VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2018 Bc. Jan Šimoník

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

BEZPEČNOSTNÍ RIZIKA V PASIVNÍCH OPTICKÝCH SÍTÍCH
SECURITY RISKS IN PASSIVE OPTICAL NETWORKS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Jan Šimoník

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Tomáš Horváth, Ph.D.

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**
Ústav telekomunikací

Student: Bc. Jan Šimoník ***ID:*** 164786
Ročník: 2 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Bezpečnostní rizika v pasivních optických sítích

POKYNY PRO VYPRACOVÁNÍ:

Cílem diplomové práce je provést základní útoky na OLT jednotku, tedy penetrační testy např. Kali Linuxem. Dále diskutujte/prezentujte proveditelnost útoků z teoretického rozboru práce (např. v distribuční části sítě). Práci směřujte, jak k sítím definovanými Institutem pro elektrotechnické a elektronické inženýrství, tak pro standardy Mezinárodní telekomunikační unie. Zaměřte se také na bezpečnost během konfigurace řídicí jednotky a její slabiny. Zrealizujte svou distribuční část sítě pro testovací účely.

DOPORUČENÁ LITERATURA:

[1] HORVATH, Tomas, Lukas MALINA a Petr MUNSTER. On security in gigabit passive optical networks. In: 2015 International Workshop on Fiber Optics in Access Network (FOAN). Brno: IEEE, 2015, s. 51-55. DOI: 10.1109/FOAN.2015.7320479. ISBN 978-1-4673-7625-9.

[2] HOOD, Dave a Elmar. TROJER. Gigabit-capable passive optical networks. Hoboken: Wiley, c2012. ISBN 978-0470936870.

Termín zadání: 5.2.2018 ***Termín odevzdání:*** 21.5.2018

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

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Tato diplomová práce se zabývá historickým vývojem pasivních optických sítí podle standardů, které byly definovány Mezinárodní telekomunikační unií (APON, BPON, GPON, XG-PON a NG-PON). Dále se práce zabývá bezpečností pasivních optických sítí, ale také riziky, která s sebou nasazení a používání pasivní optické technologie nese. V úvodních kapitolách této práce je popsána problematika pasivních optických sítí, následuje popis jednotlivých standardů pasivních optických sítí z hlediska jejich historického vývoje. Další část je věnována bezpečnosti pasivních optických sítí a možným bezpečnostním rizikům. V závěru je uveden popis praktické části této práce – kompletace racku, který poslouží pro budoucí testování. Popsána je také základní konfigurace optických linkových zakončení, která jsou v racku osazena. Poslední část této diplomové práce je věnována testování vybraných bezpečnostních rizik, která byla popsána v rámci teoretické části této práce.

KLÍČOVÁ SLOVA

APON, bezpečnost, bezpečnostní rizika, BPON, FTTx, GPON, historický vývoj, konfigurace, NG-PON, OLT, ONU, PON, XG-PON.

ABSTRACT

This diploma thesis deals with the historical development of passive optical networks, according to the standards that was defined by International Telecommunication Union (APON, BPON, GPON, XG-PON and NG-PON). Further, the thesis describes the security of passive optical networks, but also a security threats which the deployment and use of passive optical technology carry. In the introductory chapters of this thesis the passive optical networks are described. The following is a description of the standards of passive optical networks in terms of their historical development. The next part is dedicated to the security of passive optical networks and possible security threats. In conclusion a description of the practical part of this thesis is given – rack assembly, which will serve for future testing. The basic configuration of the optical line terminations that are fitted in the rack is also described. The last part of this diploma thesis is dedicated to the testing of selected security risks, which was described in the theoretical part of this thesis.

KEYWORDS

APON, security, security threats, BPON, FTTx, GPON, historical development, configuration, NG-PON, OLT, ONU, PON, XG-PON.

ŠIMONÍK, Jan. *Bezpečnostní rizika v pasivních optických sítích*. Brno, 2018, 126 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Tomáš Horváth, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Bezpečnostní rizika v pasivních optických sítích“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Tomáši Horváthovi, Ph.D. za příkladné odborné vedení, konzultace, vstřícný přístup, trpělivost, ochotu a čas, který mi během tvorby této diplomové práce věnoval. Dále bych na tomto místě rád poděkoval své rodině, přítelkyni a přátelům, kteří mě po celou dobu mého studia podporovali.

Brno ....

podpis autora

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Technicka 12, CZ-616 00 Brno
Czech Republic
http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno ....

podpis autora

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

Úvod

V současné době je kladen stále větší nárok na přenosovou kapacitu přístupových sítí. Tento trend je způsoben především neustálým technologickým pokrokem, se kterým nutně souvisí i rozvoj v oblasti telekomunikací.

Na scénu přicházejí stále nové služby, které je možné díky dnešním přenosovým rychlostem provozovat. Jsou to především multimediální služby kladoucí na síťovou infrastrukturu vysoké nároky – přitom kvalita audiovizuálních záznamů se stále zvyšuje. Na tento trend musí reagovat nejen poskytovatelé telekomunikačních služeb, ale také celé telekomunikační odvětví. Jde hlavně o vývoj nových standardů nebo zdokonalování těch současných tak, aby byly schopny uspokojit dnešní vysoké nároky provozovaných služeb.

Současným trendem přístupových sítí je přechod z metalických vedení na vedení optická – stávající metalické přístupové sítě přestávají neustále se zvyšujícím požadavkům dostačovat. V souvislosti se závazkem, který Česká republika přijala, je třeba zvolit vhodnou technologii, která bude pro nahrazení metalických vedení na přístupových sítích nejvhodnější.

Česká republika přijala závazek zajistit do roku 2020 pro všechny své obyvatele přenosovou rychlost alespoň 30 Mb/s, minimálně pro polovinu obyvatelstva potom rychlost 100 Mb/s. Jako perspektivní se jeví pasivní optické sítě, které jsou schopny svými přenosovými rychlostmi tento závazek splnit. Nasazení pasivních optických sítí s sebou však nese i jistá bezpečnostní rizika, která jsou v rámci této práce popsána a vybraná rizika otestována.

Cílem této diplomové práce je zachytit historický vývoj jednotlivých standardů pasivních optických sítí, které definovala Mezinárodní telekomunikační unie. Další část diplomové práce je zaměřena na již zmiňovaná bezpečnostní rizika. První kapitola této diplomové práce obsahuje úvod do problematiky pasivních optických sítí. Obsahem kapitoly je stručný popis historického vývoje a také jsou uvedeny organizace, které mají na tomto vývoji zásluhu. V závěru kapitoly je uveden také popis nasazení pasivních optických sítí.

Další kapitoly jsou již věnovány jednotlivým standardům pasivních optických sítí. Tyto standardy jsou popsány především z hlediska jejich historického vývoje, je uveden také princip komunikace a rozdíly oproti standardům předchozím. Následuje popis zabezpečení jednotlivých standardů a také obecný popis bezpečnostních rizik pasivních optických sítí.

Cílem praktické části této diplomové práce je osazení racku pasivní optickou technologií pro účely pozdějšího testování, včetně realizace optické distribuční sítě. V rámci praktické části je také provedena konfigurace vybraných optických linkových zakončení, včetně testování vybraných bezpečnostních rizik.

1 Pasivní optické sítě

Perspektivním řešením pro výstavbu nových nebo rekonstrukci stávajících přístupových sítí je použití pasivní technologie. *Pasivní optická síť – Passive Optical Network* (PON) na rozdíl od sítě AON (Aktivní optická síť – Active Optical Network) nepoužívá na trase mezi uživateli žádných aktivních prvků, které by vyžadovaly napájení. Tato skutečnost má za následek podstatné snížení nákladů na provoz a údržbu takové sítě [57].

Následuje výčet zkratek a definic pojmů, které se v souvislosti s pasivními optickými sítěmi používají, jedná se o prvky, ze kterých se sítě PON typicky skládají, a to nezávisle na použitém standardu [10, 27]:

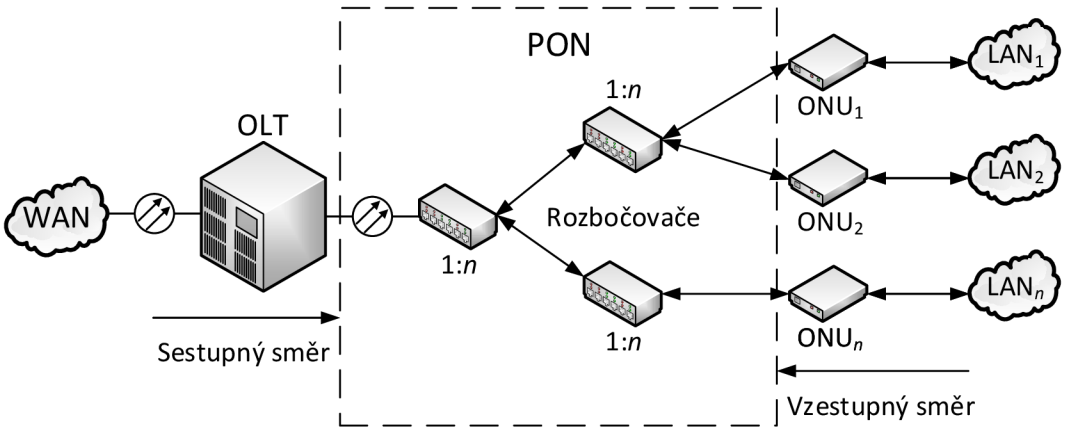
OAN: Optická přístupová síť – Optical Access Network, zpravidla zahrnuje několik optických distribučních sítí (ODN), které jsou připojeny ke stejnému optickému linkovému zakončení (OLT).

ODN: Optická distribuční síť – Optical Distribution Network, reprezentuje stromové rozvětvení optických vláken v rámci přístupové sítě. Jednotlivé koncové body přístupové sítě jsou propojeny pasivními optickými prvky, jako jsou například: optické vazební členy, optické filtry a pasivní rozbočovače (splittery). ODN propojuje jednotlivé součásti PON.

OLT: Optické linkové zakončení – Optical Link Termination, je zařízení, které zakončuje ODN. Jeho hlavním úkolem je implementace protokolů a jejich přizpůsobení pro komunikaci skrze rozhraní poskytovatele služeb. OLT tedy zakončuje pasivní infrastrukturu u daného poskytovatele služeb. Jedná se o mezilehlý síťový prvek, který odděluje pasivní síť od ostatních sítí. Tyto sítě mohou být založeny již na jiných technologiích. OLT poskytuje možnost řízení a správy koncových jednotek ONT a ONU, tyto jednotky jsou OLT podřízeny.

ONT: Optické síťové zakončení – Optical Network Termination, je koncové zařízení, které ukončuje jeden ze sdílených koncových bodů ODN, umístěné je zpravidla u koncového uživatele. Úkolem ONT je implementace protokolů a jejich přizpůsobení mezi sítí poskytovatele služeb a sítí zákazníka, které tato jednotka odděluje. ONT je speciálním případem jednotky ONU, obě tyto jednotky již vyžadují externí napájení.

ONU: Optická síťová jednotka – Optical Network Unit, je opět koncovým zařízením, umístěným u koncového uživatele. Její funkce jsou shodné s jednotkou ONT. Odlišností této jednotky ale je, že připojení uživatele je již realizováno jinou technologií. Na jednotku ONU je tedy možné připojit více koncových uživatelů. Typická architektura pasivní optické sítě je zobrazena na obrázku 1.1.



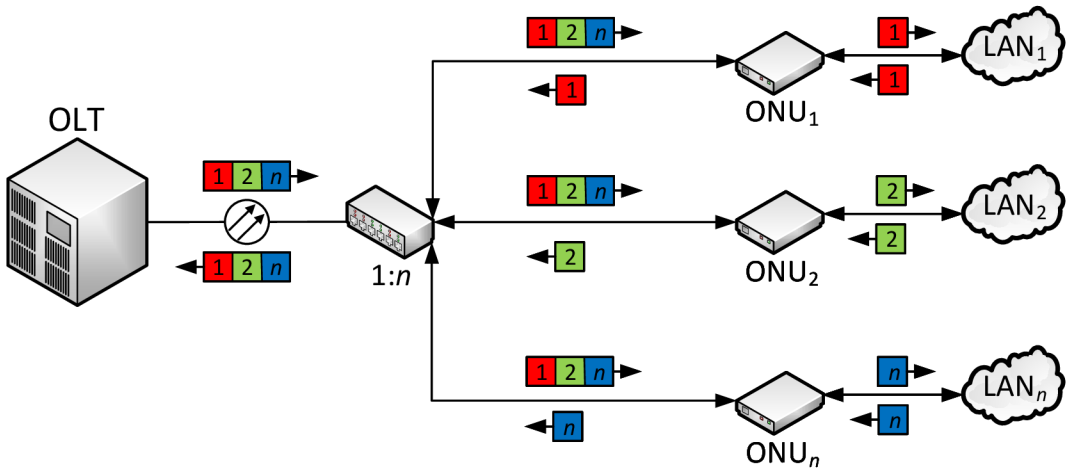
Obr. 1.1: Architektura PON [17].

Pasivní optické sítě využívají pasivních optických rozbočovačů (splitterů). Tyto rozbočovače se vyrábí v různých dělicích poměrech 1:n, kde n představuje počet výstupů daného rozbočovače. Nejčastěji používané dělicí poměry jsou: 1:2, 1:4, 1:8, 1:16, 1:32 a 1:64. Velikost rozbočovacího poměru je však limitována použitou technologií a vzdáleností mezi koncovými jednotkami. Pasivní rozbočovač totiž do optické trasy vnáší útlum, který ovlivňuje celkový dosah dané sítě i celkový počet připojených uživatelů [11].

Typický pasivní rozbočovač je obousměrným prvkem, ve směru ke koncovému uživateli (sestupný směr, downstream) rozbočovač optický signál, který obdrží na svém vstupním portu rozdělí na všechny své výstupní porty. Ve směru opačném od koncového uživatele (vzestupný směr, upstream) jsou jednotlivé optické signály obdržené na jednotlivých výstupních portech sloučeny a rozbočovač opouštějí přes jeho vstup. Rozbočovač však kromě rozbočování a slučování optického signálu tento signál nijak neupravuje [11]. Princip komunikace v PON je zachycen na obrázku 1.2. Datové jednotky jsou vysílány všesměrově všem ONU v síti. ONU zpracují pouze jim určené datové jednotky, ostatní zahodí.

1.1 Historický vývoj PON

Původní myšlenka na vývoj pasivních optických sítí pochází z roku 1980 [17]. Opoždění vývoje a následného nasazení těchto sítí však bylo zapříčiněno několika faktory. Prvním z těchto faktorů bylo hromadné nasazení technologie ADSL (Asymetrická digitální účastnická linka – Asymetric Digital Subscriber Line), došlo tak k využití stávajících telefonních sítí, které se obešlo bez větších finančních investic, jelikož ne-



Obr. 1.2: Komunikace v PON.

bylo nutné provádět výrazné zásahy do stávající infrastruktury [37]. Další technologií bylo HFC (Hybridní opticko-koaxiální vedení – Hybrid Fiber-Coax), které umožnilo naopak využití stávajících koaxiálních rozvodů CATV (Kabelová televize – Cable Television) také pro datové přenosy [56]. Druhým důvodem byla neexistence trhu s pasivní optickou technologií, nebyli zákazníci (především poskytovatelé služeb), kteří by o tuto technologii jevili zájem.

Přenosové rychlosti technologie ADSL však pro většinu koncových uživatelů přestávaly být dostatečné. Standard ADSL prošel za dobu své existence mnohými změnami, které spočívaly především ve zvyšování přenosových rychlostí, vyvíjeny byly i další varianty tohoto standardu, například VDSL (Vysokorychlostní DSL – Very High Speed DSL). U standardů xDSL je však nevýhodou použití metalických vedení, která mají své limity. Budoucí vývoj zcela nových systémů pro přístupové sítě se tak stává důležitým [37].

Pokračující vývoj v oblasti optických přenosových médií měl za následek zejména zvýšení dostupnosti optické technologie. Optická přenosová média byla postupně nasazována na páteřních sítích, příznivým důsledkem bylo zvýšení přenosových rychlostí a také snížení výrobních nákladů [17]. Nasazení optických vedení i na přístupových sítích se stalo aktuálním tématem. Bylo nezbytné zaměřit se na vývoj systémů, které by byly cenově dostupné a flexibilní [37].

Vývoj pasivních optických sítí byl opět spuštěn, původně se uvažovalo o kruhové topologii sítí PON. To ale nebylo vhodné řešení zejména z důvodu nežádoucích odrazů optického signálu. Jako vhodnější se jevilo použití hierarchické stromové topologie. Bylo navrženo několik řešení využívajících optických přenosových médií,

založeny byly však na starých technologiích a přinášely tak pouze výhody spojené s použitím optiky. Jednalo se o služby klasické telefonie a digitálního standardu ISDN (Digitální síť integrovaných služeb – Integrated Services Digital Network) [17].

Pro první standard PON se počítalo s využitím aktuální technologie ATM (Asynchronní přenosová technologie – Asynchronous Transfer Mode), která byla v době svého vzniku považována za perspektivní, jelikož řešila problém spojení klasických telefonních sítí a sítí datových [50].

1.2 Organizace

V souvislosti s vývojem pasivních optických sítí je nutné zmínit i organizace, které se na vývoji podílely.

FSAN: Síť plného přístupu ke službám – Full Service Access Network, členové této organizace jsou poskytovatelé telekomunikačních služeb. Organizace se podílí na vzniku doporučení ITU (Mezinárodní telekomunikační unie – International Telecommunication Union), důležité je zmínit pracovní skupinu OAN, zabývající se výzkumem v oblasti optických přístupových sítí. Pod skupinu OAN spadá také skupina zabývající se novou generací pasivních optických sítí, známých pod označením NG-PON (Síť PON nové generace – Next Generation PON) [12]. Výzkum je zaměřen na vysokorychlostní PON sítě a nové architektury, pracuje se i s technologiemi pro tyto nové architektury, které ještě nebyly schváleny [37].

EFM: Ethernet na první míli – Ethernet in the First Mile je organizací spadající pod IEEE (Institut elektrotechnického a elektronického inženýrství – Institute of Electrical and Electronics Engineers). Cílem této organizace je vývoj nových technologií založených na Ethernetu. Pod hlavičkou EFM vznikl i standard PON sítí založených právě na Ethernetu, známý pod označením EPON (Ethernetová pasivní optická síť – Ethernet Passive Optical Network) [37].

ACTS: Pokročilé komunikační technologie a služby – Advanced Communication Technologies and Services, je organizace, která se podílela na výzkumu nové technologie PON, tzv. SuperPON – tyto sítě se měly vyznačovat vysokým rozbočovacím poměrem. Mělo se jednat o sítě velkého dosahu, počítalo se s využitím optických zesilovacích prvků [63].

1.3 Nasazení PON

Vůbec první test sítě založené na optické technologii byl proveden již v roce 1977 v Japonsku. Poskytovány byly interaktivní video služby sloužící především ke vzdě-

lávacím účelům, dále VoD (Video na vyžádání – Video on Demand) a další telekomunikační služby [56].

V roce 1982 rozhodla francouzská vláda o podpoře vývoje a zavádění nových širokopásmových sítí do běžného provozu. Jako přenosové médium bylo vybráno optické vlákno. Ve Francii byla na základě tohoto rozhodnutí instalována testovací pasivní optická síť ve městě Biarritz, v provozu byla v letech 1984 až 1985.

Technické parametry této testovací sítě byly následující: pro přenos bylo využito vlnových délek 840 a 1 300 nm, zdrojem záření byla LED dioda a jako přenosové médium bylo použito vícevidové optické vlákno. Síť byla zapojena do hvězdy, pomocí frekvenčního multiplexu bylo možné na každé lince určené pro koncové uživatele provozovat [20]:

- 2 TV kanály (celkem na výběr ze 30 TV kanálů),
- 1 rozhlasový kanál (opět celkem na výběr ze 30 rozhlasových kanálů),
- obousměrný digitální kanál pro ISDN (přenosová rychlost 144 kb/s),
- obousměrný datový kanál o rychlosti 4,8 kb/s.

Toto řešení se ale ve Francii nerozšířilo z důvodu vysokého pokrytí technologií ADSL, jejíž zavedení bylo podstatně méně nákladné. Podstatným závěrem testu provedeného ve Francii bylo, že nasazení optické přístupové sítě je možné [20].

Další testování optické technologie bylo provedeno i v jiných lokalitách, souhrn nejvýznamnějších lokalit je uveden níže [56]:

- Higashi-Ikoma, Japonsko.
- Biarritz, Francie.
- Milton-Keynes, Velká Británie.
- Berlín, Německo.
- Elie, Kanada.

Ve všech výše uvedených lokalitách bylo testování úspěšné a položilo významný základ pro vývoj budoucích standardů pasivních optických sítí [56]. Prvnímu standardu pasivních optických sítí je věnována následující kapitola.

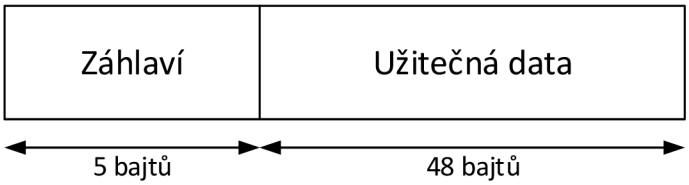
2 Standard APON

Pasivní optická síť založená na technologii ATM – ATM Passive Optical Network (APON), jedná se o první standard pasivní optické sítě schválený ITU v roce 1998. Celý tento standard pracoval na technologii ATM a je definovaný v doporučení G.983.1 [24].

Technologie ATM je síťová architektura, která byla používána v rozlehlých sítích. Záměrem technologie ATM bylo zajištění síťového standardu pro současný přenos hlasových a datových služeb. Pro přenos je využito buněk, použití těchto datových jednotek mělo za cíl vyřešit konflikt mezi sítěmi s přepojováním okruhů a paketů. Datový tok těchto sítí – bitový a paketový je transformován do jednoho datového toku, který je složen z buněk.

Buňky jsou datové jednotky konstantní délky poměrně malé velikosti. Buňka v ATM síti má velikost 53 bajtů, kde je vyčleněno 5 bajtů pro záhlaví a zbývajících 48 bajtů pro data, viz obrázek 2.1. Zpracování buněk v uzlech sítě (ATM přepínačích) je čistě hardwarové a velmi rychlé. Pořizovací cena ATM přepínačů byla ovšem poměrně vysoká, technologie se nejen z tohoto důvodu příliš nerozšířila [50].

ATM sítě mohou poskytnout vysoké přenosové rychlosti, komunikaci je možné uskutečnit po pevných nebo virtuálních okruzích. Sítě ATM také garantují kvalitu služeb pro různé typy datových toků, není ovšem zajištěna detekce chyb ani řízení těchto datových toků. Je možné dosáhnout vysokých přenosových rychlostí od 1,5 Mb/s do 2,4 Gb/s [50].



Obr. 2.1: Struktura ATM buňky.

Technologie ATM byla postupně zaváděna do provozu na konci osmdesátých let minulého století. Prvotním impulzem, který měl za následek hromadné zavádění ATM bylo přijetí ATM jako transportní technologie pro širokopásmové digitální sítě B-ISDN (Širokopásmové ISDN – Broadband ISDN), které bylo schváleno ITU. Původní filozofií ATM sítí bylo poskytování integrovaných služeb pro širokou škálu aplikací, které budou dostupné firmám i jednotlivým koncovým uživatelům. Na začátku devadesátých let minulého století byla tato technologie přijata i počítačovým

průmyslem – důvodem byly stále se zvyšující nároky na šířku pásma a podpora multimediálních aplikací [63]. Implementace ATM přinášela následující výhody [63]:

- infrastruktura a její rozhraní jsou nezávislá na aplikacích,
- plná podpora multiplexování a demultiplexování,
- efektivní zacházení s proměnnými i konstantními bitovými rychlostmi,
- podpora multimediálních služeb citlivých na zpoždění,
- zjednodušená správa a provoz sítě,
- budoucí bezpečnost.

2.1 Historický vývoj standardu APON

První testování tohoto standardu v běžném provozu bylo realizováno již v devadesátých letech minulého století. Od roku 1995 vznikla mezinárodní iniciativa poskytovatelů telekomunikačních služeb a výrobců telekomunikačních zařízení (FSAN), která se významně podílela na vzniku celé této technologie [19]. Standardizace organizací ITU, jak již bylo zmíněno, vyšla v platnost v roce 1998. Nasazení tohoto standardu urychlil zejména vývoj v oblasti elektricko-optických součástek, jejichž cena se výrazně snížila, a tím pádem se zlepšila i jejich dostupnost. V roce 2001 se standard APON stal uvažovanou technologií pro nasazení v přístupových sítích FTTH (Vlákno do domu – Fiber To The Home) [54].

Při vývoji standardu APON organizace FSAN spojila dvě klíčové technologie: ATM a PON. V případě přístupových sítí založených na tradiční podobě technologie ATM je využíváno statického multiplexu. Multiplexování v síti zajišťují přístupové přepínače, které slučují velké množství příchozích datových toků od koncových uživatelů do jednoho odchozího datového toku. Jedná se však o aktivní prvky, které vyžadují napájení, umístěny musí být na trase mezi poskytovatelem služeb a koncovým uživatelem. Náklady potřebné na údržbu těchto přístupových přepínačů, spolu s náklady na jejich napájení, nejsou zanedbatelnou položkou a zvyšují tak celkové náklady na provoz přístupové sítě. V případě implementace technologie PON jsou tyto aktivní přístupové přepínače nahrazeny pasivními optickými rozbočovači [42].

Jedna z prvních specifikací standardu APON počítala s přenosovou rychlostí 155 Mb/s, maximální rozbočovací poměr byl stanoven na 32. To v důsledku znamenalo maximálně 32 koncových uživatelů, při plné obsazenosti pasivního optického rozbočovače by byla maximální přenosová rychlost pro jednoho uživatele přibližně 4,8 Mb/s. Tato první generace by nebyla žádným výrazným zlepšením, jednalo se sice o symetrickou variantu, nicméně byla schopna dosáhnout podobných přenosových rychlostí, jako již v té době rozšířená technologie ADSL. Pro služby Triple Play (video, hlas, data) by rovněž tato první generace nebyla vhodná [37].

U druhé generace standardu APON byla definována asymetrická varianta. Sestupný směr (downstream) disponoval přenosovou rychlostí 622 Mb/s, přenosová rychlost vzestupného směru (upstream) byla shodná s první generací APON, tedy 155 Mb/s. Maximální rozbočovací poměr byl opět 32. V tomto případě by již při plném obsazení rozbočovače byla maximální přenosová rychlost pro jednoho uživatele 19,4 Mb/s (v sestupném směru).

Třetí generací APON je symetrická varianta s přenosovou rychlostí 622 Mb/s a maximálním rozbočovacím poměrem stejným, jako u předchozích generací [37].

Z ekonomických důvodů se optické vedení nezakončovalo u koncových uživatelů. Na jednu jednotku ONU tak bylo zpravidla připojeno více koncových uživatelů pomocí navazující metalické sítě. Jelikož data v sestupném směru jsou posílána všem jednotkám ONU v síti, počet ONU jednotek připojených do optické stromové topologie byl omezen na 64 – důvodem byly uvažované náklady na napájení systému (na straně poskytovatele připojení). Typický dosah systému APON byl 10 km [13].

2.2 Přístupové metody ke sdílenému médiu

Návrh vhodné přístupové metody pro standard APON byl zpočátku problémem. Celková přenosová kapacita musela být rovnoměrně rozdělena mezi všechny aktivní ONU jednotky. Přístupová metoda by také neměla narušit transportní profily samotné technologie ATM. Struktura PON je obecně centralizovaná, hlavním prvkem je zde jednotka OLT, která řídí přidělování dostupné šířky pásma [13].

Již v roce 1987 byly zahájeny práce na výzkumu systému, který by využíval přístupovou metodu TDMA (Časový multiplex s vícenásobným přístupem – Time Division Multiple Access). Tento výzkum byl iniciován společností British Telecom a probíhal v laboratořích této společnosti známých pod označením BT Laboratories. Výzkum byl prováděn na systému označeném TPON (Telefonie prostřednictvím PON – Telephony over PON), který nabízel služby klasické telefonie. První systém založený na metodě TDMA byl poté sestrojen a v roce 1989 bylo provedeno i testování v reálném provozu. Přístupová metoda se osvědčila a bylo přistoupeno ke spojení této techniky s tehdy perspektivní technologií ATM [19].

V sestupném směru (OLT → ONU) je používán časový multiplex (TDM), naopak ve vzestupném směru (ONU → OLT) je používán časový multiplex s vícenásobným přístupem (TDMA). V případě přenosu ve vzestupném směru je ATM buňkám přidáno záhlaví, které je využito pro účely synchronizace rozsahu výkonu a časové synchronizaci.

ATM buňky z koncových síťových jednotek jsou ve vzestupném směru sloučeny na výstupu pasivního optického rozbočovače do výsledného datového toku. Právě zde může dojít ke kolizi mezi buňkami, které jsou ve vzestupném směru vysílány

různými zdroji. Z tohoto důvodu je pro vzestupný směr používán právě multiplex TDMA, v sestupném směru ke kolizím nedochází [42].

2.3 Komunikace v APON

Rámce posílané v sestupném směru v případě základní přenosové rychlosti 155 Mb/s obsahují celkem 56 ATM buněk (každá z buněk má velikost 53 bajtů). V případě přenosové rychlosti 622 Mb/s obsahuje rámec celkem 224 ATM buněk. Dvě buňky z celkového počtu jsou vždy vyhrazeny, jedná se o buňky PLOAM (Provoz, správa a údržba fyzické vrstvy – Physical Layer Operation, Administration and Maintenance). Jedna tato buňka se nachází na začátku rámce a druhá uprostřed. Zbývající buňky obsažené v rámci jsou již ATM buňky přenášející uživatelská data [58].

