdrojovú IP adresu vo všeobecnosti pri pripájaní zo súkromnej IP adresy na verejnú IP adresu. Je to najbežnejšia forma NAT, ktorá sa používa, keď interný hostiteľ potrebuje iniciovať reláciu s externým hostiteľom alebo verejným hostiteľom. Táto metóda umožňuje viacerým zariadeniam vo vnútornej sieti zdieľať jednu verejnú IP adresu. Je to praktické v prostrediach, kde je verejných IP adries obmedzené množstvo. SNAT mení zdrojovú adresu odchádzajúcich paketov z internej adresy na verejnú. Vďaka tomu môže interný hostiteľ komunikovať s externými servermi a službami bez toho, aby bolo potrebné prideliť každému zariadeniu unikátnu verejnú IP adresu.
- **DNAT (Destination NAT)** – je technika, ktorá prekladá cieľovú IP adresu, najmä pri pripojení z verejnej IP adresy na súkromnú IP adresu. Používa sa najmä na presmerovanie paketov určených pre konkrétnu IP adresu alebo špecifický port na IP adrese. Tento presmerovaný paket sa zvyčajne smeruje na inú adresu, zvyčajne na inom hostiteľovi. Tento proces umožňuje, že vnútorné servery, ktoré bežne nie sú priamo dostupné z internetu, môžu byť sprístupnené externým používateľom, čo je často využívané pre web servery, FTP servery alebo herné servery.

Smerovače využívajú rôzne techniky na správu a optimalizáciu sieťového toku ako napríklad smerovacie protokol (Routing Protocols), kvality služby (QoS), preklad adries (NAT) a iné. Technika NAT umožňuje viacerým zariadeniam v sieti zdieľať jednu verejnú IP adresu. Táto technika je zvlášť relevantná pri prepojení sietí, kde je potrebné rýchlo a efektívne riadiť dátový tok medzi súkromnými a verejnými sieťami. NAT môže v niektorých prípadoch zvýšiť latenciu, keď sú potrebné dodatočné kroky pre preklad adresy a portov, čo zdôrazňuje potrebu optimálnych konfigurácií smerovačov na zabezpečenie hladkého a rýchleho dátového toku.

Použitie NAT (Network Address Translation) a najmä double NAT môže mať významný vplyv na sieťové aplikácie ako je IP televízia, ktorá je citlivá na latenciu. Príkladom je scenár, kde sú doma dve televízie, ktoré sledujú IP televíziu. Jedna televízia je pripojená cez jedno NAT zariadenie a druhá cez dve NAT zariadenia (double NAT).

Jednoduché NAT pripojenie: Televízia zapojená cez jedno NAT zariadenie môže mať relatívne stabilnú a rýchlu sieťovú komunikáciu. NAT zariadenie tu prekladá internú IP adresu televízie na externú IP adresu, ktorú využíva pre komunikáciu na internete. Tento proces pridáva malé množstvo oneskorenia.

Double NAT pripojenie: Druhá televízia je pripojená cez dva NATy. Prechod dát cez dvojitý NAT zapríčiňuje vyššiu latenciu a potenciálne aj ďalšie sieťové problémy. Tu každý zo smerovačov (NAT zariadenia) musí spracovávať a prekladať IP adresy a porty, čo vyžaduje viac spracovateľského času a spôsobuje ďalšie oneskorenie. Táto komplikovanejšia konfigurácia môže viesť k vyššej latencii, ale aj k ťažšej diagnostike a správe sieťových problémov.

Pri sledovaní IP televízie (IPTV) môže mať double NAT rozdielny dopad na zážitok zo sledovania v závislosti na konfigurácii a výkonnosti siete:

- **Synchronizácia zvuku a obrazu**
  Vysoká latencia v sieti môže ovplyvniť doručovanie a synchronizáciu dátových paketov, čo môže viesť k výpadkom zvuku a videa. Ak pakety nedorazia v správnom poradí alebo sú výrazne oneskorené, prehrávač ich nemusí byť schopný správne usporiadať, čo vedie k asynchronizácii.
  Prerušenie zvuku sa prejavuje ako prerušovaný alebo oneskorený zvuk. Toto sa často prejavuje, keď zvuk nezodpovedá postupnosti videa alebo keď sa v zvuku objavujú vlny, ktoré miešajú okamihy ticha s okamihmi normálneho zvuku.
  Prerušenie videa znamená, že video vyzerá nesúvisle alebo sa občas objavia fragmenty videa, ktoré nie sú správne vykreslené. Tento problém môže nastať, pretože prehrávač videa nedokáže dostatočne rýchlo vyrovnať vyrovnávaciu pamäť prichádzajúcich video paketov.

Ak je oneskorenie vysoké, môžu byť tieto dva aspekty ovplyvnené súčasne a užívatelia si môžu všimnúť, že video a zvuk nie sú výrazne synchronizované. Inými slovami, video môže byť čisté, ale zvuk oneskorený, alebo naopak, zvuk môže byť čistý, ale video oneskorené alebo prerušované. Aby bola zabezpečená synchronizácia obrazu a zvuku, je dôležité optimalizovať sieť tak, aby sa minimalizovalo oneskorenie, najmä v aplikáciách citlivých na oneskorenie, ako sú služby streamovania videa a telekonferencie.

- **Buffering a prerušenie**
  Buffer (vyrovnávacia pamäť v televízii), sa používa na hladké prehrávanie videa tým, že ukladá dáta pred ich prehraním. Keď prúdové video cez IPTV prechádza cez viacnásobný NAT (napríklad double NAT), môže to viesť k vyššej latencii,. To znamená, že trvá dlhší čas, kým dáta dorazia do televízie. Tento nárast latencie môže spôsobiť, že vyrovnávacia pamäť sa spotrebuje rýchlejšie, než sa stihne obnoviť, čo môže viesť k častejšiemu bufferingu alebo prerušeniu prehrávania. Tento jav môže byť obzvlášť znateľný pri sledovaní živého obsahu, kde je synchronizácia v reálnom čase kritická. Keďže buffer je navrhnutý na to, aby zmiernil následky nepravidelného príjmu dát a udržiaval plynulosť prehrávania, akékoľvek zvýšenie časového oneskorenia v dôsledku NAT môže negatívne ovplyvniť celkový zážitok zo sledovania. To znamená, že užívatelia môžu zažívať častejšie prerušenia, keď sa video snaží dobiť vyrovnávaciu pamäť.
- **Kvalita streamu**
  Sieťová latencia a jitter môžu ovplyvniť rozhodovanie algoritmu pre adaptívne streamovanie, ktoré mení kvalitu streamu v závislosti od sieťových podmienok. To môže viesť k tomu, že IPTV stream v miestnosti s double NATom bude mať nižšiu kvalitu obrazu, aby sa prispôsobil vyššej latencii.
- **Celková záťaž siete**
  Double NAT môže tiež zvýšiť celkovú záťaž na smerovač, pretože musí spracovať väčší počet NAT prekladov, čo môže mať za následok spomalenie celej siete.

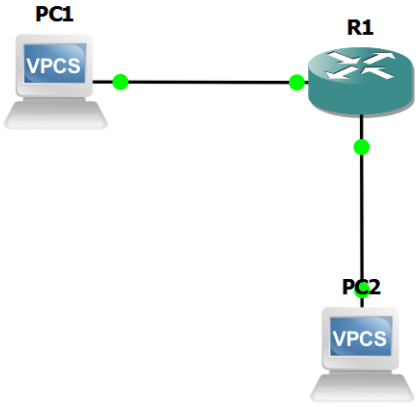
7.3 Pracovný postup

7.3.1 Vybavenie pracoviska

- Počítač s programom GNS3

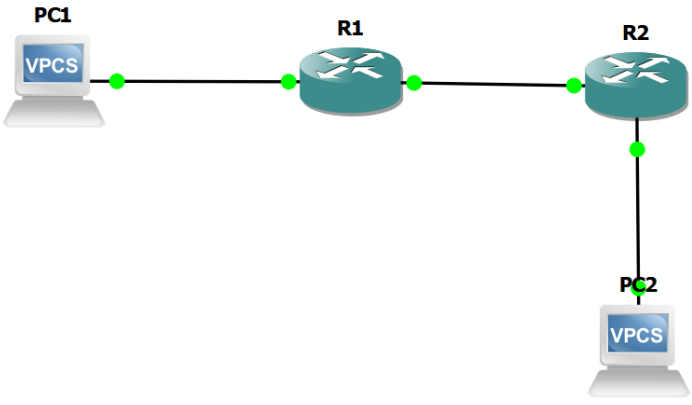
7.3.2 Schémy zapojenia

Obrázok 7.2 predstavuje zapojenie pre konfiguráciu NAT na jednom smerovači.



Obr. 7.2: Schéma zapojenia s využitím jedného smerovača

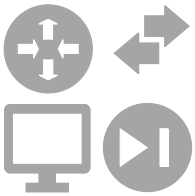
Obrázok 7.3 znázorňuje zapojenie pre konfiguráciu NAT na dvoch smerovačoch. Jedná sa o schému s využitím dvojitého NAT (double NAT).



Obr. 7.3: Schéma zapojenia s využitím dvoch smerovačov

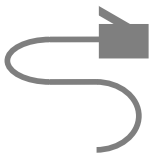
7.3.3 Konfigurácia NAT na jednom smerovači

Táto časť sa venuje základnej konfigurácií smerovača v programe GNS3. Spustite program GNS3, ktorý sa nachádza na ploche PC. V hlavnom okne programu vytvorte nový projekt **File-> New blank project**, ktorý pomenujete podla svojho ID. Do vytvoreného projektu vložte smerovač **c2691** a dva počítače ako je zobrazené na obrázku 7.2. jednotlivé komponenty sú v záložke pod obrázkom 7.4. PC1 predstavuje server umiestnený v internetovom prostredí, zatiaľ čo PC2 predstavuje koncové zariadenie v lokálnej sieti. PC2 je integrované do siete prostredníctvom smerovača R1, ktorý zabezpečuje jeho konektivitu s externým internetovým prostredím a umožňuje komunikáciu s PC1. Smerovač R1 funguje ako brána s NAT funkciou, ktorá oddeľuje internet od lokálnej siete. Router R1 zabezpečuje preklad interných IP adries na verejné IP adresy cez NAT, čím umožňuje bezpečnú a efektívnu komunikáciu medzi internetom a zariadeniami v lokálnej sieti.



Obr. 7.4: Ikona pre vloženie zariadení

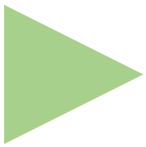
Po vložení komponentov je potrebné jednotlivé zariadenia prepojiť (obrázok 7.5). Po kliknutí na smerovač je možné na tomto zariadení zvoliť rozhrania, ktoré je možné zapojiť. **Interface FastEthernet 0/0** na smerovači prepojte na **PC1** a **Interface FastEthernet 0/1** pripojte na **PC2**.



Obr. 7.5: Prepojenie zariadení

Následne po prepojení smerovača s jednotlivými počítačmi je potrebné spustiť všetky zariadenia a to kliknutím sa zelenú šípku (obrázok 7.6).

Dvojklikom na zariadenie sa otvorí Putty pomocou ktorej sa dané zariadenie konfiguruje. Jednotlivé **Interfaces** smerovača a oba počítače budú nakonfigurované podla tabuľky 7.2.



Obr. 7.6: Ikona pre spustenie zariadení

Tab. 7.2: Adresná tabuľka pre NAT

Zariadenie	**Interface**	**IP adresa a prefix**
PC1	Ethernet0	203.0.113.100/24
PC2	Ethernet0	192.168.1.100/24
R1	FastEthernet 0/0	203.0.113.50/24
R1	FastEthernet 0/1	192.168.1.1/24

Ako prvé je potrebné nakonfigurovať smerovač s príslušnými adresami a prekladom adries. Vo výpise nižšie sa nachádzajú príkazy ktorými je potrebné smerovač R1 nakonfigurovať. Taktiež sa nižie nachádza popis a význam jednotlivých príkazov. Následne je taktiež potrebné nakonfigurovať jednotlivé počítače s príslušnou adresou v danej sieti.

```
1  R1#conf t
2  R1(config)#interface f0/0
3  R1(config-if)#description Connection-to-PC1
4  R1(config-if)#ip address 203.0.113.50 255.255.255.0
5  R1(config-if)#ip nat outside
6  R1(config-if)#no shutdown
7  R1(config-if)#exit
8  ----------------------------------------------------------------
9  R1(config)#interface f0/1
10 R1(config-if)#description Connection-to-PC2
11 R1(config-if)#ip address 192.168.1.1 255.255.255.0
12 R1(config-if)#ip nat inside
13 R1(config-if)#no shutdown
14 R1(config-if)#exit
15 ----------------------------------------------------------------
16 R1(config)#access-list 10 permit 192.168.1.0 0.0.0.255
17 R1(config)#ip nat inside source list 10 interface FastEthernet0/0 overload
```

Konfigurácia rozhraní R1

1. Interface ethernet0/0

- **description Connection-to-PC1**: Tento príkaz pridáva popis k rozhraniu, čo pomáha pri identifikácii a dokumentácii účelu daného rozhrania.

- **ip address 203.0.113.50 255.255.255.0**: Priradenie IP adresy a subnetovej masky rozhraniu, ktoré bude použité pre komunikáciu s vonkajším svetom (internetom).
- **ip nat outside**: Označuje toto rozhranie ako „vonkajšie"pre účely NAT, čo znamená, že IP adresy prechádzajúce cez toto rozhranie budú prekladané do alebo z internetu.
- **no shutdown**: Tento príkaz aktivuje rozhranie, keďže rozhrania sú implicitne vypnuté.

2. Interface ethernet0/1

- **description Connection-to-PC2**: Priradí popis rozhraniu pre lepšiu identifikáciu jeho účelu, tentokrát ako spojenie s interným zariadením PC2.
- **ip address 192.168.1.1 255.255.255.0**: Nastavuje IP adresu a masku pre internú sieť, ktorá bude používaná pre komunikáciu s vnútornými zariadeniami.
- **ip nat inside**: Označuje toto rozhranie ako „vnútorné"v kontexte NAT, čo znamená, že IP adresy prechádzajúce týmto rozhraním budú kandidátmi na preklad do vonkajšieho sveta.
- **no shutdown**: Aktivuje rozhranie pre použitie.

Konfigurácia NAT na R1

- **access-list 10 permit 192.168.1.0 0.0.0.255**: Vytvára prístupový zoznam (ACL), ktorý definuje rozsah IP adries, ktoré majú byť povolené pre NAT. V tomto prípade sa povoluje celá subnet 192.168.1.0/24.
- **ip nat inside source list 10 interface ethernet0/0 overload**: Tento príkaz nastavuje dynamické NAT pravidlo, kde inside source list 10 určuje, že zdrojové IP adresy definované v ACL číslo 10 budú prekladané. Interface ethernet0/0 určuje, že prekladané IP adresy budú mapované na IP adresu rozhrania ethernet0/0. Slovo overload umožňuje viac interných IP adries zdieľať jednu verejnú IP adresu pomocou rôznych portov (PAT - Port Address Translation).

Konfigurácia IP adries počítačov s príslušnými bránami

```
1 PC1> ip 203.0.113.100/24 203.0.113.50
2 PC2> ip 192.168.1.100/24 192.168.1.1
```

PC1

Príkaz: `ip 203.0.113.100/24 203.0.113.50`

- IP adresa a sieťová maska: `203.0.113.100/24` - Toto je IP adresa pridelená počítaču PC1, kde `/24` označuje dĺžku prefixu siete, čo zodpovedá subnet maske `255.255.255.0`. Táto adresa je súčasťou siete, ktorá zahrňuje adresy od `203.0.113.0` do `203.0.113.255`.
- Default gateway: `203.0.113.50` - Toto je IP adresa predvolenej brány pre PC1.

PC2

Príkaz: `ip 192.168.1.100/24 192.168.1.1`

- IP adresa a sieťová maska: `192.168.1.100/24` - Toto je IP adresa pridelená počítaču PC2, s rovnakou dĺžkou prefixu siete `/24`, čo zodpovedá subnet maske `255.255.255.0`. Táto adresa je tiež súčasťou siete, ktorá zahrňuje adresy od `192.168.1.0` do `192.168.1.255`.
- Default gateway: `192.168.1.1` - Toto je IP adresa predvolenej brány pre PC2, určená na smerovanie mimo lokálnu sieť.