V sestupném směru se PLOAM buňky používají k doručování grantů. Tyto granty nepřetržitě vysílá jednotka OLT všem připojeným jednotkám ONU a slouží jako povolení pro jednotlivé ONU k přenosu uživatelských dat v ATM buňkách. Tímto může jednotka OLT ovlivnit přidělenou šířku pásma pro jednotku ONU [58].

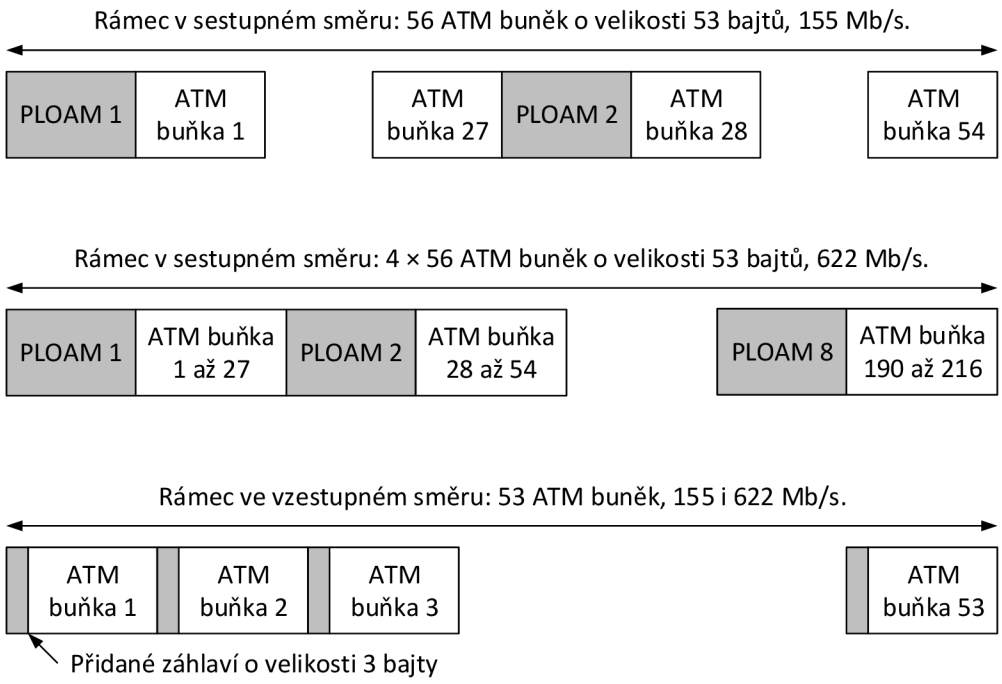
Přenos rámců ve vzestupném směru je shlukem ATM buněk, každá buňka obsahuje režijní záhlaví o velikosti 3 bajty, které slouží pro oddělení jednotlivých buněk a synchronizaci v přijímači (PLOAM i ATM buněk). Těmito přijímači musí disponovat jednotka OLT, důležité je, aby jednotka OLT byla schopna synchronizace s jednotkami ONU, které se mohou nacházet v různé vzdálenosti od OLT [58].

Ve vzestupném směru jsou PLOAM buňky používány jednotkami ONU k přenosu informací o velikosti jejich fronty pro jednotku OLT. Tuto informaci může OLT opět využít k přidělení šířky pásma [58].

Struktura APON rámce je zobrazena na obrázku 2.2, rámce posílané v sestupném směru se liší v závislosti na přenosové rychlosti, naproti tomu rámce posílané ve vzestupném směru jsou shodné pro symetrickou i asymetrickou variantu.

2.4 Dynamické přidělování šířky pásma

V případě pasivních optických sítí se jedná o spojení point-to-multipoint, v síti je tedy přítomen centrální bod (jednotka OLT), který je nadřazen všem koncovým bodům. Jedná se o hierarchickou strukturu, která je pro stromovou topologii typická. To však s sebou nese i jisté odlišnosti od klasických spojení point-to-point – zde je možné používat statické přidělení šířky pásma pro určitý spoj. Pokud by bylo využito statického přidělení šířky pásma pro APON systém s přenosovou rychlostí například 155 Mb/s (1. generace, symetrická varianta), znamenalo by to, že



Obr. 2.2: Struktura APON rámce [24].

každý z 32 koncových uživatelů by disponoval přenosovou rychlostí 4,8 Mb/s v obou směrech.

Dynamické přidělení šířky pásma – Dynamic Bandwidth Assignment (DBA) je založeno na myšlence, že všichni z připojených koncových uživatelů nebudou potřebovat plnou šířku pásma v jeden okamžik. Realizace tohoto mechanismu není v APON síti problémem, jelikož přenosová rychlost je poměrně vysoká a problémy s latencí jsou omezeny na minimum [37].

V roce 2001 bylo vydáno organizací ITU doporučení G.983.4 [26]. Jedná se o doporučení zavádějící mechanismus DBA i do systémů vycházejících z původního doporučení G.983.1, které ještě tímto mechanismem nedisponovaly. DBA mechanismus obsahuje tři různé strategie [37]:

1. Hlášení bez stavů.
2. Hlášení samotného stavu.
3. Hybridní hlášení.

V případě hlášení číslo 1 je monitorován provoz procházející jednotkou OLT. Pokud se zvyšuje obsazenost front, jednotka tuto událost vyhodnotí jako požadavek na zvýšení šířky pásma. Ve druhém případě (hlášení číslo 2) jednotka ONU hlásí svůj stav jednotce OLT. Pokud jednotka ONU vyžaduje vyšší šířku pásma, odešle tento

požadavek jednotce OLT. Hybridní hlášení je potom kombinací dvou předešlých typů [37]. Následující standard pasivních optických sítí již mechanismus dynamického přidělování šířky pásma podporoval.

2.5 Nasazení systému APON

V rámci testovacího provozu byly testovány různé systémy pasivních optických sítí založené na ATM [63]:

- 1990: British Telecom (APON).
- 1993: France Telecom (SAMPAN).
- 1993: Nippon Telegraph and Telephone.
- 1993: Siemens.
- 1994: Evropská komise (Broadband Access Facilities project).

Prvním komerčně dostupným APON systémem byl však systém vyvinutý společností Alcatel. Testován byl hned v několika lokalitách [63]:

- 1994: Bermudy, 100 připojených subjektů.
- 1995: Velká Británie, připojeno bylo 2 500 domácností.
- 1996: Belgie, 50 připojených subjektů.
- 1996: Francie, 100 připojených subjektů.

Při prvním testování v roce 1994 poskytoval systém koncovým uživatelům služby POTS (Klasická telefonie – Plain Old Telephone Service) a VoD. Tyto služby byly poskytovány celkem pro 100 subjektů (87 domácností a 13 firem). Jednotliví účastníci byli připojeni pomocí pasivní optické sítě, která byla zakončena jednotkou ASU (Účastnická jednotka technologie ATM – ATM Subscriber Unit). Připojení těchto koncových jednotek bylo realizováno architekturou FTTB (Vlákno do budovy – Fiber To The Building) nebo FTTH, všichni uživatelé v dané budově sdíleli jedinou jednotku ASU [53].

Vůbec největším testem APON systému však bylo testování ve Velké Británii. Připojeno bylo celkem 2 500 koncových uživatelů, poskytovány byly především multimediální služby, VoD a jiné. Účastníci byli připojeni pomocí technologie ADSL, využito tak bylo stávajících metalických vedení. Celkem 500 jednotek ONU bylo připojeno pomocí optických kabelů a technologie APON. Propojena byla dvě města – Colchester a Ipswich, při propojení bylo využito několika širokopásmových přepínačů. Ty byly propojeny do kruhu pomocí technologie SDH (Synchronní digitální hierarchie – Synchronous Digital Hierarchy), přenosová rychlost byla 2,4 Gb/s.

Příprava tohoto testu byla dokončena v polovině roku 1995, síť byla uvedena do provozu 2. 10. 1995. British Telecom poté začal připojovat jednotlivé uživatele (50 denně). Testování systému probíhalo až do června roku 1996 [63].

2.6 SuperPON

Již v době vývoje standardu APON byly započaty výzkumné práce na zcela nové technologii PON. Vycházelo se z předpokladu, že velikost přístupových sítí se bude nadále zvyšovat. Výzkumný projekt organizace ACTS pojmenovaný AC50 PLANET (Fotonová lokální síť – Photonic Local Access Network) byl proto zaměřen na vývoj nové PON technologie pro rozlehlé sítě s vysokým rozbočovacím poměrem [63].

V březnu roku 1997 byl proveden laboratorní test optického přenosu rozhlehlou sítí s vysokým rozbočovacím poměrem. V roce 1998 bylo v Bruselu realizováno testování přenosu multimediálních služeb na SuperPON síti.

SuperPON měl opravdu ambiciózní parametry, uvažován byl dosah až 100 km, celkový rozbočovací poměr byl stanoven na 2 048. Byly podporovány dvě přenosové rychlosti – v sestupném směru 2,4 Gb/s, ve směru vzestupném potom 311 Mb/s. Bylo vypočítáno, že šířka pásma by byla dostatečná pro 15 000 koncových uživatelů, na jednu jednotku ONU by však v případě realizace architektury FTTC (Vlákno do uzlu – Fiber To The Curb) nebo FTTB bylo možné připojit uživatelů i více [52].

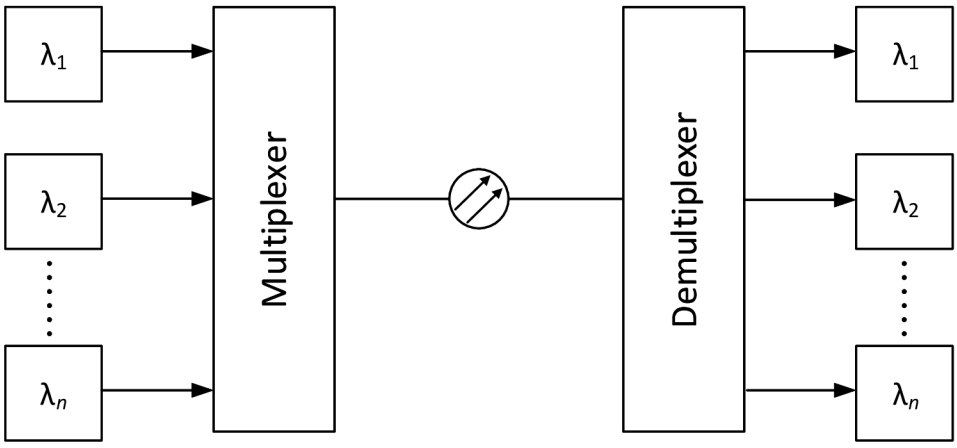
Celá technologie SuperPON měla být založena na přenosu ATM buněk. Pro síť tak velkého dosahu však bylo nutné použít optické zesilovače. Navrženo bylo následující: pro sestupný směr měl být použit zesilovač EDFA (Erbiem dotovaný vláknový zesilovač – Erbium Doped Fibre Amplifier), pro směr vzestupný mělo být ale využito odlišného typu optického zesilovače SOA (Polovodičový optický zesilovač – Semiconductor Optical Amplifier). Důvodem využití zesilovače SOA byla potřeba rychlého přepínání, které by snížilo hodnotu šumu [52].

3 Standard BPON

Širokopásmová pasivní optická síť – Broadband Passive Optical Network (BPON) je v pořadí druhým standardem sítí PON definovaných pod hlavičkou ITU. Definován je v doporučení G.983.3 [25]. Schválení tohoto doporučení v roce 2001 mělo za následek umožnění implementace multiplexu WDM (Vlnový multiplex – Wavelength Division Multiplex), který tak přispěl k vícenásobnému využití stávajících optických přenosových cest. Standard BPON vychází z předchozího standardu APON, se kterým je zpětně kompatibilní. Pro přenos využívá i stejné přenosové rychlosti. Hlavním přínosem tohoto standardu bylo zavedení vlnového multiplexu WDM do pasivních optických sítí [10].

Princip vlnových multiplexů spočívá ve využití různých vlnových délek pro přenos signálu jedním optickým vláknem. Zdrojů záření je více a každý vyzařuje na jiné vlnové délce. Výhodou tohoto řešení je navázání více kanálů do jediného optického vlákna, tyto kanály by jinak byly přenášeny každý zvlášť po jiném optickém vlákně (prostorové oddělení) [10]. Princip WDM je zobrazen na obrázku 3.1.

WDM je hybridním multiplexem, z hlediska využití přenosových kapacit optických vláken je velice perspektivní. Technologie WDM je nejvíce podobná frekvenčnímu multiplexu FDM (Frekvenční multiplex – Frequency Division Multiplex). U multiplexu FDM se přenosy uskutečňují na různých kmitočtech, multiplexy WDM uskutečňují přenosy na různých vlnových délkách. Na začátku optické trasy je nutné signál z více vysílačů sloučit pro přenos po jednom optickém vlákně. K tomuto účelu slouží multiplexer, na straně přijímačů je zapojen demultiplexer, který z přijímaného signálu na základě vlnových délek oddělí signály určené pro jednotlivé přijímače [51].



Obr. 3.1: Vlnový multiplex [51].

3.1 Princip vlnových multiplexů

Původně nebyl přenos po optickém vlákně přizpůsobený současnému přenosu více signálů. Signál byl přenášen jako soustředěný svazek světelných paprsků, jejichž rozsah vlnových délek byl co nejmenší. Vyslat do optického vlákna více těchto paprsků nebylo problémem, problém ale nastal na straně příjemce, kde bylo nutné tyto svazky paprsků od sebe rozlišit. Optické vlákno tedy mohlo sloužit pouze k jednosměrnému přenosu. Na základě tohoto předpokladu byly budovány optické přenosové trasy [51].

Pomocí WDM bylo možné zvýšit přenosovou kapacitu již instalovaných optických spojů. Jednalo se o finančně méně nákladnou variantu v porovnáním s pokládkou dalších optických kabelů. Tyto náklady byly vyšší především pro optické spoje s dosahem v řádech desítek kilometrů [46].

Multiplexer jednotlivé kanály slučuje pro přenos po jediném optickém vlákně. Princip demultiplexeru spočívá v oddělení jednotlivých přenášených kanálů pro dané přijímače. Realizovat demultliplexer je možné následujícími způsoby [60]:

1. soustavou dielektrických filtrů,
2. pomocí vlnovodů uspořádaných do mřížky,
3. pomocí vláknové Braggovy mřížky.

Demultiplexer uvedený v bodě 1 tvoří soustava dielektrických filtrů. Na tuto soustavu dopadá signál obdržený na vstupu demultiplexeru. Jednotlivé filtry signál rozdělí odpovídajícím přijímačům. Signál se postupně odráží na jednotlivé filtry, filtr propustí kanál odpovídající vlnové délky na přijímač, kterému je tento filtr přiřazen. Signál se poté odráží k dalšímu filtru a tento proces se opakuje do okamžiku, kdy dojde k rozdělení všech kanálů [60].

Realizace demultiplexeru uvedeného v bodě 2 spočívá v navaření vlnovodu na optické vlákno. Navařený vlnovod je poměrně široký, postupně se ale zužuje v úzké vlnovody, které mají obdobnou tloušťku jako vlákno, na které byl vlnovod původně navařen. Úzké vlnovody jsou zatočené do soustředných oblouků, každý z oblouků má odlišnou délku a jejich počet odpovídá počtu přenášených kanálů prostřednictvím multiplexu. Odlišná délka jednotlivých oblouků má za následek odlišné fázové zpoždění jednotlivých signálů v daném oblouku (vyšší zpoždění pro složky signálu s kratšími vlnovými délkami). Rozdělení celkového WDM signálu proběhne následovně: celková intenzita prvního kanálu vstupujícího do demultiplexeru putuje do první výstupní větve, druhý kanál do druhé větve. Tento proces se opět opakuje, dokud nejsou rozděleny všechny kanály [60].

V případě demultiplexeru uvedeného v bodě 3 je základním prvkem Braggova mřížka. Signál z optického vlákna je pomocí této mřížky vyzařován do několika diskrétních směrů, kde každý ze směrů je přiřazen určitému kmitočtovému pásmu.

Multiplexery je možné realizovat stejnými technologiemi, jako jsou ty uvedené v bodech 1 až 3 [60].

3.2 Historický vývoj standardu BPON

Standard BPON přinesl oproti svému předchůdci několik zlepšení. Rozdělení provozu do tříd se rozrostlo o hlasové služby, jednalo se zejména o služby klasické telefonie a VoIP (Přenos hlasu přes Internet protokol – Voice over Internet Protocol). Spektrum vlnových délek používané pro sestupný směr bylo rozděleno do dvou pásem. První z těchto nových pásem bylo využíváno pro stávající BPON protokoly, nové pásmo bylo zamýšleno vyhradit pro přenos video služeb [17]. U standardu BPON bylo možné použít pro přenos jedno nebo dvě optická vlákna. V případě použití jednoho vlákna byla pro sestupný směr použita vlnová délka 1 310 nm a pro vzestupný směr 1 550 nm. V případě použití dvou optických vláken (jedno pro sestupný, druhé pro vzestupný směr) byla využita pouze vlnová délka 1 310 nm [37].

Organizace ITU přidělila nové pásmo vlnových délek v rozsahu 1 500 až 1 550 nm, které bylo využito pro WDM. Vlnová délka 1 550 nm pak byla využívána pro přenos video signálu [2]. Pro případ použití vlnového multiplexu byly upraveny používané vlnové délky pro přenos po jediném optickém vlákně. Pro sestupný směr bylo opět využito vlnové délky 1 310 nm, pro směr vzestupný potom 1 490 nm [37].

Pokračující vývoj v oblasti vlnových multiplexů přinesl zcela nový multiplex DWDM (Hustý vlnový multiplex – Dense Wavelength Division Multiplex), spektrum vlnových délek bylo upraveno pro použití s tímto novým multiplexem. Dynamické přidělování šířky pásma bylo standardizováno v již zmíněném doporučení G.983.4 [26], přínosem bylo zvýšení přenosové kapacity ve vzestupném směru [17].

Postupné nasazování BPON sítí dosáhlo svého vrcholu. S příchodem nového tisíciletí dochází k rozvoji v oblasti digitálního videa. Je zřejmé, že nejvyšší možná rychlost standardu BPON (622 Mb/s) by byla pro přenos digitálního signálu ve vysokém rozlišení nedostatečná, zvláště když je tato rychlost rozdělena mezi 32 koncových uživatelů. Vývoj v oblasti pasivních optických sítí se dále zaměřil na nové standardy, které by poskytly vyšší přenosové rychlosti i možnost připojení většího počtu koncových bodů [17].

3.3 Nasazení systému BPON

Testování systému BPON bylo uskutečněno již v roce 1999 americkou společností BellSouth. Ta při svých testech připojila celkem 400 subjektů na předměstí Atlanty. Při tomto testování byly koncovým uživatelům poskytovány služby Triple Play, VoD

bylo distribuováno po samostatném optickém kabelu, příjem byl realizován prostřednictvím video jednotky ONT, ve které bylo zakončeno vedení zajišťující přenos právě video služeb. Pro vysokorychlostní Internet a telefonní služby sloužila další jednotka ONT. Nasazený BPON systém byl provozován na vlnových délkách 1 490 nm (sestupný směr), 1 310 nm (vzestupný směr) a 1 550 nm (video signály). Byla nasazena asymetrická varianta s přenosovou rychlostí 622 Mb/s v sestupném směru a 155 Mb/s ve směru vzestupném [2].

V roce 2002 se začínají budovat sítě založené na standardu BPON také v Japonsku. V roce 2004 americká společnost Verizon připojila technologií BPON již více než milion domácností [2].

V průběhu roku 2001 však přichází organizace IEEE s novým standardem pasivních optických sítí EPON, který se stává poměrně silnou konkurencí. Důvodem jsou především pořizovací náklady ATM přepínačů, které jsou oproti pořizovacím nákladům Ethernetových přepínačů poměrně vysoké. Stejně tak je tomu i v případě síťových karet a dalších komponent. Standard EPON nachází široké uplatnění především v Asii, nejvíce potom v Číně, Koreji a Japonsku [19]. Počínaje rokem 2005 se v Japonsku stává dominantní technologií v oblasti PON sítí právě standard EPON [14].

4 Standard GPON

Gigabitová pasivní optická síť – Gigabit Passive Optical Network (GPON) je standard definovaný organizací ITU, konkrétně se jedná o sadu doporučení G.984. První doporučení G.984.1, které popisuje základní charakteristiku GPON sítí, bylo schváleno v roce 2003 [27]. Standard GPON podporuje všechny v současnosti známé telekomunikační služby.

4.1 Historický vývoj standardu GPON

Vývoj nových standardů pasivních optických sítí byl zapříčiněn především neustále se zvyšujícími nároky na šířku pásma. Technologie ATM, na které byly založeny dva předcházející PON standardy se příliš nerozšířila.

Velkou nevýhodou této technologie byla absence podpory všesměrového vysílání (tzv. broadcast). Prostřednictvím ATM však bylo možné realizovat skupinové vysílání (tzv. multicast). Princip multicastového spojení spočívá v existenci zdroje dat, který vysílá pouze pro účastníky, kteří mají o dané vysílání zájem a jsou registrováni v určité multicastové skupině. Prostřednictvím této multicastové skupiny jsou oprávněni k příjmu dat od určitého zdroje. Technologie ATM však nepodporovala vysílání od více zdrojů, zdroj dat mohl být pouze jeden. Všesměrové vysílání (broadcast) bylo možné realizovat prostřednictvím multicastového, kdy příjemci byly všechny uzly dané sítě. Nevýhod technologie ATM však bylo více [50].

Při návrhu standardu GPON byla standardizována i podpora technologie ATM, především pro zpětnou kompatibilitu s BPON. Od používání ATM však bylo postupně upuštěno (v roce 2014). Významným pokrokem je však zavedení nové zapouzdřovací metody GEM (Metoda zapouzdření GPON sítí – GPON Encapsulation Method), prostřednictvím které je možné zapouzdřit rámce různých přenosových technologií, nejčastěji se jedná o Ethernetové rámce [17]. Ovšem standard GPON není kompatibilní se standardem EPON, který je založený právě na technologii Ethernet [6].

Na vývoj měli také vliv poskytovatelé telekomunikačních služeb, kteří požadovali, aby bylo možné jejich již nasazená zařízení postupně modernizovat. Problém byl ovšem v tom, že v rámci jedné optické sítě nemůže být nasazen současně systém BPON i GPON, jelikož BPON disponuje pro přenos rozdílnými vlnovými délkami. Budovat však souběžně se stávající optickou telekomunikační infrastrukturou infrastrukturu novou by bylo ekonomicky příliš nákladné. Stejně tak by bylo technicky velmi náročné vyměnit všechny jednotky ONU umístěné u koncových uživatelů, popřípadě dočasně odstavit stávající telekomunikační síť z provozu. Proto bylo

přistoupeno k rezervaci vlnových délek pro GPON, která umožnila postupné nasazování nové generace PON sítí. Důležité bylo také zavedení filtrů do jednotek ONU, tyto filtry měly za úkol blokovat určitou vlnovou délku a umožnit tak plynulejší přechod na novou technologii. K nasazení technologie GPON ve větším měřítku došlo v letech 2008 a 2009 [17].

Se stále větším rozšířením protokolu IP (Internet Protocol) a rozšiřováním služeb VoD, docházelo také k navyšování počtu koncových uživatelů. Ochota koncových uživatelů platit za vyšší šířku pásma ovšem nebyla zrovna velká, bylo tedy nutné najít kompromis, který uspokojí potřeby koncových uživatelů (zákazníků) i poskytovatelů služeb. Začalo docházet k většímu nasazování pasivní optické technologie na přístupových sítích [14].

Nejvíce jsou PON sítě rozšířeny v Asii – v roce 2004 zde tvořil celosvětový podíl připojených koncových účastníků prostřednictvím PON 93 %, jednalo se o počet 1,4 milionu koncových uživatelů. Z tohoto celkového počtu bylo v Asii v roce 2004 bezmála 84 % koncových uživatelů připojeno prostřednictvím standardu BPON a ve zbývajících 16 % se jednalo o konkurenční technologii EPON. Druhým kontinentem, kde docházelo k plošnému nasazování PON sítí byla Amerika, především pak Spojené státy americké, kde podíl koncových uživatelů připojených prostřednictvím standardu BPON dosahoval v roce 2004 počtu 81 % a zbývajících 19 % připadalo opět technologii EPON. K pozvolnému nasazení systému GPON začalo docházet až v roce 2006, kdy tento standard začal postupně nahrazovat svého předchůdce BPON [14].

Standard GPON nabízí nové rozsahy přenosových rychlostí. V sestupném směru je možné využít rychlosti 1 244 nebo 2 488 Mb/s, ve směru vzestupném jsou podporovány rychlosti 155, 622, 1 244 a 2 488 Mb/s [27]. Tyto rychlosti je možné kombinovat, nejpoužívanější variantou je asymetrická varianta s přenosovou rychlostí 2 488 Mb/s ve směru sestupném a 1 244 Mb/s pro vzestupný směr. Stejně jako u předchozích standardů jsou podporovány přenosové rychlosti 155 a 622 Mb/s, je tedy zachována zpětná kompatibilita [6].

Pro přenos jsou vyhrazeny následující rozsahy vlnových délek: v sestupném směru se jedná o rozsah 1 480 až 1 500 nm, ve směru vzestupném je stanoven rozsah 1 260 až 1 360 nm. Pro přenos video signálů je možné využít doplňkový rozsah vlnových délek 1 550 až 1 560 nm [6].

Došlo také ke zvýšení rozbočovacího poměru na dvojnásobek. Sítě založené na standardu GPON mohou využívat rozbočovacího poměru 1:64, do budoucna je uvažován rozbočovací poměr 1:128. Logický dosah GPON sítě je 60 km, typický fyzický dosah GPON sítě je potom 10, případně 20 km [27].

4.2 Komunikace v GPON

Standard GPON používá již zmíněnou metodu zapouzdřování GEM, pomocí které je možné zapouzdřit různé datové typy. Komunikace je spojově orientovaná [6].

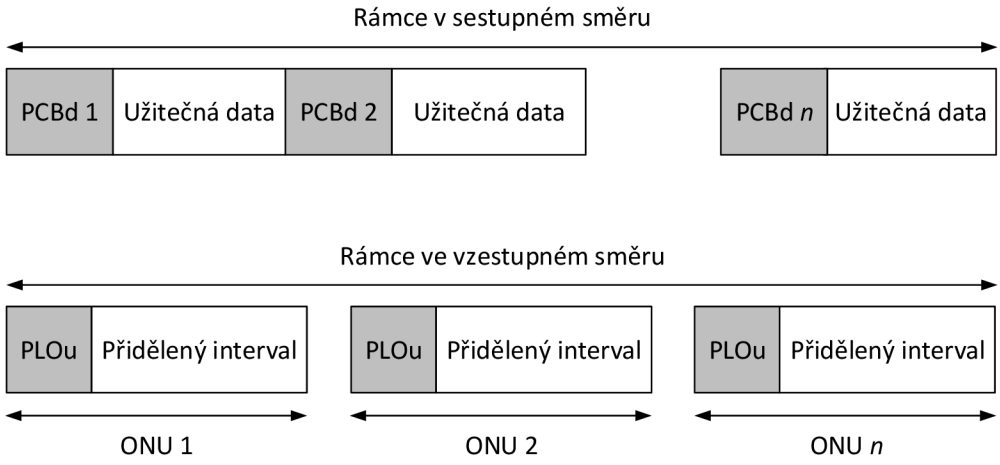
Rámce jsou v sestupném směru vysílány všesměrově, putují tedy ke všem koncovým jednotkám. Pro sestupný směr je využito časového multiplexu TDM, obdobně jako u standardu BPON. Každá z koncových jednotek však musí přijmout pouze rámce, které jsou určeny právě pro ni. Toto je zajištěno pomocí unikátních identifikátorů obsažených v rámci. Data tedy zpracuje pouze jednotka, pro kterou byla tato data určena.

Standard GPON provádí dvojité zapouzdření dat. Rámce různých síťových technologií (nejčastěji Ethernetové) jsou zapouzdřeny do rámce GEM, který je následně zapouzdřen do rámce GTC (Přenosová vrstva standardu GPON – GPON Transmission Convergence). Rámec GTC může obsahovat ATM buňky a také TDM provoz [1].

Rámce posílané v sestupném směru jsou složeny z PCBd (Kontrolní blok fyzické vrstvy v sestupném směru – Physical Control Block downstream), které jsou následovány částí vyhrazenou pro ATM buňku a částí vyhrazenou pro GEM, v obrázku označeno jako užitečná data. Délka záhlaví PCBd má stejnou velikost pro všechny přenosové rychlosti, právě v PCBd se nachází informace, podle kterých jednotka ONU rozpozná data určená pro ni. V případě, že na odeslání nečekají žádná data, rámce jsou v sestupném směru přenášeny i nadále – slouží k časové synchronizaci [1, 6].

Ve vzestupném směru je stejně jako u standardu BPON využito techniky TDMA. Jednotka OLT pomocí této techniky přiřazuje jednotkám ONU proměnlivé časové intervaly, které slouží především k synchronizaci přenosu shluku dat, které jednotky ONU ve vzestupném směru vysílají. Struktura GPON rámců ve vzestupném i sestupné směru je zobrazena na obrázku 4.1.

Podstatným zlepšením je také používání techniky FEC (Samoopravný kód – Forward Error Correction). Pomocí tohoto kódování je možné chybu v přenosu nejen odhalit, ale také ji opravit. K zakódované posloupnosti bitů jsou přidány nadbytečné (redundantní) informace, velikost přidaných informací je však minimální a nedochází tak ke zvyšování režie spojené s přenosem dat. Pokud je ale použita vyšší hodnota FEC, má tato skutečnost za následek pokles přenosové rychlosti [6].



Obr. 4.1: Struktura GPON rámce [28].

4.3 Dynamické přidělování šířky pásma

Pro přidělování šířky pásma ve vzestupném směru jsou používány přepravní kontejnery označené jako T-CONT (Přenosový kontejner – Transmission Container). Přínosem používání těchto kontejnerů je zlepšení využití celkové šířky pásma, jednotka ONU při své komunikaci vysílá jeden nebo více těchto kontejnerů. Kontejnery T-CONT umožňují implementaci QoS (Kvalita služeb – Quality of Services) při přenosech ve vzestupném směru. Definováno je celkem pět druhů transportních kontejnerů sloužících různým účelům [1, 6]:

1. Garance pevně přidělené šířky pásma pro služby citlivé na zpoždění (VoD, VoIP).
2. Garance pevně přidělené šířky pásma pro služby, které nejsou citlivé na zpoždění (datové přenosy).
3. Kombinace pevně a dynamicky přidělené šířky pásma (služby Triple Play).
4. Dynamické přidělení šířky pásma, přidělení šířky pásma pro přenos není garantováno (best effort). Využívá se například pro:
   - Emailové služby, např. protokol SMTP (Protokol pro přenos elektronické pošty – Simple Mail Transfer Protocol).
   - Přenos souborů, například protokol FTP (Protokol pro přenos souborů – File Transfer Protocol).
   - Procházení webových stránek.
5. Kombinace všech předchozích, vhodné pro obecné datové toky.

Přidělování dostupné šířky pásma pro jednotlivé koncové jednotky ONU má na

starost opět jednotka OLT. K přidělování šířky pásma dochází pouze ve vzestupném směru, ve směru sestupném jsou data vysílána všesměrově pro všechny koncové jednotky [1].

Pro zjištění požadované šířky pásma využívá jednotka OLT informace obsažené v transportním kontejneru T-CONT, který je přiřazen určité jednotce ONU. Transportní kontejner obsahuje informaci, jaký počet datových jednotek je obsažen ve vyrovnávací paměti příslušné jednotky ONU. Tuto informaci vyhodnocuje jednotka OLT, která může znovu rozdělit granty pro koncové jednotky ONU. Pokud ONU nemá žádná data k odeslání, tak po obdržení grantu vyšle pouze prázdnou datovou jednotku. Tento stav znamená prázdnou vyrovnávací paměť jednotky ONU, jednotka OLT může tedy grant poskytnout jiné ONU. Pokud má jednotka ONU plnou vyrovnávací paměť, OLT může takové jednotce poskytnou více grantů [6].

4.4 Nasazení systému GPON

V roce 2006, 20 let po spuštění první testovací PON sítě (zmíněné v kapitole 1.3 na straně 18), jsou ve Francii zahájeny přípravy na realizaci OAN. Různí francouzští poskytovatelé telekomunikačních služeb začínají připojovat koncové uživatele prostřednictvím FTTH. Počátkem léta roku 2006 francouzská společnost France Telecom zahájila testování vysokorychlostních přípojek založených na technologii GPON. Systém byl testován v celkem šesti pařížských čtvrtích a v menší míře také v okolních městech. Optické vlákno bylo přivedeno až do domácností koncových uživatelů (FTTH) a připojeno bylo několik stovek domácností [20].

Dalším testem standardu GPON bylo testování provedené v Německu společností Deutsche Telekom. Testování bylo provedeno v Berlíně a městě Potsdam (Postupim). Hlavním záměrem tohoto testování byla zkouška technologie GPON a také nových technologií pokládky. V těchto městech byla realizována pokládka zafouknutím optického kabelu do již položených chrániček. Na poslední míli byla optická vlákna pro jednotlivé koncové uživatele zafouknuta do mikrotrubiček, jednalo se tedy o realizaci FTTH. Připojeno bylo celkem 9 institucí, koncoví uživatelé byli vybaveni jednotkami ONT, které disponovaly 100 Mb/s porty [65].

Dalším městem, kde byl GPON systém testován společností Deutsche Telekom byly Drážďany. Zde bylo skoro celé město připojeno prostřednictvím VDSL, bylo však již využito optických přenosových vedení, která byla zakončena v rozvodných uzlech (FTTC). Výhodou také bylo, že v části města vybrané pro testování GPON systému bylo optické vedení instalováno již na počátku devadesátých let. Vedení využíval optický systém HYTAS94, prostřednictvím kterého byly provozovány telefonní služby (POTS i ISDN). Tento systém však nebyl schopen poskytnout dostatečné

přenosové rychlosti pro služby Triple Play, systém nebyl standardizován ani dále vyvíjen [65].

Po zkušenostech z testu GPON systému v Berlíně se společnost Deutsche Telekom v roce 2008 rozhodla systém otestovat ve velkém právě v Drážďanech. Připojeno bylo na 3 500 budov, které celkově čítaly 27 000 domácností. Ve velkých budovách bylo připojení realizováno pomocí FTTB, ve sklepních prostorách byly umístěny jednotky ONU, na které se pomocí stávajících metalických vedení připojovali koncoví uživatelé. Zakončení FTTH bylo realizováno pouze pro nejmenší budovy, typicky rodinné domy [65].

V současné době jsou GPON sítě nasazovány především v Evropě, konkurenční technologie EPON dominuje v Asii. [18].

5 Standard XG-PON

X Gigabitová pasivní optická síť – X Gigabit Passive Optical Network (XG-PON) je dalším ze standardů definovaných ITU, a to v sadě doporučení G.987. První doporučení z této sady G.987.1 [30], které popisuje základní charakteristiku XG-PON sítí bylo schváleno v roce 2010 (jeho první verze). Standard je někdy také označován jako 10G-PON[1].

Jakmile byl standard GPON více rozšířen, organizace FSAN logicky obrátila svoji pozornost na následovníka úspěšného standardu GPON. Od roku 2007 začaly přípravy na vývoj nové generace pasivních optických sítí vedené organizací FSAN společně s ITU. Prvotním cílem bylo definování požadavků na novou generaci PON, které bylo dokončeno v průběhu roku 2009 [17].

Výsledkem této práce byl vznik výše zmíněné sady doporučení G.987, která standard XG-PON definuje. Standard XG-PON má s předchozím standardem GPON mnoho společných vlastností [21].

5.1 Historický vývoj standardu XG-PON

Jedním z hlavních požadavků na vývoj nových standardů pasivních optických sítí je zajištění vyšší šířky pásma pro koncové uživatele ve srovnání s předchozími standardy. Důležitým požadavkem je také zajištění co možná nejméně problémového přechodu na novou technologii PON, a to jak pro poskytovatele služeb, tak i pro koncové uživatele [16].

Většina z provedených studií dokazuje, že poptávka po vyšší šířce pásma stále roste, a to 6 až 10× v průběhu každých 6 let a nic nenasvědčuje tomu, že tento trend nebude pokračovat [36]. Nárůst je způsoben stále se zvyšujícím podílem televizních a jiných video služeb, které jsou prostřednictvím Internetu provozovány. Do budoucna se dá navíc očekávat další zvýšení tohoto podílu, jelikož se zvyšuje i počet zařízení, která tyto služby podporují, zejména pak televizních přijímačů, ale také mobilních zařízení. V případě televizních přijímačů se zvyšuje také jejich rozlišení, stejně jako rozlišení samotného videa, které má velký vliv na potřebnou šířku pásma k jeho přenosu [36].

Významným milníkem bylo také schválení doporučení G.984.5 [29], které rozšířilo specifikaci stávajícího standardu GPON. Primárním cílem doporučení bylo umožnit co možná nejjednodušší přechod ze standardu GPON na nově vyvíjený standard. Došlo k novému přidělení vlnových délek a také k definici speciálního WDM členu, který zajistí společné fungování dvou odlišných standardů. Definovány byly také

[1] Písmeno *X* v označení je římskou číslicí odkazující na přenosovou rychlost 10 Gb/s.

filtry pro koncové jednotky, které mají za úkol blokovat určité vlnové délky. Cílem je zabránit nežádoucímu vzájemnému ovlivňování při společném fungování dvou generačně odlišných standardů [29].

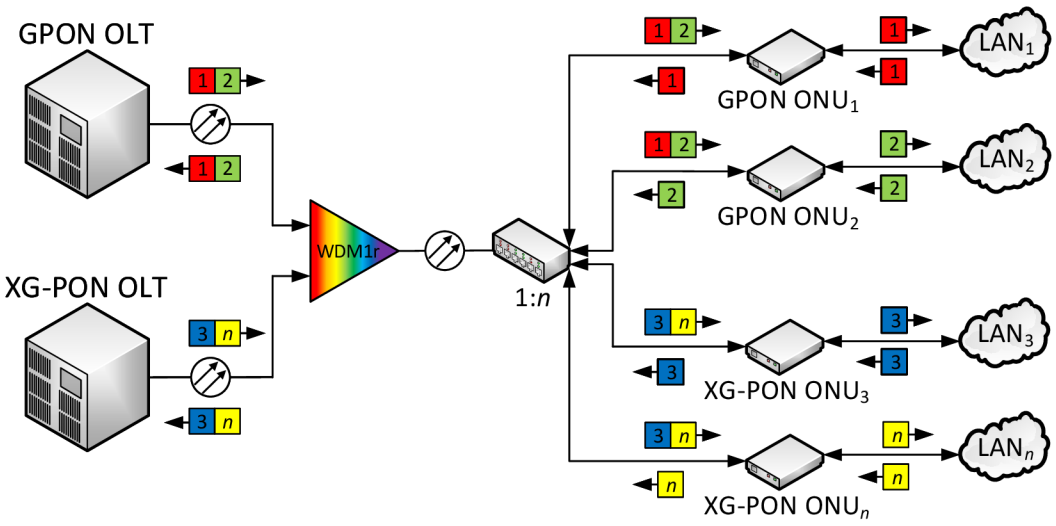
5.1.1 Nová generace PON

Při vývoji nové generace pasivních optických sítí, označované jako NG-PON, byl tento vývoj rozdělen na dvě dílčí generace: NG-PON1 a NG-PON2, v závislosti na možnostech společného provozu se staršími standardy PON na společné síťové infrastruktuře [16]. Studie NG-PON uvažovala s rozvojem a nasazením nového standardu v rozmezí let 2012 až 2015 (NG-PON1), technologie, které zatím nebyly vhodné pro implementaci v tomto období byly zařazeny do studie pro další generaci (NG-PON2) [36].

V případě NG-PON1 je zaručena podpora společného fungování (koexistence) tohoto standardu na stejné ODN spolu se standardem GPON. Výhodou možnosti koexistence je snadnější přechod na nový standard bez nutnosti velkých zásahů do stávající síťové infrastruktury a tedy i narušení funkčnosti služeb stávajících koncových uživatelů. Při výběru vhodné metody pro zajištění koexistence bylo zvažováno použití TDM nebo WDM. Nakonec byla vybrána technologie WDM jak pro sestupný, tak i pro vzestupný směr [8]. Zaveden byl tzv. WDM1r filtr, který slouží k sloučení, případně filtraci vlnových délek jednotlivých signálů (GPON a XG-PON), příležitostně slučuje i video signály. Slouží pro propojení OLT jednotek obou standardů s optickou distribuční sítí ODN [30]. Příklad možné koexistence dvou odlišných standardů PON je zobrazen na obrázku 5.1, předpokladem koexistence je, že jednotky ONU obsahují filtry, které v závislosti na standardu PON filtrují příslušnou vlnovou délku.

Požadavky na novou generaci NG-PON1 byly především na možnost připojení vyššího počtu uživatelů, lepší opatření k zajištění QoS a bezpečnost [16]. Pro NG-PON1 bylo uvažováno hned několik možných variant: TDM PON, WDM PON, CDMA PON, i kombinace těchto technologií. Problémem však byla odlišnost jednotlivých řešení v jejich architektuře i profilu služeb [8]. Pro svou jednoduchost a možnost budoucího finančně výhodného nasazení však nakonec byla vybrána 10 gigabitová varianta PON založená na přístupové metodě TDM [36].

Naproti tomu druhá generace pasivních optických sítí nové generace NG-PON2 obsahovala systémy, které nebyly zpětně kompatibilní se staršími standardy. To bylo způsobeno zejména nutností vybudování nové distribuční části sítě (ODN), případně byly potřebné nové technologie, které však nebyly dostupné v blízkém časovém horizontu [8].



Obr. 5.1: Koexistence standardů GPON a XG-PON [30].

5.1.2 XG-PON1 a XG-PON2

Jako nejlepší kandidát pro NG-PON1 byl nakonec zvolen systém označený jako XG-PON [45]. XG-PON se dále dělí na XG-PON1 a XG-PON2, rozdíl je pouze v podporovaných přenosových rychlostech [36]. XG-PON1 podporuje přenosovou rychlost 10 Gb/s v sestupném směru a 2,5 Gb/s ve vzestupném směru. Naproti tomu XG-PON2 je symetrickým systémem, který v obou směrech podporuje přenosovou rychlost 10 Gb/s. Pro XG-PON2 se používá také označení XGS-PON (10 Gigabitová symetrická PON – 10 Gb/s Symmetrical PON), které více zdůrazňuje, že se jedná o symetrickou variantu [30]. Důvod pro rozdělení je především ekonomický, symetrická varianta je nákladnější a na trhu nebyla zaznamenána velká poptávka po tomto řešení, vývoj byl dočasně přerušen [17].

Využito je rozsahu vlnových délek 1 575 až 1 580 nm pro sestupný směr a 1 260 až 1 280 nm pro směr vzestupný. Jako minimální rozbočovací poměr pro zajištění bezproblémové koexistence standardů GPON a XG-PON je udáván poměr 1:64. Podporován je pak rozbočovací poměr 1:256, do budoucna se počítá s jeho rozšířením. Standard musí podporovat přenos na vzdálenost minimálně 20 km, maximální možná udávaná vzdálenost je pak 60 km [30].

Při vývoji standardu XG-PON bylo uvažováno několik možných variant přidělení vlnových délek, především z důvodu zajištění již zmíněné koexistence. Výběr vhodné vlnové délky pro sestupný směr byl relativně snadný, uvažováno bylo pásmo okolo 1 578 nm. Tento krok byl shodný s volbou vlnové délky při vývoji standardu 10GEPON (10 Gigabitová Ethernetová pasivní optická síť – 10 Gigabit Ethernet

Passive Optical Network), který vznikal pod hlavičkou IEEE. Naproti tomu výběr vhodného rozsahu vlnových délek pro vzestupný směr již tak snadný nebyl. Bylo zvažováno celkem pět možností [8]:

1 595–1 615 nm: tento rozsah byl zamítnut, důvodem byly obavy z nedostatečné specifikace optických vláken a komponentů PON pro tyto vlnové délky.

1 540–1 560 nm: rozsah byl opět zamítnut, důvodem byla nekompatibilita s překryvným video signálem, navíc tento rozsah používá velká část implementovaných PON na celém světě.

1 530–1 540 nm: důvodem zamítnutí tohoto rozsahu byly náklady na pořízení jednotek ONU pro tento rozsah vlnových délek a také fakt, že stávající ONU technologie GPON nejsou schopny tento rozsah blokovat.

1 340–1 360 nm: v případě vybrání tohoto rozsahu by bylo nutné k zajištění koexistence použít „koexistenční“ filtr. Takový filtr by však podstatně zvyšoval útlum celé PON. Rozsah byl z tohoto důvodu také zamítnut.

Další rozhodnutí směřovalo k výběru rychlosti linky a kódování. Při výběru se rozhodovalo mezi řešeními, která byla standardizována a komerčně používána – SDH a Ethernet. V této fázi výběru se objevila také otázka, zda by standard XG-PON nebyl schopný koexistence také se standardem 10GEPON, jelikož díky použití WDM je možná koexistence s EPON systémy (1 Gb/s). Pokud by byla vyžadována taková komplexní koexistence, bylo by logické zvolit právě Ethernet. Bylo však rozhodnuto, že tato koexistence různých generací typově odlišných systémů nebude potřebná. Nebylo totiž pravděpodobné, že by poskytovatelé služeb nasazovali současně XG-PON a 10GEPON na společnou síťovou infrastrukturu [8]. Jiná situace by ale nastala v momentě, kdy by se poskytovatel služeb z nějakého důvodu rozhodl přejít ze standardu GPON na standard 10GEPON. Tento způsob koexistence by vyžadoval vhodné oddělení jednotlivých rozsahů vlnových délek pomocí filtru jednotky OLT, tímto způsobem by se předešlo možnému rušení. Jedná se však o méně pravděpodobný způsob koexistence [1].

Mezi novinky zavedené standardem XG-PON patří také opatření přispívající k šetření energie. V případě, že dojde k výpadku primárního zdroje napájení a jednotka OLT je napájena ze záložního zdroje (typicky baterie), je cílem snížit zatížení jednotky tak, aby baterie byla schopna jednotku napájet déle. Při napájení z primárního zdroje je pak snaha snížit spotřebu elektrické energie na nejnižší možnou hodnotu. Jednou z možností je vypnutí uživatelského síťového rozhraní, které není aktivně využíváno. Další z možností je deaktivace vysílače v případě, že uživatel nemá žádná data k odeslání (Dozing). V případě neaktivního uživatele deaktivuje jednotka ONU svůj vysílač i přijímač (Sleeping), poslední jmenované řešení pak vykazuje nejvyšší úsporu energie [8].

5.2 Komunikace v XG-PON

Standard XG-PON vychází ze svého předchůdce – standardu GPON, oba standardy mají řadu společných vlastností, standard XG-PON přináší i řadu vylepšení. Princip komunikace je shodný s předešlými standardy. Rámce technologie XG-PON jsou složeny ze záhlaví XGTC (Konvergence přenosu XG-PON – XG-PON Transmission Convergence) a části vyhrazené pro užitečná data. Záhlaví XGTC je potom v sestupném směru složeno z dalších tří částí [31]:

1. Část s pevnou velikostí, obsahuje informace o délce následujících částí záhlaví. Chráněna je pomocí HEC (Korekční kód hlavičky – Header Error Correction).
2. Přidělení šířky pásma (Bandwidth Map), zde jsou obsaženy informace o přidělené šířce pásma pro danou jednotku ONU.
3. Poslední část je určena pro přenos PLOAM zpráv.

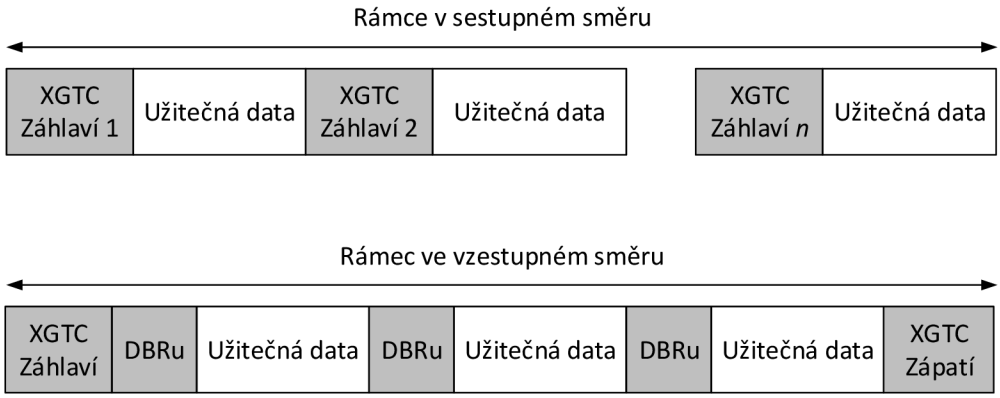
Oproti standardu GPON mohou rámce posílané v sestupném směru obsahovat více než jednu zprávu PLOAM. Výhodou je lepší odezva kanálu, tento fakt využívají již zmíněné metody určené k šetření energie. Byla zvýšena i samotná velikost PLOAM.

U shluku dat, který je posílán ve vzestupném směru existují opět různé druhy záhlaví. Na začátku shluku dat je hlavička s pevně danou a proměnlivou velikostí. První jmenovaná hlavička obsahuje identifikační číslo jednotky ONU, toto identifikační číslo je u standardu XG-PON rozšířeno, z důvodu podpory většího rozbočovacího poměru. Je podporováno až 1 023 koncových jednotek ONU. Hlavička s proměnnou velikostí obsahuje zprávu PLOAM vyslanou ve vzestupném směru (pokud tedy byla vyslána). Dále může být obsažena volitelná hlavička, sloužící k přenosu zprávy DBRu (Zpráva o přidělení šířky pásma ve vzestupném směru – Dynamic Bandwidth Report upstream) [8]. Rámce technologie XG-PON jsou zobrazeny na obrázku 5.2.

Podobně jako standard GPON používá metodu zapouzdření GEM, ve standardu XG-PON je metoda označena jako X-GEM (Metoda zapouzdření XG-PON sítí – XG-PON Encapsulation Method). Metoda zajišťuje tři hlavní úkoly [31]:

1. Značkování provozu prostřednictvím 16 bitového ID.
2. Fragmentaci.
3. Zajištění soukromí pro přenášená data.

Při fragmentaci je možné přenášené datové jednotky rozdělit tak, že první část (fragment) je přenášena v aktuálním rámci a jeho druhá část hned při příští příležitosti. Pravidla tvorby fragmentů byla upravena tak, aby nedocházelo k vytváření příliš malých fragmentů [8].



Obr. 5.2: Struktura XG-PON rámce [31].

5.3 Nasazení systému XG-PON

Jedním z prvních testů technologie XG-PON byl test provedený v roce 2009 americkou společností Verizon ve městě Taunton. Společnost Verizon začala nasazovat pasivní optické sítě od roku 2004, kdy nasazovala sítě založené na standardu BPON, s rostoucími požadavky na přenosové rychlosti postupně přecházela po schválení standardu GPON právě na tento standard.

Cílem testu bylo ověření schopnosti současného fungování technologie XG-PON a GPON na společné síťové infrastruktuře a zároveň schopnosti technologie XG-PON dosáhnout až čtyřnásobného zvýšení propustnosti v sestupném směru. Při testu tak došlo k překryvu optického signálu technologie XG-PON na stávající síti GPON.

Na straně poskytovatele služeb byla v rámci testu nainstalována OLT jednotka technologie XG-PON. Jednalo se o prototyp XG-PON1, vyrobený firmou Huawei ještě před samotným schválením standardu. Podporovány tedy byly přenosové rychlosti 10 Gb/s v sestupném směru a 2,5 Gb/s ve vzestupném směru. Pomocí WDM (WDM1r člen) byl zkombinován optický signál technologie XG-PON a GPON spolu s optickým signálem, který zajišťoval přenos video služeb. Video služby byly distribuovány jak ONT jednotce technologie XG-PON, tak i GPON ONT jednotce. Stávající GPON OLT jednotka byla spolu s nově instalovanou XG-PON OLT jednotkou připojena prostřednictvím hraničních směrovačů do Internetu.

Stávající GPON ONT jednotky byly vybaveny filtry blokující vlnové délky využité technologií XG-PON, konkrétně pásmo 1 575 až 1 625 nm bylo vyhrazeno pro sestupný směr. Pro vzestupný směr technologie XG-PON byl využit rozsah vlnových délek 1 260 až 1 280 nm, z tohoto důvodu byl původní rozsah technologie GPON pro vzestupný směr omezen na 1 290 až 1 330 nm. Potřeba bylo i speciálního WDM1r

členu, který zajistil sloučení vlnových délek technologií XG-PON a GPON a jejich následný přenos po společném vlákně. Podobný člen již společnost Verizon využila při koexistenci standardů BPON a GPON [36].

Na straně koncových uživatelů zapojených do tohoto testování byl nainstalován pasivní optický rozbočovač s rozbočovacím poměrem 1:2, který měl za úkol rozdělit optický signál mezi XG-PON a GPON ONT jednotky. Tímto bylo dosaženo možnosti sledovat případné dopady koexistence těchto dvou technologií, bylo také možné sledovat chování každé z technologií zvlášť.

XG-PON systém byl při koexistenci se systémem GPON schopen poskytnout přenosovou rychlost 9,868 Gb/s ve směru sestupném a 2,398 Gb/s ve směru vzestupném, a to i bez ohledu na přítomnost signálu technologie GPON [36].

Před testováním v terénu byl prototyp XG-PON systému otestován v laboratořích společnosti Verizon. Toto testování bylo zaměřeno především na fyzickou vrstvu, prototyp v těchto testech vyhověl. Zmíněný prototyp umožňoval bezchybný přenos dat až na vzdálenost 60 km.

Testování technologie XG-PON bylo úspěšné, při testech nebyl prokázán žádný dopad koexistence technologie XG-PON a GPON provozovaných na společné síťové infrastruktuře. Tato skutečnost umožňuje poskytovatelům služeb plynulý přechod z technologie GPON na technologii XG-PON bez významného ovlivnění stávajících koncových uživatelů [36].

Je také možné, že k hromadnému nasazení a dalšímu rozvoji XG-PON2 nakonec nedojde. Organizace IEEE již standardizovala standard 10GEPON, který disponuje přenosovou rychlostí 10 Gb/s v obou směrech. Poskytovatelé telekomunikačních služeb by mohli tento standard upřednostnit a ITU by tak mohla začít pracovat na vývoji další generace PON [17].

V roce 2016 organizace ITU vydala nové doporučení podporující nasazení standardu XG-PON2 (XGS-PON) [5].

6 Standard NG-PON2

Mezi nejnovější standardy PON vznikající pod hlavičkou Mezinárodní telekomunikační unie patří standard označený jako NG-PON2. Definovaný je v sadě doporučení G.989, první doporučení z této sady G.989.1 popisující základní požadavky na nový systém bylo schváleno v roce 2013 [32].

6.1 Historický vývoj standardu NG-PON2

NG-PON2 původně neobsahoval žádné požadavky k zajištění koexistence se staršími standardy PON. V roce 2010 bylo rozhodnuto, že NG-PON1 a NG-PON2 budou standardizovány nezávisle na sobě. Vývoj nového standardu byl však opožděn. Důvodem byl pokles zájmu provozovatelů telekomunikačních služeb o novou architekturu PON a také zpomalení trhu, které ovlivnily investice provozovatelů služeb do přístupových sítí. Bylo však patrné, že současné standardy založené především na přístupové metodě TDMA, přestanou časem vyhovovat neustále se zvyšujícím požadavkům na šířku pásma. NG-PON2 v této době ještě neměl stanovenu žádnou preferovanou technologii, opět byl zvažován výběr mezi TDMA PON, WDM PON a CDMA PON [16]. Jako velmi pravděpodobné se jevilo, že bude vybrána varianta WDM PON [17]. Požadavky na novou generaci PON byly následující [22]:

- Vysoká finanční efektivita.
- Vysoká kapacita.
- Velký dosah a široké pokrytí.
- Efektivní přidělení síťových prostředků.
- Konkurenceschopnost.
- Vysoká energetická účinnost.

Níže následuje stručný popis jednotlivých variant zvažovaných pro NG-PON2 [1, 22]:

TDM/WDM PON: jedná se o hybridní variantu, která využívá výhody TDM (flexibilní přidělení šířky pásma) a WDM (především vysoká kapacita). Tato varianta je dále rozdělena podle způsobu přidělování vlnových délek jednotlivým koncovým jednotkám. V případě statické varianty, jsou vlnové délky pro vzestupný a sestupný směr jednotkám ONU přiděleny pevně a nelze je během provozu měnit. Naproti tomu u dynamické varianty je možná dynamická změna vlnových délek v závislosti na datovém provozu.

WDM PON: jak již název napovídá, využívá pro přenos vlnového multiplexu. Každé koncové jednotce ONU je pro komunikaci s OLT přidělena rozdílná vlnová délka (jak pro sestupný, tak i pro vzestupný směr). Výhodou je, že dostupná šířka pásma není mezi jednotkami ONU sdílena, WDM PON umožňuje

každé ONU využívat maximální přenosovou rychlost. Podle počtu podporovaných vlnových délek a technologie vlnového multiplexu jsou WDM PON rozděleny do dvou tříd:

- DWDM PON založené na multiplexu DWDM (Hustý vlnový multiplex – Dense Wavelength Division Multiplex) a
- PON založené na multiplexu CWDM (Hrubý vlnový multiplex – Coarse Wavelength Division Multiplex), tedy CWDM PON.

CDMA PON: v této variantě je pro komunikaci mezi OLT a ONU použito různých kódů. Kódy jsou přiděleny jednotlivým uživatelům, data těchto uživatelů jsou poté pomocí přidělených kódů kódována do sekvencí pulzů (nebo z těchto sekvencí dekódována). Nespornou výhodou CDMA PON je vyšší bezpečnost. Jednotka ONU je schopna dekódovat pouze data, která jsou určena výhradně pro ni.

OFDM PON: pro své fungování využívá metodu OFDM (Ortogonální multiplex s frekvenčním dělením – Orthogonal Frequency Division Multiplex). Princip OFDM spočívá v rozdělení širokopásmového signálu do mnoha subnosných s nižší šířkou pásma. Subnosné se částečně překrývají, ale vzájemně se neovlivňují, je možné je modulovat pomocí modulací vyššího řádu, dosáhne se tak snížení požadavků na šířku pásma. V sestupném směru je pomocí OFDM dosaženo vysoké bitové rychlosti, ve směru vzestupném slouží k vícenásobnému řízení přístupu. Systém se také vyznačuje dobrou škálovatelností a umožňuje poskytnout přenosovou rychlost 40 Gb/s každému koncovému uživateli. OFDM dále umožňuje flexibilní přidělování šířky pásma a podporuje více služeb, ke svému fungování využívá cenově dostupné elektronické komponenty namísto optických prvků.