Po úspešnej konfigurácii je možný ping medzi počítačmi a taktiež je možné sledovať aj preklady adries pomocou nasledujúcich príkazov.

Ako prvé je potrebné vykonať ping na PC1 z PC2 pomocou príkazu:

```
1 PC2> ping 203.0.113.100
```

Následne sa presunte do Putty pre R1 a zadajte príkaz:

```
1 R1#show ip nat translations
```

Tento príkaz je potrebné vykonať po dokončení príkazu ping nakoľko sa záznam v tabuľke prekladov uchováva len určitú dobu. Po uplynutí tejto doby je tento záznam vymazaný. Na obrázku 7.7 je možné vidieť výpis prekladu adries na smerovači R1.

Výpis ukazuje stav prekladov adries NAT (Network Address Translation) na smerovači R1. Tieto záznamy sú výsledkom použitia NAT na prekladanie privátnych IP adries na verejné IP adresy.

Rozbor výpisu:

- Pro Inside Global: Toto je verejná IP adresa a port, ako sú viditeľné zvonka (z internetu).
- Inside Local: Toto je privátna IP adresa a port, ako sú viditeľné z vnútra siete.

R1#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
icmp	203.0.113.50:16466	192.168.1.100:16466	203.0.113.100:16466	203.0.113.100:16466
icmp	203.0.113.50:16722	192.168.1.100:16722	203.0.113.100:16722	203.0.113.100:16722
icmp	203.0.113.50:16978	192.168.1.100:16978	203.0.113.100:16978	203.0.113.100:16978
icmp	203.0.113.50:17234	192.168.1.100:17234	203.0.113.100:17234	203.0.113.100:17234
icmp	203.0.113.50:17490	192.168.1.100:17490	203.0.113.100:17490	203.0.113.100:17490

Obr. 7.7: Výpis prekladu adries

- Outside Local: Toto je cieľová IP adresa a port, ako sú viditeľné z vnútra siete po preklade.
- Outside Global: Toto je skutočná cieľová IP adresa a port v internete.

Analýza príkladu:

V tomto prípade, smerovač prekladá ICMP (Internet Control Message Protocol) komunikáciu z vnútornej siete na internet. Vnútorné IP adresy (napríklad `192.168.1.100`) sú prekladané na verejnú IP adresu `203.0.113.50` s rôznymi portmi (ako `16466`, `16722`, atď.). To zabezpečuje, že viacero zariadení môže používať tú istú verejnú IP adresu. Skrytie vnútorných IP adries zvyšuje bezpečnosť, keďže externé zariadenia nevidia skutočné vnútorné adresy.

Taktiež je možné zobraziť štatistiky Network Address Translation (NAT) na smerovači R1 (obrázok 7.8). Tieto štatistiky poskytujú prehľad o efektívnosti a použití NAT na danom zariadení. Nižšie sa nachádza príkaz na zobrazenie výpisu a taktiež rozbor významu jednotlivých polí.

```
1 R1#show ip nat statistics
```

Rozbor štatistík NAT:

- Total active translations: Počet aktívnych prekladov adries, ktoré sú momentálne vo využití.
- Outside interfaces: Ukazuje rozhrania, ktoré sú označené ako vonkajšie (napr. pripojené k internetu). Tu je uvedené `FastEthernet0/0`.
- Inside interfaces: Ukazuje rozhrania, ktoré sú označené ako vnútorné (pripojené k lokálnej sieti). Tu je uvedené `FastEthernet0/1`.
- Hits: Počet úspešných prekladov paketov, kde NAT našiel existujúcu položku v tabuľke NAT pre spracovanie paketu.

- Misses: Počet prípadov, keď NAT nemohol nájsť zodpovedajúci záznam v tabuľke NAT, čo si vyžiadalo vytvorenie nového záznamu.
- CEF Translated packets: Počet paketov, ktoré boli preložené pomocou Cisco Express Forwarding, čo je vysoko efektívny spôsob spracovania paketov na Cisco zariadeniach.
- Expired translations: Počet prekladov, ktoré expirovali a boli odstránené z tabuľky NAT. Tu je uvedených 15 expirovaných prekladov.
- Dynamic mappings: Detaily o dynamických mapovaniach, kde `access-list 10` znamená, že prístupový zoznam číslo 10 je používaný pre dynamické mapovanie na rozhraní `FastEthernet0/0`.

```
R1#show ip nat statistics

Total active translations: 5 (0 static, 5 dynamic; 5 extended)
Outside interfaces:
  FastEthernet0/0
Inside interfaces:
  FastEthernet0/1
Hits: 25  Misses: 24
CEF Translated packets: 48, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
 -- Inside Source
[Id: 1] access-list 10 interface FastEthernet0/0 refcount 5
```

Obr. 7.8: Výpis štatistiky pre NAT

Po vykonaní úspešného pingu z počítača PC2 na adresu **203.0.113.100** je možné pozorovať informácie o oneskorení (latencii) a čase života (TTL) pre každý ICMP echo request (ping)

TTL (Time to Live): Hodnota TTL naznačuje, koľko sieťových zariadení (napr. smerovačov) môže paket prejsť predtým, ako bude zahodený. Hodnota TTL sa zníži o 1 za každé zariadenie, cez ktoré paket prechádza.

Čas: Latencia alebo odozva v milisekundách (`ms`). Tieto hodnoty ukazujú, ako dlho trvalo, kým bola na ping request prijatá odpoveď. Do tabuľky číslo 7.3 poznamenajte priemernú hodnotu latencie každého z troch pokusov o ping.

Tab. 7.3: Tabuľka latencie pre jeden preklad adries

Ping na adresu - 203.0.113.100	**Latencia [ms]**
1	
2	
3	

7.3.4 Samostatná úloha - Konfigurácia NAT na dvoch smerovačoch

Táto časť sa venuje základnej konfigurácií dvoch smerovačov. V hlavnom okne programu vytvorte nový projekt, ktorý pomenujete podla svojho ID (ID.2). Do vytvoreného projektu vložte komponenty a zapojte ich ako je zobrazené na obrázku 7.3. PC1 predstavuje server umiestnený v internetovom prostredí, zatiaľ čo PC2 predstavuje koncové zariadenie v lokálnej sieti. PC2 je integrované do siete prostredníctvom smerovačov R1 a R2, ktoré zabezpečujú jeho konektivitu s externým internetovým prostredím a umožňuje komunikáciu s PC1.

Smerovač R1 funguje ako brána s NAT funkciou, ktorá oddeľuje internet od lokálnej siete medzi R1 a R2. Router R1 zabezpečuje preklad interných IP adries na verejné IP adresy cez NAT, čím umožňuje bezpečnú a efektívnu komunikáciu medzi internetom a zariadeniami v lokálnej sieti.

Smerovač R2 slúži ako ďalšia brána s NAT, ktorá oddeľuje vnútornú sieť medzi R1 a R2 od ďalšej vnútornej siete, kde sa nachádza PC2. Tento dvojitý NAT (double NAT) poskytuje dodatočnú úroveň bezpečnosti a izolácie pre zariadenia v najvnútornejšej sieti, kde je PC2, a zároveň udržiava schopnosť komunikácie s vonkajším svetom cez R1.

Jednotlivé rozhrania zapojte podla tabuľky číslo 7.4 tak, aby jednotlivé smerovače oddeľovali tri predom definované siete. Sieť **203.0.113.0/24** je verejná. Sieť **10.0.0.0/24** predstavuje vnútornú sieť medzi R1 a R2. Sieť **192.168.1.0/24** je taktiež vnútorná/lokálna sieť.

Pri konfigurácií smerovačov je taktiež potrebné zadefinovať aj statické smerovanie medzi viacerými sieťami.

```
1 R1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

Tento príkaz slúži na nastavenie štandardnej (default) trasy na smerovači (v tomto prípade R1). Tento príkaz je kľúčový v sieťovej konfigurácii a jeho detailný popis je nasledujúci:

Tab. 7.4: Adresná tabuľka pre dvojitý NAT

Zariadenie	Interface	IP adresa a prefix
PC1	Ethernet0	203.0.113.100/24
PC2	Ethernet0	192.168.1.100/24
R1	FastEthernet 0/0	203.0.113.50/24
R1	FastEthernet 0/1	10.0.0.1/24
R2	FastEthernet 0/0	10.0.0.2/24
R2	FastEthernet 0/1	192.168.1.1/24

Popis príkazu

- `ip route`: Znamená konfiguráciu statickej trasa v IP smerovacej tabuľke zariadenia.
- `0.0.0.0 0.0.0.0`: Tieto dve adresy predstavujú sieťovú adresu a sieťovú masku pre štandardnú trasu. V tomto prípade, `0.0.0.0` predstavuje sieťovú adresu a `0.0.0.0` masku, čo spolu označuje všetky možné IP adresy. V praxi to znamená, že tento záznam v smerovacej tabuľke bude použitý pre akúkoľvek destináciu, pre ktorú nie je špecificky definovaná iná trasa.
- `10.0.0.2`: Toto je next-hop IP adresa, ktorá hovorí, že ak sieťový paket zodpovedá tejto trase (t.j. ak pre danú destináciu neexistuje špecifická trasa), paket bude poslaný na zariadenie s IP adresou 10.0.0.2. Táto adresa je typicky adresa najbližšieho smerovača alebo brány na ceste k výslednej destinácii.

Rovnaké nastavenie smerovania je potrebné vykonať aj pre smerovač R2 ale s inou adresou **next-hop IP**.

Overte, či po konfigurácií dochádza na oboch smerovačoch k prekladu adries a záznam o tomto preklade uchovajte na kontrolu vyučujúcim. Taktiež poznamenajte do tabuľky číslo 7.5 priemernú hodnotu latencie každého z troch pokusov o ping na dresu 203.0.113.100.

Tab. 7.5: Tabuľka latencie pre dvojitý preklad adries

Ping na adresu - 203.0.113.100	Latencia [ms]
1	
2	
3	

Porovnajte Vami získané výsledky latencií pre zapojenie s jedným smerovačom

a pre zapojenie s dvoma smerovačmi. Analyzujte aký vplyv má počet zariadení s konfiguráciou prekladu adries v jednej sieti na latenciu prenosu.

7.4 Kontrolné otázky

1. Na akej vrstve pracuje smerovač?
2. S akými adresami pracujú smerovače?
3. Čo je to latencia a pre aké služby je podstatná?
4. Čo je NAT?
5. Aké dva základe druhy NAT existujú a aký je medzi nimi rozdiel?
6. Ako NAT prispieva k bezpečnosti siete?
7. Aké sú potenciálne nevýhody použitia NAT v sieťovom prostredí?
8. Ako môže double NAT ovplyvniť sieťový výkon a komunikáciu?
9. Čo značí skratka CEF ?
10. Čo je TTL?
11. Aký vplyv má NAT a dvojitý NAT na latenciu?

8 Analýza a konfigurácia systému DOCSIS

8.1 Ciele a úlohy

8.1.1 Ciele

Cieľom laboratórnej úlohy je zoznámenie sa s medzinárodným štandardom DOCSIS (Data Over Cable Service Interface Specification), ktorý umožňuje vysoko rýchlostný prenos dát cez káblové televízne systémy. Taktiež je cieľom konfigurácia zariadení DAH100 (DOCSIS Acces Hub) a káblového modemu vrátane konfigurácie downstreamu a upstreamu.

8.1.2 Úlohy

1. Prvá úloha sa venuje konfigurácií zariadení ako je DAH100 a káblový modem a následnému overeniu prístupu na Internet.
2. Druhou časťou laboratórnej úlohy je oboznámenie sa s konfiguráciou súboru káblového modemu
3. Treťou a zároveň poslednou časťou laboratórnej úlohy je samostatná úloha, v ktorej študenti otestujú rôzne konfigurácie systému DOCSIS a ich vplyv na prenosové rýchlosti dátovej komunikácie.

8.2 Teoretický úvod

8.2.1 Koaxiálny kábel

1.1 Definícia a princípy Koaxiálny kábel je typ elektrického kábla s vonkajším valcovým vodičom, jedným vnútorným drôtovým alebo trubkovým vodičom a plášťom, ktorý slúži na ochranu kábla. Vonkajší vodič sa nazýva tienenie a vnútorný vodič jadro. Jadro a tienenie sú oddelené nevodivou vrstvou (dielektrikom). Tento dizajn umožňuje koaxiálnym káblom prenášať elektronické signály s minimálnou interferenciou z externých zdrojov, nazývané ako EMI (Electromagnetic Interference). Káble sú zvyčajne zakončené konektormi, ktoré umožňujú pripojenie k rôznym elektronickým zariadeniam. Medzi pár základných konektorov patrí:

- IEC – používa sa k pripojeniu set-top boxu alebo TV prijímača s účastníckou zásuvkou,
- F – slúži k pripojeniu káblového modemu s dátovým otvorom na účastníckej sade.

Medzi jeden z najpoužívanejších typov koaxiálnych káblov je RG6. Vyznačuje sa svojimi špecifickými a elektrickými vlastnosťami, ktoré ho robia ideálnym pre aplikácie v oblasti televízneho vysielania a internetových pripojení. RG6 má hrubší stredový vodič, čo zabezpečuje nízky odpor a vysokú kvalitu signálu. Izolácia s pevného polyetylénu minimalizuje straty signálu a udržuje stabilitu signálu aj pri vysokých frekvenciách. Väčší počet tienenia zabezpečuje ochranu proti EMI a RFI (Radio-frequency Interference). RG6 káble majú štandardnú impedanciu 75. Vďaka nižšiemu útlmu dokáže prenášať signál na väčšie vzdialenosti. Koaxiálny kábel dokáže efektívne prenášať signály na veľké vzdialenosti bez významnej straty signálu. Medzi hlavné výhody patrí [3]:

- **Odolnosť voči rušeniu:** Vďaka štruktúre je koaxiálny kábel viac odolnejší voči rušeniu.
- **Vysoká šírka pásma:** Koaxiálne káble prenášajú veľké množstvo dát, pre televízne vysielanie, internet a iné komunikačné aplikácie.

Použitie koaxiálnych káblov

- **Televízne vysielanie:** Koaxiálne káble sú používané na rozvod televízneho signálu v káblových televíziách.
- **Internetové pripojenia:** Mnohé formy širokopásmového internetu využívajú koaxiálne káble na prenos dát.
- **Bezpečnostné systémy:** CCTV (Closed-circuit television) systémy často využívajú koaxiálne káble na prenos video signálu z bezpečnostných kamier.

8.2.2 DOCSIS

DOCSIS (Data Over Cable Service Interface Specification) je medzinárodný telekomunikačný štandard, ktorý poskytuje obojsmerné širokopásmové dátové prenosy po existujúcich televíznych káblových rozvodoch.

Účelom DOCSIS bolo špecifikovať obojsmerné dátové spojenie medzi CM (Cable Modem) a CMTS (Cable Modem Termination System) tak, aby bolo možné poskytnúť prístup na internet. V Európe sa používa mierne upravená verzia systému „Euro-DOCSIS", ktorá pre downstream kanál využíva DVB-C namiesto J83B, ktorý je využívaný v originálnom DOCSIS. DVB-C používa primárne 64QAM alebo 256QAM moduláciu. J83B využíva 64QAM alebo 256QAM, ale s inými parametrami systému a môže taktiež používať 32QAM. DVB-C používa frekvencie pre downstream približne od 50 do 865 MHz a pre upstream približne od 5MHz do 65MHz. J83B môže používať podobné frekvenčné rozsahy ale líši sa v podrobnostiach o symbolových rýchlostiach a modulačných schémach. Taktiež sú závislé aj na špecifikáciách poskytovateľov služieb. V tabuľke číslo 8.1 sú uvedené špecifikácie jednotlivých verzí DOCSIS.

Verzie štandardu DOCSIS

DOCSIS 1.0: Táto verzia obsahuje funkčné prvky pozostávajúce z predchádzajúcich proprietárnych káblových modemov.
DOCSIS 1.1: Štandardizovala základné QoS (Quality of Services), ktoré neboli súčasťou DOCSIS 1.0
DOCSIS 2.0: Verzia poskytuje zvýšené prenosové rýchlosti dát na základe zvýšeného dopytu po symetrických službách ako je napríklad IP telefónia.
DOCSIS 3.0: Táto verzia výrazne poskytla zvýšenie prenosových rýchlostí (pre upstream aj downstream) a priniesla aj podporu pre internetový protokol verzie 6 (IPv6).
DOCSIS 3.1: Prináša pre downstream kapacitu až 10 Gbit/s a pre upstream 1 Gbit/s pomocou 4096 QAM. Tieto nové špecifikácie eliminovali 6 MHz a 8 MHz široký kanálový odstup a namiesto toho používa užšie 25 alebo 50 kHz subnosné. Táto verzia taktiež poskytuje funkcie správy napájania, ktoré poskytujú zníženie energetickej spotreby a vďaka algoritmu DOCSIS-PIE znižuje aj bufferbloat (jedná sa o latenciu a jitter v sieťach s prepínaním paketov spôsobených nadmerným ukladaním paketov do vyrovnávacej pamäte a taktiež môže spôsobiť aj zmeny oneskorenia paketov a znížiť celkovú priepustnosť siete).
DOCSIS 4.0: Zameriava sa na zvýšenie prenosovej rýchlosti dát s cieľom dosiahnuť rovnaké rýchlosti pre upstream a aj downstream a to až 10 Gbit/s. CableLabs

predstavil celú špecifikáciu v Októbri 2017. Táto technológia, ktorá bola predtým označovaná ako DOCSIS 3.1 FullDuplex, bola premenovaná na súčasť DOCSIS 4.0 [30]. Stále vo vývoji.

Tab. 8.1: Špecifikácie pre jednotlivé verzie DOCSIS [30]

Verzia	Prenosová rýchlosť Down-stream [Mb/s]	Prenosová rýchlosť Upstream [Mb/s]	Frekvenčný rozsah Down-stream [MHz]	Frekvenčný rozsah Upstream [MHz]	Šírka pásma Down stream [MHz]	Šírka pásma Upstream [MHz]
1.0	40	10	91-857	5-42	6	6,4
1.1	40	10	91-857	5-42	6	6,4
2.0	40	30	50-864	5-42	6	6,4
3.0	1 000	200	108-1002	5-85	8	6,4
3.1	10 000	1 000	258-1794	5-204	200	200
4.0	10 000	6 000	108-1794	5-684	1 800	679

Architektúra DOCSIS zahŕňa dva základné komponenty, a to káblový modem umiestnený v priestoroch zákazníka a koncový systém káblového modemu (CMTS - cable modem termination system) umiestnený v ústredni CATV (cable television). Počítač zákazníka a súvisiace periférne zariadenia sa označujú ako zariadenie v priestoroch zákazníka (CPE - customer-premises equipment). CPE sú pripojené ku káblovému modemu, ktorý je zasa pripojený prostredníctvom HFC siete k CMTS. CMTS potom smeruje prevádzku medzi HFC (Hybrid Fiber-Coaxial) a internetom. Pomocou systémov poskytovania a prostredníctvom CMTS vykonáva prevádzkovateľ káblovej siete kontrolu nad konfiguráciou káblového modemu.

DOCSIS definuje dve najnižšie vrstvy architektúry a to fyzickú a spojovú. Nad fyzickou vrstvou je podvrstva konvergencie, ktorá sa používa pre downstream. Tu sa dáta zapuzdrujú do rámca MPEG-2. Táto podvrstva taktiež podporuje digitálne televízne vysielanie v sieti HFC [29].

DOCSIS zahŕňa bezpečnostné služby vrstvy riadenia prístupu k médiám (MAC). DOCSIS 1.0 používal pôvodnú špecifikáciu BPI (Baseline Privacy Interface). BPI bol neskôr vylepšený vydaním špecifikácie Baseline Privacy Interface Plus (BPI+), ktorú používa DOCSIS 1.1 a 2.0. Najnovšie bolo do základného rozhrania pridaných niekoľko vylepšení ako súčasť DOCSIS 3.0 a špecifikácia bola premenovaná na SEC (Security) [29].

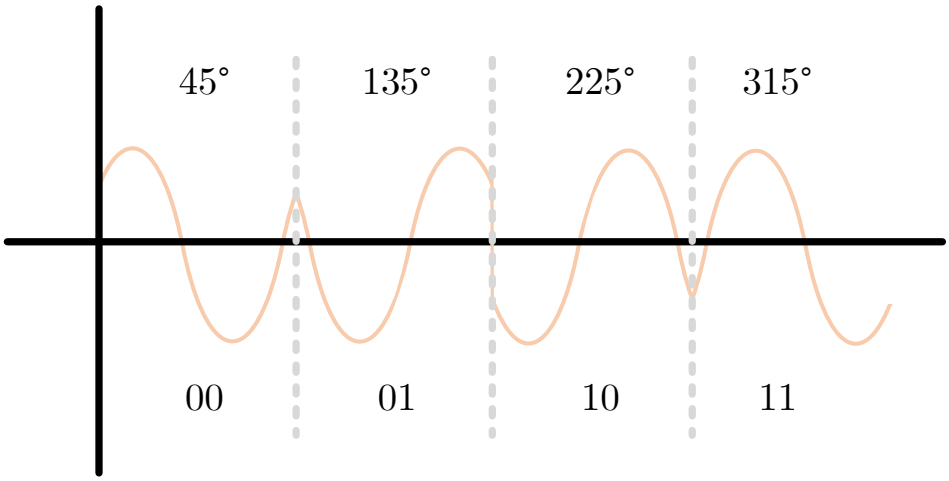
Vodafone v Českej republike používa pre svoje káblové internetové služby štandard DOCSIS 3.1. Tento štandard umožňuje využívať rýchlosti až do 1 Gbit/s pre downstream. DOCSIS 3.1 umožňuje využívanie OFDM (Ortogonal Frequency-Division Multiplexing), OFDMA (Ortogonal Frequency-Division Multiple Access) a SC-QAM (Single-Carrier Quadrature Amplitude Modulation), ktoré zvyšujú kapacitu a efektivitu prenosu dát v porovnaní so staršími technológiami. Pre dosiahnutie prenosových rýchlostí 1 Gbit/s (downstream) sú využívané typy kanálov (24 kanálov) SC-QAM s moduláciou 256QAM a dva typy kanálov OFDM s moduláciou 4096QAM. Pre dosiahnutie prenosových rýchlostí 100 Mbit/s (upstream) sú využívané typy kanálov (5 kanálov) SC-QAM s moduláciou 64QAM a dva typy kanálov OFDM s moduláciou 1024QAM.