U PON založených na TDMA s vysokou přenosovou kapacitou by bylo nutným předpokladem vyřešit problém s disperzí a také se snížením citlivosti přijímače. Dále by bylo nutné navýšit počet portů pro připojení většího počtu koncových uživatelů.

U WDM PON byl problém s použitím vhodných zařízení na straně koncových uživatelů, selektivních na určitou vlnovou délku. Navzdory rychlému pokroku v oblasti přijímačů pro jednotky ONU pro využití ve WDM PON sítích, byly tyto přijímače však podstatně dražší ve srovnání s přijímači určenými pro TDMA PON. Řešení WDM PON zatím nesplňovalo požadavky na finanční efektivitu.

Systémy CDMA PON byly teprve ve fázi výzkumu, bylo nutné vyřešit nedostatky s mechanismem přidělování šířky pásma. Dalším problémem byla nedostatečná vyspělost a nedostatek optických kodérů a dekodérů pro tuto technologii PON [22]. Současně se zvyšováním přenosových rychlostí v přístupových sítích prostřednictvím zavádění nových standardů do provozu se však muselo brát v potaz, že spolu se zvy-

šováním přenosové kapacity přístupových sítí je samozřejmě nutné mít dostatečně dimenzované i sítě transportní [16].

Mezi další systémy, ze kterých by v budoucnu mohl být vytvořen další standard patří například OFDM PON, nebo koherentní PON. Tato řešení by v budoucnu mohla uspokojit požadavky na velmi vysokou přenosovou kapacitu, vyšší dělicí poměr a tedy i vyšší pokrytí. Uvedená řešení by ale spadala spíše do další generace PON [22].

Řešením, které bylo nakonec vybráno pro standardizaci je hybridní varianta PON využívající TDM a WDM, označovaná jako TWDM PON (Časový a vlnový multiplex – Time and Wavelength Division Multiplex). Výběr byl proveden v roce 2012, v roce 2013 došlo k potvrzení výběru organizací ITU. Jako efektivnější řešení se jevilo využití dostupných a ověřených optických komponent. Významnou roli také hrála podpora průmyslu, která je pro výslednou cenu a širokou dostupnost technologie klíčová [1, 47].

Podobný závazek jako Česká republika, resp. Evropská unie (zajistit přenosovou rychlost 30 Mb/s pro všechny obyvatele a 100 Mb/s alespoň pro 50 % obyvatel a zároveň všechny nové zákazníky do roku 2020) [62] přijaly i Spojené státy americké. V roce 2009 zde byl spuštěn program pod názvem „Connecting America: The National Broadband Plan“, v tomto programu byly plány poněkud ambicióznější. Cílem bylo zajistit přenosové rychlosti 100 Mb/s v sestupném a 50 Mb/s ve vzestupném směru pro 100 milionů amerických domácností. Dále se počítalo s přenosovou rychlostí 1 Gb/s pro místní komunity [45].

Logickým požadavkem na PON nové generace je, aby v souvislosti se zvyšujícími se nároky na šířku pásma poskytovaly lepší přenosové parametry než stávající PON standardy. Systém NG-PON2 musí podporovat přenosovou rychlost 40 Gb/s (v důsledku přidělení vlnových délek) v sestupném směru a 10 Gb/s ve vzestupném směru. Dosah NG-PON2 musí být 40 km (pasivní infrastruktura), celková vzdálenost je poté stanovena na 60 km [32]. NG-PON2 využívá nově přidělená pásma vlnových délek: pro sestupný směr se jedná o rozsah 1 596 až 1 603 nm, pro vzestupný směr je potom přidělen rozsah 1 524 až 1 544 nm. Kromě výše uvedeného rozsahu je ještě pro vzestupný směr definováno redukované pásmo vlnových délek 1 528 až 1 540 nm a úzké pásmo o rozsahu 1 532 až 1 540 nm [33].

Důležitým krokem je také nasazení tzv. „bezbarvých“ jednotek ONU, které nejsou určeny pouze pro specifickou vlnovou délku. Cena koncových jednotek je také důležitým parametrem, toto řešení navíc usnadní i správu koncových jednotek, protože v síti bude pouze jeden typ [32]. Vysoká cena koncových jednotek by navíc mohla být překážkou pro rozsáhlejší nasazení PON. Bezbarvé jednotky ONU tak zajistí provoz, který bude nezávislý na vlnové délce [45].

Dále se předpokládá, že NG-PON2 bude víceúčelovou infrastrukturou, která

umožní sloučit různé telekomunikační služby a splní také požadavky na služby nové. Nejen z tohoto důvodu je žádoucí, aby bylo možné síť založenou na NG-PON2 flexibilně rozšiřovat. Se stále se zvyšujícím podílem mobilních sítí a rostoucími nároky na jejich přenosovou kapacitu a rychlost bude nutné uspokojit požadavky také pro tento druh přístupových sítí. Zde se NG-PON2 jeví jako perspektivní řešení [47].

6.2 Koexistence se staršími standardy

Z původního ustanovení, že NG-PON2 nebude podporovat koexistenci s předchozími standardy PON bylo nakonec upuštěno [45]. Původní předpoklad organizace FSAN totiž byl, že v ODN budou využity pasivní optické rozbočovače vlnové délky namísto standardních rozbočovačů optického výkonu, koexistence by tak nebyla možná. Náklady na vybudování úplně nové síťové infrastruktury jsou vysoké, je tedy žádoucí, aby byl NG-PON2 kompatibilní s již vybudovanou ODN [47]. K tomuto účelu by měl sloužit speciální síťový prvek CE (Koexistenční prvek – Coexistence Element), který koexistenci rozdílných standardů zajistí [5].

Dalším z požadavků na NG-PON2 je tedy ochrana investic do ODN zajištěním bezproblémové migrace koncových uživatelů na nový systém. Nové rozdělení vlnových délek bere požadavek na koexistenci v potaz, je také podporován přenos video signálů na samostatné vlnové délce (např. pro televizní vysílání), stejně jako u předchozích standardů. Pro přechod na NG-PON2 byly definovány dva scénáře [32]:

1. „Brownfield migration scenario.“
2. „Greenfield migration scenario.“

V případě prvního scénáře byla již vybudována pasivní optická infrastruktura a nasazen jeden z předchozích standardů PON. Tato stávající infrastruktura pak bude využita pro postupný přechod na novou generaci PON. Další možností je okamžitý přechod na nový standard, ovšem i v tomto případě by bylo vhodnější stále provozovat i starší PON systém, jelikož výměna koncových jednotek u uživatelů může být časově náročná. Z tohoto důvodu je požadováno, aby stávající koncoví uživatelé byli přechodem na nový standard pokud možno co nejméně omezeni (nejlépe vůbec). NG-PON2 musí být v případě úplné migrace schopen podporovat všechny služby, které poskytovaly starší standardy, mezi které patří: GPON, XG-PON1, EPON a 10GEPON [32].

Druhý scénář popisuje situaci, kdy se síťová infrastruktura bude teprve budovat (proto označení výstavba „na zelené louce“), případně se jedná o rekonstrukci stávající síťové infrastruktury (např. nahrazení stávající metalické sítě optickou). V tomto scénáři již není nutné brát zajištění koexistence v potaz [32].

6.3 Komunikace v NG-PON2

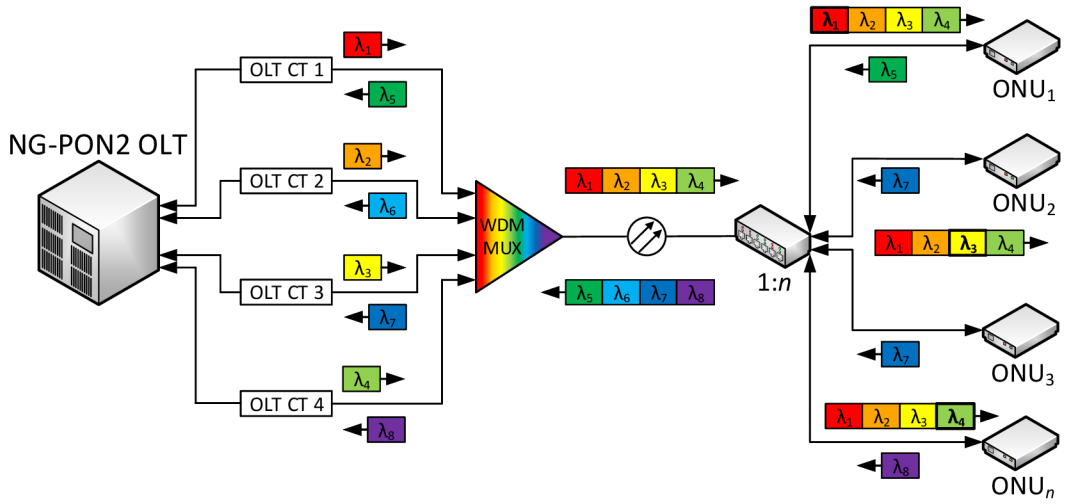
Pro komunikaci prostřednictvím TWDM je využito čtyř obousměrných kanálů λ. Každý z těchto kanálů disponuje přenosovou rychlostí 10 Gb/s v sestupném směru a 2,5 Gb/s ve vzestupném směru. Tímto způsobem je dosaženo výsledné přenosové rychlosti NG-PON2 (40 Gb/s sestupný směr, 10 Gb/s vzestupný směr). Došlo tak k dalšímu vývoji a využití původního standardu XG-PON1, pomocí λ kanálů došlo k navýšení kapacity [47].

NG-PON2 umožňuje také provozovat překryvné PtP (Komunikace typu bod-bod – Point-to-Point) WDM. Mezi přednosti tohoto řešení patří vyhrazení λ kanálu pro každou jednotku ONU. V základní konfiguraci je obsaženo celkem 8 kanálů pro PtP WDM, které zaručují koexistenci se staršími standardy PON. Nevyužitý rozsah vlnových délek je potom možné přiřadit pro další kanály PtP WDM. Pro PtP WDM je vyhrazen rozsah vlnových délek 1 603 až 1 625 nm pro vzestupný i sestupný směr, případně rozšířené spektrum 1 524 až 1 625 nm. Základní rozsah (nazývaný také jako sdílený) je využíván pro dosažení plné koexistence se staršími standardy PON. Rozšířené spektrum umožňuje nevyužitá pásma přiřadit pro použití s PtP WDM, rozšířené pásmo se uplatní také při realizaci nové infrastruktury pro PON („Greenfield scenario“), kde není nutné zajistit podmínky pro koexistenci [47]. Při komunikaci prostřednictvím PtP WDM se jedná o komunikaci typu bod-bod. NG-PON2 je tak historicky prvním standardem PON podporujícím kanály, které pro přenos využívají více vlnových délek [41]. PtP WDM kanály podporují přenosové rychlosti 1,25 Gb/s, 2,5 Gb/s a 10 Gb/s [34].

Pro TWDM i PtP WDM využívá NG-PON2 opět řídící zprávy PLOAM, které slouží pro podporu více vlnových délek, správu bezpečnostních klíčů, správu napájení pro koncové jednotky, správu kanálů vlnových délek a ochranu. Jedná se o rozšíření funkčnosti zpráv PLOAM z předchozího standardu XG-PON. Pro komunikaci s jednotkou OLT potřebují koncové jednotky pro každý směr jeden kanál na určité vlnové délce [41].

Každý z kanálů (TWDM nebo PtP WDM) je přidělen k jednomu OLT CT (Ukončení kanálu – Channel Termination). CT ukončuje daný kanál na straně jednotky OLT, pomocí WDM multiplexoru jsou tyto členy připojeny na optické vedení. Jednotky ONU lze přesouvat mezi jednotlivými kanály TWDM, tímto způsobem je možné pružně reagovat na různé situace v síti. Je tak možné rovnoměrně rozdělovat zátěž mezi jednotlivé kanály nebo v případě selhání CT členu přesunout dotčené koncové jednotky na funkční CT člen. Správné fungování při použití více vlnových délek a jejich změnách má na starost protokol ICTP (Protokol pro ukončení interních kanálů – Inter-Channel-Termination Protocol). Tento protokol mimo jiné zodpovídá i za přesun jednotky ONU na jinou vlnovou délku (handover), monitorování

výkonu, bezpečnost TWDM nebo zmírnění následků způsobených modifikovanou ONU [34, 41]. Příklad komunikace v rámci standardu NG-PON2 je zobrazen na obrázku 6.1, jednotky ONU jsou bezbarvé, nebo obsahují laditelné filtry.



Obr. 6.1: Komunikace v rámci standardu NG-PON2 [41].

Stejně jako předchozí standard, také NG-PON2 podporuje metodu zapouzdření X-GEM, která vychází z metody GEM standardu GPON. X-GEM rámec má stejnou strukturu jako rámec standardu XG-PON, zobrazený na obrázku 5.2, rámce X-GEM je opět možné použít pro zapouzdření datových jednotek různých síťových technologií [34].

6.4 Nasazení systému NG-PON2

Jedním z faktorů, na kterých je nasazení systému závislé je cenová dostupnost laditelných přijímačů, které jsou nezbytnou součástí koncových jednotek ONU. Autoři [64] vytvořili a úspěšně otestovali prototyp PON založený na TWDM. Tento prototyp disponuje 4 kanály pro sestupný směr (10 Gb/s na kanál) a stejný počet kanálů využívá i pro směr vzestupný (2,5 Gb/s na kanál). Jednotka OLT využívá předzesilovač SOA, každá jednotka ONU byla vybavena laditelným filtrem, který slouží pro volbu vlnové délky. K nastavení vlnové délky bylo využito proprietárních zpráv PLOAM, které sloužily k informování o změnách vlnové délky.

Autoři [4] navrhli řešení založené na SDM (Prostorové oddělení – Space Division Multiplex), systém byl schopen symetrického přenosu rychlostí 40 Gb/s. Využito bylo optických vláken MCF (Optické vlákno obsahující více jader – Multi Core

Fiber), pomocí těchto vláken je možné uskutečnit prostorové oddělení jednotlivých datových toků a dosáhnout tak vyšší přenosové kapacity i rychlosti. Systém byl schopen přenosu 6 prostorově oddělených kanálů. Díky prostorovému oddělení je možné dosáhnout nízké chybovosti (BER 10^{-9}), je také možné dosáhnout vyššího rozbočovacího poměru.

Autoři [55] úspěšně prověřili možnost koexistence systémů NG-PON2 a EPON nebo 10GEPON na společné síťové infrastruktuře. Vytvořen byl také prototyp WDM filtru, který úspěšně eliminoval přeslechy způsobené technologií TWDM.

Tab. 6.1: Přehled provedených implementací TWDM [1].

Přenosová rychlost [Gb/s]	Rozbočovací poměr	Vzdálenost [km]	Úlum [dB]
40/40	1:256	25	31
40/40	1:1000	40	39
40/40	1:1024	50	43
40/40	1:256	75	–
40/40	1:46	100	–
100/100	1:1024	25	42
40/10	1:64	20	36

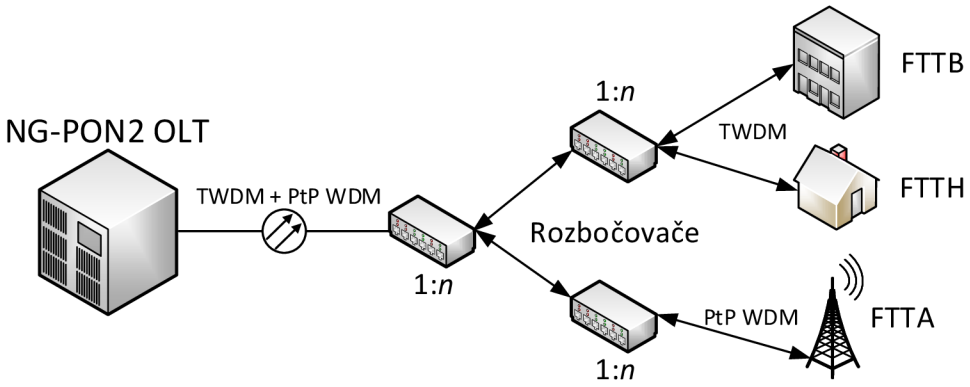
Americká společnost Verizon plánuje nasadit standard NG-PON2 v průběhu roku 2018, laboratorní testování systému již proběhlo a bylo plánováno jej dokončit začátkem roku 2018. Má se jednat o řešení vyvinuté společností Calix, označené jako AXOS E9-2 Inteligent Edge System. Tento systém umožňuje nasazení jednotné přístupové sítě pro různé druhy služeb, včetně těch mobilních. Mělo by se jednat o vůbec první nasazení standardu NG-PON2 v reálném provozu. Realizace je plánována ve městě Tampa na Floridě [3].

6.5 Budoucí vývoj NG-PON2

NG-PON2 je vyvíjen s ohledem na poskytnutí přenosové kapacity pro široké spektrum aplikací a služeb. Uvažováno je nasazení systému také pro mobilní sítě, kdy pro mobilní přístupovou síť[1] bude vyhrazeno PtP WDM a jeho pásma vlnových délek. Pro zbývající služby sítě budou vyhrazeny rozsahy vlnových délek TWDM. Příklad výše popsané síťové infrastruktury je zobrazen na obrázku 6.2. Nedávná aktualizace doporučení G.989.2 přináší podporu přenosové rychlosti 80 Gb/s, dále

[1] *Vlákno do antény – Fiber To The Antenna* (FTTA)

je také uvažováno o zvýšení přenosové rychlosti z 10 Gb/s na 25 Gb/s pro jeden λ kanál [48].



Obr. 6.2: Využití TWDM a PtP WDM [1].

Probíhá také výzkum zaměřený na mobilní sítě, které budou založeny na pasivní optické infrastruktuře. S dalším rozvojem NG-PON2 je očekáváno zvýšení pokrytí území mobilními sítěmi a snížení nákladů na vybudování potřebné infrastruktury (jedna společná víceúčelová síťová infrastruktura, slučující více telekomunikačních služeb). Šířka pásma, kterou standard NG-PON2 nabízí je, ideální pro cloudové služby, a také se nabízí využití pro aplikace zpracovávající tzv. big data [1].

V Japonsku připadá odhadem 30 % z celkového datového toku klasickým kabelovým sítím, 50 % poté sítím rádiovým [59]. Podle společnosti Cisco pak síťový provoz generovaný mobilními (chytrými) telefony překročí do roku 2020 počítačový síťový provoz. Poskytovatelé mobilních služeb využívají makro buněk, které jsou schopné obsloužit tisíce koncových uživatelů, stejně tak využívají malých buněk, které jsou schopny obsloužit desítky až stovky koncových uživatelů (záleží na oblasti a poptávce po mobilních službách). Neustálé zahušťování mobilní infrastruktury nutí poskytovatele mobilních služeb nasazovat také odpovídající síťovou infrastrukturu propojující tyto buňky, která splní vysoké nároky na šířku pásma i do budoucna [5].

Očekává se také nasazení páté generace mobilních sítí, jejich standardizace by mohla být dokončena v roce 2020. Předpokládá se, že některé funkcionality mobilních sítí 5G budou mít kapacitu až 10 Gb/s, optická přenosová média budou pro fungování těchto sítí důležitá. Sítě 5G by měly být paketově orientované, tudíž by jednotlivé přenosy mohly být uskutečněny přes klasické PON založené na metodách TDM/TDMA, stejně tak by mohlo být využito TWDM a PtP WDM technologie NG-PON2. Vývoj páté generace mobilních sítí tak může ovlivnit i budoucí vývoj

PON [48].

Snahou poskytovatelů telekomunikačních služeb je snížit náklady na budování nových sítí a také na provoz těch stávajících. Konvergence telekomunikačních sítí dopomohla k sjednocení více telekomunikačních služeb pro provoz po společné síťové infrastruktuře. Objevují se však stále nové technologie, jako například virtualizace sítí nebo SDN (Softwarově definovaná síť – Software Defined Network) [48]. Kromě tradičních služeb triple play, tedy hlas video a data, které byly na počátku zavádění sítí FTTH, stále vzrůstá podíl datových toků nových služeb. Jedná se například o datová centra, již zmiňované mobilní sítě nebo např. IoT (Internet věcí – Internet of Things), velké oblibě se těší také cloudové aplikace [59].

7 Bezpečnost PON

Následující kapitola se zabývá zabezpečením standardů pasivních optických sítí, které byly popsány v předchozích kapitolách.

7.1 Bezpečnost APON a BPON

Standard APON zavedl novou techniku šifrování označenou jako *churning*. Tato technika měla zajistit důvěryhodnost přenášených dat, ovšem *churning* obsahuje řadu kritických chyb a je snadné jej prolomit. Koncoví uživatelé APON systému jsou tedy vystaveni hrozbě, že jejich komunikace může být odposlouchávána. Například i při použití techniky SSL (Vrstva zabezpečených soketů – Secure Sockets Layer) existuje riziko, že útočník může odhalit jaké webové servery koncový uživatel navštěvuje. Telefonie provozovaná prostřednictvím ATM není standardně zabezpečena, je tedy závislá pouze na zabezpečení jednotlivých spojů [61].

Adresní informace obsažená v záhlaví každé datové jednotky udává konkrétní koncovou jednotku, pro kterou je tato datová jednotka určena. Ostatní koncové jednotky by měly datové jednotky, které nejsou určeny přímo jim ignorovat. Při přenosu ve vzestupném směru jsou již jednotlivé datové jednotky doručovány pouze řídící jednotce OLT, ostatní koncové jednotky již do této komunikace nejsou zapojeny.

APON podporuje autentizaci pomocí hesla, jednotka ONU se tímto způsobem autentizuje vůči OLT. Jednotka OLT však nemusí být zodpovědná za správu databáze hesel, standardizace tuto situaci připouští. V případě, že jednotka OLT nemá na starost údržbu hesel, je možné očekávat, že bude důvěřovat hned prvnímu heslu, které obdrží od koncové jednotky. Existuje tedy riziko, že toto heslo bude používat pro budoucí ověřování dané koncové jednotky. Jedná se o první závažné bezpečnostní riziko, tento způsob autentizace je sice slabý, problémem ovšem je, že je pouze volitelný, tudíž nemusí být vůbec používán [61].

7.2 Technika churning

Jak již bylo zmíněno, úkolem této techniky je zajistit důvěryhodnost komunikace mezi OLT a ONU. Jedná se o poměrně jednoduchou substituční šifrovací techniku. Substituční funkce je nelineární a využívá osmibitových klíčů, osmibitové znaky ve formátu prostého textu jsou namapovány do zašifrované podoby, která je opět osmibitová. Toto mapování je řízeno jediným 24bitovým klíčem [61].

Mapování prostého textu do zašifrované podoby není provedeno do okamžiku aktualizace klíče. Aktualizace klíčů se provádí minimálně jednou za sekundu [24].

V případě přenosové rychlosti 622 Mb/s však aktualizace jednou za sekundu poskytuje velké množství šifrovaných informací pro kryptoanalýzu [61].

Technika *churning* je využívána pouze v sestupném směru k zašifrování komunikace od řídící jednotky OLT. Není však žádný problém, aby případný útočník mohl zachytit všechna data, která jsou v sestupném směru posílána. Synchronizace časování APON rámce ani další signály fyzické vrstvy nejsou schopny zabránit případnému pasivnímu odposlechu šifrovaného datového toku, který je posílán v sestupném směru [61].

Pokud není zabezpečení pomocí techniky *churning* dostačující, je doporučeno použít další zabezpečení na vyšší vrstvě [24].

7.3 Bezpečnost GPON

U standardu GPON je opět použití zabezpečení volitelné a závisí tedy především na provozovateli systému, zda zabezpečení nasadí. Komunikace v sestupném směru může být šifrována pomocí šifrovacího klíče, který generuje jednotka ONU. Stejným způsobem může být šifrován také provoz ve směru vzestupném [17]. Standard GPON využívá AES (viz následující podkapitola 7.4) k šifrování komunikace v sestupném směru, je možné použít klíče o délce 128, 192 a 256 bitů [28]. Použití tohoto standardu pro zabezpečení činí odposlech komunikace v sestupném směru složitým. Pro zvýšení bezpečnosti je možné klíče měnit pravidelně, a to bez narušení datového toku [6]. Výměna klíčů probíhá prostřednictvím PLOAM, klíče se však přenášejí ve formě prostého textu [18].

Existují také dva způsoby spínání zabezpečení: automatické a nucené. V případě automatického spínání dojde k jeho aktivaci v případě detekce poruchy (např. ztráta nebo degradace signálu, ztráta rámce). Nucené spínání je aktivováno v případě přeložky optického vlákna nebo při jeho výměně [6].

7.4 Standard AES

Standard pokročilého šifrování – Advanced Encryption Standard (AES) je symetrickým šifrovacím systémem, kdy odesílatel i příjemce používají jeden jediný klíč pro šifrování a dešifrování komunikace. Prostřednictvím AES je možné zpracovávat datové bloky délky 128 bitů za použití šifrovacích klíčů délky 128, 192 a 256 bitů [9].

V případě využití techniky AES pro šifrování komunikace v sestupném směru u standardu GPON jsou šifrována pouze přenášená data prostřednictvím GEM rámců, samotné záhlaví tohoto rámce šifrováno není [28].

7.4.1 Výměna klíčů

Samotnou výměnu klíčů řídí jednotka OLT, která vyšle zprávu *Request_Key* prostřednictvím PLOAM kanálu. Koncové jednotky poté reagují generováním, uložením a odesláním klíče, v jednotce ONU je klíč uložen v registru pojmenovaném *shadow_key_register*. ONU by měla generovat kryptograficky nepředvídatelný klíč.

Z důvodu omezené délky zprávy PLOAM je nutné klíč rozdělit na dvě části a až poté jej odeslat. K označení, která část klíče se právě odesílá slouží pole fragmentace. Pro zvýšení spolehlivosti jsou části klíče odeslány celkem třikrát, všechny tyto části mají stejnou hodnotu označenou jako *Key_Index*. Důvodem je nutnost potvrzení správnosti přenosů ze strany OLT. Hodnota pole *Key_Index* je automaticky zvýšena pro každý klíč, který jednotka ONU vygeneruje na vyžádání jednotky OLT.

Pokud však jednotka OLT nepřijme všechny tři odeslané klíče, odešle požadavek, aby ONU vygenerovala klíče znovu a celý tento proces zopakovala. V případě, že přenos klíče třikrát selže, OLT tuto situaci vyhodnotí jako ztrátu klíčů a provede deaktivaci příslušné ONU. Při úspěšném přenosu klíče OLT tento klíč uloží do svého registru *shadow_key_register* [28].

7.4.2 Změna klíče

Jednotka OLT zvolí číslo rámce, který bude v budoucnu použit pro přenos nového klíče, jednotce ONU toto číslo doručí prostřednictvím zprávy *Key_Switching_Time*. Tato zpráva je odeslána opět třikrát, v tomto případě ale stačí, aby ONU tuto zprávu přijala pouze jednou. OLT vyžaduje potvrzení přijetí této zprávy jednotkou ONU, pokud po třech vyslaných zprávách neobdrží OLT žádné potvrzení, je tato situace vyhodnocena jako ztráta požadovaného potvrzení a OLT deaktivuje příslušnou ONU.

Může nastat situace, kdy jednotka ONU potvrdí zprávu *Key_Switching_Time*, ale obdrží další zprávu *Request_Key*. Pokud tato situace nastane, ONU vygeneruje nový klíč a přepíše předchozí klíč uložený v *shadow_key_register*. Smazáno je také předchozí zvolené číslo rámce, který měl být původně použitý pro přenos nového klíče, toto číslo musí být stanoveno znovu způsobem popsaným výše.

Při změně klíče jednotka OLT zkopíruje nový klíč z *shadow_key_register* do *active_key_register*, stejnou operaci provede také ONU. Po úspěšném provedení těchto kroků již jednotky OLT a ONU používají nový klíč pro všechny datové jednotky, které si od tohoto okamžiku vymění [28].

7.5 Technika FEC

Samoopravný kód – Forward Error Correction (FEC), je technika využívaná na transportní vrstvě komunikačních systémů. Data přenášená prostřednictvím této techniky jsou zakódována s přidáním nadbytečních (redundantních) informací, které umožní příjemci detekovat a opravit případné chyby, které vznikly při přenosu. Použití této techniky umožňuje dosáhnout nízké chybovosti a snížit tak počet opakovaných přenosů. Například při hodnotě BER (Bitová chybovost – Bit Error Ratio) 10^{-4} je možné při použití FEC snížit tuto hodnotu na 10^{-15}.

Důsledkem použití FEC je schopnost překlenout vyšší útlum na trase (ODN) přibližně o 3 až 4 dB, nicméně podpora vysokých přenosových rychlostí, vyšších vzdáleností mezi OLT a ONU i vyššího rozbočovacího poměru zůstává zachována [28].

7.6 Bezpečnost XG-PON

Při vývoji nového standardu XG-PON byl již kladen větší důraz na zabezpečení komunikace. V původním standardu GPON existoval předpoklad, že kanál ve vzestupném směru je dostatečně fyzicky zabezpečený. Z tohoto předpokladu pak vycházelo relativně slabé zabezpečení komunikace ve vzestupném směru a z toho plynoucí bezpečnostní rizika. Zabezpečení standardu GPON bylo poté posíleno, změny byly definovány v nepovinných doplňcích [8].