Modulácie v DOCSIS

V komunikácii prostredníctvom káblových a telekomunikačných sietí zohrávajú kľúčovú úlohu modulačné techniky. Modulácia je proces, počas ktorého sa modifikujú vlastnosti nosnej vlny - amplitúda, frekvencia alebo fáza - tak, aby mohla efektívne niesť informáciu cez komunikačný kanál. Modemové zariadenie ako napríklad DAH100 využíva rôzne typy modulácií na prenos digitálnych dát cez analógové prenosové média, ako je koaxiálny kábel. V prípade DAH100 sú kľúčové modulačné techniky, ako je Quadrature Amplitude Modulation (QAM) a Quadrature Phase Shift Keying (QPSK). Novšie verzie (3.1 a 4.0) využívajú aj OFDM (Ortogonal Frequency-Division Multiplexing) a OFDMA (Ortogonal Frequency-Division Multiple Acces).

Quadrature Phase Shift Keying (QPSK) je modulačná technika často využívaná pre upstream, teda pre prenos dát od používateľa späť k centrálnej stanici. Jej robustnosť voči chybám z dôvodu šumu a iných prenosových problémov robí QPSK vhodnou pre situácie, kde je stabilita a spoľahlivosť prenosu dôležitejšia ako spektrálna efektívnosť. Napriek tomu, že QPSK neponúka takú vysokú spektrálnu efektívnosť ako QAM, je predsa len spoľahlivejšia v náročných podmienkach.

QPSK pracuje s dvoma nosnými vlnami - sínus a kosínus, ktoré sú vzájomne ortogonálne. Tento typ modulácie používa štyri bodové pozície v konštelačnom diagrame, umožňujúce prenos dvoch bitov (00, 01, 10 a 11) na jeden symbol [31]. V QPSK sa nosná mení z hľadiska fázy, nie frekvencie, a existujú štyri možné fázové posuny. Tieto štyri body reprezentujú štyri rozličné fázové hodnoty posunuté o 90°, teda 45°, 135°, 225° a 315° (obrázok 8.1). Tieto uhly sa dajú jednoducho generovať pomocou I/Q (In-phase/quadrature) modulačných techník, pretože sčítanie I a Q signálov, ktoré sú buď invertované alebo neinvertované, vedie k týmto štyrom fázovým posunom. Tabuľka 8.2 obsahuje spôsob fázových posunov.



Obr. 8.1: Modulácia QPSK [31]

Tab. 8.2: I/Q modulačná technika [31]

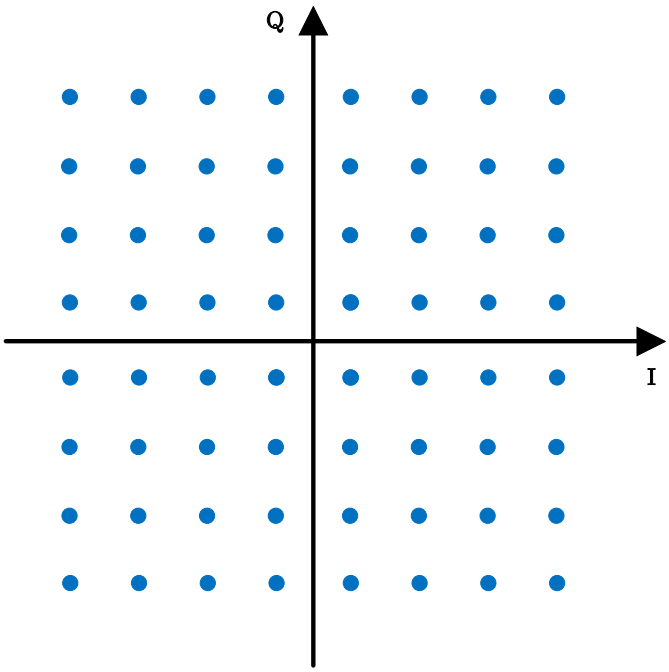
I	**Q**	**Fázový posun**
Neinvertovaný	Neinvertovaný	45°
Invertovaný	Neinvertovaný	135°
Invertovaný	Invertovaný	225°
Neinvertovaný	Invertovaný	315°

Použitie QPSK je predovšetkým rozšírené v vzostupnom smere, kde sa často kombinuje s 16QAM moduláciou, aby sa dosiahla lepšia efektívnosť v šumovom prostredí. Pridanie oboch nosných zložiek, sínus a kosínus, vedie k vytvoreniu výsledného signálu, ktorý je potom vysielaný z modemu do siete.

Quadrature Amplitude Modulation (QAM)je obzvlášť užitočná v káblových a širokopásmových sieťach, kde vysoká spektrálna efektívnosť umožňuje prenos veľkého množstva dát na jednotku šírky pásma. DAH100 používa QAM pre downstream, teda prenos dát z centrálnej stanice k užívateľovi, kde rôzne úrovne modulácie, ako 64QAM alebo 256QAM, môžu byť implementované v závislosti od kvality prenosového kanálu a požiadaviek na prenosovú rýchlosť. Modulácia využíva amplitúdové kľúčovanie na dve vzájomne ortogonálne nosné vlny, ktoré sú nezávislé a využívajú funkcie sínus a kosínus. Tento typ modulácie spája amplitúdovú a fázovú moduláciu, pričom kapacitu kanálu určuje frekvencia nosnej a pomer signál/šum. V súlade so štandardom DOCSIS sa pre downstream najčastejšie využíva moduláciu

cia 256-QAM pričom v najnovšej verzii štandardu je možné využiť až 4096QAM. Upstream obvykle využíva nižšie úrovne QAM kvôli väčšej náchylnosti použitého frekvenčného rozsahu k rušeniu.

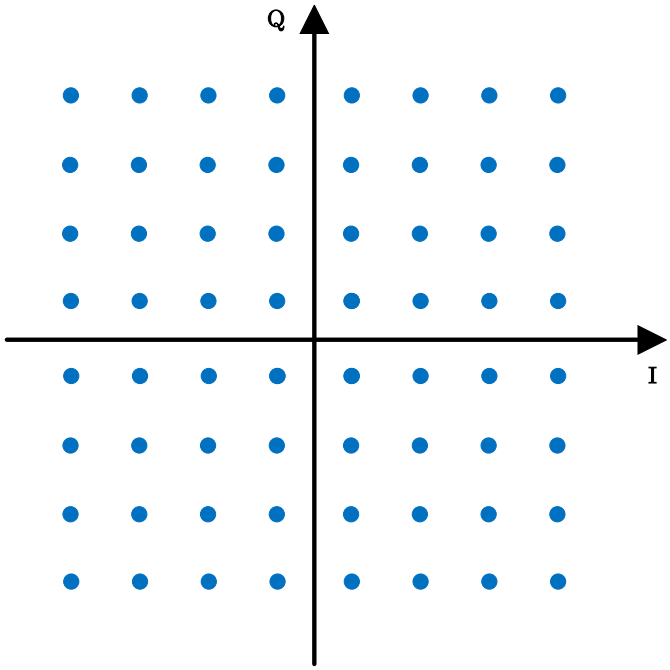
- **64QAM** Je jeden z typov kvadratúrnej modulácie (QAM), v ktorej nosná vlna s pevnou frekvenciou môže existovať v jednom zo šesťdesiatich štyroch rôznych diskrétnych a merateľných stavov v konštelačnej schéme. Konštelačný graf pozostáva z dvoch zložkových osí, a to z fázovej (os X) a kvadratúrnej (os Y). Tieto dve zložky sú navzájom ortogonálne alebo fázovo posunuté o 90°. Na obrázku 8.2 sa nachádza konštelačný diagram 64QAM. Každý symbol v 64QAM je stav konštelácie, ktorý obsahuje šesť bitov a každý symbol je jednou možnou kombináciou zo 64 rôznych stavov v rozsahu od **000 000** do **111 111** [32]. Pomocou 64-QAM je možné modulovať amplitúdu aj fázu nosnej vlny a prenášať relatívne väčší počet bitov, čím sa dosiahne vyššia bitová rýchlosť v porovnaní s inými modulmi QAM nižšieho rádu.



Obr. 8.2: Modulácia 64-QAM [32]

- **256QAM** Je ďalší z typov kvadratúrnej amplitúdovej modulácie (QAM), v ktorej môže nosná vlna konštantnej frekvencie existovať v jednom z 256 rôznych diskrétnych a merateľných stavov v konštelačnej schéme. Fázová aj kvadratúrna os modulovaného signálu sú taktiež navzájom ortogonálne (fázovo posunuté o 90°). Na obrázku 8.3 sa nachádza konštelačný diagram 256QAM.

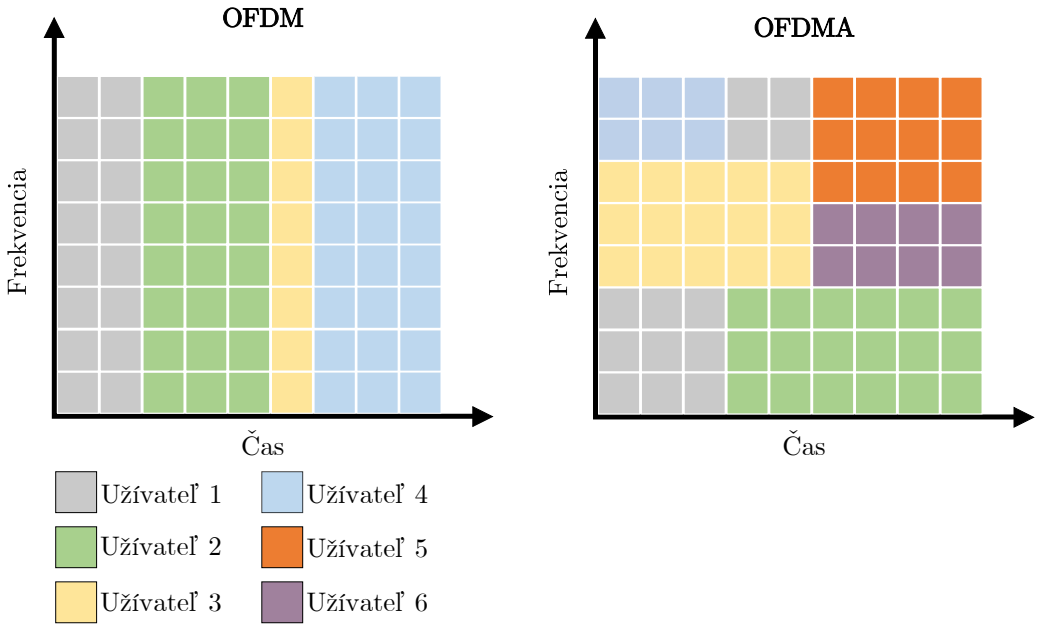
Každý symbol v 256QAM je stav konštelácie, ktorý obsahuje osem bitov a každý symbol je jednou možnou kombináciou z 256 rôznych stavov v rozsahu od **0000 0000** do **1111 1111** [33]. Keďže táto modulačná schéma používa na prevádzku binárne dáta, celkový počet možných kombinácií pre 8 bitov je 256. Počet bitov možno vypočítať v zmysle logaritmickej hodnoty ako (1/6 bitovej rýchlosti). Pomocou 256QAM je možné modulovať amplitúdu aj fázu nosnej vlny a prenášať väčší počet bitov, čo vedie k vyššej bitovej rýchlosti v porovnaní s inými QAM nižšieho rádu, ako je napríklad 64QAM.



Obr. 8.3: Modulácia 256-QAM [33]

- **Ortogonal Frequency-Division Multiple Acces (OFDMA)** je technika multiplexovania a prístupová metóda, ktorá umožňuje efektívne využitie spektra v bezdrôtových a káblových komunikačných systémoch. Je kľúčovou komponentnou v moderných komunikačných štandardoch ako je napríklad LTE (Long Term Evolution) a DOCSIS 3.1. Rozdeľuje dostupný kanál na menšie čiastkové pásma alebo čiastkové nosné frekvencie. Tieto čiastkové pásma sa označujú ako zdrojové jednotky (RU) a každá zdrojová jednotka je priradená individuálnemu užívateľovi klienta, čím sa umožňuje prístupovým bodom (AP) využívať RU na súčasné obsluhovanie viacerých užívateľov [34].
  V OFDM, sa každý signál alebo dátový rámec od používateľa prenáša sekvenčne, takže ostatní používatelia musia čakať, kým aktuálny používateľ do-

končí prenos všetkých OFDM symbolov. OFDMA umožňuje prístupovým bodom komunikovať s viacerými používateľmi ich optimálnym priradením ku konkrétnym RU v závislosti od potrebnej šírky pásma, veľkosti dát a stavu kanála. Rozdelením kanála a priradením týchto RU viacerým užívateľom sa môže súčasne prenášať viacero dátových rámcov. Podobne ako pri OFDM je dostupný kanál rozdelený na viacero čiastkových nosných, pričom každá čiastková nosná je navzájom ortogonálna (ostatných čiastkových nosných sa bude zhodovať s vrcholom ktorejkoľvek čiastkovej nosnej). Princíp a rozdiel medzi OFDM a OFDMA je zobrazený na obrázku 8.4. OFDMA zabezpečuje, že používatelia môžu súčasne prenášať dátové rámce. Medzi rôznymi používateľmi vysielajúcimi na rôznych čiastkových nosných frekvenciách teda nedochádza k žiadnemu presluchu.



Obr. 8.4: Modulácia 256-QAM [35]

Typy modulácii pre jednotlivé verzie downstreamu

- Všetky verzie pred verziou 3.1 špecifikujú 64 alebo 256 úrovňovú QAM.
- DOCSIS 3.1 pridáva 16, 128, 512, 1024, 2048 a 4096QAM.
- DOSCIS 4.0 pokračuje v používaní modulácie QAM ako je 4096-QAM a vyššie aby sa využila zvýšená šírka pásma a zlepšila sa tak celková prenosová rýchlosť dát.

Typy modulácii pre jednotlivé verzie upstreamu

- DOCSIS 1.x využíva modulácie QPSK alebo 16-QAM.
- DOCSIS 2.0 a 3.0 využíva QPSK a 8, 16, 32, 64-QAM.
- DOCSIS 2.0 a 3.0 podporuje mriežkovú kódovú moduláciu 128-QAM v režime S-CDMA.
- DOCSIS 3.1 podporuje modulácie od QPSK až po 1024-QAM, s voliteľnou podporou pre 2048 a 4096-QAM.
- DOSCIS 4.0 bude podporovať pokročilejšie modulácie QAM ako je 4096-QAM aby sa zlepšila celková prenosová rýchlosť dát. Dôležité to je pre full duplex operácie, ktoré umožňujú súčasne vysielanie a prijímanie dát.

8.2.3 CMTS

CMTS sa väčšinou nachádza v hlavnej stanici prevádzkovateľa CATV. Existuje viacero typov zariadení CMTS, ktoré disponujú jedným downstreamovým výstupom a jedným upstreamovým vstupom, ktoré sú určené pre pripojenie stoviek modemov. Existujú aj väčšie modulárne CMTS, ktoré sú určené pre pripojenie až desiatok tisíc modemov. Tieto väčšie CMTS možno osadiť rôznymi modulmi a sú navrhnuté tak, aby zvládli redundantné fungovanie v prípade poruchy niektorého z modulov. Hlavnou úlohou CMTS je modulácia signálu zo vstupného rozhrania (Ethernet) na výstupné (downstream) rozhranie reprezentované koaxiálnym výstupom. Upstream je opačný proces, pri ktorom dochádza k demodulácii signálu z koaxiálneho rozhrania a signál je ďalej odosielaný na Ethernet rozhranie.

Pre riadenie siete CMTS sa používa protokol SNMP (Simple Network Management Protocol) na správu siete [29]. Tento protokol prináša množstvo informácií o celkovej sieti. Každý modem má svoju unikátnu MAC adresu, podľa ktorej sú vedené údaje v CMTS a ak sa do siete pripojí modem, ktorý nie je registrovaný v CMTS, nemôže tento modem v sieti komunikovať. K nastaveniam CMTS sa dá pristupovať dvoma spôsobmi a to buď cez USB (Universal Serial Bus) port pre pripojenie do konzoly a konfiguráciu zariadenia priamo v konzole, alebo druhým spôsobom, použitím WEB UI, graficky spracovaného rozhrania, ktoré umožňuje sledovať grafické zaťaženie kanálov. Pri základnej konfigurácii je dôležité dbať na typ modulácie, frekvenčné pásmo, registráciu modemov a nastavenie konfiguračného súboru pre modem.

DOCSIS ACCESS HUB

Teleste DAH100, známy tiež ako DOCSIS Access Hub, predstavuje mini-CMTS (Cable Modem Termination System) zariadenie navrhnuté na rozšírenie vysokorých-

lostných širokopásmových pripojení a vysielania televíznych programov k zákazníkom prostredníctvom existujúcich dvojsmerných koaxiálnych sietí [36].

DAH100 ponúka riešenie pre širokopásmové pripojenie, ktoré je nielen nákladovo efektívne, ale aj rýchlo implementovateľné, využívajúc existujúce koaxiálne káble na doručovanie dátových, IPTV a OTT (Over The Top) služieb koncovým používateľom. Toto zariadenie je kompatibilné s DOCSIS 2.0 a 3.0 káblovými modemami a je schopné podporovať až 200 odberateľov. Jeho typické využitie nájdeme v sieťach FTTB/C (Fiber To The Building/Curb) [36].

Na obrázku 8.5 je možné vidieť DOCSIS Acces Hub100 bez vrchného krytu. Konfigurácia tohoto zariadenia je možná pomocou USB portu alebo predom nastaveným manažovateľným webovým rozhraním. DAH100 disponuje dvoma Ethernet portmi, ktoré slúžia k pripojeniu do internetu. Zariadenie obsahuje taktiež dva koaxiálne porty. Jeden je určený pre upstream a disponuje 4 kanálmi. Druhý je určený pre downstream a poskytuje až 16 kanálov.

Obr. 8.5: DOCSIS Access Hub 100 [37]

Kľúčové funkcie a parametre

- Integrovaný DHCP (Dynamic Host Configuration Protocol) server: DAH100 funguje ako samostatné zariadenie, ktoré nevyžaduje externý PC server na poskytovanie káblových modemov. Táto funkcia zjednodušuje implementáciu a správu zariadenia.
- Vysoká kapacita a modulácia: Zariadenie podporuje 16 downstream a 4 upstream kanály s podporovanými downstream moduláciami 64, 256 a 1024-QAM a upstream moduláciami QPSK alebo 16, 64 a 256-QAM. Toto umožňuje kapacitu až 960 Mbit/s downstream a 160 Mbit/s upstream, čo zabezpečuje vysokorýchlostné pripojenie pre koncových používateľov.
- Úspora nákladov a rýchla implementácia: Vďaka využitiu existujúcej koaxiálnej infraštruktúry umožňuje DAH100 poskytovateľom služieb rýchlo a s výrazne nižšími nákladmi rozšíriť širokopásmové služby.

8.2.4 Káblový modem

Káblový modem je zariadenie, ktoré sa primárne stará o demoduláciu analógového signálu na digitálny a o moduláciu digitálneho signálu na analógový. Pracuje hlavne na prvej a druhej vrstve OSI modelu. Modem sa obvykle používa ako externé zariadenie, avšak existuje aj možnosť mať modem v podobe PCI karty. Smerom k počítaču sa využíva rozhranie Ethernet a smerom k CMTS koaxiálne rozhranie. Na konfiguráciu zariadenia je možné použiť USB rozhranie alebo Ethernet rozhranie.

Cisco EPC3925

Domáca brána Cisco model DPC3925 predstavuje pokročilé riešenie pre používateľov hľadajúcich kombináciu vysoko rýchlostného internetového a kvalitného digitálneho telefónneho pripojenia. Kompatibilná s normami DOCSIS 3.0 a EuroPacketCable. Toto zariadenie poskytuje robustné širokopásmové pripojenie a podporuje súčasný prístup k dátovým a hlasovým službám bez potreby zásahu do domácej infraštruktúry [40].

Obr. 8.6: Cisco Modem EPC3925 [40]

Na obrázku 8.6 je vidieť káblový modem Cisco EPC3925. Káblový modem disponuje integrovaným digitálnym hlasovým adaptérom a štyrmi ethernetovými portami 1000/100/10BASE-T pre pripojenie k lokálnej sieti, ponúka aj bezdrôtové pripojenie vďaka štandardu 802.11n, čo umožňuje flexibilitu umiestnenia bez nutnosti káblovej inštalácie. Okrem toho modem zahŕňa funkcie WPS pre jednoduché a bezpečné nastavenie bezdrôtovej siete a pokročilé bezpečnostné prvky ako firewall, ktorý identifikuje a chráni domácu sieť pred neoprávneným prístupom.

8.2.5 Inicializácia a vzájomná závislosť systémov

V momente keď sa káblový modem prvý krát pripojí ku CMTS, tak medzi ním a jeho CMTS prebehne 8 krokov inicializácie. Modem nevie o prítomnosti iných modemov, vie len o CMTS ku ktorej je pripojený. Postupnosť inicializácie káblového modemu je nasledovná [41].

- **Synchronizácia downstreamu**
  Káblový modem začne skenovať 6 MHz downstream video kanál pre signál CMTS. Ak bol modem už použitý tak sa po dočasnom zlyhaní (napríklad vypnutí) jednoducho reštartuje. Modem sa najprv pokúsi zablokovať signál CMTS na poslednom použitom downstreamovom kanáli. Pokračuje v skenovaní, kým nenájde signál, ktorý dokáže správne rozpoznať a synchronizovať.
- **Získanie upstream parametrov**
  CMTS pravidelne prenáša správy **UDC** (deskriptory upstream kanálov) na všetkých downstreamových kanáloch. UCD popisujú správne parametre, ktoré musí modem použiť na prenos na rôznych upstream kanáloch. Keď modem prijme UCD s parametrami pre kanál, ktorý môže použiť, uloží tieto informácie a použije ich na určenie vysielacích parametrov pre budúce upstream prenosy. Rovnako ako UCD, CMTS pravidelne vysiela správy **SYNC**. Tieto správy umožňujú modemu správnu synchronizáciu s CMTS a ostatnými modemami v sieti. Na obrázku 8.7 je skrátený výpis UCD správy.

Downstream MAC type = UCD
MAC FC (HEX) = C2
MAC LEN (HEX) = 016A
Upstream Channel ID (HEX) = 01
Config. Change Count = 3
Mini-Slot Size = 64
Downstream Channel ID (HEX) = 0B
Symbol Rate = 160000 symbols/sec
Upstream Frequency = 26750000 Hz
Preamble Pattern = CC CC CC CC CC CC 0D 0D
Burst Descriptor = Request
IUC = 1
Modulation Type = 16QAM
Scrambler = ON
Burst Descriptor = Initial Maintenance
IUC = 3
Modulation Type = QPSK
Preamble Pattern = CC CC CC CC CC CC 0D 0D
Burst Descriptor = Station Maintenance
IUC = 4
Modulation Type = QPSK
Preamble Pattern = CC CC CC CC CC CC 0D 0D
Burst Descriptor = Short Data Grant
IUC = 5
Modulation Type = 16QAM
Preamble Pattern = F3 F3 F3 F3 33 F7
Burst Descriptor = Long Data Grant
IUC = 6
Modulation Type = 16QAM
Preamble Pattern = F3 F3 F3 F3 F3 33 F7

Obr. 8.7: Zjednodušený výpis správy UDC [42]

Popis základných parametrov

- **MAC LEN (Dĺžka MAC rámca)**: Udáva veľkosť správy v hexadecimálnom formáte.
- **Upstream Channel ID (ID upstream kanálu)**: Identifikuje konkrétny upstream kanál.
- **Config. Change Count (Počet zmien konfigurácie)**: Indikuje, koľkokrát bola konfigurácia zmenená.
- **Mini-Slot Size (Veľkosť mini-slotu)**: Používa sa na časovanie prenosov.
- **Downstream Channel ID (ID downstream kanálu)**: Identifikuje konkrétny downstream kanál.
- **Symbol Rate (Symbolová rýchlosť)**: Počet symbolov prenesených za

sekundu.
  - **Upstream Frequency (Upstream frekvencia)**: Frekvencia upstream kanálu v hertzoch.
  - **Preamble Pattern (Vzor preambuly)**: Používa sa na synchronizáciu prenosov.
  - **Burst Descriptor (Typ burstu)**: Definuje konfiguráciu burstu pre prenosové okno.
  - **Modulation Type (Modulácia)**: Určuje typ modulácie pre prenos (napr. QPSK, 16QAM).
  - **Scrambler**: Indikuje, či je scrambler zapnutý.
- **Synchronizácia a riadenie časovania v DOCSIS sieťach**
  V rámci káblových sietí DOCSIS, CM a CMTS musia efektívne spolupracovať, aby bola zabezpečená správna komunikácia a distribúcia dát. Každý modem si musí udržiavať synchronizáciu nielen s hodinami CMTS, ale aj s prenosovým oneskorením, aby sa predišlo prekrývaniu dátových prenosov. CMTS pridelením časových intervalov, tzv. minislotov, riadi, kedy môže ktorý modem vysielať, čím znižuje možnosť kolízie dát na linke. Konfliktné a nekonfliktné minisloty umožňujú efektívne riadenie prenosov podľa aktuálnej sieťovej záťaže. Periodické merania a úpravy prevádzkových parametrov, ako sú vysielací výkon alebo frekvencia, zabezpečujú, že všetky modemy na linke zostanú správne zarovnané a efektívne fungujúce.
- **Vytvorenie IP pripojenia**
  V momente keď sú parametre prenosu správne nastavené, CM by mal byť schopný správne komunikovať s CMTS. Teraz sa odošle požiadavka na „objavenie“ protokolu **DHCP**. Ako odpoveď DHCP server poskytne modemu pridelenú IP adresu, ako aj adresu iného DHCP servera, ktorý môže poskytnúť modemu viac parametrov. Počiatočná odpoveď DHCP obsahuje aj názov súboru, ktorý obsahuje ďalšie konfiguračné parametre špecifické pre sieť pre CM.
- **Synchronizácia času dňa**
  CM a CMTS musia zdieľať spoločnú predstavu o približnom čase dňa, ktorý možno použiť na zaznamenávanie abnormálnych udalostí.
- **Prenos prevádzkových parametrov**
  CM stiahne konfiguračný súbor, ktorého názov poskytol pôvodný server DHCP. Toto sťahovanie používa protokol TFTP (Trivial File Transfer Protocol). Tento jednoduchý protokol je používaný na prenos súborov medzi klientom a serverom v sieti. TFTP je jednoduchší a má menej funkcií než protokol FTP (File Transfer Protocol). Prevádzkové parametre prepisujú všetky predvolené hodnoty nakonfigurované v modeme počas výroby.

V konfiguračnom súbore môže byť prítomný veľký počet parametrov, ako sú frekvencie a prenosové rýchlosti kanálov upstream a downstream, ako aj adresy rôznych sieťových serverov, hodnoty časovačov atď.

- **Registrácia**
  Keď modem získa a spracuje konfiguračný súbor, informuje svoj CMTS o hodnotách svojich prevádzkových parametrov v správe so žiadosťou o registráciu.
- **Inicializácia Baseline Privacy Plus** Je to jedna z dôležitých požiadaviek na káblovú prístupovú sieť, pretože existuje aspoň teoretická možnosť, že sused môže odpočúvať komunikáciu medzi CM a CMTS. Aby sa vytvorilo bezpečnostné priradenie, modem teraz inicializuje svoju konfiguráciu Baseline Privacy Plus (BPI+), ktorá efektívne zabezpečuje spojenie pred náhodnými odpočúvaním. Po správnej inicializácii BPI+ je modem súčasťou siete.

8.2.6 Software Excentis pre úpravu konfiguračných súborov

Excentis Cable Modem Config File Editor je softvér navrhnutý na vytváranie a úpravu konfiguračných súborov pre káblové modemy podľa štandardov DOCSIS. Tento editor je obľúbený pre jeho grafické rozhranie (GUI), ktoré umožňuje technikom a sieťovým administrátorom ľahko nastavovať potrebné parametre bez potreby hlbokých technických znalostí špecifikácií DOCSIS.

Kľúčové Vlastnosti

- Editor podporuje rôzne verzie DOCSIS (1.0, 1.1, 2.0, 3.0, a 3.1), čo umožňuje široké využitie naprieč rôznymi generáciami technológie.
- TLV (Type-Length-Value) formát je základ pre DOCSIS konfiguračné súbory, kde každý parameter je definovaný svojim typom, dĺžkou a hodnotou. Editor poskytuje jednoduchý spôsob, ako tieto hodnoty nastaviť.
- Program umožňuje nielen úpravu a tvorbu súborov, ale tiež ich testovanie a validáciu, čo zaisťuje, že konfigurácie budú správne fungovať v reálnych sieťových podmienkach.

Konfiguračný súbor obsahuje špecifikácie pre nastavenie rôznych parametrov modemu, ktoré riadia jeho správanie v sieti. Tieto parametre zahŕňajú:

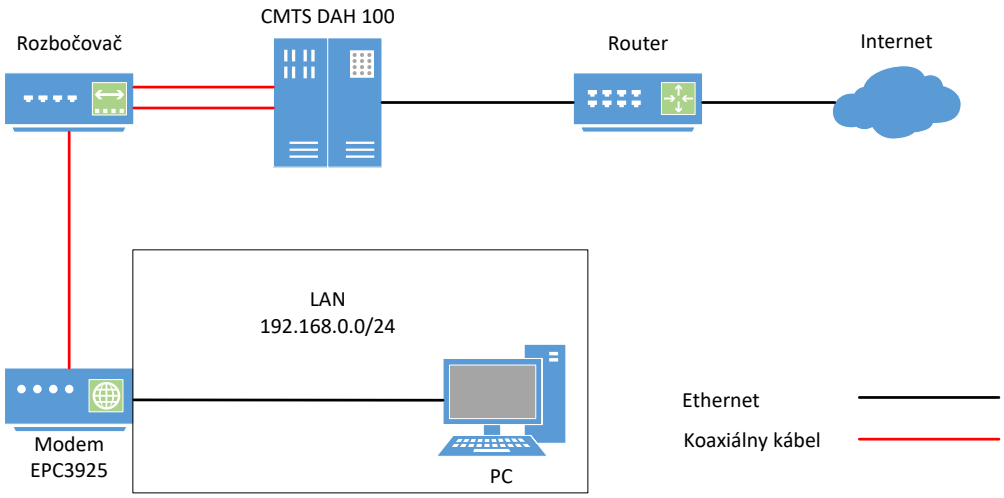
- Rýchlosti prenosu dát (Upstream a Downstream Maximum Sustained Traffic Rate).
- Kvalitu služby (Quality of Service).
- Kontrolu prístupu do siete (Network Access Control).
- Bezpečnostné nastavenia.
- Parametre pre správu a monitorovanie siete.

8.3 Pracovný postup

8.3.1 Vybavenie pracoviska

- CMTS DAH100
- Cisco modem EPC3925
- PC (využité pre webové rozhranie na konfiguráciu DAH100 a následnom teste úspešného pripojenia na internet)
- Rozbočovač FV 9
- Koaxiálny kábel RG-6
- Ethernetový kábel

8.3.2 Schéma zapojenia

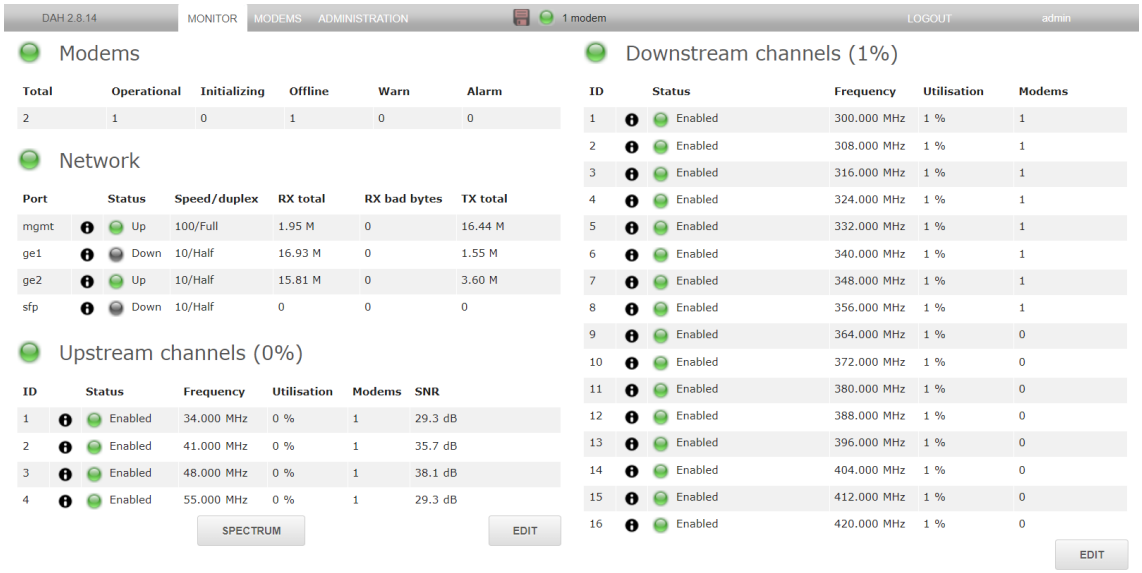


Obr. 8.8: Schéma zapojenia systému DOCSIS

Na obrázku 8.8 je možné vidieť zapojenie DAH100 s káblovým modemom (Cisco EPC3925). Nakoľko DAH100 obsahuje dva vstupy/výstupy, kde každý z nich je učený buď pre upstream alebo downstream, je potrebné tieto dva signály prepojiť do jedného toku. Pre toto prepojenie je použitý rozbočovač, ktorý následne vedie toto zlúčenie signálov do vstupu káblového modemu. Prenosovým médiom medzi DAH100 a káblovým modemom je koaxiálny káble RG-6 s príslušnými konektormi typu F. Prepoj medzi káblovým modemom a samotným počítačom je pomocou UTP káblu.

8.3.3 Konfigurácia DAH100 a káblového modemu

Zapnite prehliadač na počítači a do vyhľadávania zadajte IP adresu **10.0.0.80** (Manažovatelná adresa DAH100). Táto adresa bola predom nastavená ako manažovatelná, aby bolo možné pristupovať ku konfigurácií DAH100 pomocou webového rozhrania. V inom prípade by bolo potrebné konfigurovať zariadenie v terminály pripojením pomocou USB portu a Putty. Po zadaní tejto IP adresy sa otvorí webové rozhranie DAH100 ako je zobrazené na obrázku 8.9. Potrebné je ešte zadať prihlasovacie meno a heslo. Tieto údaje Vám poskytne vyučujúci.



Obr. 8.9: Webové rozhranie DAH100

Hlavné okno webového rozhrania slúži na správu káblových modemov a sieťovej prevádzky. Rozhranie poskytuje rôzne informácie a možnosti konfigurácie pre downstream aj upstream kanály. Nižšie sú uvedené rozbory jednotlivých častí okna.