Ve standardu XG-PON je již zavedena povinná podpora silné vzájemné autentizace a použití ověřování k zajištění důvěrnosti komunikace, především pak zpráv sloužících při správě systému. Důraz je kladen také na vyšší úroveň zabezpečení šifrovacích klíčů. Mezi novinky patří šifrování provozu vysílaného všesměrově, a také šifrování provozu ve vzestupném směru [21]. Šifrovat je možné i multicastovou komunikaci, za generování šifrovacích klíčů pro multicastový přenos odpovídá jednotka OLT [1].

Šifrovány jsou také klíče sloužící k autentizaci, proces vzájemné autentizace OLT a ONU lze zabezpečit také pomocí hesla, dále je podporován protokol IEEE 802.1X, jehož výhodou je možnost podpory dalších autentizačních protokolů. V případě vygenerování nebo aktualizace klíče, který slouží k šifrování unicastového přenosu, je tento klíč při přenosu chráněn KEK (Klíč sloužící k zabezpečení přenášeného klíče – Key Encryption Key). Tento způsob zabezpečení klíče je možné použít volitelně i pro standard GPON. Zabezpečeny jsou také řídící zprávy PLOAM v obou směrech přenosu (zprávy byly vysílány ve formě prostého textu). Zabezpečení je realizováno pomocí MIC (Kontrola integrity zpráv – Message Integrity Check), který je schopný rozpoznat chybu, chybné zprávy jsou odmítnuty a zahozeny [17].

Tato vylepšení znesnadňují případnému útočníkovi maskování jeho identity za jednotku ONU i jednotku OLT i v případě, že má přístup k optickému vedení dané sítě a také v případě, kdy by mohl své vysílání prokládat s vysíláním jednotky ONU, která je obětí tohoto útoku [8].

Standard XG-PON využívá opět standardu AES s klíči o délce 128 bitů. Samozřejmostí je použití techniky FEC, která je používána v obou směrech přenosu. V případě, že ve vzestupném směru je linka dostatečně kvalitní, může být FEC pro tento směr vypnuto.

Metoda X-GEM zajišťuje mimo jiné také soukromí pro přenášená uživatelská data. Ke každému X-GEM fragmentu je přidělen seznam klíčů, zde je uložen klíč, který byl vyjednán mezi OLT a ONU. Tento seznam disponuje velmi dobrým mechanismem výměny klíčů v XG-PON, nedochází ke ztrátovosti dat. Spolu se silnou vzájemnou autentizací patří systém XG-PON k nejbezpečnějším širokopásmovým komunikačním systémům [8].

7.7 Bezpečnost NG-PON2

NG-PON2 přebírá od svého předchůdce, standardu XG-PON již dříve definované bezpečnostní mechanismy, včetně těch kryptografických. Patří sem zabezpečení vzájemné autentizace mezi jednotkami OLT a ONU, možnost izolace kanálů, samozřejmostí je také již dříve zmíněné šifrování unicastového i multicastového provozu. Zašifrovat je možné i užitečná data rámce X-GEM [34].

Systém NG-PON2 by měl být schopen monitorovat přenosy mezi jednotkami OLT a ONU, jedná se o preventivní opatření na ochranu před OLT nebo ONU, které nerespektují přidělené časové intervaly nebo vlnové délky pro komunikaci [32].

PON založené na TWDM umožňují oproti PON založeným na TDM pokročilé síťové funkcionality, zejména díky použití laditelných TWDM vysílačů koncových jednotek ONU. Z analýz provozu je možné získat představu o tom, jak je síť během dne vytížená a tyto poznatky poté využít pro realizaci různých opatření, např. pro úsporu energie. V době nízkého vytížení sítě je možné aktivní jednotky převést na společnou vlnovou délku a nepoužívané porty jednotky OLT dočasně vypnout – tento stav je označován jako „OLT port sleep“. Výhodou je nejen úspora elektrické energie, ale také zvýšení bezpečnosti a odolnosti sítě proti případnému útoku. K převedení jednotek ONU na odlišnou vlnovou délku může dojít také v případě ztráty spojení na určité vlnové délce [47].

Implementace bezpečnostních mechanismů na PtP WDM není složitá. Základní způsob autentizace je založen na *Registration_ID*, které funguje na principu sdíleného tajemství, *Registration_ID* není tedy přenášeno prostřednictvím přenosového

kanálu. Veškerý síťový provoz vedený prostřednictvím PtP WDM je unicastový a zašifrovaný [41].

V případě selhání procesu autentizace může OLT CT zahájit proces, jehož cílem je zabránění možnému narušení bezpečnosti. Tento proces může provést opětovnou autentizaci, blokaci provozu v sestupném i vzestupném směru, deaktivaci nebo zablokování modifikované nebo poškozené jednotky ONU, případně i zahájení diagnostických testů [34].

U kanálů PtP WDM nemusí být použita technika FEC, důvodem je snížení latence, kterou do přenosu technika dodatečně vnáší [48].

8 Bezpečnostní rizika PON

Komunikace v PON probíhá po sdíleném médiu, data v sestupném směru jsou posílána všem koncovým jednotkám v síti, v každém rámci je obsažena adresa příjemce. Stejně jako v ostatních sítích, které využívají sdílené médium, je i v případě pasivních optických sítí nutné zajistit ochranu takto přenášených dat a důvěrnost komunikace. Na pasivní optické sítě je možné použít i známé útoky [7, 18]:

DoS: Odepření služby – Denial of Service, útočník provádí aktivní útok, při kterém se snaží znepřístupnit síťové služby uživatelům sítě. Útočník by takto mohl zablokovat datovou komunikaci jednotky ONU ve vzestupném směru. Tomuto útoku je věnována podkapitola 8.4.

ToS: Odcizení služby – Theft of Service, útočník neoprávněně využívá jednu nebo více jednotek ONU pro získání služeb, případně pro získání vyšší přenosové rychlosti, které ale hradí uživatel, kterému byly zcizeny. Odcizení služby lze zabránit šifrováním komunikace v sestupném směru. Tomuto typu síťového útoku je věnována podkapitola 8.5.

V následujících podkapitolách jsou popsána známá bezpečnostní rizika pasivních optických sítí. V poslední části této kapitoly jsou zmíněny i možnosti detekce útoků a protiopatření proti útokům na pasivní optickou infrastrukturu.

8.1 Problém modifikované koncové jednotky

Při zvažování bezpečnostních rizik PON se nejčastěji předpokládá útok prostřednictvím modifikované koncové jednotky. Za modifikovanou je považována jednotka ONU, jejíž firmware byl neoprávněně pozměněn, či jinak upraven.

Z podstaty pasivní optické sítě je poměrně těžké detekovat modifikovanou koncovou jednotku. Mechanismy pro detekci a odpojení modifikované jednotky nicméně existují. Například autoři [43] navrhli, aby v případě výskytu vysokého počtu kolizí ve vzestupném směru jednotka OLT automaticky přešla do diagnostického režimu. V tomto režimu by poté OLT zjišťovala přítomnost modifikované ONU:

1. OLT vyšle požadavek na přenos periodického testovacího signálu s určitým vzorem.
2. Nemodifikované ONU požadavek přijmou a začnou tento signál podle parametrů, které zadala OLT vysílat.
3. Testovací signál je v případě přítomnosti modifikované ONU smíchán se signálem, který vysílá modifikovaná jednotka.

Pomocí analýzy výkonového spektra smíšeného signálu ve vzestupném směru může OLT zjistit, zda je v síti přítomna modifikovaná ONU [43]. Tento a další mechanismy

však nejsou efektivní proti DoS útoku pomocí laserové diody, jelikož útočník by tuto diodu mohl vypnout a později opět zapnout. Jednotka OLT by tak navíc byla zatížena prováděním analýzy v diagnostickém režimu [7].

Provedení útoku pomocí modifikované koncové jednotky vyžaduje poměrně velké úsilí. Pozměnit firmware jednotky ONU není jednoduchou záležitostí.

8.1.1 Detekce modifikované koncové jednotky

Při detekci modifikované koncové jednotky se vychází z předpokladu, že případná modifikovaná ONU bude vykazovat nejnižší počet zahozených rámců a také nejnižší FER (Chybovost rámců – Frame Error Rate) oproti ostatním ONU v dané síti. Důležité proto je, aby jednotka OLT sledovala FER pro každou připojenou ONU. Autoři [7] rozdělili detekci modifikované ONU pro standard EPON na dvě fáze:

1. detekce útoku,
2. zmírnění následků útoku.

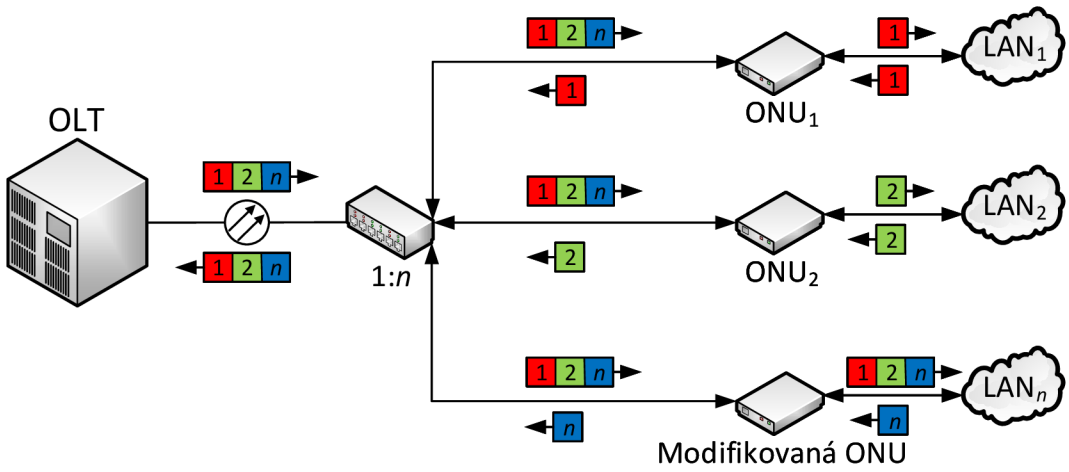
Při fázi detekce autoři předpokládali detekci pouze jediného útočníka v síti. Předpokladem pro úspěšnou detekci je také schopnost jednotky OLT rozpoznat, zda je přenosový kanál volný, případně zda není přenášen rámec, který by mohl způsobit kolizi. Při této fázi je využito již dříve uvedeného sledování FER. Pokud je překročen nastavený limit FER pro určitou ONU, jednotka OLT určí, o kterou ONU se jedná a přejde do další fáze.

Další fází je samotné zmírnění následků nestandardní situace (možného útoku). V této fázi OLT zjistí na základě MAC adresy původ rámců. Rámce pocházející od modifikované jednotky ONU jsou následně zpožděny o určitý čas D a až poté předány dále. Rámce pocházející od nemodifikovaných jednotek, tedy těch se standardním chováním jsou předány dále bez vložení zpoždění. Cílem této fáze je obnovení propustnosti a znevýhodnění nestandardně se chovající ONU [7].

8.2 Odposlech komunikace

Z podstaty komunikace prostřednictvím PON vyplývá riziko pasivního odposlechu komunikace. Komunikaci v sestupném směru je možné zabezpečit, ovšem velkou nevýhodou je, že použití zabezpečení je pouze volitelné. Případný útočník by mohl pozměnit firmware jednotky ONU a odposlouchávat tak veškerou komunikaci v sestupném směru [6]. Provoz v sestupném směru je možné zachytit pomocí detektorů optického záření, nemusí se nutně jednat o detektor jednotky ONU, z tohoto důvodu bylo nutné zavedení šifrování dat posílaných v sestupném směru [17]. Zásadní

je však následné zpracování zachyceného signálu. Situace, kdy modifikovaná koncová jednotka přijímá všechny rámce, včetně těch, které nebyly určeny přímo jí, je zobrazena na obrázku 8.1.



Obr. 8.1: Odposlech veškeré komunikace v sestupném směru.

K odposlechu by mohlo dojít také ve směru vzestupném, jelikož pro komunikaci ve vzestupném směru není používáno žádné zabezpečení. Tento způsob odposlechu je složitý, nicméně je proveditelný. V doporučeních není definováno žádné zabezpečení pro komunikaci ve vzestupném směru, vychází se z faktu, že prostřednictvím jednotky ONU není možné zachytávat komunikaci ostatních koncových uživatelů ve vzestupném směru a komunikaci tedy není nutné šifrovat. Pro odposlech komunikace ve vzestupném směru by musel případný útočník narušit optické vedení PON. Tato situace by ovšem měla vliv na přenosové vlastnosti dané sítě, které by zachytilo dohledové centrum poskytovatele služeb. Tento způsob odposlechu komunikace ve vzestupném směru je tedy velmi málo pravděpodobný [28].

Právě z výše uvedeného důvodu nedefinovaly jednotlivé standardy PON žádnou metodu zabezpečení ve vzestupném směru. V případě, že byl přenos v sestupném směru zabezpečen např. pomocí AES, nebo jiné techniky využívající tajných klíčů, byly tyto klíče posílány ve vzestupném směru v nezabezpečené podobě – ve formě prostého textu. Vycházelo se z předpokladu, že komunikace ve vzestupném směru je bezpečná a není tedy nutné ji dodatečně zabezpečovat [40].

Výzkum popsaný v článku [44] se zaměřil právě na možnost odposlechu komunikace ve vzestupném směru. Bylo testováno, zda je možné odposlechnout komunikaci prostřednictvím zpětných odrazů optického signálu. Tyto odrazy mohou být způsobeny použitými optickými komponenty – pasivními optickými rozbočovači a použi-

tým typem konektorů. Vliv na zachycení komunikace ve vzestupné směru mají také použité detektory optického signálu (PIN[1] a APD[2]) a také předzesilovače. Testování probíhalo na různých konfiguracích ODN, testován byl především zpětný odraz signálu. Úspěšnost potencionálního útočníka závisí především na typu použitého konektoru a také fotodetektoru. Z hlediska bezpečnosti sítě byl vyhodnocen jako nevhodný konektor PC (Konektor s kolmou kontaktní plochou – Polished Connector). Konektor APC (Konektor s šikmou kontaktní plochou – Angled Polish Connector) právě díky kolmému broušení potlačuje odrazy signálu. Použití fotodetektoru APD zvyšuje pravděpodobnost úspěšného odposlechu právě komunikující jednotky ONU. Schopnost odposlechu komunikace ve vzestupném směru však není závislá na konkrétní přenosové rychlosti, nejvíce závisí na výkonové úrovni zpětných odrazů a použitém typu konektoru [44].

Odposlech komunikace je možné považovat za první (přípravnou) fázi útoku na síťovou infrastrukturu. Útočník může tímto způsobem získat základní informace jako např. uživatelská data, sestavy aktivit, IP a MAC adresy zařízení. Získané údaje může útočník použít pro pozdější útok DoS nebo ToS [15].

8.3 Rizika komunikace ve vzestupném směru

Pro komunikaci ve vzestupném směru využívají PON již zmíněnou přístupovou metodu TDMA. Tato přístupová metoda zajišťuje sdílení vzestupného směru více koncovými jednotkami (ONT, ONU). Veškerý provoz ve vzestupném směru je rozdělen do časových intervalů (time-slots). Jednotka OLT přiděluje vždy přesný počet těchto intervalů koncovým jednotkám, intervaly se nepřekrývají a nedochází tedy ke vzniku kolizí. OLT tyto intervaly může přidělovat staticky nebo dynamicky [7].

Podstatným nedostatkem komunikace ve vzestupném směru je absence jakéhokoliv zabezpečení. Případný útočník by mohl pomocí modifikované koncové jednotky vysílat data mimo přidělené časové intervaly a tímto způsobem zapříčinit vznik kolizí. Tímto způsobem by tedy narušil komunikaci ve vzestupném směru, jelikož kolizní rámce jsou zahazovány. Pro ostatní nemodifikované koncové jednotky by to znamenalo zvýšení FER, a tedy snížení kvality poskytovaných služeb. Tuto degradaci ještě zvyšuje použití protokolu TCP (Spojově orientovaný protokol – Transmission Control Protocol), jelikož dojde k zatížení sítě opětovnými přenosy. Protokol TCP z důvodu minimalizace zatížení sítě sníží přenosovou rychlost a tím pádem také propustnost sítě [7]. Jednotka, která porušuje tato pravidla je označována jako „Rogue ONU“ [35]. Dalším způsobem, jak narušit průběh komunikace ve vzestupném směru

[1] *Polovodičová dioda – Positive Instrinsic Negative* (PIN).
[2] *Lavinová fotodioda – Avalanche Photodiode* (APD).

je DoS útok prostřednictvím poškozené laserové diody nacházející se v koncové jednotce (porucha na straně koncové jednotky, nebudou respektovány přidělené časové intervaly pro komunikaci ve vzestupném směru). Tento útok je blíže popsán v následující podkapitole věnované DoS útokům.

8.4 DoS útok

Je známým útokem na síťovou infrastrukturu. Při DoS útoku dochází k velké spotřebě dostupné šířky pásma, dochází také k vytížení fyzického vybavení (hardwaru) sítě. Důsledkem tohoto útoku může být v lepším případě snížení kvality přenosu. V horším případě se může jednat o výpadek síťových služeb, případně celkový výpadek konektivity. DoS útok může mít za následek také snížení bezpečnosti dané sítě, následuje souhrn rizik souvisejících s DoS útokem [15]:

- Nadměrná spotřeba výpočetního výkonu síťových prvků.
  - Nadměrná spotřeba místa na disku, paměti, času procesoru.
- Narušení citlivých síťových informací.
  - Směrovací informace, MAC a IP adresy, značení VLAN (Virtuální lokální síť – Virtual Local Area Network).
- Narušení spojení již na fyzické vrstvě, u PON např. kontinuální vysílání silného laserového signálu.
  - Znemožnění komunikace koncovým uživatelům.

8.4.1 Kontinuální vysílání laserového paprsku

První dva výše uvedené body jsou obecné důsledky DoS útoku. Specifickým typem DoS útoku na pasivní optické sítě je použití zdroje laserového záření, může se jednat o již zmíněnou modifikovanou laserovou diodu koncové jednotky. Pokud je tato dioda modifikována tak, aby nepřetržitě vysílala na stejné vlnové délce, která je použita pro přenos ve vzestupném směru, dojde k blokaci ostatních koncových jednotek, které již nebudou schopny komunikovat. Ochrana proti tomuto typu útoku je možná následujícími způsoby [15, 23]:

1. Snížením výkonu PON systému a zahájení detekce původce DoS útoku (část systémových prostředků bude využita pro detekci).
2. Dynamické posunutí kanálu ve vzestupném směru tak, aby nedocházelo k dalšímu rušení přenosu (pouze u laserů, které umožňují přeladění).
3. Využití metody CDMA (Kódový multiplex – Code Division Multiple Access) pro přenos dat ve vzestupném směru (od koncových uživatelů) při zarušení komunikace.

Řešení uvedené v bodě 1 je proveditelné, nicméně v důsledku útoku a při následné detekci útočníka je snížena výkonnost celého PON systému.

Naproti tomu řešení uvedené v bodě 2 je na provedení složitější. Důvodem jsou laserové zdroje záření umístěné v jednotkách ONU, které mají zpravidla pevnou vlnovou délku. Pro posunutí přenosu ve vzestupném směru na jiný kanál by také bylo nutné zavést vhodný signalizační protokol.
V bodě číslo 3 je využito výhody techniky CDMA, která je schopna fungovat i v silně zarušené síti. Pokud ve vzestupném směru dojde k nedodržení vysílání ve stanovených intervalech, dojde k narušení průběhu komunikace koncových jednotek a jednotka OLT nebude schopna rozeznat příchozí data. Tento typ DoS útoku tak může mít velmi vážný dopad na fungování a bezpečnost pasivní optické sítě [15].

Autoři [23] navrhují, aby v případě selhání komunikace ve vzestupném směru OLT vyslala požadavek na přerušení vysílání TDM signálů a každá z koncových jednotek by pomocí CDMA odeslala OLT svoje identifikační číslo. Každá ONU přitom využívá pro tento přenos unikátní kód PN s unikátní maskou. Jednotka OLT je pomocí tohoto kódu schopna rozlišit, zda se jedná o oprávněnou jednotku.

Problém kontinuálně vysílající laserové diody může vzniknout především v systémech založených na technice TDM, kde ONU sdílejí jednotlivé časové intervaly. V případě použití WDM má však každá skupina jednotek ONU pro přenos přidělenu určitou vlnovou délku a skupiny jednotek jsou tak od sebe vzájemně odděleny [23].

V případě, že chce útočník pouze narušit komunikaci, nepotřebuje složitě modifikovat koncovou jednotku. K provedení takového útoku postačuje pouze laserový zdroj a optický propojovací kabel (patchcord) s vhodnými konektory [17]. Uvedené komponenty jsou dobře dostupné a proveditelnost tohoto útoku není složitá, laserový zdroj stačí připojit na optické vedení a zapnout jej. Je tedy poměrně zbytečné k tomuto typu DoS útoku pozměňovat firmware jednotky (nebo více jednotek) ONU. Pokud komunikaci narušuje kontinuální vysílání laserového paprsku, nemusí se nutně jednat o útok, ale o možnou poruchu některé z koncových jednotek.

8.4.2 Další varianty DoS útoku

Při DoS útoku na pasivní optické sítě je možné narušit také DBA mechanismus prostřednictvím nadměrného počtu žádostí o přidělení dostupné šířky pásma. V případě špatně navrženého DBA mechanismu může dojít k nespravedlivému rozdělení systémových zdrojů pro modifikované ONU na úkor ostatních, oprávněných uživatelů. Modifikovaná ONU může také generovat velký síťový provoz. Pokud je dostupná šířka pásma přidělována dynamicky, může opět dojít k nepřiměřenému přidělení šířky pásma právě modifikované ONU [66].

Dalším možným narušením může být jednotka ONU, která neustále mění svoji MAC adresu. Možným důsledkem je vyčerpání dostupného počtu instancí OLT jednotky pro nové MAC adresy koncových jednotek (MAC flood). Jednotka OLT by v tomto případě mohla zamítnout registraci dalších (oprávněných) ONU do sítě [15].

Další možností je vysílání dlouhé sekvence jedniček nebo nul s cílem narušit synchronizaci na vzdáleném optickém přijímači [17].

Následky útoku DoS je možné znásobit provedením stejného typu útoku v jeden okamžik, ale za pomoci většího počtu zařízení. Tento útok je označován jako DDoS (Distribuovaný DoS útok – Distributed Denial of Service).

8.5 ToS útok

V případě ToS útoku se útočník snaží skrýt svoji identitu za jiného, oprávněného koncového uživatele dané sítě nebo služby. Důsledkem úspěšného ToS útoku je, že útočník může využívat služby, ke kterým původně nebyl oprávněn přistupovat, dochází k odcizení identity oprávněného uživatele [40]. Pokud jsou tyto služby zpoplatněny, jsou samozřejmě účtovány uživateli, kterému byly zcizeny.

K možnému odcizení služeb může dojít odcizením údajů, které patří jednotce ONU, oprávněné využívat služby. Veškeré informace jsou napsány přímo na jednotce ONU, případně také na obalu, ve kterém byla dodána. Útočník může tyto údaje snadno odcizit a vydávat se tak za oprávněnou jednotku. Dostal by se tak samozřejmě ke službám, ke kterým mohla oprávněná jednotka původně přistupovat. Jednotka OLT samozřejmě neautentizuje ONU, která patří do jiné PON. V případě, že jednotka byla na stejné PON pouze přemístěna, OLT s touto skutečností mnoho nezmůže. Není však specifikováno, jak by se měla OLT zachovat v případě, že se na PON vyskytnou dvě ONU se shodnými sériovými čísly, OLT by na tento stav měla upozornit [17].

Další hrozbou je odcizení identity jednotky OLT. Mohlo by k němu dojít v případě, že útočník získá přístup k PON. Tento útok už je spíše nepravděpodobný a poměrně složitý na provedení. Situaci by také muselo zachytit dohledové centrum poskytovatele služeb [17].

Počátkem tohoto útoku je pasivní monitorování a sběr informací o koncové jednotce. Získané informace poslouží útočníkovi k zamaskování modifikované ONU pomocí manipulace s citlivými daty. Tato data jsou obsažena v každém vysílaném rámci a útočník je v každém rámci musí nahradit. Upravené rámce poté vypadají, že pochází od jiné jednotky ONU. Pokud jsou navíc identifikační data vysílána ve formě prostého textu, není složité je odposlechnout [15].

Tento typ útoku, maskování identity útočníka (tzv. masquerade) je možné provést v sestupném i vzestupném směru pomocí nahrazování informací v rámcích.

Jednotka OLT není schopna rozlišit, zda se jedná skutečně o oprávněného uživatele nebo se za něj vydává někdo jiný [66].

Případný útočník by také mohl zaznamenávat vysílané rámce a později je podvrhnout (jedná se o tzv. replay attack). Terčem útoku by mohly být například zprávy PLOAM [17].

8.6 Bezpečnostní rizika APON a BPON

Velkou slabinou je použití pouze osmibitového šifrování (technika *churning*), je velmi snadné vyzkoušet všechny možné kombinace znaků k prolomení tohoto zabezpečení (tzv. útok hrubou silou). V záhlaví nebude složité rozpoznat správnou hodnotu klíče, jelikož záhlaví obsahuje velké množství prostého textu. V případě přenosové rychlosti 622 Mb/s a již zmíněné doby pro aktualizaci klíčů, je případnému útočníkovi poskytnut dostatečný čas pro analýzu přenášených dat. Opakováním útoku je možné získat klíč po přibližně 2^9 dešifrovacích pokusech.

Standard požaduje výměnu klíčů techniky *churning* každou sekundu. Nový klíč je přenášen ve formě prostého textu od jednotky ONU k jednotce OLT, přenos tedy probíhá ve vzestupném směru a proto není snadné tento klíč odposlechnout. Zavedení této metody mělo posílit zabezpečení standardu APON. Výměna klíčů však neposkytuje dostatečnou úroveň zabezpečení vůči útoku hrubou silou, jelikož tento útok je možné opakovat při každé změně klíče.

Na techniku *churning* je však možné použít i klasické techniky kryptoanalýzy jednoduchých substitučních šifer. Tato technika tedy není nejvhodnějším řešením pro zabezpečení přenosu prostřednictvím PON sítí [61].

Tato bezpečnostní rizika lze však minimalizovat použitím dalších technik k zabezpečení komunikace. Zmírnit riziko odposlechu komunikace je možné například využitím SSL, IPsec (Zabezpečený IP protokol – IP Security), případně VPN (Virtuální privátní síť – Virtual Private Network). Nasazení dodatečného zabezpečení však s sebou nese zvýšení režijních nákladů [61].

8.7 Bezpečnostní rizika GPON

Podstatným bezpečnostním rizikem standardu GPON jsou zprávy PLOAM. Tyto zprávy jsou ve formátu prostého textu a případný útočník by je tedy mohl zneužít k provedení útoku. Útočník by mohl provést opakování PLOAM zpráv, důsledkem tohoto útoku by bylo omezení služeb pro ostatní koncové uživatele. PLOAM zprávy dále nejsou nijak zabezpečeny proti jejich falšování, tato skutečnost by mohla vést

k útokům MitM („Člověk uprostřed“ – Man in the Middle), odepření služby, případně k odcizení identity, kdy by se útočník mohl vydávat za jinou osobu [18].

Dalším rizikem je nezabezpečený přenos šifrovacího klíče pro data posílaná v sestupném směru. Tento klíč je používán jednotkou OLT k šifrování provozu v sestupném směru. V případě, že by došlo k zachycení provozu ve vzestupném směru, došlo by i k zachycení tohoto nezabezpečeného klíče. Útočník by tak získal klíč, kterým by byl schopen dešifrovat data v sestupném směru [44].

8.8 Bezpečnostní rizika XG-PON

Po dokončení specifikace standardu XG-PON, považovali někteří poskytovatelé telekomunikačních služeb nový bezpečnostní model za nedostatečný, hlavní obavou byla možnost odposlechu komunikace ve vzestupném směru. Existovaly obavy z podvržení jednotek ONU a dokonce i jednotek OLT. Jak již bylo zmíněno v podkapitole 7.6 věnované bezpečnosti standardu XG-PON, šifrování provozu bylo posíleno. Jistá bezpečnostní rizika však existují i v případě standardu XG-PON.

Může dojít například k odcizení služeb (ToS) vysílaných multicastově, i v případě, že je toto spojení šifrované. Stačí, aby si skupina uživatelů objednala služby VoD (pouze jednu licenci), kterou pak mezi sebou rozšířila, případně i modifikovala koncovou jednotku pro příjem videa [17]. Nejedná se vyloženě o bezpečnostní riziko, důsledkem by v tomto případě byla „jen“ ekonomická ztráta na straně poskytovatele služeb. Jedná se ale o způsob, jak se dostat k zašifrovanému obsahu, který je šířen pomocí multicastového spojení.

8.9 Bezpečnostní rizika NG-PON2

V předchozích standardech PON mohla modifikovaná koncová jednotka narušovat fungování PON vysíláním mimo stanovené časové intervaly. Při přenosu v rámci NG-PON2 jsou pro přenos využity různé vlnové délky, komunikaci by v tomto případě mohla narušovat modifikovaná koncová jednotka nerespektující přidělenou vlnovou délku. Vždy však existuje možnost výskytu poruchy u jednotky ONU. V tomto případě využití různých vlnových délek pro přenos umožňuje přemístění koncových jednotek zasažených útokem nebo poruchou na jiný kanál, jehož vlnová délka je tímto stavem nedotčena [47].

NG-PON2 řeší i problém odposlechu komunikace ve vzestupném směru při registraci jednotky ONU. V této fázi by případný útočník mohl vygenerovat vlastní klíče. Výhodou využití TWDM je však sestavení virtuálního spojení typu bod-bod,

které riziko odposlechu spolehlivě eliminuje. Při použití AWG (Vlnovod s mřížkovým uspořádáním – Array Wavelength Gratings) však může docházet k přeslechům mezi jednotlivými kanály [1].

8.10 Bezpečnostní opatření proti útokům

Předpokladem pro bezpečnostní opatření, která by měla zabránit případnému útoku, je detekce a odpojení uživatele, který ať už úmyslně nebo například v důsledku poruchy narušuje normální provoz sítě a její uživatele. Detekci a případné odpojení takového uživatele by bylo možné provést i vzdáleně, bez nutnosti výjezdu technika poskytovatele služeb.

8.10.1 Detekce útoků

Pro monitorování pasivní sítě by bylo možné využít například OTDR (Optická reflektometrie v časové oblasti – Optical Time Domain Reflectometry), otázkou je však směr měření od OLT. OTDR je jednostranná měřicí metoda, která se využívá pro provozní měření útlumu optické trasy, velkou výhodou je získání přehledu o útlumu po celé měřené trase. Tato metoda ale není schopna zjistit přerušení optického kabelu na některém z výstupů pasivního optického rozbočovače.

Možným monitorovacím nástrojem by bylo využití metody OFDR (Optická reflektometrie ve frekvenční oblasti – Optical Frequency Domain Reflectometry). Metoda OFDR překrývá nízkofrekvenční a nízkoenergetickou sinusovou modulaci signálu v sestupném směru. OFDR oproti OTDR umožňuje rychlejší extrakci signálu, ale snižuje SNR (Odstup signálu od šumu – Signal-to-noise ratio).

Tyto techniky by mohly být použity jako doplňkové k dalším detekčním a monitorovacím mechanismům používaným na vyšších vrstvách. Tímto způsobem by byla zvýšena spolehlivost detekce případného útoku. Detekce případného útoku na síťovou infrastrukturu je prvním důležitým krokem. Druhým krokem je potlačení útoku a odpojení útočníka ze sítě [40].

8.10.2 Preventivní opatření

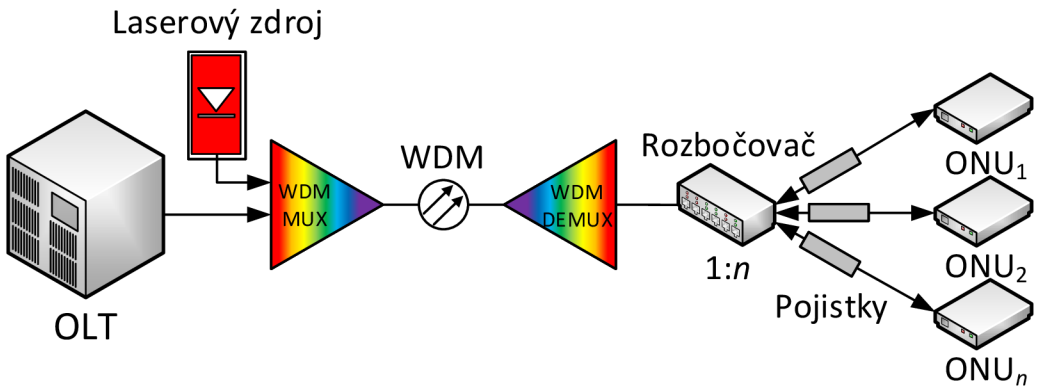
Možným bezpečnostním opatřením by bylo zavedení aktivních optických přepínačů, které by realizovaly zabezpečení přepínání rámců. Takové řešení by však bylo nákladné, jelikož k selhání optického vedení i případným útokům nedochází příliš často. Aktivní prvky by navíc vyžadovaly napájení.

Nabízí se tedy čistě pasivní řešení, které by nebylo tolik nákladné. Autoři [40] navrhují použití speciálních optických vláken, která by byla citlivá na vysoký výkon

použitého laseru a byla použita jako pojistkový obvod. Toto „pojistkové“ vlákno by bylo součástí pasivního optického rozbočovače a sloužilo by jako tavná pojistka – řešení je zobrazeno na obrázku 8.2.

Jednotka OLT by mohla v případě překročení definovaných limitů vyslat pomocí laserové pumpy silný laserový impulz, který by tuto pojistku roztavil a odpojil tak daného koncového uživatele od sítě. Předpokladem je použití WDM a přiřazení vlnových délek jednotlivým koncovým uživatelům. Jednotka OLT musí vyslat silný laserový signál na odpovídající vlnové délce tak, aby došlo pouze k odpojení požadovaného koncového uživatele. Problémem je ale topologie sítě, na jedné vlnové délce komunikuje zpravidla více ONU. Dalším předpokladem je pak spolehlivá detekční metoda. Tento způsob odpojení by potom neměl žádný dopad na ostatní uživatele sítě [40].

Dalším důležitým aspektem je také zajištění fyzické bezpečnosti instalovaných prvků ODN. Je vhodné umožnit přístup k těmto prvkům pouze oprávněným osobám [34].



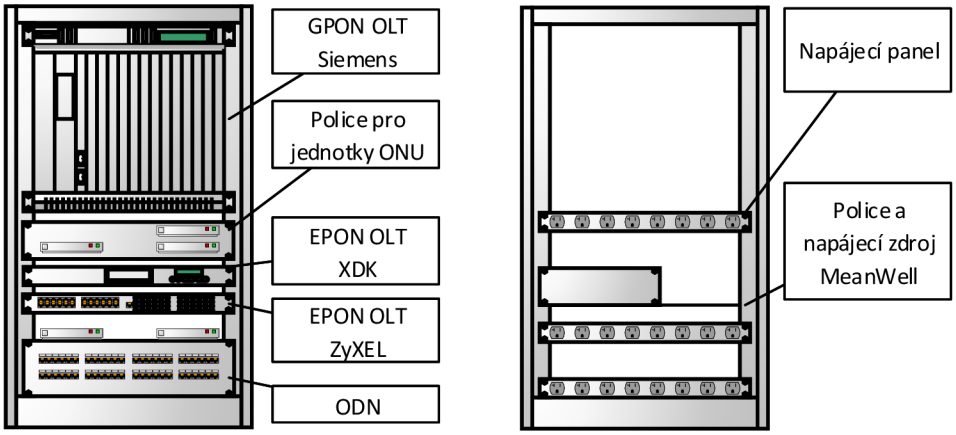
Obr. 8.2: Použití tavné pojistky [40].

9 Kompletace racku

V rámci praktické části této diplomové práce bylo realizováno kompletní osazení racku pro účely pozdějšího testování. Do racku byla osazena GPON OLT jednotka od firmy Siemens, konkrétně se jedná o typ hiX 5750. Tato jednotka je napájena pomocí zdroje MeanWell (48 V, 50 A), který je umístěn na polici v zadní části racku. Dále jsou osazeny dvě EPON OLT jednotky. První z nich je jednotka E8110T od výrobce XDK. Druhá osazená EPON OLT jednotka byla vyrobena firmou ZyXEL. Jedná se o typ 1308S-22. Mezi OLT jednotkami je umístěna police, která je určena pro umístění jednotek ONU.

V zadní části racku jsou osazeny tři napájecí panely s klasickými zásuvkami pro napájení zařízení. Přívody k těmto panelům jsou vyvedeny podlahou racku.

Odvod tepla z racku je řešen pomocí panelu s ventilátory. Tento panel je zabudován do stropu racku a obsahuje celkem šest ventilátorů. Panel je vybaven teplotním senzorem a je možné nastavit teplotu, při které dojde k sepnutí ventilátorů. V současné době je sepnutí nastaveno na teplotu 30 °C, termostat je umístěn na pravém boku. Na podlaze racku je umístěna optická distribuční síť nacházející se v boxu velikosti 4U. Popis realizace ODN je uveden v podkapitole 9.4. Schématický nákres osazení racku je zobrazen na obrázku 9.1.

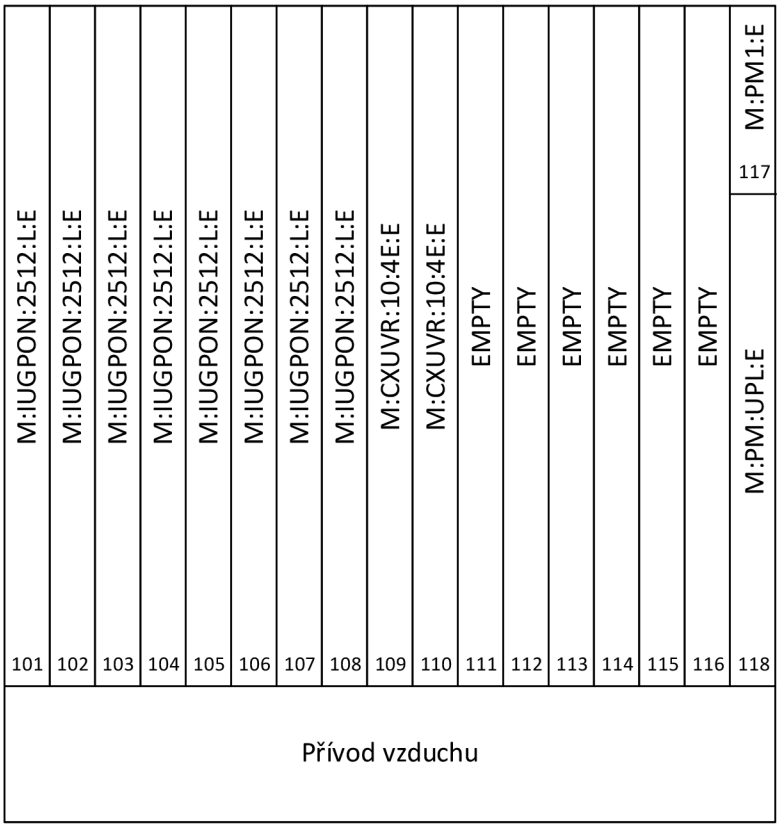


(a) Přední pohled. (b) Zadní pohled.

Obr. 9.1: Osazení racku.

9.1 OLT jednotka Siemens

Šasi jednotky obsahuje celkem 18 slotů, poslední ze slotů je rozdělen na dvě poloviny. Ve slotu číslo 117[1] je umístěn napájecí modul M:PM1:E, který je osazen konektorem pro připojení napájecího zdroje, tento modul není možné odebrat. Slot číslo 118 je osazen modulem M:PM:UPL:E, který disponuje druhým konektorem pro připojení záložního napájení a několika porty RJ45. Jednotka je však napájena pouze z jednoho zdroje. Do šasi OLT jednotky je tedy možné umístit celkem 17 modulů. Rozmístění jednotlivých modulů v šasi je zobrazeno na obrázku 9.2.



Obr. 9.2: OLT jednotka Siemens.

Konfigurovaná jednotka je vybavena celkem 8 moduly M:IUGPON:2512:L:E. Každý z těchto modulů obsahuje 4 optické porty s konektorem typu SC/UPC. Na tyto moduly se připojují jednotlivé distribuční sítě. Moduly jsou osazeny ve slotech 101 až 108. Do volných slotů jednotky je možné přidat další GPON moduly.

Modul M:CXUVR:10:4E:E je vybaven jedním konektorem SFP+ (Zásuvný konektorový modul – Small Form-factor Pluggable) pro připojení do sítě poskytova-

[1]Čísluje se včetně samotného šasi.

tele služeb, tento konektor podporuje 10Gb Ethernet. Dále je modul osazen čtyřmi SFP konektory podporujícími gigabitový Ethernet. Moduly M:CXUVR:10:4E:E jsou v jednotce dva, osazeny jsou ve slotech 109 a 110. Oba moduly jsou vybaveny konzolovými porty s konektorem RJ45 pro konfiguraci jednotky. Pro vzdálenou správu slouží port FE LCT, k jednotce je možné se vzdáleně připojit pomocí SSH (Zabezpečený protokol SSH – Secure Shell) nebo je možné použít Telnet. Pro vyšší bezpečnost je však lepší použít SSH, jelikož komunikace prostřednictvím SSH je šifrovaná. Pro zvýšení bezpečnosti je vhodné zakázat výchozí uživatelský účet, případně změnit výchozí heslo.

V tomto modulu se také nachází vnitřní paměť zařízení, uložena je zde konfigurace. Paměť obsahuje dva obrazy softwaru jednotky. Prvním je aktuálně běžící verze softwaru, která je načtena vždy po (re)startu jednotky. Druhý obraz je neaktivní a bude přepsán při aktualizaci softwaru.

Šasi je pro větší spolehlivost možné osadit dvěma moduly M:CXUVR:10:4E:E. V tomto případě je jeden modul aktivní a druhý je v tzv. standby módu (pasivní). Při selhání aktivního modulu převezme jeho úlohu pasivní modul. Je tedy nutné, aby oba moduly obsahovaly shodnou verzi softwaru.

9.2 OLT jednotka XDK

Další osazenou jednotkou je EPON OLT jednotka vyrobená firmou XDK. Jednotka je velikosti pouze 1U, vybavena je jedním optickým portem s konektorem SC/UPC, dále obsahuje port pro SFP modul, port s konektorem RJ45, port pro správu (MGMT) a také konzolový port.

9.3 OLT jednotka ZyXEL

Poslední osazenou jednotkou je EPON OLT jednotka od firmy ZyXEL. Jednotka je opět velikosti 1U, osazena je celkem 4 optickými porty s konektorem SC/UPC, dále obsahuje 4 sloty pro zapojení SFP, 2 porty s konektorem RJ45, port pro správu (MGMT) a samozřejmě také konzolový port.

9.4 Optická distribuční síť

Dalším krokem praktické části této diplomové práce byla realizace optické distribuční sítě pro účely měření a testování, která je také součástí racku. Z důvodu osazení do racku byl zvolen „box“ velikosti 4U, do kterého byl navinut 1 km optického kabelu – obsahuje celkem 24 vláken. Kabel se bohužel nepodařilo navinout vcelku

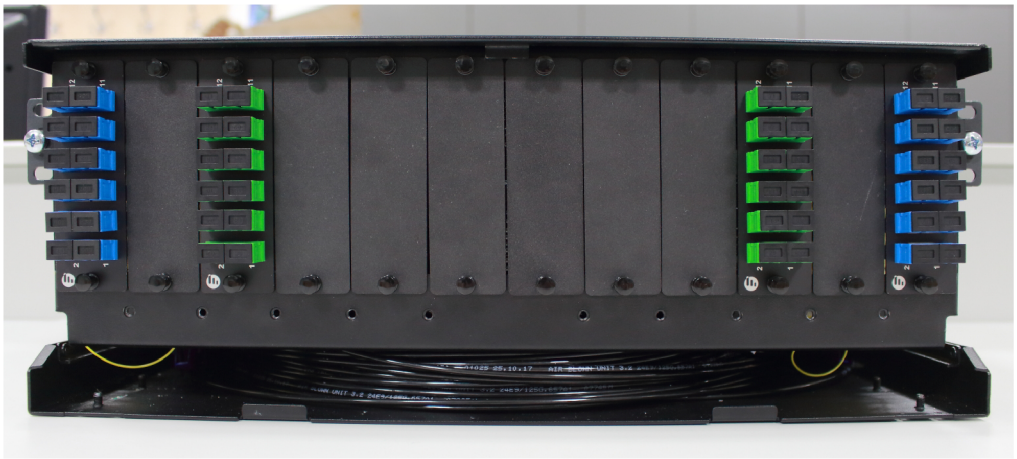
a po zhruba 200 metrech bylo nutné provést svaření jednotlivých vláken. Na oba konce optického kabelu byla navařena optická vlákna opatřená konektory (pigtaily). Polovina konektorů je typu SC/UPC (modré konektory), druhá polovina SC/APC (zelené konektory). Všechny sváry jsou opatřeny ochranami a uloženy v kazetách.

V tabulce 9.1 je uveden přehled jednotlivých vláken kabelu, informace o konektoru, kterým jsou zakončena a také informace o útlumu provedeného sváru (hodnota odhadnutá svářečkou) – tyto informace jsou uvedeny také na štítku, kterým je každý konektor opatřen. *Poznámka:* pořadí označuje umístění konektoru v optické spojce, barva vlákna ohraničená spojovníky značí žíhané vlákno, $A_{\text{Levá}}$ značí útlum sváru na levé straně, obdobně je označen útlum svárů na pravé straně ($A_{\text{Pravá}}$).

Tab. 9.1: Kompletní přehled vláken optického kabelu ODN.

Pořadí	Barva vlákna	Konektor	$A_{\text{Levá}}$ [dB]	$A_{\text{Pravá}}$ [dB]
01	-Hnědá-	SC/UPC	0,00	0,02
02	-Zelená-	SC/UPC	0,01	0,04
03	-Bílá-	SC/UPC	0,03	0,01
04	-Čirá-	SC/UPC	0,01	0,00
05	-Červená-	SC/UPC	0,03	0,03
06	-Fialová-	SC/UPC	0,03	0,02
07	-Tyrkysová-	SC/UPC	0,03	0,02
08	-Šedá-	SC/UPC	0,03	0,01
09	-Oranžová-	SC/UPC	0,03	0,01
10	-Žlutá-	SC/UPC	0,00	0,00
11	-Modrá-	SC/UPC	0,03	0,01
12	-Růžová-	SC/UPC	0,02	0,01
13	Hnědá	SC/APC	0,00	0,02
14	Zelená	SC/APC	0,02	0,01
15	Bílá	SC/APC	0,02	0,04
16	Černá	SC/APC	0,01	0,03
17	Červená	SC/APC	0,00	0,00
18	Fialová	SC/APC	0,03	0,00
19	Tyrkysová	SC/APC	0,02	0,00
20	Šedá	SC/APC	0,03	0,00
21	Oranžová	SC/APC	0,03	0,01
22	Žlutá	SC/APC	0,00	0,04
23	Modrá	SC/APC	0,00	0,02
24	Růžová	SC/APC	0,01	0,00

Na čelním panelu 4U „boxu“ jsou umístěny panely s optickými spojkami, opět je 24 spojek určeno pro konektory typu SC/UPC a zbylých 24 pro SC/APC. Pomocí spojek je možné propojit jednotlivé páry vláken optického kabelu a vytvořit tak libovolnou ODN, nebo i více oddělených sítí požadované délky, maximálně však 24 km. Finální provedení ODN je zobrazeno na obrázku 9.3, kompletní fotodokumetace je k dispozici na přiloženém CD.



Obr. 9.3: Realizovaná ODN.

Po dokončení ODN bylo provedeno měření útlumu přímou metodou a také pomocí OTDR. Útlum byl měřen na jednotlivých vláknech, poté byla změřena trasa obsahující pouze konektory SC/UPC (modrá trasa), následně trasa obsahující pouze konektory SC/APC (zelená trasa) a nakonec byl změřen i útlum kompletní trasy. Měření bylo provedeno na vlnových délkách 1 310 a 1 550 nm, při měření přímou metodou bylo nutné nastavit referenci mezi měřicími přístroji. Tabulka 9.2 obsahuje výsledky měření přímou metodou.

Pomocí metody OTDR byla poté změřena zvlášť modrá a zelená trasa, nakonec byla samozřejmě změřena i celá trasa. Útlum trasy změřený pomocí OTDR je uveden v tabulce 9.3, kromě hodnoty útlumu je uvedena i délka trasy a koeficient útlumu. Obrázek 9.4 zobrazuje OTDR náměr modré trasy, obrázek 9.5 zobrazuje OTDR náměr zelené trasy ODN.

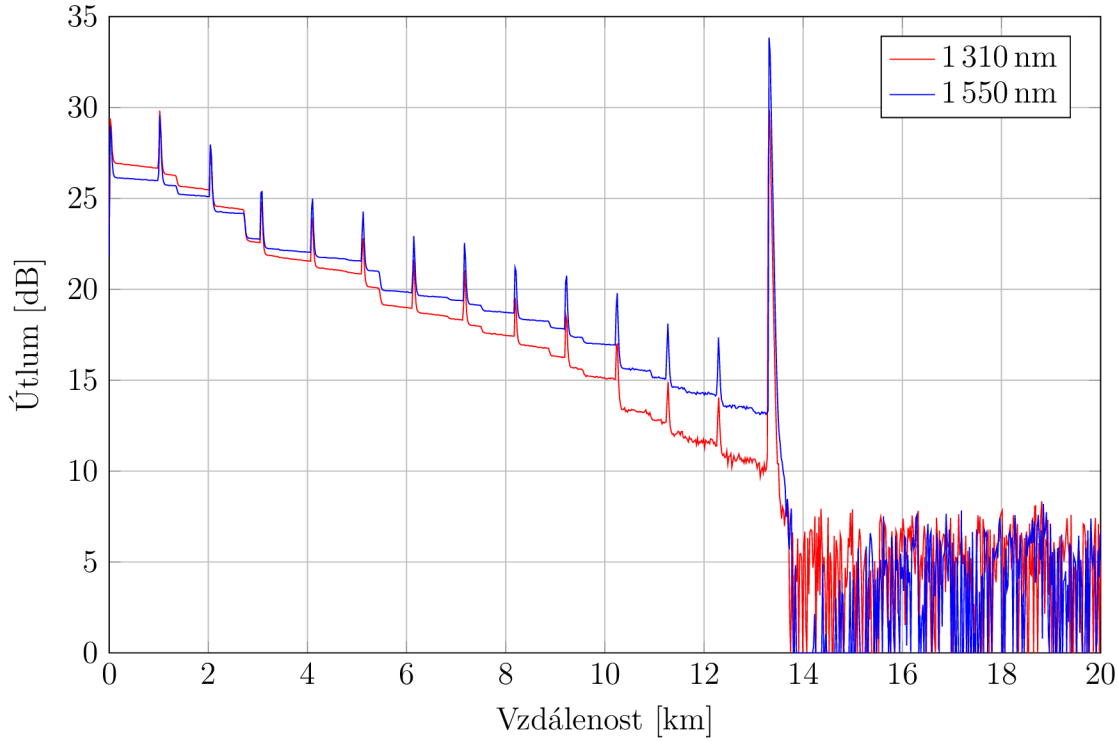
Výsledky získané přímou metodou je možné brát jako nejpřesnější. Metoda optické reflektometrie poskytuje díky grafickému zobrazení (závislost útlumu na vlnové délce) dobrý přehled o měřené trase, výsledky získané pomocí této metody je možné brát jako referenční. Kompletní výsledky měření útlumu ODN obsahuje protokol o provedeném měření, který je umístěn na přiloženém CD.

Tab. 9.2: Útlum optické distribuční sítě, výsledky přímé metody.

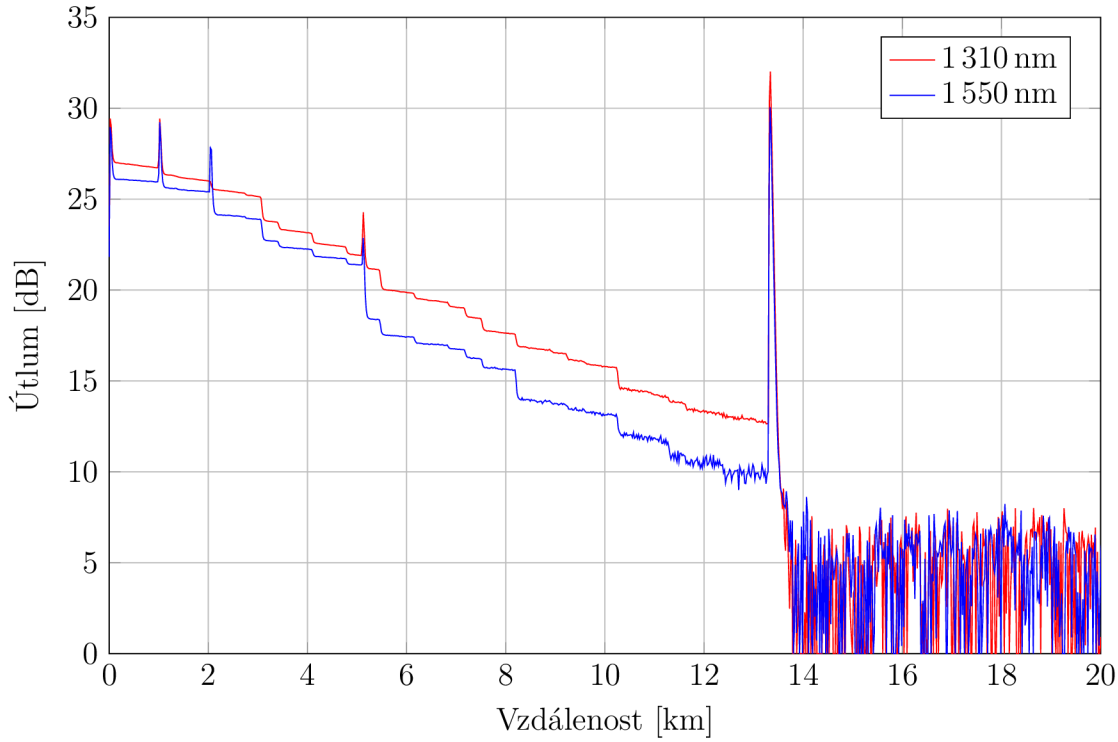
Vlákno	A_{1310} [dB]	A_{1550} [dB]	Vlákno	A_{1310} [dB]	A_{1550} [dB]
01	1,01	1,11	13	1,14	1,30
02	2,47	2,26	14	0,87	1,22
03	0,98	0,93	15	1,82	1,94
04	0,66	0,59	16	1,42	3,16
05	1,61	2,48	17	1,70	1,60
06	0,73	0,83	18	1,08	0,96
07	0,95	1,05	19	1,39	1,89
08	1,07	1,14	20	1,21	1,24
09	1,39	1,06	21	1,14	1,94
10	1,37	1,04	22	1,07	1,62
11	1,45	1,07	23	1,03	2,30
12	1,50	1,15	24	0,80	1,15
Modrá trasa	15,20	9,00	Zelená trasa	14,20	16,50
			Celkem	**30,50**	**29,40**

Tab. 9.3: Útlum optické distribuční sítě, výsledky metody OTDR.

Trasa	λ [nm]	A_{m} [dB]	l [km]	α [dB/km]
Modrá	1 310	16,63	13,29	1,25
	1 550	12,93		0,97
Zelená	1 310	14,31	13,31	1,08
	1 550	16,29		1,22
Celková	1 310	27,92	25,60	1,09
	1 550	24,99		0,94



Obr. 9.4: OTDR náměr modré trasy.



Obr. 9.5: OTDR náměr zelené trasy.

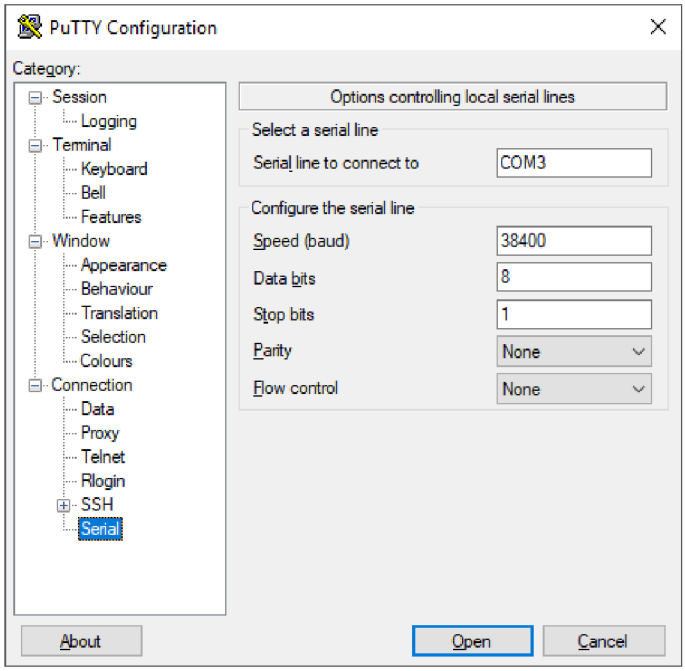
10 Konfigurace OLT jednotek

V této kapitole je popsána konfigurace GPON OLT jednotek Siemens hiX 5750, Huawei MA5683T a EPON OLT jednotky ZyXEL 1308S-22. Pro účely základní konfigurace a ověření funkčnosti byly k jednotlivým jednotkám OLT připojeny koncové jednotky ONU. Připojení bylo realizováno pomocí cívky s optickým vláknem a pasivním optickým rozbočovačem. V případě jednotky Siemens bylo použito vlákno délky 3 km a rozbočovače s rozbočovacím poměrem 1:16, pro jednotky Huawei a ZyXEL bylo použito vlákno délky 20 km a rozbočovače 1:16 a 1:4.

10.1 Konfigurace GPON OLT jednotky Siemens

Pro prvotní připojení k jednotce je nutné použít konzolového portu, který je součástí modulu CXU. Jednotka je s počítačem propojena pomocí sériového rozhraní, respektive redukce COM/USB. Pro komunikaci s jednotkou prostřednictvím CLI (Příkazový řádek – Command Line Interface) byl zvolen program PuTTY. Program je však třeba pro připojení k jednotce správně nastavit.

Pro připojení k jednotce je nutné v programu PuTTY vybrat typ připojení *Serial*. Poté je zvoleno sériové rozhraní, ke kterému je jednotka připojena – v tomto případě COM3. Rychlost pro komunikaci na sériové lince je nastavena na 38 400 bit/s. Kompletní nastavení sériového rozhraní je zobrazeno na obrázku 10.1.



Obr. 10.1: Nastavení sériového portu pro komunikaci s OLT Siemens.