Modems

- Total: Určuje celkový počet modemov pripojených k systému.
- Operational: Počet modemov, ktoré sú aktuálne funkčné a online.
- Initializing: Počet modemov, ktoré sú vo fáze inicializácie.
- Offline: Počet modemov, ktoré sú offline.

Network

- Port: Zobrazuje stav jednotlivých portov (mgmt, ge1, ge2, sfp).
  - mgmt: Manažment port je nastavený na rýchlosť 100 Mbit/s a full duplex.
  - ge1 a ge2: Gigabit Ethernet porty, oba nastavené na rýchlosť 10 Mbit/s a half duplex. `ge1` je v stave „down", zatiaľ čo `ge2` je „up".

– sfp: Port pre optický modul, ktorý je vypnutý.

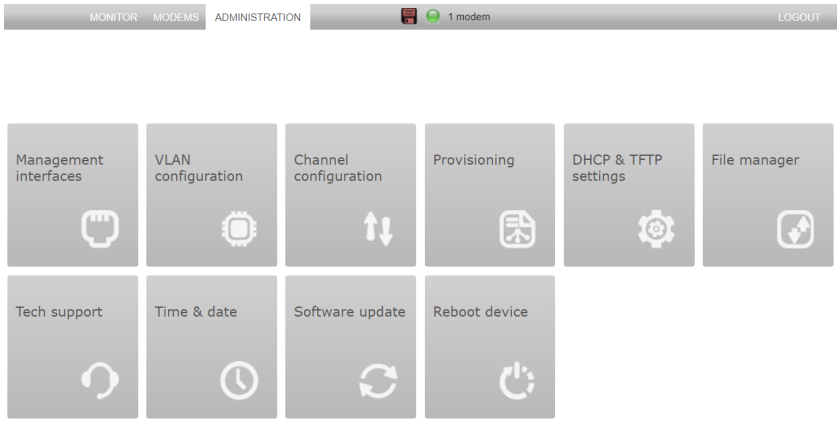
Downstream channels

- Frequency: Frekvencie jednotlivých downstream kanálov.
- Utilisation: Využitie kapacity kanálu v percentách.
- Modems: Počet modemov, ktoré sú pripojené na daný kanál.
- SNR (Signal to Noise Ratio): Pomer signálu k šumu, čo je dôležitý ukazovateľ kvality signálu na danom kanáli.

Upstream channels

- Frequency: Frekvencie jednotlivých upstream kanálov.
- Utilisation: Využitie kapacity kanálu.
- Modems: Počet modemov, ktoré používajú daný upstream kanál.
- SNR (Signal to Noise Ratio): Pomer signálu k šumu.

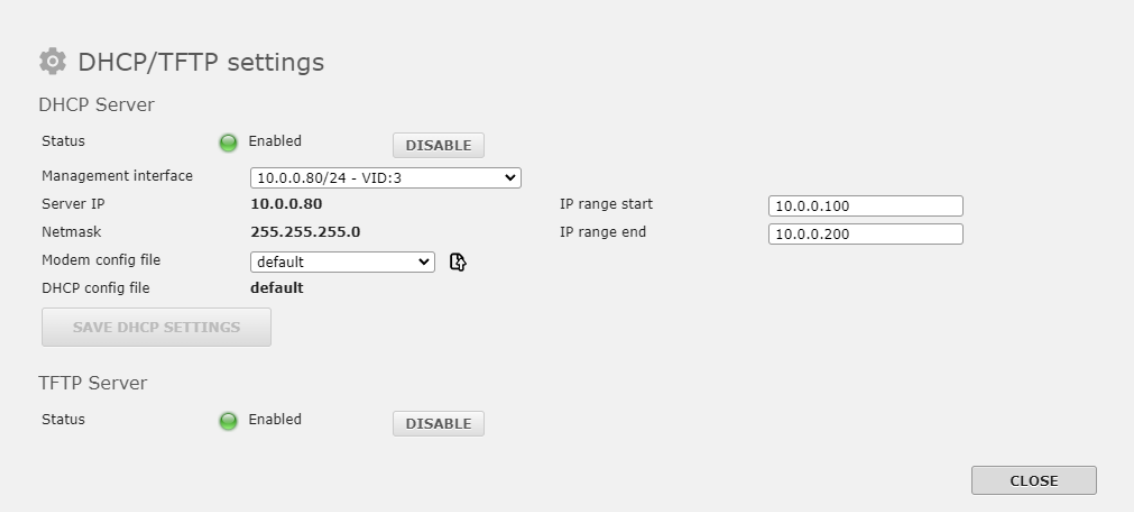
Obrázok 8.10 zobrazuje všetky druhy služieb, ktorými je možné DAH100 konfigurovať.



Obr. 8.10: Administratívne služby webového rozhrania

Presuňte sa do **ADMINISTRATION-> DHCP & TFTP settings** ako je zobrazené na obrázku 8.11. DHCP (Dynamic Host Configuration Protocol) server je povolený, čo znamená, že automaticky prideľuje IP adresy zariadeniam v sieti. **Management Interface** určuje IP adresu a subnetovú maska pre rozhranie, cez ktoré DHCP server komunikuje. **VID:3** určuje, že táto adresa je priradená k VLAN s ID 3. **Server IP** je IP adresa DHCP servera, ktorá sa používa ako zdroj pre DHCP komunikáciu. **Modem Config File** obsahuje konfiguračný súbor použitý pre modemy. Tomuto konfiguračnému súboru sa neskôr venuje laboratórna úloha. **IP Range Start** určuje začiatok rozsahu IP adries, ktoré môže DHCP server prideliť a **IP Range End** určuje koniec rozsahu IP adries, ktoré môže DHCP server

prideliť. DHCP server automaticky prideľuje IP adresy a ďalšie sieťové konfigurácie zariadeniam pripojeným do siete, čo eliminuje potrebu manuálneho nastavenia týchto parametrov na každom zariadení. Rozsah IP adries, ktorý je nastavený medzi 10.0.0.100 a 10.0.0.200, určuje, ktoré adresy môže server jednotlivým zariadeniam prideliť.



Obr. 8.11: Nastavenie DHCP pre DAH100

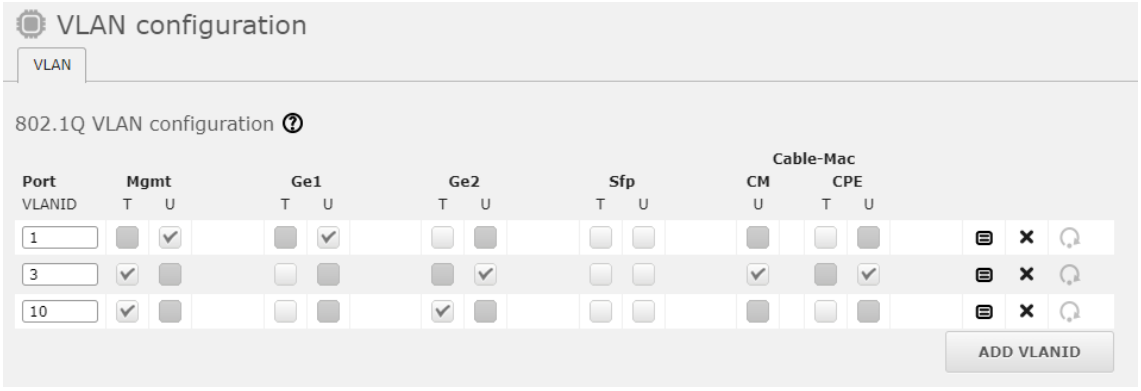
Presuňte sa do **ADMINISTRATION-> VLAN configuration** ako je zobrazené na obrázku 9.11. Toto rozhranie slúži na konfiguráciu VLAN (Virtual Local Area Network) na zariadení, ktoré používa štandard 802.1Q pre VLAN tagging. Nastavenie VLAN umožňuje oddeliť rôzne typy sieťovej prevádzky a zabezpečiť lepšiu organizáciu a zabezpečenie siete. Napríklad, VLAN 3 môže byť určená pre špecifickú skupinu zariadení alebo pre konkrétny typ komunikácie v rámci siete. Na obrázku 8.12 sú zobrazené rôzne porty, ktoré môžu byť nakonfigurované pre príslušné VLAN. Tieto porty zahŕňajú:

- Mgmt (Management)
- Ge1 (Gigabit Ethernet 1)
- Ge2 (Gigabit Ethernet 2)
- Sfp (Small Form-factor Pluggable)
- Cable-Mac (CM - Cable Modem)
- CPE (Customer Premises Equipment)

T (Tagged) označuje, že porty budú značiť (tagovať) rámce s VLAN ID, teda komunikácia cez tento port bude obsahovať informáciu o VLAN 3.

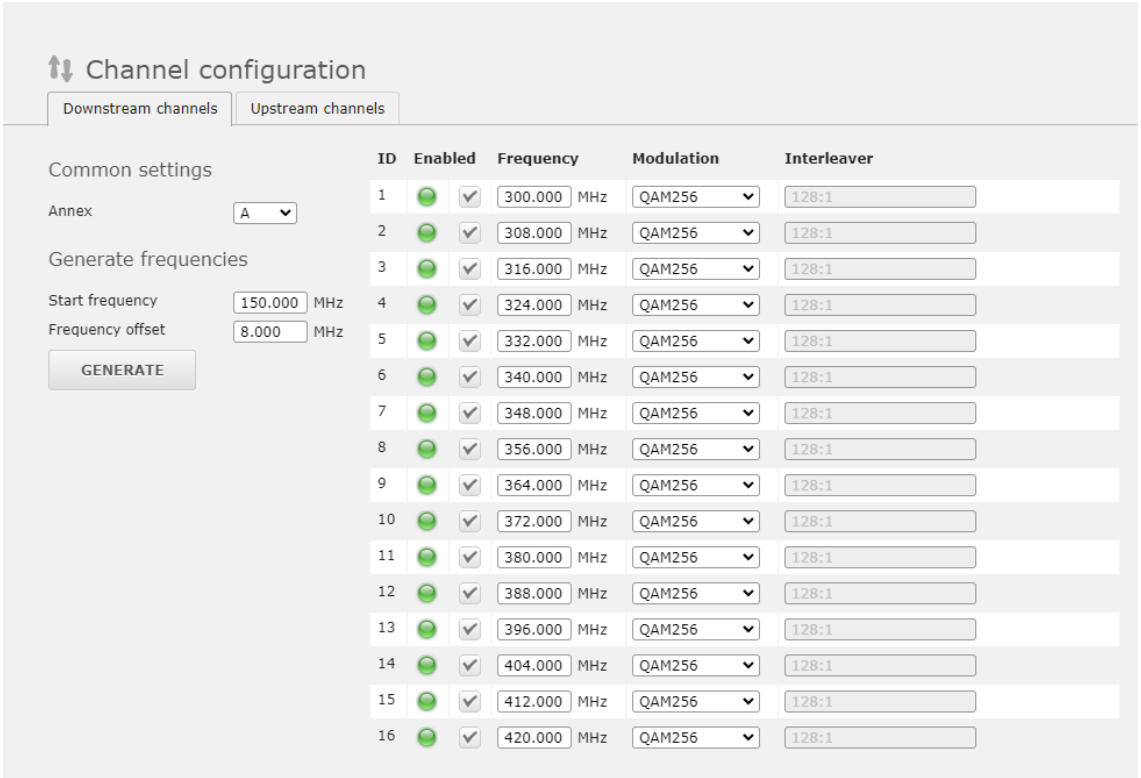
U (Untagged) označuje, že porty budú posielať rámce bez VLAN značenia (tagovania), čo znamená, že prichádzajúce rámce bez tagu budú priradené do tejto

VLAN.

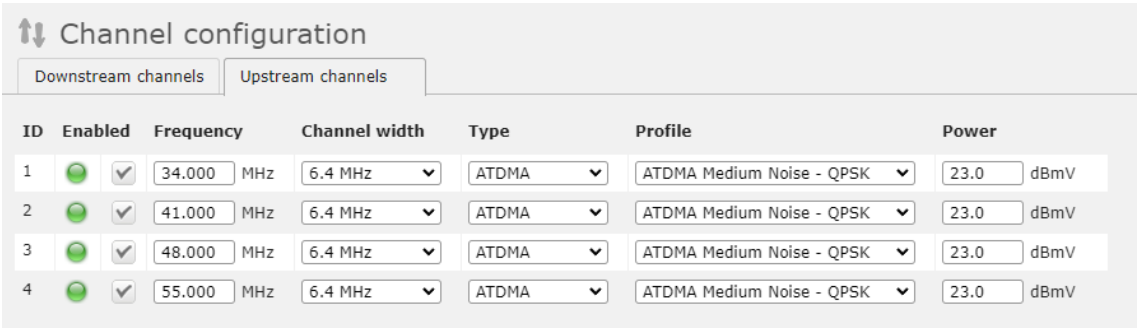


Obr. 8.12: Nastavenie VLAN pre DAH100

Presuňte sa do **ADMINISTRATION-> Channel configuration**. Na obrázku 8.13 je možné vidieť konfiguráciu kanálov pre downstream a na obrázku 8.14 konfiguráciu pre upstream kanály. Uistite sa, že je zariadenie nakonfigurované rovnako pre upstream a downstream ako na obrázkoch ako na obrázkoch 8.13 a 8.14.



Obr. 8.13: Nastavenie downstream kanálov pre DAH100



Obr. 8.14: Nastavenie upstream kanálov pre DAH100

Rozbor konfigurácie pre downstream kanály

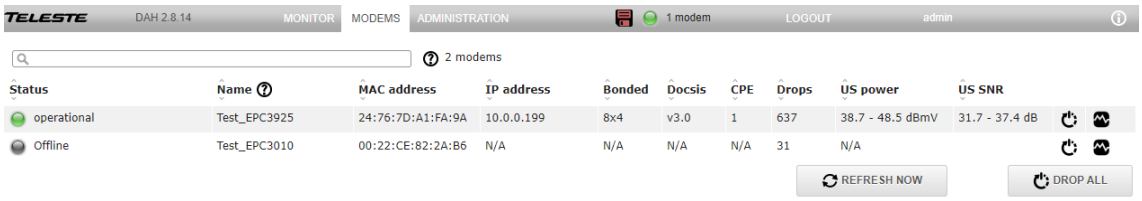
- Annex: Umožňuje vybrať špecifikáciu Annex, ktorá sa použije pre moduláciu signálov. Annexy sa líšia v závislosti od geografickej oblasti a špecifík štandardu, ako napríklad Annex A (Európa) a B (USA)
- Start Frequency: Nastavuje začiatočnú frekvenciu pre generovanie kanálov. Toto je základná frekvencia, od ktorej sa odvíja frekvenčné spektrum pre downstream kanály.
- Frequency Offset: Definuje frekvenčný posun medzi jednotlivými kanálmi. Toto je hodnota, ktorá sa pridáva k začiatočnej frekvencii na vytvorenie frekvencie pre nasledujúci kanál.
- Enabled: Ukazuje, či je kanál povolený. Štvorcové políčko umožňuje administrátorovi zapnúť alebo vypnúť konkrétny kanál.
- Frequency: Frekvencia, na ktorej kanál operuje. Každý kanál môže operovať na inej frekvencii, čo umožňuje paralelnú distribúciu dát.
- Modulation: Typ modulácie použitej na danom kanáli. QAM256 (Quadrature Amplitude Modulation) je bežne používaný typ pre káblovú televíziu a internet, pretože umožňuje vysokú hustotu dát na kanál.

Rozbor konfigurácie pre upstream kanály

- Enabled: Ukazuje, či je kanál povolený. Štvorcové políčko umožňuje administrátorovi zapnúť alebo vypnúť konkrétny kanál.
- Frequency: Určuje frekvenciu, na ktorej každý upstream kanál operuje. Tieto hodnoty sú vyjadrené v MHz (Megahertz) a určujú, na ktorej frekvencii je kanál nastavený pre odosielanie dát.
- Channel Width: Šírka kanálu, vyjadrená v MHz, určuje šírku pásma, ktoré je dostupné pre prenos dát na tomto kanáli. Tu sú všetky kanály nastavené na 6.4 MHz.
- Type: Typ modulácie použitej na danom kanáli. V tomto prípade je pre každý

kanál použitý ATDMA (Advanced Time Division Multiple Access), čo je metóda umožňujúca efektívnejšiu distribúciu dostupného časového slotu a pásma.
- Profile: Profil modulácie určuje, ako sú dáta modulované a odosielané. Tu je pre každý kanál použitý profil ATDMA Medium Noise - 64QAM. Toto označenie naznačuje, že profil je navrhnutý tak, aby efektívne fungoval aj v prostrediach s strednou úrovňou šumu.
- Power: Výkon odosielaného signálu, vyjadrený v dBmV (decibel-millivolts). Hodnota 23.0 dBmV pre každý kanál ukazuje, aká sila signálu je použitá pre odosielanie dát.

Presuňte sa do **MODEMS**, ako je zobrazené na obrázku 8.15. Na obrázku je možné vidieť informácie o dvoch káblových modemoch v sieti. Každý riadok poskytuje detailné informácie o stave, konfigurácii a výkonnosti každého modemu. Tlačidlo **DROP ALL** slúži k reštartovaniu káblových modemov a k opätovnej re-inicializácií modemov.



Obr. 8.15: Prehľad všetkých pripojených káblových modemov ku DAH100

Pre podrobnejší opis pripojeného modelu so všetkými potrebnými informáciami je potrebné kliknúť na ikonku statusu modemu (obrázok 8.16). Po kliknutí na ikonku sa otvorí okno s prehľadným popisom daného káblového modemu (obrázok 8.17).

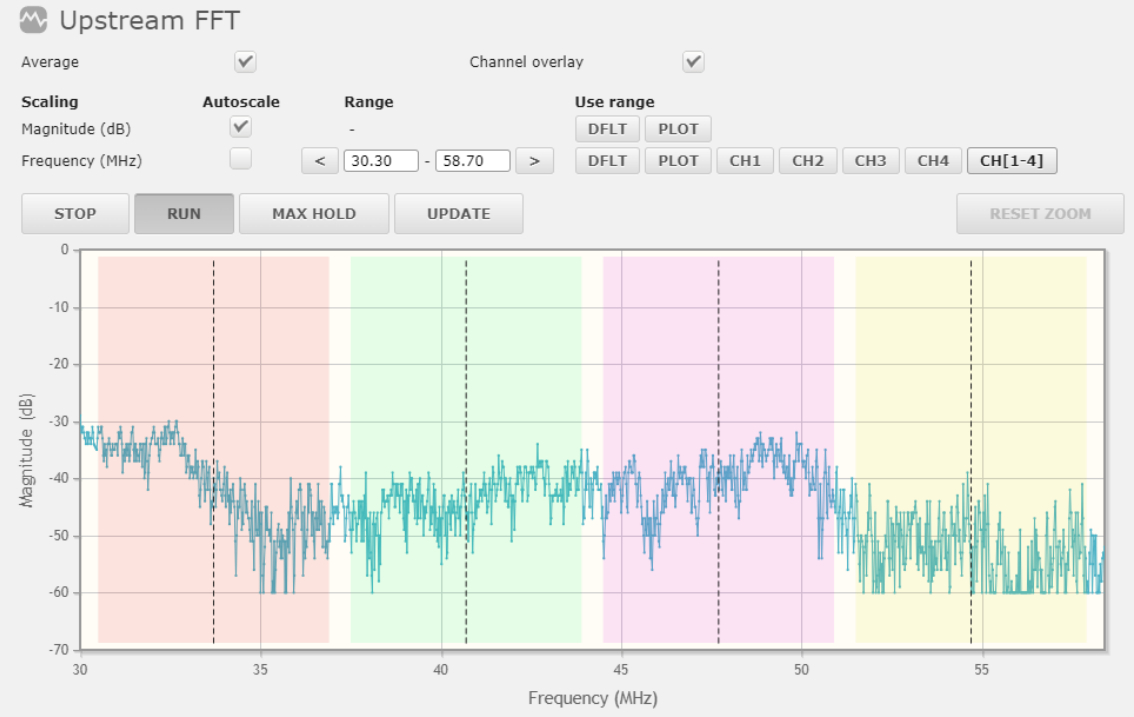
Obr. 8.16: Ikona pre status modemu

Obr. 8.17: Informácie o zapojenom modeme

Popis základných informácií o modeme

- Status: Modem je v operačnom stave (operational).
- Operational State: Modem je zapnutý (On).
- MAC Address: Fyzická adresa modemu
- IP Address: Modemu je pridelená IP adresa 10.0.0.199 z rozsahu, ktorý bol nastavený v DHCP sekcií.
- Model: Názov modelu modemu.
- Hardware Revision: Verzia hardvéru je 1.0.
- Software Revision: Verzia softvéru modemu.
- Downstreams: Zobrazené sú identifikátory kanálov (ID), výkony (Power) a pomer signálu k šumu (SNR) pre jednotlivé downstream kanály. Hodnoty výkonu sú približne okolo 20 dBmV a hodnoty SNR sú vysoké, čo znamená dobrú kvalitu signálu.
- Upstream: Pre upstream kanály sú zobrazené informácie ako výkon vysielania (TX Pwr), výkon prijímania (RX Pwr), korekcie a nekorigované chyby, čo sú dôležité metriky pre posúdenie kvality a spoľahlivosti upstream komunikácie.

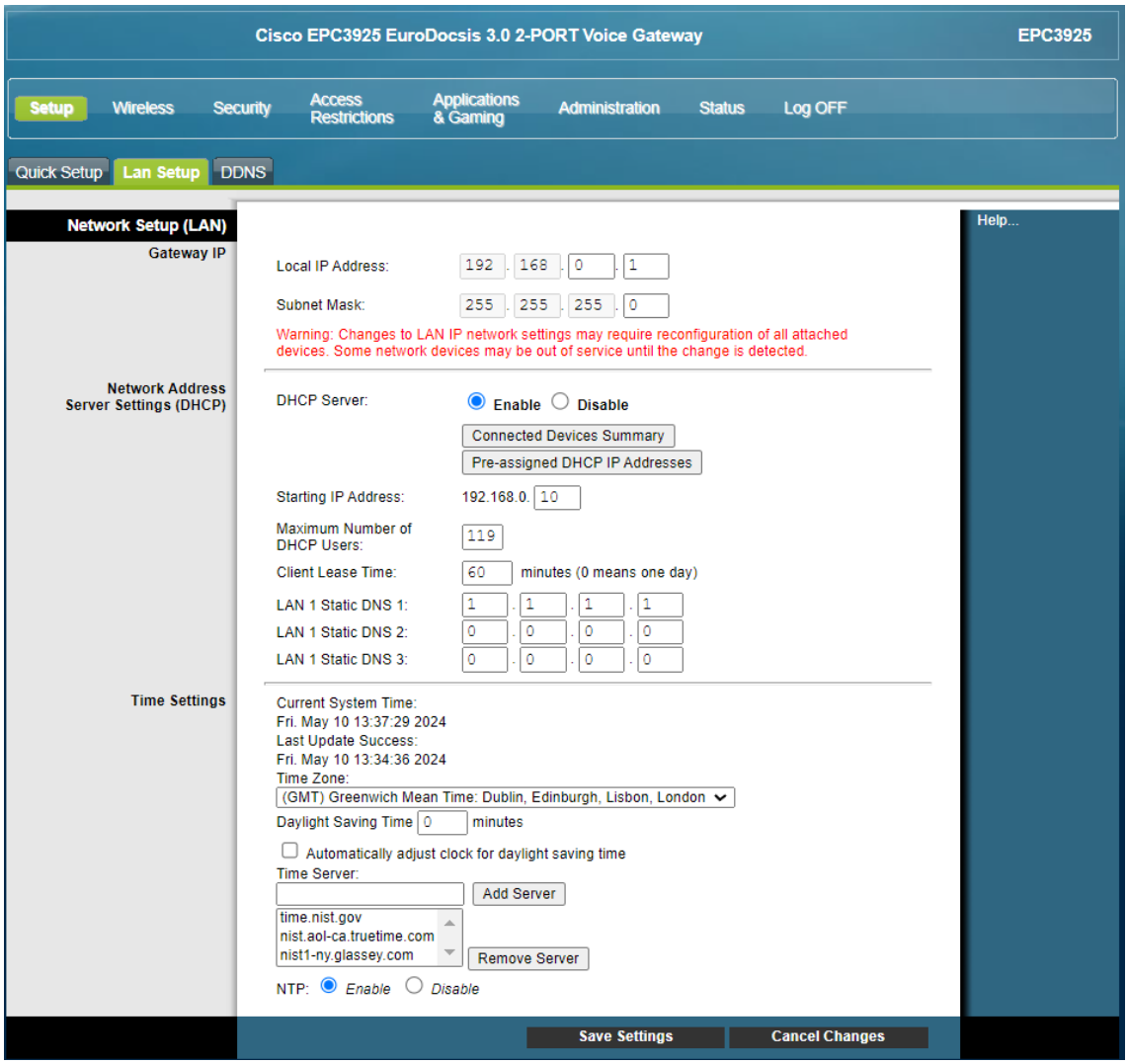
Presuňte sa do **MONITOR** a pri výpise **Upstream channels** kliknite na ikonku **SPECTRUM**. Kliknutím na ikonku sa otvorí okno s grafickým rozhraním pre analýzu upstream frekvenčného spektra pomocou FFT (Fast Fourier Transform) (obrázok 8.18).



Obr. 8.18: Grafické rozhranie pre analýzu upstream frekvenčného spektra

Graf zobrazuje charakteristiky spektra v rôznych farebných pásmach, ktoré indikujú pridelenie frekvenčných pásiem pre rôzne kanály alebo typy služieb. Farby pomáhajú vizuálne oddeliť rôzne oblasti spektra pre jednoduchšiu analýzu. **Magnitude (dB)** značí amplitúdu signálu v decibeloch na vertikálnej osi. **Frequency (MHz)** zobrazuje frekvenciu v megahertzoch, čo umožňuje vidieť distribúciu signálu cez rôzne frekvencie.

Teraz v prehliadači zadajte do vyhľadávania IP adresu **192.168.0.1**. Následne sa Vám otvorí webové rozhranie na konfiguráciu káblového modemu **CISCO EPC3925**. Prihláste sa pomocou mena **admin** a hesla **admin**. Prejdite do **Status->Lan Setup** (obrázok 8.19). V tejto sekcií sa nastavujú potrebné údaje pre lokálnu sieť, ktorú dané zariadenie vytvára. Toto nastavenie slúži k tomu, aby všetkým zariadeniam, ktoré sú ku káblovému modemu pomocou DHCP, pridelilo IP adresy.



Obr. 8.19: Konfigurácia CISCO EPC3925

Popis konfigurácie káblového modemu

- Gateway IP: Určuje adresa brány pre LAN.
- Local IP Address: Adresa modemu v lokálnej sieti.
- Subnet Mask: Maska podsiete je nastavená na 255.255.255.0, čo je typické pre domáce alebo malé kancelárske siete.
- DHCP Server: V tomto prípade je DHCP server povolený (Enable).
- Starting IP Address: Začiatočná adresa pre DHCP pridelenia je nastavená na 192.168.0.10.
- Maximum Number of DHCP Users: Maximálny počet užívateľov, ktorým môže byť pridelená IP adresa prostredníctvom DHCP, je 119.
- LAN 1 Static DNS 1: Toto pole slúži pre nastavenie statických DNS (Domain Name System) serverov.

Po týchto konfiguráciách káblový modem obdrží IP adresu od DHCP serveru DAH100 a taktiež počítač obdrží IP adresu od káblového modemu. Následne je možný prístup na internet.

Otestovanie prístupu na internet vykonajte v prehliadači na adrese:
http://www.speedtest.net/

Následne do tabuľky 8.3 poznamenajte namerané hodnoty rýchlosti pre upstream a downstream. Po meraní nastavte kanály tak, aby pre upstream a aj downstream bol zapnutý len jeden prenosový kanál a meranie opäť vykonajte. Namerané hodnoty poznamenajte do tabuľky 8.3. Porovnajte získané prenosové rýchlosti pre jeden kanál s teoretickými hodnotami z teoretického úvodu.

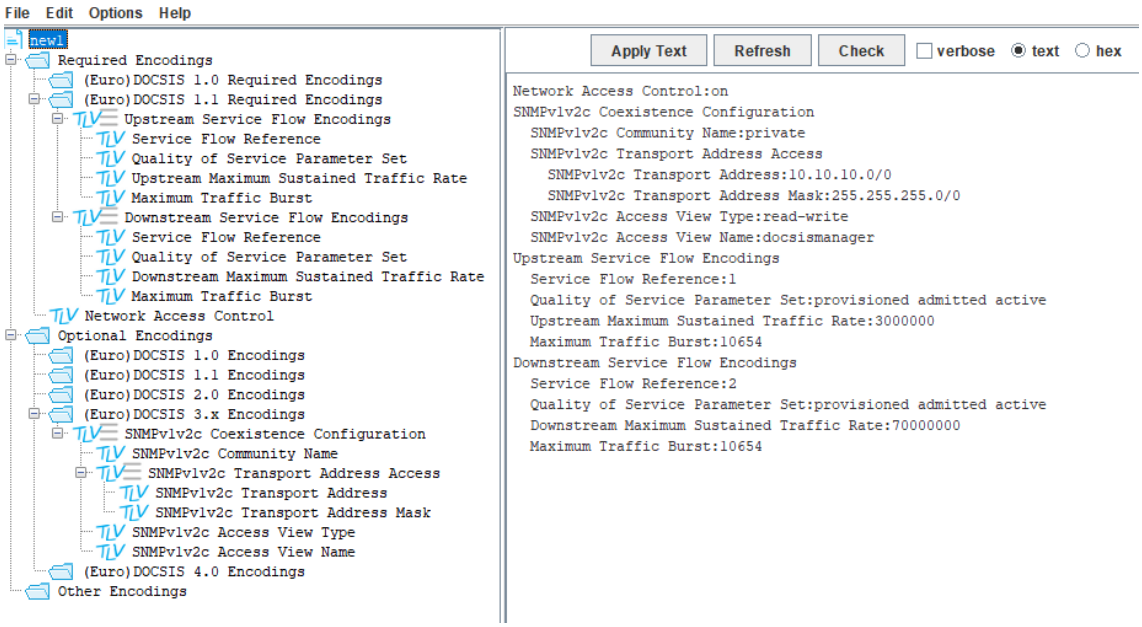
Tab. 8.3: Tabuľka prenosových rýchlosti pre upstream a downstream

	Upstream [Mb/s]	**Downstream [Mb/s]**
Všetky kanály		
Jeden kanál		

8.3.4 Konfigurácia súboru káblového modemu