Po navázání spojení s jednotkou je zobrazena výzva k zadání uživatelského jména a odpovídajícího hesla. Ve výchozím nastavení je uživatelské jméno *root* a heslo *siemens7*. Přepnutí do EXEC módu se provádí příkazem `enable`. Pro konfiguraci zařízení je nutné vstoupit do konfiguračního módu pomocí příkazu `configure terminal`, případně zkráceně `conf t`.

Jednotka byla pojmenována *GPON-OLT-SIEMENS*, pro přístup do EXEC módu bylo nastaveno heslo. Dále bylo nastaveno šifrování hesel – ve výpisech konfigurace jednotky se heslo nezobrazí jako prostý text. Pokud je uživatel nečinný déle jak 30 minut, dojde k jeho automatickému odhlášení z EXEC módu.

Pro přístup k jednotce byly vytvořeny nové účty: administrátorský účet *GPO-Nadmin* a studentský účet *Student*. Počet současně přihlášených uživatelů byl omezen na pět. Na jednotce bylo dále povoleno automatické zálohování konfigurace do lokální paměti, záloha se ukládá automaticky každých 30 minut. Pokud chce uživatel konfiguraci uložit ihned, je možné použít příkaz `write memory`, poté je nutné vyčkat na uložení konfigurace, které jednotka potvrdí výpisem `[OK]`. Výše popsaná konfigurace byla provedena pomocí příkazů uvedených ve výpisu 10.1:

Výpis 10.1: Prvotní konfigurace jednotky OLT.

```
SWITCH login: root
Password: siemens7
SWITCH> enable
SWITCH# conf t
SWITCH(config)# hostname GPON-OLT-SIEMENS
GPON-OLT-SIEMENS(config)# passwd enable ***
GPON-OLT-SIEMENS(config)# service password-encryption
GPON-OLT-SIEMENS(config)# exec-timeout 30 0
GPON-OLT-SIEMENS(config)# write memory
[OK]
```

Při zadávání hesla prostřednictvím CLI se jednotlivé znaky nezobrazují, ve výpisu 10.1 a výpisech následujících jsou však hesla uvedena nebo nahrazena znaky `***`. U příkazu `exec-timeout` udává první číslo čas v minutách, druhé v sekundách.

Pro vyšší spolehlivost bylo nastaveno automatické ukládání konfigurace do paměti OLT jednotky. Toho je možné docílit následujícím způsobem: nejprve je automatické ukládání povoleno a poté je možné nastavit po jakém čase se konfigurace automaticky uloží, čas se v tomto případě zadává v minutách. Příklad nastavení automatického ukládání konfigurace je uveden ve výpisu 10.2.

Výpis 10.2: Nastavení automatického ukládání konfigurace.

```
GPON-OLT-SIEMENS(config)# auto-backup local enable
GPON-OLT-SIEMENS(config)# auto-backup local waiting-time 30
```

10.1.1 Vytvoření uživatelů

Přidání nového uživatele je možné pomocí příkazu `user add`, který je následován parametry *Name* a *Description*. První z parametrů udává přihlašovací jméno nového uživatele, druhý parametr slouží k popisu. Příklad vytvoření nového uživatele obsahuje výpis 10.3, pomocí příkazu `login connect 5` byl počet současně přihlášených uživatelů omezen na pět.

Výpis 10.3: Příklad vytvoření nového uživatele.

```
GPON-OLT-SIEMENS(config)# user add GPONadmin administrator
Changing password for GPONadmin
Enter the new password (minimum of 5, maximum of 8 characters).
Please use a combination of upper and lower case letters and numbers.
Enter new password: ***
Re-enter new password: ***
Password changed successfully
```

10.1.2 Přidání jednotky ONU

Jednotku ONU je možné na OLT přidat dvěma způsoby. Prvním ze způsobů je registrace koncové ONU pomocí jejího sériového čísla, druhým způsobem je tzv. *discover* mód, kdy OLT jednotku ONU vyhledá automaticky.

Přidání ONU se provádí v konfiguračním módu pomocí příkazu `create onu`, pro konfiguraci pomocí sériového čísla je syntaxe příkazu uvedena ve výpisu 10.4.

Výpis 10.4: Syntaxe přidání jednotky ONU.

```
GPON-OLT-SIEMENS(config)# create onu ONU_type Address configured Serial_number
Password Alarm_severity_profile Battery_backup Security_mode Fixed_bandwidth Line
```

`ONU_type:` definuje typ jednotky ONU, použity jsou jednotky *G25E-001*. Tento typ jednotky obsahuje čtyři Ethernetové porty, které podporují 10/100 Mb Ethernet. Dále jednotka obsahuje dva porty pro připojení telefonního přístroje, tyto porty jsou označeny zkratkou POTS.

`Address:` udává specifikaci portu, do kterého je jednotka připojena. Zápis se provádí ve tvaru *OLT-slot/GPON-port/ONU-ID*, kde *OLT-slot* je pořadové číslo slotu, ve kterém je umístěn daný GPON modul, *GPON-port* udává pořadové číslo portu na GPON modulu a *ONU-ID* je identifikační číslo jednotky ONU. Identifikační číslo slouží pro rozlišení jednotlivých jednotek ONU, zpravidla jich bývá na jednom portu připojeno více. *ONU-ID* zadává administrátor jednotky.

Configured: je zadáváno pouze v případě, že je koncová jednotka registrována pomocí svého sériového čísla.

Serial_number: parametr `configured` je následován sériovým číslem registrované jednotky. Sériové číslo jednotky ONU je nutné zadat v dekadickém tvaru. Na štítku přidávané ONU je uvedeno sériové číslo (PON SN) CIGG07060624 v ASCII, při konfiguraci je ale nutné zadat: 4349474707060624.

Password: slouží k přiřazení hesla k dané jednotce ONU. Heslo je využito k ověření registrace dané jednotky, nastavení hesla se provede zadáním parametru `password` následovaného heslem. V případě registrování jednotky bez hesla je nutné zadat parametr `nopassword`. Heslo je možné jednotce přiřadit i později.

Alarm_severity_profile: slouží k přiřazení ONU do některého z definovaných profilů. Zadává se pouze číselná hodnota 1 až 10, pro jednotky ONU je tedy možné definovat až deset profilů, jednotku je však možné přiřadit pouze do jednoho profilu.

Battery_backup: v případě, že dojde k přerušení dodávky elektrické energie pro jednotku OLT, mělo by dojít k automatickému přepnutí na náhradní zdroj elektrické energie (pokud je k němu jednotka připojena). Pro tento případ je možné nastavit, které jednotky ONU budou při výpadku primárního zdroje elektrické energie ponechány v provozu. Pro povolení dané jednotky při napájení ze záložního zdroje je zadáno `on`, v opačném případě `off`.

Security_mode: pro povolení šifrované komunikace v sestupném směru je nutné zadat číslo 1. Pokud je šifrování zapnuto, je ještě nutné nastavit čas pro periodickou výměnu klíčů mezi jednotkou OLT a konfigurovanou jednotkou ONU. Čísla jsou zadávána z rozsahu 1 až 444, kde číslo 1 odpovídá 5 minutám a číslo 444 odpovídá 37 hodinám.

Fixed_bandwidth: slouží k přidělení šířky pásma určitým službám. Dostupná šířka pásma se nastavuje zadáním čísla v rozsahu 1 až 1 099 560 000, které udává celkovou přidělenou šířku pásma v bitech za sekundu. Tento parametr se nezadává pouze jednou, šířku pásma je nutné přidělit následujícím službám:

- Pevně přidělená šířka pásma, přidělená pro všechna TDM rozhraní jednotky ONU.
- Garantovaná šířka pásma, přidělená pro všechna POTS (VoIP) rozhraní jednotky ONU.
- Garantovaná šířka pásma, přidělená pro všechny prioritní přenosy v reálném čase na daném rozhraní jednotky ONU.
- Garantovaná šířka pásma, přidělená pro všechny prioritní přenosy neprobíhající v reálném čase na daném rozhraní jednotky ONU.
- Maximální přidělená šířka pásma pro všechny prioritní přenosy neprobíhající v reálném čase na daném rozhraní jednotky ONU.

- Maximální přidělená šířka pásma pro všechna rozhraní s nastavením kvality služeb best effort.

Line: uživatelská data sloužící k popisu vytvořené jednotky ONU. Pro tyto účely je možné použít až 80 znaků.

První jednotka byla přidána na první GPON modul a jeho první port, zároveň jí bylo přiřazeno identifikační číslo 1. Příklad přidání jednotky ONU je uveden ve výpisu 10.5

Výpis 10.5: Přidání jednotky ONU.

```
GPON-OLT-SIEMENS(config)# create onu g25e-001 1/1/1 configured 4349474707060624
nopassword 1 off 0 45000 45000 45000 45000 45000 45000 ONU1
ONU 1/1/1 created successful!
```

Podobným způsobem byla přidána i druhá jednotka ONU. Tyto dvě jednotky byly připojeny na stejný port jednotky OLT přes společný pasivní optický rozbočovač – druhá přidaná jednotka ONU má tedy adresu *1/1/2*. Fyzické připojení bylo provedeno pomocí pasivního optického rozbočovače s rozbočovacím poměrem 1:16 a optického vlákna G.652D délky 3 km.

Po vytvoření a fyzickém připojení jednotek ONU však kontrolka *Optical* na jednotce ONU svítí červeně. Tím je signalizován stav, že k jednotkám ONU není připojeno žádné optické vlákno.

Dalším nutným krokem je tedy aktivace portu jednotky OLT, na kterém jsou právě vytvořené jednotky ONU fyzicky připojeny. Jednotky jsou připojeny k portu modulu GPON, který je označen jako LRE (Ethernet s dlouhým dosahem – Long Reach Ethernet). Pro konfiguraci portů je nutné se v CLI přepnout z konfiguračního módu do módu označeného *bridge*. Adresa požadovaného portu se zadává ve tvaru *OLT-slot/GPON-port*, povolení portu se provede příkazem `enable`. Aktivace portu na jednotce OLT je demonstrována ve výpisu 10.6.

Výpis 10.6: Aktivace portu jednotky OLT.

```
GPON-OLT-SIEMENS(config)# bridge
GPON-OLT-SIEMENS(bridge)# port lre 1/1 enable
```

K portu je možné přidat libovolný popis pomocí parametru `description`. Ten je však volitelný a není tedy nutné jej využít.

Po přidání je jednotka uzamčena a je možné provádět další nastavení a konfiguraci, kontrolka *Optical* na jednotkách nyní svítí přerušovaně zelenou barvou. Pomocí příkazu `show onu table` následovaného adresou požadované jednotky ONU (v již známém tvaru *OLT-slot/GPON-port/ONU-ID*) je možné zobrazit detailní informace

o jednotce. V tomto výpisu je důležité ověřit, zda je jednotka povolena – nyní jednotka ještě povolena není, jednotka je uzamčena – ve výpisu se v řádku *Adminstate* nachází hodnota *ONU locked*, na následujícím řádku *Operstate* se nachází hodnota *ONU disabled*. Odemčení jednotky se provede způsobem uvedeným ve výpisu 10.7.

Výpis 10.7: Odemčení jednotky ONU.

```
GPON-OLT-SIEMENS(config)# modify onu adminstate 1/1/1 unlock
```

Druhá připojená jednotka byla odemčena obdobným způsobem. Po odemčení jednotky ONU se zeleně rozsvítí kontrolky *Optical* a *LAN*, nyní je jednotka připravena k použití. Kompletní výpis konfigurace již aktivované jednotky ONU obsahuje výpis 10.8.

10.1.3 Konfigurace jednotky ONU

Konfigurace jednotky ONU probíhá vzdáleně prostřednictvím CLI na OLT. Pro otestování základní funkčnosti byl k Ethernetovému portu jednotky připojen počítač. Porty jsou však opět deaktivované a je nutné je aktivovat. Konfigurovaná ONU jednotka G25E-001 obsahuje čtyři Ethernetové porty a dva porty pro připojení klasických telefonních přístrojů, označeny jsou jako POTS.

Aktivace portu se provádí následujícím způsobem. Ethernetové porty jsou označeny jako *eth*, důležité je opět zadat adresu daného portu ve tvaru: *OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port*. Aktivace portu byla provedena způsobem uvedeným ve výpisu 10.9

Výpis dostupných portů jednotky ONU je možné získat způsobem uvedeným ve výpisu 10.10. V tomto výpisu je již možné vidět aktivovaný port *1/1/2/2/1*.

Připojený počítač automaticky obdržel IP adresu z rozsahu privátních adres. Ve výpisu 10.11 je možné vidět seznam MAC adres zařízení připojených k dané ONU.

10.1.4 Bezpečnostní aspekty

Pro zvýšení bezpečnosti je vhodné deaktivovat nebo omezit možnost přihlášení se k jednotce pomocí výchozího uživatelského jména a hesla. Vytvořit lze celkem 8 uživatelských účtů pro přístup k systému, mohou být vytvořeny také účty s oprávněním pouze pro čtení (read only). Systém umožňuje nastavit heslo dlouhé pouze 8 znaků, použít lze pouze malá a velká písmena a čísla. Pro zvýšení bezpečnosti je vhodné omezit počet přihlašovacích pokusů a nastavit také časový limit, kdy bude možné pokus o přihlášení opakovat. Vhodné je zakázat vzdálený přístup přes Telnet a používat SSH.

Výpis 10.8: Podrobné informace o jednotce ONU.

```
GPON-OLT-SIEMENS(config)# show onu table 1/1/2

------------------------------------------------------------
OltSlot: 1, GponPort: 1, OnuId: 2
  Configured onu type       : G25E-001
  Serialnumber method       : 1 (configured mode)
  Serialnumber    (ASCII)   : CIGGi
  Serialnumber    (HEX)     : 0x4349474707070869
  Password/Reg-Id (ASCII)   :
  Password/Reg-Id (HEX)     : 0x00000000000000000000
  Equipment-Id    (ASCII)   : 00000000113-00110-03
  Equipment-Id    (HEX)     : 0x303030303030303031313332D30303131302D3033
  Version         (ASCII)   : 00113-00110-03
  Version         (HEX)     : 0x30303131332D30303131302D3033
  Vendor-Id       (ASCII)   : CIGG
  Vendor-Id       (HEX)     : 0x43494747
  Vendor product code       : 0
  Pptp index                : 101
  Physical index            : 139329
  Alarmseverity profile     : 1
  Onu is detected           : 1   (true)
  Adminstate                : 1   (ONU unlocked)
  Operstate                 : 1   (ONU enabled)
  Security option           : 1   (AES encryption implemented)
  Security mode             : 0   (no encryption selected)
  Key length                : 128 (bit)
  Key switching time        : 1   (5 min)
  Battery backup option     :-1   (BackupOption unknown)
  Battery backup mode       : 2   (Backup disabled)
  Traffic management option : 0   (priorityControlled)
  Powerlevel                : 3
  Pvid                      : 0
  Number of Fans            : 0
  Distance                  : 3066 metre
  User data                 : ONU2
------------------------------------------------------------
Found 1 entrie(s)!
------------------------------------------------------------
```

Výpis 10.9: Povolení Ethernetového portu jednotky ONU.

```
GPON-OLT-SIEMENS(bridge)# port eth 1/1/2/2/1 enable
```

GPON porty jsou ve výchozím nastavení deaktivovány, při přidávání nové jednotky ONU je navíc nutné tuto jednotku po její konfiguraci aktivovat. Porty jednotky ONU jsou ve výchozím nastavení také neaktivní. Veškeré nastavení jednotek ONU provádí správce systému vzdáleně prostřednictvím OLT a má tak kontrolu nad sítí.

Výpis 10.10: Dostupné Ethernetové porty jednotky ONU.

```
GPON-OLT-SIEMENS(bridge)# show port onu 1/1/2

================================================================================
S/P/OId/OS/OP IF-IDX     B-PORT     LINK  NEGO  SPEED     DUPLEX    FC       TYPE
================================================================================
1/1/2/2/1     30201      142675984  Up/Up Auto  100/100   Full/Full Dis/Dis Elec
1/1/2/2/2     30202      142676000  Dn/Dn Auto  100/0     Full/-    Dis/Dis Elec
1/1/2/2/3     30203      142676016  Dn/Dn Auto  100/0     Full/-    Dis/Dis Elec
1/1/2/2/4     30204      142676032  Dn/Dn Auto  100/0     Full/-    Dis/Dis Elec
```

Výpis 10.11: MAC adresy připojených zařízení.

```
GPON-OLT-SIEMENS(bridge)# show onu 1/1/2 mac table


requesting mac table, please wait...

  BridgePort           |  MAC-Address
=======================|=====================
      1 /1 /2 /2 /1    |  78:84:3C:39:91:03
=======================|=====================
     1 entrie(s) found!
```

10.2 Konfigurace GPON OLT jednotky Huawei

OLT jednotka Huawei již byla zprovozněna dříve, nebylo nutné provádět počáteční konfiguraci jako v případě OLT jednotky Siemens. Příklad počáteční konfigurace, včetně příkladů je blíže popsán v příloze A. Jednotka je připojena do univerzitní sítě, je možný také přístup do celosvětové sítě. Jednotka byla konfigurována prostřednictvím CLI, připojení k jednotce bylo realizováno pomocí SSH a programu PuTTY. Příklady konfigurace v této kapitole jsou omezeny pouze na jednu jednotku ONU, konfigurace pro ostatní jednotky je obdobná.

10.2.1 Konfigurace DBA profilů

Konfigurovány byly celkem 4 DBA profily 5 Mb/s, 50 Mb/s, 100 Mb/s a 1 000 Mb/s („neomezený“). Způsob vytvoření nového profilu je uveden ve výpisu 10.12. Profil je možné vytvořit v konfiguračním módu pomocí příkazu `dba-profile add`, následovaný identifikačním číslem (pokud není zadáno, přiřadí se automaticky), jménem profilu, typem profilu a požadovanou hodnotou. Vlastnosti jednotlivých typů DBA profilů byly popsány v podkapitole 4.3 na straně 34.

Výpis 10.12: Vytvoření DBA profilu.

```
GPON-OLT-HUAWEI> enable
GPON-OLT-HUAWEI# config
GPON-OLT-HUAWEI(config)# dba-profile add profile-name 1000-Mbps type4 max 1024000
  Adding a DBA profile succeeded
  Profile ID  : 12
  Profile name: 1000-Mbps
```

10.2.2 Konfigurace linkového profilu

Po vytvoření DBA profilu, je tento profil třeba přiřadit do linkového profilu – toho je možné dosáhnout způsobem uvedeným ve výpisu 10.13. Byl vytvořen profil s názvem GPON, v dalším kroku byl přidán DBA profil – přidání je možné pomocí jména nebo ID již vytvořeného DBA profilu.

Následuje přidání GEM portu s číslem 230, které je přiřazeno do transportního kontejneru T-CONT 4 – tento typ se využívá pro služby typu best effort. Cílem je, aby připojené jednotky měly přístup k Internetu. K tomuto účelu byla na OLT jednotce vytvořena VLAN s číslem 2, která je prostřednictvím modulu na pozici *0/8* a portu číslo 1 předávána na přístupový přepínač. Z tohoto důvodu je nutné namapovat vytvořený GEM port do požadované VLAN. Číslo 0 ve výpisu symbolizuje pořadí mapování[1]. Konfigurace linkového profilu je dokončena příkazem `commit`.

Výpis 10.13: Konfigurace linkového profilu a přiřazení DBA profilu.

```
GPON-OLT-HUAWEI(config)# ont-lineprofile gpon profile-name GPON
GPON-OLT-HUAWEI(config-gpon-lineprofile-5)# tcont 4 dba-profile-name 1000-Mbps
GPON-OLT-HUAWEI(config-gpon-lineprofile-5)# gem add 230 eth tcont 4
GPON-OLT-HUAWEI(config-gpon-lineprofile-5)# gem mapping 230 0 vlan 2
GPON-OLT-HUAWEI(config-gpon-lineprofile-5)# commit
```

10.2.3 Konfigurace servisního profilu

Dalším krokem je vytvoření servisního profilu. Servisní profily byly vytvořeny pro každou připojenou ONU, neboť se jednalo o různé typy jednotek. V servisním profilu bylo pouze deklarováno jaké porty a kolik jich jednotka obsahuje. Příkaz `adaptive` znamená, že systém automaticky přizpůsobí počet portů skutečnému počtu portů dané ONU. Počet portů je však také možné přímo zadat. Konfigurace je opět ukončena příkazem `commit`. Vytvoření servisního profilu a deklarace portů dané ONU je uvedena ve výpisu 10.14.

[1] Jeden GEM port může být namapován do více VLAN.

Výpis 10.14: Konfigurace servisního profilu.

```
GPON-OLT-HUAWEI(config)# ont-srvprofile gpon profile-name HG8247H
GPON-OLT-HUAWEI(config-gpon-srvprofile-5)# ont-port eth adaptive pots adaptive catv
adaptive
GPON-OLT-HUAWEI(config-gpon-srvprofile-5)# commit
```

10.2.4 Přidání jednotky ONU

K OLT jednotce bylo připojeno celkem 8 jednotek ONU od firmy Huawei. První z jednotek nese označení HG8310M a je vybavena pouze jedním Ethernetovým portem, přidány byly celkem 4. Další jednotky, označené HG8245H disponují čtyřmi Ethernetovými porty a dvěma porty pro připojení telefonních přístrojů. Dále jsou vybaveny bezdrátovým rozhraním Wi-Fi a také jedním USB portem (Univerzální sériová sběrnice – Universal Serial Bus), přidány byly celkem 2 jednotky tohoto typu. Poslední připojená jednotka nese označení HG8247H, na rozdíl od předešlé jednotky je navíc vybavena jedním CATV portem, ostatní rozhraní a jejich počet je shodný. Přidány byly opět 2 jednotky tohoto typu.

Uvedené jednotky byly připojeny na GPON modul H806GPBD, umístěný v šasi na pozici *0/2*. Modul disponuje celkem 8 GPON porty, pasivní optický rozbočovač 1:16 s jednotkami ONU byl připojen prostřednictvím optického vlákna délky 20 km na port číslo 3.

Nejprve byla povolena automatická detekce jednotek ONU připojených k danému portu, dále byl zobrazen výpis nalezených jednotek ONU. Výpis nalezených jednotek, spolu s příkazy, které k tomu byly použity je uveden ve výpisu 10.15.

Výpis 10.15: Detekce a nalezené jednotky ONU.

```
GPON-OLT-HUAWEI(config)# interface gpon 0/2
GPON-OLT-HUAWEI(config-if-gpon-0/2)# port 3 ont-auto-find enable
GPON-OLT-HUAWEI(config-if-gpon-0/2)# display ont autofind 3
   ---------------------------------------------------------------------------
   Number              : 1
   F/S/P               : 0/2/3
   Ont SN              : 48575443D51DCB84 (HWTC-71FDCF76)
   Password            : 0x00000000000000000000
   Loid                :
   Checkcode           :
   VendorID            : HWTC
   Ont Version         : 4B4.B
   Ont SoftwareVersion : V3R015C10S103
   Ont EquipmentID     : 247H
   Ont autofind time   : 2018-04-16 18:48:53+08:00
   ---------------------------------------------------------------------------
```

Tímto výpisem byla zjištěna sériová čísla připojených jednotek, pomocí sériového čísla je možné ONU zaregistrovat. Sériové číslo je uvedeno také na štítku příslušné

ONU. Přidání ONU se provádí v konfiguračním módu, na požadovaném GPON modulu pomocí příkazu `ont add`. Příkaz je následován dalšími parametry, v tomto případě byla jednotka přidána pomocí svého sériového čísla. Syntaxe možného způsobu přidání jednotky ONU je uvedena ve výpisu 10.16.

Výpis 10.16: Syntaxe přidání jednotky ONU.

```
GPON-OLT-HUAWEI(config-if-gpon-0/2)# ont add portid<0,7> ontid<0,127> sn-auth
sn-value<Length 12-16> omci ont-lineprofile-id ont-lineprofile-name
ont-srvprofile-id ont-srvprofile-name desc
```

Portid: číslo v rozsahu 0–7 označující odpovídající port GPON modulu.

Ontid: číslo v rozsahu 0–127, udává identifikační číslo registrované jednotky.

Sn-auth: registrace ONU prostřednictvím sériového čísla.

Sn-value: sériové číslo registrované jednotky ONU, délka 12–16 znaků.

OMCI: Optické síťové řídicí a kontrolní rozhraní – Optical Network Unit Management and Control Interface, jedná se o kanál sloužící k přenosu OMCI zpráv mezi OLT a ONU. OMCI zprávy jsou využívány pro vyhledávání koncových jednotek.

Ont-lineprofile-id: přiřazení linkového profilu prostřednictvím jeho identifikačního čísla. Linkový profil je možné přiřadit prostřednictvím jeho ID nebo jména, není nutné zadávat oba parametry identifikující stejný profil.

Ont-lineprofile-name: přiřazení linkového profilu prostřednictvím jeho jména.

Ont-srvprofile-id: přiřazení požadovaného servisního profilu na základě jeho ID. Servisní profil lze opět přidat prostřednictvím jeho ID nebo jména, opět tedy platí, že není nutné zadávat oba atributy jako v případě linkového profilu.

Ont-srvprofile-name: přiřazení servisního profilu na základě jeho jména.

Desc: slouží k přidání popisu registrované jednotky (nepovinné).

Jednotce bylo přiřazeno identifikační číslo 3, přidána byla na port číslo 3 GPON modulu *0/2*. Příklad přidání jednotky ONU je uveden ve výpisu 10.17.

Výpis 10.17: Přidání jednotky ONU.

```
GPON-OLT-HUAWEI(config-if-gpon-0/2)# ont add 3 0 sn-auth 48575443D51DCB84 omci
ont-lineprofile-name GPON ont-srvprofile-name HG8247H desc ONU-0230
  Number of ONTs that can be added: 1, success: 1
  PortID :3, ONTID :0
```

Linkový a servisní profil je samozřejmě možné vytvořit i po přidání jednotky ONU. K jednotce je možné jej přiřadit i později pomocí příkazu `ont modify`. Po přidání jednotky byla nakonfigurována její IP adresa spolu s dalšími parametry, viz výpis 10.18.

Výpis 10.18: Konfigurace statické IP adresy.

```
GPON-OLT-HUAWEI(config-if-gpon-0/2)# ont ipconfig 3 0 static ip-address 10.0.0.230
mask 255.255.255.0 gateway 10.0.0.30 pri-dns 8.8.8.8 vlan 2
```

U jednotek HG8310M (disponují pouze jedním Ethernetovým portem), je navíc nutné přidat tento port do nativní VLAN. Toho je dosaženo příkazem uvedeným ve výpisu 10.19: číslo 3 značí port, číslo 0 je ID požadované ONU.

Výpis 10.19: Přiřazení portu do nativní VLAN.

```
GPON-OLT-HUAWEI(config-if-gpon-0/2)# ont port native-vlan 3 0 eth 1 vlan 2
```

Zařízením, která jsou připojena za těmito jednotkami je přidělena statická IP adresa, případně může adresy přiřazovat nadřazený DHCP server (Protokol pro automatickou konfiguraci IP adres – Dynamic Host Configuration Protocol), jednotky samotné DHCP server neobsahují. Úspěšné přidání jednotlivých koncových jednotek je možné ověřit v následujících výpisech. Výpis A.4 obsahuje informaci o všech jednotkách na portu číslo 3, zkrácený výpis A.5 obsahuje detailní informace zvolené jednotky ONU. Oba výpisy jsou umístěny v příloze této práce.

Konfigurace jednotek disponujících DHCP serverem je dokončena prostřednictvím jejich webového rozhraní, zde je v záložce *WAN*, přiřazena statická IP adresa, případně vybrána možnost přiřazení IP adresy nadřazeným DHCP serverem. Dále jsou přiřazena rozhraní ONU, která mohou k WAN rozhraní přistupovat. V záložce *Route* je poté nutné nakonfigurovanou cestu povolit. Nezbytným krokem je také povolení a konfigurace DHCP serveru jednotky ONU pro vnitřní síť.

10.2.5 Konfigurace servisního portu

Dalším nezbytným krokem je vytvoření servisního portu. Ještě před tím byla ale vytvořena tabulka s pravidly `traffic table ip`. Pomocí těchto tabulek je možné omezit přenosovou rychlost jak v sestupném, tak i vzestupném směru, nicméně i přesto jednotka musí mít přiřazen DBA profil[2].

Příklad vytvoření tabulky s definováním přenosové rychlosti je uveden ve výpisu 10.20. Tabulku je možné přidat pomocí jména nebo indexu, pokud není index zadán, bude nově vytvořená tabulka umístěna za již existující záznamy. Parametr CIR (Minimální garantovaná přenosová rychlost – Commited Information Rate) udává garantovanou přenosovou rychlost, parametr PIR (Špičková přenosová rychlost –

[2]DBA profil má vliv jen na přenosovou rychlost ve vzestupném směru.

Peak Information Rate) udává maximální přenosovou rychlost, kterou je možné použít nad rámec garantované, v případě potřeby vyšší přenosové rychlosti. Priorita 0 odpovídá službám best effort.

Výpis 10.20: Konfigurace tabulky s pravidly.

```
GPON-OLT-HUAWEI(config)# traffic table ip name 1000-Mbps cir 1024000 pir 1024000
priority 0 priority-policy local-Setting

Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index              : 11
  TD Name               : ip-traffic-table_11
  Priority              : 0
  Copy Priority         : -
  Mapping Index         : -
  CTAG Mapping Priority: -
  CTAG Mapping Index    : -
  CTAG Default Priority: 0
  Priority Policy       : local-pri
  CIR                   : 102400 kbps
  CBS                   : 3278800 bytes
  PIR                   : 102400 kbps
  PBS                   : 3278800 bytes
  Fix                   : 0 kbps
  CAR Threshold Profile: -
  Color Mode            : color-blind
  Color policy          : dei
  Referenced Status     : not used
  ------------------------------------------------
```

Dalším krokem v konfiguraci servisního portu je přiřazení požadované tabulky s definovanou přenosovou rychlostí. Toho je možné dosáhnout způsobem uvedeným ve výpisu 10.21, kde parametr `inbound` značí, že pravidla mají být aplikována na komunikaci v sestupném směru (ve vzestupném směru je přiřazen DBA profil). Pravidla se samozřejmě dají aplikovat také na komunikaci ve vzestupném směru, syntaxe bude podobná, jen bude využito parametru `outbound`. Posledním důležitým krokem je přiřazení tohoto servisního portu, respektive GEM portu k požadované VLAN.