Otvorte program Excentis Cable Modem Config File Editor, ktorý sa nachádza na ploche počítača. Následne kliknite na **File->Open** a otvorte súbor s názvom **new1**, ktorý sa nachádza na ploche v priečinku **DOCSIS-konfig**. Následne sa Vám otvorí daný súbor ako je zobrazené na obrázku 8.20. Pre správnu funkciu modemu sú dôležité parametre ako:

- Network Access Control (povolenie alebo zakázanie prístupu k sieti pre zákazníka)
- Upstream Service Flow (opisuje, ako budú pakety posielané v upstream smere)
- Downstream Service Flow (opisuje, ako budú pakety posielané v downstream smere)
- Upstream Maximum Sustained Traffic Rate (určuje maximálnu prenosovú rýchlosť pre upstream)
- Downstream Maximum Sustained Traffic Rate (určuje maximálnu rýchlosť pre downstream)



Obr. 8.20: Konfiguračný súbor káblového modemu

Následne sa tento konfiguračný súbor nahráva v DAH100 pomocou **ADMINISTRATION ->File manager ->UPLOAD FILE**. Následne sa musí tento konfiguračný súbor aktivovať v **ADMINISTRATION ->DHCP/TFTP settings**. V rozbaľovacom okne **Modem config file** je zvolený novo nahratý súbor. Na záver je potrebné vykonať reštartovanie a inicializáciu káblového modemu pomocou **DROP ALL**.

8.3.5 Samostatná úloha

1. Pred meraním sa uistite, že v **Modem config file** je zvolený súbor default. Vyskúšajte nastaviť pre všetky kanály upstreamu moduláciu (ATDMA Medium noise-64QAM)a pre všetky kanály downstreamu moduláciu (QAM64). Sledujte vplyv týchto modulácii na prenosovú rýchlosť.

2. Vráťte konfiguráciu upstreamu a downstreamu do pôvodných nastavení. Následne si otvorte konfiguračný súbor **new1** pomocou programu Excentis a nastavte prenosovú rýchlosť pre upstream na 15Mb/s a downstream na 85Mbi/s. Daný súbor uložte pod Vašim ID. Overte či Vami nakonfigurované hodnoty prenosových rýchlosti v danom súbore zodpovedajú výsledkom získaných na adrese http://www.speedtest.net/. Výsledky týchto prenosových rýchlostí prezentujte vyučujúcemu.

8.4 Kontrolné otázky

1. Čo znamená skratka DOCSIS?
2. Aké sú výhody koaxiálnych káblov?
3. Kde majú koaxiálne káble uplatnenie?
4. V čom sa odlišujú rôzne verzie štandardu DOCSIS?
5. Aký DOCSIS ponúka Vodafone v českej republike?
6. Popíšte hlavné rozdiely medti QPSK a QAM.
7. O koľko stupňov sa posúva fáza v QPSK?
8. Ako sa líši počet bitov na symbol pri modulácií 64 a 256QAM?
9. Aký je hlavný rozdiel medzi OFDM a OFDMA?
10. Čo je to SNR?
11. Čo je to CMTS (Cable Modem Termination System) a čo zabezpečuje?
12. Čo je to CM (Cable Modem) a čo zabezpečuje?
13. Aké kroky inicializácie prebiehajú medzi CM a CMTS?
14. Na čo slúži program Excentis?
15. Zodpovedajú namerané hodnoty v prvej časti laboratórnej úlohy teoretickým prenosovým rýchlostiam?
16. Ako vplýva typ modulácie na prenosové rýchlosti?

Záver

Cieľom diplomovej práce bolo navrhnúť tri laboratórne úlohy do predmetu Služby telekomunikačních sítí. Teoretická časť práce je rozdelená na štyri kapitoly. Prvá kapitola sa venuje základnému popisu dvoch modelov, ktoré sa využívajú na prenos dát po sieti a tými sú ISO/OSI a TCP/IP. V druhej kapitole sa uvádzajú typy sietí, ako sú metalické a optické. Obsahom je aj popis základných komponentov sietí a ich funkcií, úvod do telekomunikačných služieb v sieťach ako je IPTV a VoIP a správa sieťového prenosu zameraná na metriky pre optimálny sieťový prenos. Tretia kapitola popisuje sieťový generátor IXIA s rôznymi možnosťami využitia. Primárne je zameraná na sieťový generátor Optixia XM2 nakoľko je tento model využitý na zostavenie laboratórnej úlohy. Taktiež sú súčasťou kapitoly typy modulov a softvérov. Štvrtá kapitola sa venuje systému DOCSIS, ktorý je štandardom pre prenos dát cez káblové televízne systémy. Opisuje rôzne verzie DOCSIS, ich vlastnosti, prínosy a využívané modulácie, ako aj konkrétnu implementáciu pomocou zariadenia DAH100.

Praktická časť práce je rozdelená na štyri kapitoly. Piata kapitola obsahuje stručný popis návrhu laboratórnych úloh. Vytvorený je koncept troch laboratórnych úloh, ktoré sú odlišné a využívajú rôzne komponenty.

Posledné tri kapitoly obsahujú vypracované laboratórne úlohy. Tieto úlohy sú navrhnuté tak, aby poskytovali praktický prístup k teoretickým konceptom. Úlohy sa skladajú z teoretického úvodu, ktorý študentom poskytne základné informácie s danou problematikou a kontext na pochopenie problematiky. Ďalej je obsahom úloh podrobný postup praktických cvičení, ktoré študentom pomôžu získať praktické zručnosti a aplikovať teoretické vedomosti. Na záver každej úlohy je časť venovaná samostatnej práci, ktorú dokáže študent vypracovať po dôkladnom splnení jednotlivých úloh postupu. V samostatnej práci študenti aplikujú získané vedomosti na vypracovanie, čo im poskytne priestor pre hlbšie pochopenie a kreatívny prístup k riešeniu problémov. Po splnení samostatnej práce sú študentom položené kontrolné otázky, ktoré testujú ich porozumenie a schopnosť aplikovať teoretické koncepty v praktickej situácii.

Prvá laboratórna úloha je zameraná na testovanie parametrov sieťového prepínača a služieb QoS na linkovej vrstve. V tejto úlohe je využitý sieťový generátor IXIA XM2, ktorý je vzdialene ovládaný prostredníctvom pripojenia VPN a programov IxAutomate a IxExplorer. Generátor a testovaný prepínač sú umiestnené mimo laboratórnu učebňu. Táto úloha je rozdelená do dvoch častí a to testovanie výkonnostných parametrov prepínača a testovanie služby QoS na linkovej vrstve. V prvej časti sa študenti zameriavajú na analýzu základných výkonnostných metrík

prepínača, ako sú priepustnosť, latencia a kapacita spracovania paketov. Využitím simulovaných sieťových scenárov testujú, ako prepínač zvláda rôzne typy a intenzity sieťovej prevádzky. Tento test poskytuje cenné informácie o tom, ako rôzne konfigurácie prepínača môžu ovplyvniť celkový výkon siete. V druhej časti sa študenti venujú špecifickým nastaveniam QoS, ktoré sú kritické pre zabezpečenie preferovaného spracovania dátových tokov v závislosti od ich dôležitosti a požiadaviek na služby. Testy zahŕňajú prioritizáciu rôznych typov prevádzky, ako sú hlasové, video alebo dáta. Cieľom je overiť, ako dobre môže prepínač riadiť rozdielne požiadavky na služby, a to prostredníctvom techník ako je nastavenie tried paketov a garantovanie šírky pásma pre kritické aplikácie. Výsledky tejto laboratórnej úlohy poskytujú študentom praktické skúsenosti s testovaním hardvéru, ako aj porozumenie dôležitých aspektov výberu a konfigurácie sieťových prepínačov. Študenti sa dozvedia, ako efektívne implementovať QoS v reálnych sieťových prostrediach, čo je kľúčové pre zabezpečenie kvality služieb v moderných telekomunikačných sieťach.

Druhá úloha sa zameriava na analýzu vplyvu prekladu adries (NAT) na kvalitu IP televízie. Prostredníctvom simulačného programu GNS3 študenti konfigurujú smerače a sledujú vplyv NAT na latenciu prenosu. Úloha je rozdelená na dve hlavné časti. V prvej časti sa študenti zameriavajú na konfiguráciu NAT na jednom smerovači a v druhej časti rozširujú konfiguráciu na dva smerovače, čím sa snažia simulovať realistické sieťové scenáre. Cieľom úlohy je poskytnúť študentom hlbší pohľad na to, ako NAT ovplyvňuje dátové toky v sieti, a to konkrétne pri aplikáciách náročných na kvalitu prenosu, ako je IP televízia. Študenti analyzujú, ako preklad adries a počet zariadení v sieti môže ovplyvniť latenciu, čo je jednou z kritických metrík pre kvalitu video prenosu. Okrem technických aspektov konfigurácie a analýzy NAT, úloha študentom umožňuje získať praktické skúsenosti so základnou konfiguráciou smerovačov a pochopenie, ako sa rôzne nastavenia NAT prejavujú na rôznych typoch sieťovej prevádzky.

Tretia laboratórna úloha sa detailne zaoberá analýzou a konfiguráciou systému DOCSIS, ktorý je kľúčový pre poskytovanie káblového internetu a digitálnej televízie. V rámci tejto úlohy sú použité zariadenia CMTS DAH100 a káblový modem CISCO EPC3925, ktoré sú nevyhnutné pre realizáciu a testovanie DOCSIS siete. Táto úloha naučí študentov, ako správne konfigurovať a optimalizovať DOCSIS siete za účelom zabezpečenia stabilného a vysokorýchlostného prenosu dát. Laboratórna úloha je rozdelená do dvoch hlavných častí. Prvá časť sa zameriava na konfiguráciu CMTS DAH100, kde študenti nastavujú parametre ako frekvencia, modulácia a šírka kanálu, čo sú základné nastavenia pre efektívny prenos. Druhá časť úlohy pokrýva konfiguráciu káblového modemu CISCO EPC3925, kde je dôraz kladený na správne nastavenie sieťových parametrov, ako sú IP adresy, subnet masky a gateway. Výsledkom úlohy je nielen pochopenie teórie a praxe fungovania DOCSIS sietí,

ale študenti tiež získajú praktické zručnosti v oblasti konfigurácie. Navyše, úloha im umožňuje experimentovať s rôznymi nastaveniami a vidieť priamy dopad týchto zmien na kvalitu služieb poskytovaných cez DOCSIS siete, čo prispieva k hlbšiemu porozumeniu dynamiky telekomunikačných sietí a ich správy.

Laboratórne úlohy sú efektívnym nástrojom pre hlbšie pochopenie a praktické zvládnutie komplexných výziev, ktoré telekomunikačné siete predstavujú. Študenti majú možnosť prehĺbiť svoje teoretické vedomosti prostredníctvom praktickej práce s technológiami.

Literatúra

[1] JEŘÁBEK, J. Komunikační technologie. Brno: Vysoké učení technické v Brně, 2023. s. 1-175. ISBN první verze: 978-80-214-4713-4. (cs) [cit. 2023-11-04].

[2] JEŘÁBEK, J., Pokročilé komunikační techniky (MPC-PKT). Skripta VUT v Brně,s. 1-172, aktualizace 2023. (cs) [cit. 2023-11-04].

[3] FILKA, M. Přenosová média. Online. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Brno, Česká republika, 2012. ISBN 978-80-214-4444-7. [cit. 2024-05-15].

[4] S. Zeadally, H. Moustafa a F. Siddiqui, Ïnternet Protocol Television (IPTV): Architecture, Trends and Challenges,"v IEEE Systems Journal , zv. 5, č. 4, s. 518-527, december 2011, doi: 10.1109/JSYST.2011.2165601. Dostupné z URL:<https://ieeexplore.ieee.org/abstract/document/6031895>. [cit. 2023-11-15].

[5] Bradner, S., McQuaid, J. Benchmarking Methodology for Network Interconnect Devices. Internet Engineering Task Force, 1999. s. 1-43. Dostupné z URL: <https://www.ietf.org/rfc/rfc2544.txt>. [cit. 2024-05-19].

[6] Apposite Technologies. RFC 2544 Performance Test Methodology. Dostupné z URL: <https://www.apposite-tech.com/rfc-2544-performance-test-me,dology/> . [cit. 2023-11-15].

[7] Mandeville, R., Perser, J. Benchmarking Methodology for LAN Switching Devices. Internet Engineering Task Force, 2000. s. 1-43. Dostupné z URL:<https://www.ietf.org/rfc/rfc2889.txt> . [cit. 2023-11-15].

[8] Bi, Q., Zhou, G., Zhang, J. Network Management and Control for 5G: Challenges, Solutions, and Opportunities. IEEE Communications Magazine, 2008. s. 38-45. Dostupné z URL:<https://ieeexplore.ieee.org/abstract/document/4908978>. (en) [cit. 2023-11-15].

[9] B. Goode, "Voice over Internet protocol (VoIP),"v Proceedings of the IEEE , zv. 90, č. 9, str. 1495-1517, september 2002, doi: 10.1109/JPROC.2002.802005. Dostupné z URL:<https://ieeexplore.ieee.org/abstract/document/1041060> . [cit. 2023-11-15].

[10] WALLINGFORD, Theodore. Switching to VOIP. Ö'Reilly Media, Inc.", 2005.

[11] KUMAR, Ajay. An overview of voice over internet protocol (voip). Rivier college online academic journal, 2006, 2.1: 1-13.

[12] Networking Signal. What is Throughput in Networking? 2024. Dostupné z URL:<https://www.networkingsignal.com/what-is-throughput-in-networking/#:~:text=Throughput%20in%20networking%20is%20a,two%20points%20on%20a%20network>. (en) [cit. 2023-12-08].

[13] DNSstuff. Network Throughput vs. Bandwidth. 2024. Dostupné z URL:<https://www.dnsstuff.com/network-throughput-bandwidth#:~:text=What%20Is%20Throughput%20in%20Networking%3F,arrive%20at%20their%20destinations%20successfully>. (en) [cit. 2023-12-08].

[14] PhoenixNAP. Network Latency: What Is It and How to Reduce It. 2024. Dostupné z URL:<https://phoenixnap.com/blog/network-latency#:~:text=What%20Is%20Latency%20in%20Networking%3F,reply%20arrives%20from%20the%20server>. (en) [cit. 2023-12-08].

[15] DNSstuff. Network Latency. 2024. Dostupné z URL:<https://www.dnsstuff.com/network-latency>. (en) [cit. 2023-12-08].

[16] Opsview. What Is Packet Loss and How Does It Affect Your Network? 2024. Dostupné z URL:<https://www.opsview.com/resources/network/blog/what-packet-loss-and-how-does-it-affect-your-network#:~:text=Packet%20loss%20is%20a%20problem,of%20capacity%20or%20failing%20devices>. (en) [cit. 2023-12-08].

[17] TechTarget. Packet Loss: Definition and Causes. 2024. Dostupné z URL:<https://www.techtarget.com/searchnetworking/definition/packet-loss#:~:text=Packet%20loss%20is%20typically%20caused,the%20causes%20of%20packet%20loss>. (en) [cit. 2023-12-08].

[18] IR. What Is Network Packet Loss? 2024. Dostupné z URL:<https://www.ir.com/guides/what-is-network-packet-loss>. (en) [cit. 2024-05-19].

[19] Obkio. What is Jitter? 2024. Dostupné z URL:<https://obkio.com/blog/what-is-jitter/#:~:text=Jitter%20refers%20to%20the%20variation,is%20what%20we%20call%20jitter>. (en) [cit. 2024-05-19].

[20] How-To Geek. What is Jitter? 2024. Dostupné z URL:<https://www.howtogeek.com/824032/what-is-jitter/#:~:text=Jitter%20is%20measured%20in%20milliseconds,or%20lower%20tolerance%20for%20jitter>. (en) [cit. 2024-05-19].

[21] IR. What Is Network Jitter? 2024. Dostupné z URL:<https://www.ir.com/guides/what-is-network-jitter#anchor1>. (en) [cit. 2024-05-19].

[22] Ixia Chassis Family. Online. Yumpu.com. Dostupné z URL:<https://www.yumpu.com/en/document/read/29800068/ixia-chassis-family> . [cit. 2023-11-15].

[23] XM2 Portable Chassis Highlights - Ixia. Online. Dostupné z URL:<https://support.ixiacom.com/sites/default/files/resources/datasheet/ch_optixia_xm2.pdf> [cit. 2023-11-04].

[24] Chapter 5: Optixia XM2 Chassis. Online. May 30, 2014. Dostupné z URL:<https://downloads.ixiacom.com/library/user_guides/IxOS/6.70_EA/EA_6.70_Rev_A/IxiaReferenceGuide/OptixiaXM2.html> [cit. 2023-11-04].

[25] IxExplorer User Guide [online]. October 2016 [cit. 2023-11-04]. Dostupné z URL:<http://downloads.ixiacom.com/library/user_guides/IxOS/8.13_EA/EA_8.13_Rev_A/IxExplorer/IxExplorer.pdf>

[26] Ixia - Enabling a Converged World [online]. © 1998-2013 [cit. 2023-11-04]. Dostupné z URL:<http://www.ixiacom.com/>

[27] IXIA. Ixia Platform Reference Manual [online]. Release 6.30. Calabasas:Ixia, 2012. Dostupné z URL:<https://downloads.ixiacom.com/library/user_guides/IxOS/6.30/EA_6.30_Rev_A/IxiaReferenceGuide/IxiaReferenceGuide.pdf>

[28] Netcor. Network Performance Metrics. 2024. Dostupné z URL:<https://netcor.de/download.php?file=1108> (en) [cit. 2024-05-19].

[29] Jha, S., Hassan, M. M. Engineering Internet QoS. IEEE Communications Magazine, 2001. s. 72-79. Dostupné z URL:<https://ieeexplore.ieee.org/abstract/document/910608>. (en) [cit. 2024-05-19].

[30] Cable Television Laboratories, Inc. Data-Over-Cable Service Interface Specifications DOCSIS 3.1: Physical Layer Specification. 2015. s. 1-455. Dostupné z URL:<https://volpefirm.com/wp-content/uploads/2017/01/CM-SP-PHYv3.1-I08-151210.pdf. (en) [cit. 2024-05-19].

[31] All About Circuits. Quadrature Phase Shift Keying (QPSK) Modulation. 2024. Dostupné z URL:<https://www.allaboutcircuits.com/technical-articles/quadrature-phase-shift-keying-qpsk-modulation/. (en) [cit. 2024-05-19].

[32] Everything RF. What is 64-QAM Modulation? 2024. Dostupné z URL:<https://www.everythingrf.com/community/what-is-64-qam-modulation. (en) [cit. 2024-05-19].

[33] Everything RF. What is 256-QAM Modulation? 2024. Dostupné z URL:<https://www.everythingrf.com/community/what-is-256-qam-modulation. (en) [cit. 2024-05-19].

[34] Everything RF. What is OFDMA? 2024. Dostupné z URL:<https://www.everythingrf.com/community/what-is-ofdma. (en) [cit. 2024-05-19].

[35] Network World. What's the Difference Between OFDMA and MU-MIMO in 11ax? 2024. Dostupné z URL:<https://www.networkworld.com/article/967147/what-s-the-difference-between-ofdma-and-mu-mimo-in-11ax.html. (en) [cit. 2024-05-19].

[36] Teleste. DOCSIS Mini-CMTS. 2024. Dostupné z URL:<https://www.teleste.com/broadband-networks/products/distributed-access/docsis-mini-cmts/. (en) [cit. 2024-05-19].

[37] PIROHANIČ, L. DOCSIS v přístupových sítí. Brno, Rok, 58 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. T. Horváth, Ph.D.

[38] Tady je citace na základě vámi poskytnutého odkazu a vzoru:

Teleste. Teleste DAH User Manual. 2024. s. 1-64. Dostupné z URL:<https://www.intersatsrl.it/docs/file/User%20Manual/Teleste/Teleste_DAH.pdf. (en) [cit. 2024-05-19].

[39] Teleste. Teleste DAH Product Brochure. 2018. s. 1-8. Dostupné z URL:<https://www.teleste.com/wp-content/uploads/2022/01/teleste-dah-product-brochure-2018.pdf. (en) [cit. 2024-05-19].

[40] Vodafone. Cisco EPC3925. 2024. Dostupné z URL:<https://www.vodafone.cz/pece/internet-data/datova-zarizeni/cisco-epc3925/. (cs) [cit. 2024-05-19].

[41] Zarowin, S. Mastering ColdFusion Variables and Data Types. InformIT, 2002. Dostupné z URL:<https://www.informit.com/articles/article.aspx?p=167851&seqNum=3. (en) [cit. 2024-05-19].

[42] Volpe Firm. DOCSIS 101: Understanding UCD. 2024. Dostupné z URL:<https://volpefirm.com/docsis101_ucd/. (en) [cit. 2024-05-19].

[43] D-Link. DES-108: 8-Port Fast Ethernet Switch. 2024. Dostupné z URL:<https://www.dlink.com/uk/en/products/des-108-8-port-fast-ethernet-switch. (en) [cit. 2024-05-19].

[44] ŤÁPAL, T. Zefektivnění analýzy počítačové sítě 10Gbit/s [online]. Brno, 2013 [cit. 2023-11-05]. Dostupné z URL:<http://hdl.handle.net/11012/26778>.Diplomová práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací. Vedoucí práce V. Škorpil, CSc.

[45] NetworkLessons.com. QoS CoS vs DSCP. 2024. Dostupné z URL:<https://notes.networklessons.com/qos-cos-vs-dscp. (en) [cit. 2024-05-19].

[46] WatchGuard. QoS Marking: VLAN and Layer 2. 2024. Dostupné z URL:<https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/qos_trafficmanagement/qos_marking_vlan_layer2.html. (en) [cit. 2024-05-19].

[47] PingPlotter. Is My Connection Good? 2024. Dostupné z URL:<https://www.pingplotter.com/wisdom/article/is-my-connection-good/. (en) [cit. 2024-05-19].

Zoznam symbolov a skratiek

AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
bit/s	Bits per second
BPI/SEC	Baseline Privacy Interface/Security
Cat5E	Category 5 Enhanced
CATV	Community Antenna Television
CD-ROM	Compact Disc Read-Only Memory
CoS	Class of Service
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CPE	Customer Premises Equipment
CM	Cable Modem
CMTS	Cable Modem Termination System
DAH100	DOCSIS Access Hub 100
DHCP	Dynamic Host Configuration Protocol
DES	Data Encryption Standard
DNAT	Destination Network Address Translation
DOCSIS	Data Over Cable Service Interface Specification
DRM	Digital Rights Management
DSCP	Differentiated Services Code Point

DSL Digital Subscriber Line

DUT Device Under Test

DVD-ROM Digital Versatile Disc Read-Only Memory

DDoS Distributed Denial of Service

DVB-C Digital Video Broadcasting - Cable

EMI Electromagnetic Interference

EM Electromagnetic

FTP File Transfer Protocol

FTTB Fiber to the Building

FTTC Fiber to the Curb

GHz Gigahertz

HD High Definition

HFC Hybrid Fiber-Coaxial

HTTPS Hypertext Transfer Protocol Secure

I In-phase

IETF Internet Engineering Task Force

IoT Internet of Things

IP Internet Protocol

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IPTV Internet Protocol Television

ISO International Organization for Standardization

Kbit/s Kilobits per second

LAN Local Area Network

LSOH Low Smoke Zero Halogen

LTE Long Term Evolution

MAC Media Access Control

Mbit/s Megabits per second

MHz Megahertz

MPEG Moving Picture Experts Group

ms Milliseconds

NAT Network Address Translation

NGFW Next-Generation Firewall

NPVR Network Personal Video Recorder

ODE Open Development Environment

OFDM Orthogonal Frequency-Division Multiplexing

OFDMA Orthogonal Frequency-Division Multiple Access

OS Operating System

OSI Open Systems Interconnection

OSPF Open Shortest Path First

OTT Over The Top

PE Polyethylene

PEG Polyethylene Glycol

PCI Peripheral Component Interconnect

PKI Public Key Infrastructure

PoS Point of Sale

POS Position

PSTN Public Switched Telephone Network

PVC Polyvinyl Chloride

Q Quadrature

QAM Quadrature Amplitude Modulation

QPSK Quadrature Phase Shift Keying

QoS Quality of Service

RAM Random Access Memory

RFC Request for Comments

RFI Radio Frequency Interference

RM Reference Model

RSA Rivest-Shamir-Adleman

RSVP Resource Reservation Protocol

RTP Real-Time Protocol

RTCP Real-Time Control Protocol

RTSP Real Time Streaming Protocol

RTTP Real-Time Transport Protocol

SCTP Stream Control Transmission Protocol

SD Standard Definition

SDP Session Description Protocol

SEC Security

SIP Session Initiation Protocol

SMTP Simple Mail Transfer Protocol

SNAT Source Network Address Translation

SNMP Simple Network Management Protocol

STB Set-Top Box

STP Shielded Twisted Pair

SYNC Synchronization

TFTP Trivial File Transfer Protocol

TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TOS/QoS	Type of Service/Quality of Service
UDP	User Datagram Protocol
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VoD	Video on Demand
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WEB UI	Web User Interface
Wi-Fi	Wireless Fidelity
WPS	Wi-Fi Protected Setup
µm	Micrometer

A Obsah elektronickej prílohy

Elektronická príloha obsahuje tri laboratórne úlohy, ktoré boli navrhnuté v rámci diplomovej práce. Tieto laboratórne úlohy sú vytvorené pre predmet Služby telekomunikačních sítí, a preto sú uvedené v prílohe v českom jazyku.

```
/ ..... Koreňový adresár priloženého archívu
└── LAB ..... Súbory troch laboratórnych úloh
    ├── Výkonnostní_parametry_přepínače_a_QoS_na_linkové_vrstvě.pdf
    ├── Vliv_překladu_adres_(NAT)_na_kvalitu_služeb.pdf
    └── Analýza_a_konfigurace_systému_DOCSIS.pdf
```