Výpis 10.21: Konfigurace servisního portu jednotky ONU.

```
GPON-OLT-HUAWEI(config)# service-port 4 inbound traffic-table index 11
GPON-OLT-HUAWEI(config)# service-port 4 vlan 2 gpon 0/2/3 ont 0 gemport 230
multi-service user-vlan 2 tag-transform translate
```

10.2.6 Bezpečnostní aspekty

Každou z koncových jednotek ONU je možné konfigurovat prostřednictvím webového rozhraní. Pomocí webového rozhraní je možné konfigurovat především parame-

try lokální sítě daného koncového uživatele (nastavení DHCP serveru, Wi-Fi, USB portu, atd.). Existují dva typy účtů: administrátorský, který má oprávnění k plné konfiguraci jednotky a uživatelský, jehož možnosti konfigurace jsou omezené. Důležité je u těchto účtů nepoužívat výchozí hesla, jelikož není složité přihlašovací údaje dohledat. Jednotka na tuto skutečnost po prvním přihlášení upozorní a nasměruje uživatele na stránku, kde je možné přihlašovací jméno a heslo ihned změnit.

Dále je jednotky možné konfigurovat i pomocí CLI, prostřednictvím služby Telnet a SSH. Ve webovém konfiguračním rozhraní je však možné tento způsob přístupu k jednotce zakázat. Je vhodné lokální síť za jednotkou ONU odpovídajícím způsobem zabezpečit, především zakázat přístup ke službám, které nebudou využívány.

Některé jednotky jsou vybaveny také USB portem, kde je možné připojit externí úložiště a provozovat zde například FTP server. K jednotce a případnému FTP serveru je možné nastavit i vzdálený přístup prostřednictvím WAN. Pokud ale k těmto službám z vnější sítě nebude přistupováno, je vhodné tento způsob přístupu zakázat. Je také důležité odpovídajícím způsobem zabezpečit bezdrátovou síť Wi-Fi.

Jednotka OLT obsahuje celou řadu bezpečnostních mechanismů. Je schopna například detekovat přítomnost jednotky, která nerespektuje přidělené časové intervaly pro vysílání ve vzestupném směru, viz podkapitola 11.1.

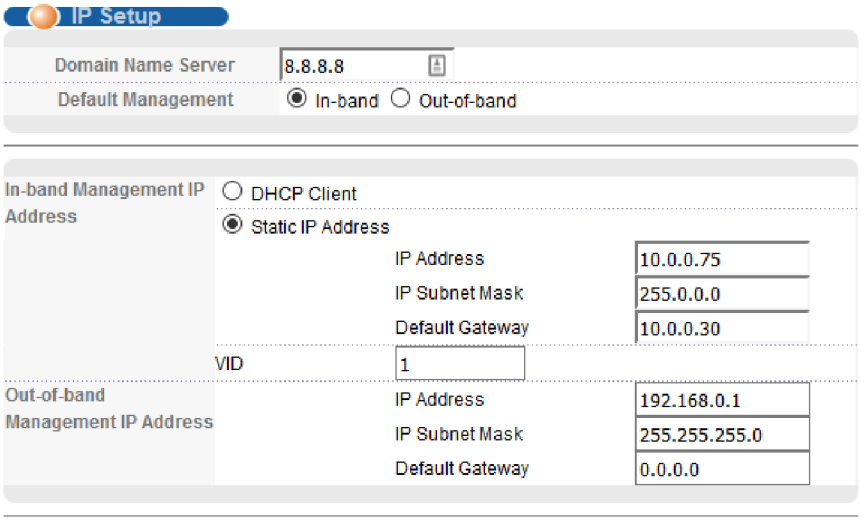
10.3 Konfigurace EPON OLT jednotky ZyXEL

Poslední konfigurovanou jednotkou byla EPON OLT jednotka ZyXEL, tato jednotka byla konfigurována prostřednictvím webového rozhraní. Pro přístup k webovému rozhraní je třeba připojit počítač, ze kterého bude konfigurace prováděna k portu MGMT a provést následující nastavení síťového rozhraní počítače:

- IP adresa: 192.168.0.100,
- síťová maska: 255.255.255.0,
- výchozí brána: 192.168.0.1.

Webové konfigurační rozhraní je ve výchozím nastavení dostupné na adrese výchozí brány (*192.168.0.1* na MGMT portu). Z vnitřní sítě je výchozí adresa *192.168.1.1* (opět je nutné odpovídajícím způsobem upravit konfiguraci síťového rozhraní počítače).

Jednotka byla prostřednictvím přístupového přepínače připojena do univerzitní sítě a Internetu. Na OLT jednotce tedy bylo nutné nastavit statickou IP adresu. Nastavení se provádí v nabídce *Basic Setup*, v záložce *IP Setup*. V případě, že IP adresy v síti přiděluje DHCP server, stačí zvolit možnost DHCP Client a IP adresa bude automaticky přidělena DHCP serverem (tato možnost byla také testována). Nastavené hodnoty jsou zobrazeny na obrázku 10.2.



Obr. 10.2: Nastavení statické IP adresy OLT jednotky ZyXEL.

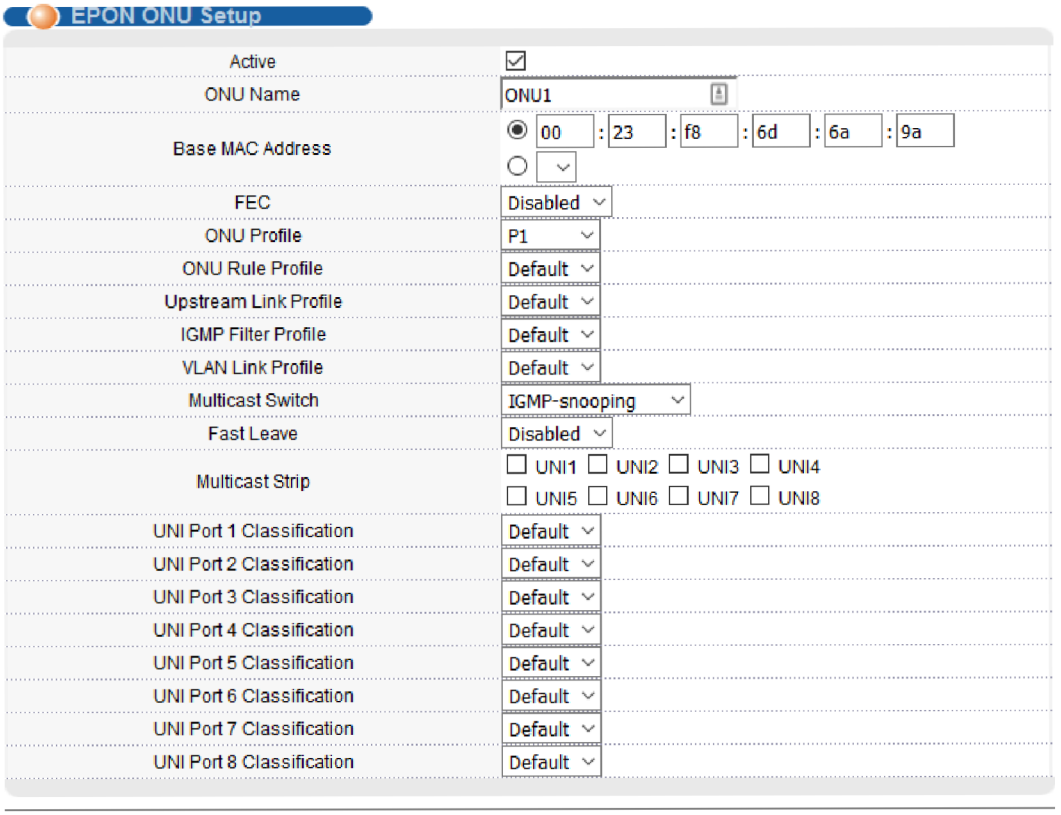
Funkčnost nastavení byla ověřena pomocí diagnostických nástrojů OLT jednotky. Dále byla nastavena adresa NTP serveru (Protokol pro synchronizaci času – Network Time Protocol).

10.3.1 Přidání jednotky ONU

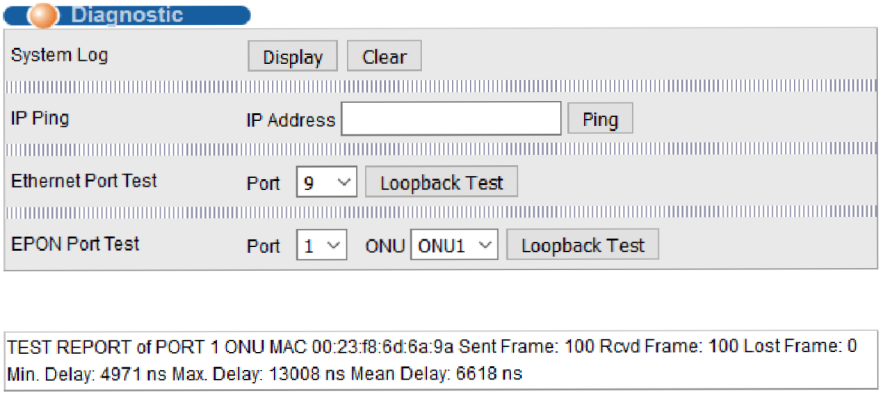
Jednotku ONU je možné přidat v nabídce *Basic Setup*, v záložce ONU Setup. Zde je vybrán port, na kterém je příslušná jednotka ONU připojena. Poté je třeba zadat MAC adresu registrované jednotky, nebo vybrat MAC adresu ze seznamu adres, které OLT na daném portu našla. Vybráním položky *Active* je jednotka aktivována, jednotku je také nutné pojmenovat. Možnosti nastavení ONU jsou zobrazeny na obrázku 10.3.
Na tomto obrázku je již přidán profil s nastavením DBA, toto nastavení je popsáno v následující podkapitole (10.3.2). Ověření je možné pomocí diagnostických nástrojů jednotky, viz výpis na obrázku 10.4. Připojení k OLT signalizuje také zeleně svítící kontrolka *PON* na ONU, červeně svítící kontrolka *LOS* naopak značí, že k ONU není připojeno žádné optické vedení (ONU nekomunikuje s OLT).

10.3.2 Konfigurace DBA profilů

Nastavení je možné opět v nabídce *Basic Setup*, v záložce ONU Profile. Zde je možné provést požadované nastavení DBA, jednotlivých portů ONU, atd. Po pojmenování profilu a jeho aktivování (volba *Active*) je třeba profil uložit a přiřadit požadované ONU. Při změně nastavení profilu je nutné profil u dané ONU odebrat, provést

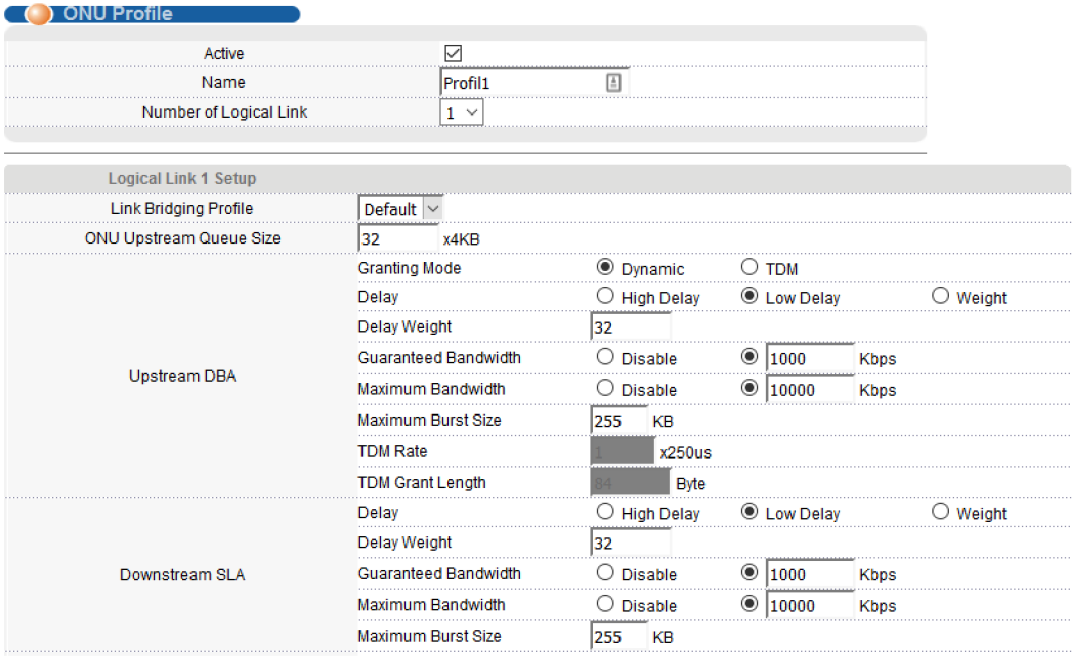


Obr. 10.3: Přidání jednotky ONU a další možnosti nastavení.



Obr. 10.4: Ověření funkčnosti připojené ONU.

požadované modifikace, profil uložit a opět přidat k požadované ONU. Nastavení DBA je zobrazeno na obrázku 10.5.



Obr. 10.5: Nastavení DBA.

10.3.3 Bezpečnostní aspekty

Opět je důležité nepoužívat výchozí přihlašovací jméno a heslo, pro vyšší bezpečnost je vhodné umožnit konfiguraci pouze prostřednictvím MGMT portu a vyhrazené VLAN. OLT umožňuje nastavit rozsah povolených IP adres pro přístup k jednotce. Vzdálený přístup k CLI prostřednictvím Telnetu je vhodné zakázat a používat šifrovanou komunikaci prostřednictvím SSH.

Všechny porty OLT jsou navíc ve výchozím nastavení aktivovány, nepoužívané porty je však vhodné vypnout a přiřadit do jiné než nativní VLAN.

11 Testování bezpečnostních rizik

Kapitola popisuje testování vybraných bezpečnostních rizik popsaných v teoretické části této práce. Testování probíhalo na OLT jednotkách Huawei (standard GPON) a jednotce ZyXEL (standard EPON). Provedení penetračních testů bylo realizováno pomocí operačního systému Linux, konkrétně distribuce Kali. Tato distribuce je založena na operačním systému Debian, obsahuje široké spektrum nástrojů pro bezpečnostní audity. Za vývojem tohoto systému stojí společnost Offensive Security. Kompletní informace o systému spolu s popisem jednotlivých nástrojů je možné najít v oficiální dokumentaci [38, 39].

11.1 Narušení komunikace laserovým zdrojem

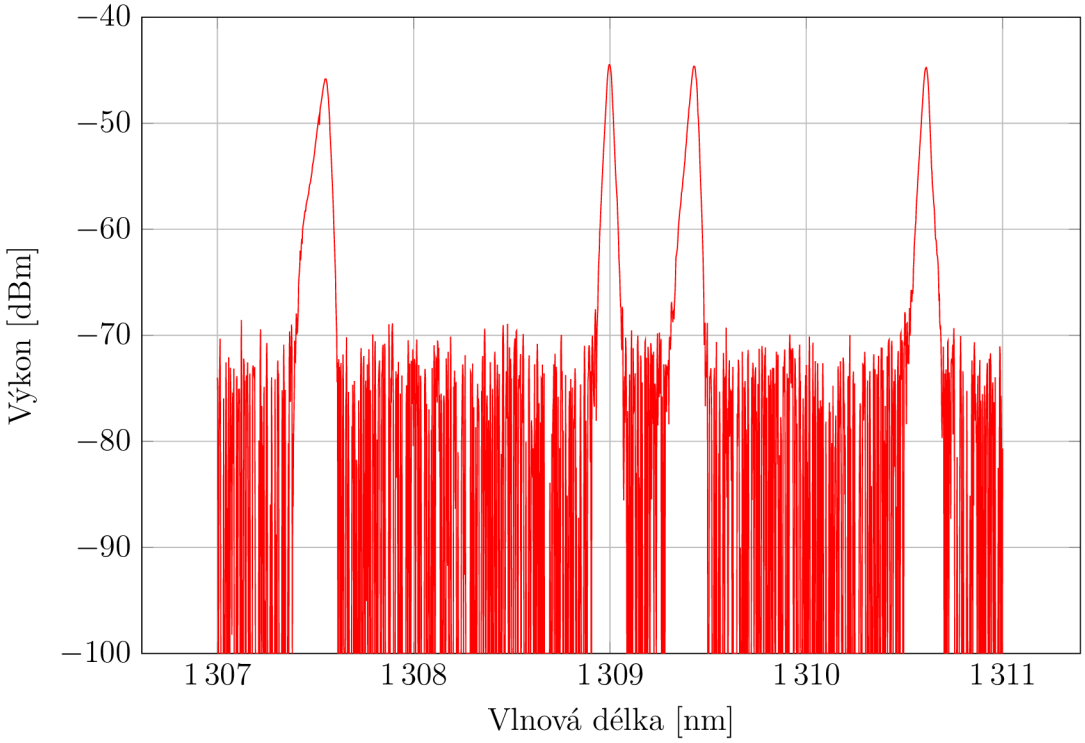
Jedná se o test bezpečnostního rizika popsaného v kapitole 8.4 věnované DoS útokům (konkrétně podkapitola 8.4.1). Testování probíhalo na GPON OLT jednotce Huawei a EPON OLT jednotce ZyXEL. První dva laserové zdroje použité pro testování však komunikaci ani u jedné z jednotek nenarušily. Testované OLT jednotky byly pomocí pasivních optických rozbočovačů postupně připojeny na optický spektrální analyzátor tak, aby bylo možné současně analyzovat sestupný i vzestupný směr.

Spektrum optického signálu systému GPON je zobrazeno na obrázku 11.1 (vzestupný směr) a na obrázku 11.2 (sestupný směr), spektrum optického signálu systému EPON ve vzestupném směru zobrazuje obrázek 11.3 a obrázek 11.4 poté zobrazuje spektrum signálu v sestupném směru.

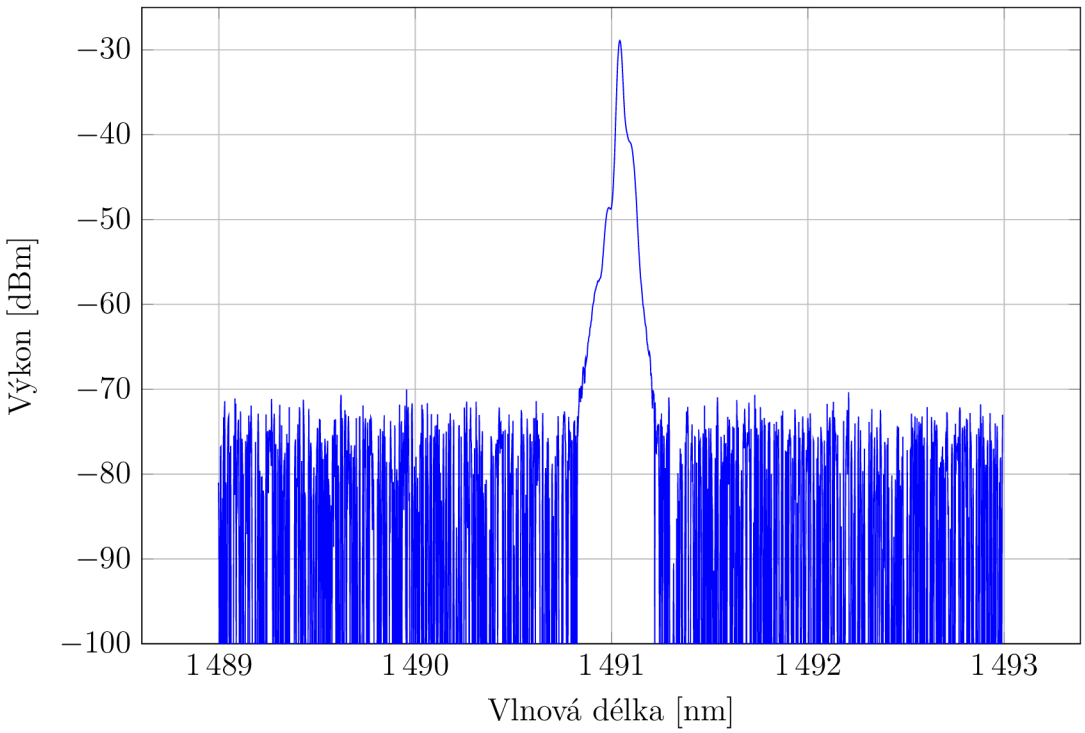
Ze spektra signálu systému GPON je zřetelné, že jsou připojeny 4 koncové jednotky, které se však nenacházejí přesně na vlnové délce 1 310 nm. Z tohoto důvodu nemohlo být narušení komunikace použitými laserovými zdroji úspěšné.

Ze spektra signálu systému EPON není přímo zřetelné, že jsou připojeny 2 koncové jednotky, připojené jednotky se opět nenacházejí přesně na vlnové délce 1 310 nm. Navíc jsou u těchto jednotek použity méně kvalitní laserové zdroje než v případě systému GPON. Spektrum signálu systému GPON, zachycené na obrázku 11.1, odpovídá spektrální charakteristice laseru DFB (Laser s rozloženou zpětnou vazbou – Distributed Feedback Laser). Naproti tomu spektrum signálu systému EPON, zachycené na obrázku 11.3 odpovídá spektrální charakteristice Fabry-Perotova laseru.

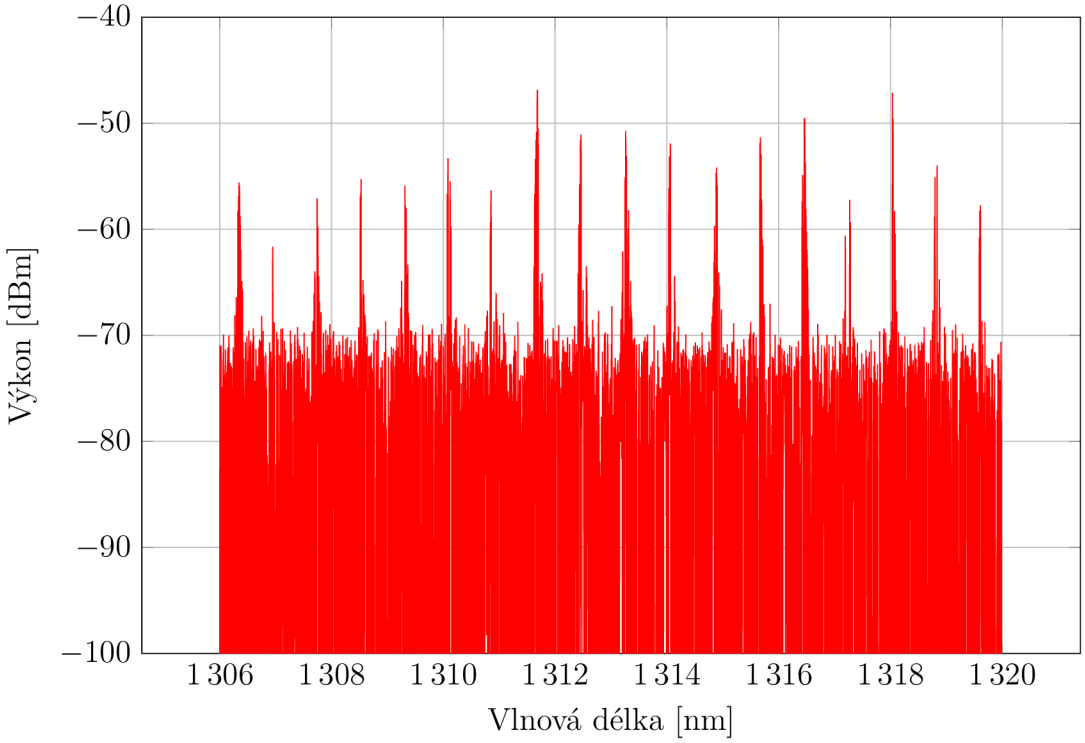
K rušení komunikace byl použit media konvertor, který byl připojen do stejného pasivního optického rozbočovače, jako koncové jednotky. Vysílací výkon media konvertoru však nebyl dostatečný k narušení komunikace na ODN (délka trasy 20 km, použitý pasivní rozbočovač s rozbočovacím poměrem 1:16).



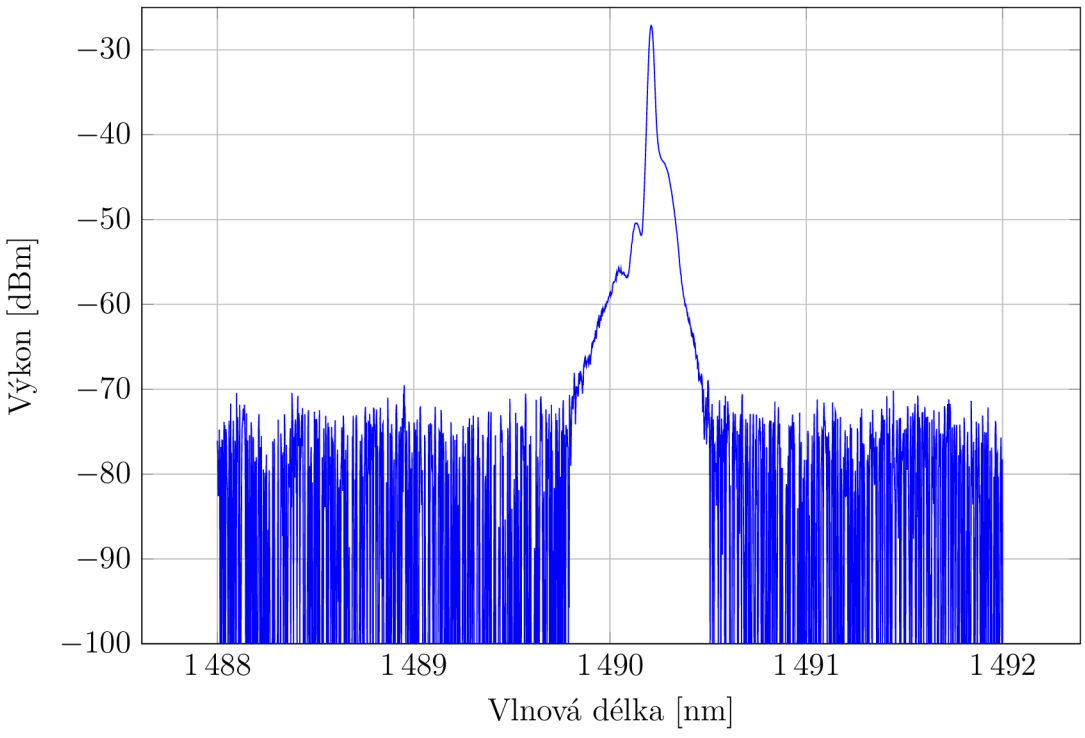
Obr. 11.1: Spektrum signálu systému GPON, vzestupný směr.



Obr. 11.2: Spektrum signálu systému GPON, sestupný směr.



Obr. 11.3: Spektrum signálu systému EPON, vzestupný směr.



Obr. 11.4: Spektrum signálu systému EPON, sestupný směr.

Bylo přistoupeno k testování na pasivním optickém rozbočovači s nižším dělicím poměrem 1:4. K tomuto rozbočovači byly připojeny 3 GPON ONU jednotky (od každého druhu jedna), v případě standardu EPON byly připojeny 2 dostupné jednotky ONU. Media konvertor však nebyl schopen komunikaci systému EPON narušit.

Komunikace na GPON síti však narušena byla. První indikací tohoto stavu je přerušovaně svítící kontrolka *PON* na jednotkách ONU. Tento signál značí stav, kdy jednotka není zaregistrována k OLT. Pomocí příkazu `display ont optical-info` je možné zobrazit si informace o optických rozhraních připojených koncových jednotek. Výpis 11.1 zobrazuje normální stav (před přepojením 3 jednotek na robočovač 1:4). Ve výpisu 11.2 je již možné vidět stav, kdy je komunikace narušena vysíláním media konvertoru.

Výpis 11.1: Informace o optickém rozhraní připojených ONU.

```
GPON-OLT-HUAWEI(config-if-gpon-0/2)# display ont optical-info 3 all
  ------------------------------------------------------------------------------
  ONT   Rx power     Tx power     OLT Rx ONT   Temperature  Voltage      Current
  ID    (dBm)        (dBm)        power(dBm)   (C)          (V)          (mA)
  ------------------------------------------------------------------------------
    0   -13.13       1.84         -18.30       32           3.300        11
    1   -14.11       2.11         -18.90       37           3.260        13
    2   -14.04       2.02         -19.75       39           3.280        14
    3   -14.64       1.93         -19.92       45           3.280        14
    4   -13.85       2.03         -19.29       42           3.280        15
    5   -13.80       2.00         -19.32       42           3.280        14
    6   -13.77       2.33         -19.51       45           3.320        17
    7   -14.08       2.13         -20.32       41           3.280        15
  ------------------------------------------------------------------------------
```

Výpis 11.2: Informace o optickém rozhraní připojených ONU v průběhu rušení.

```
GPON-OLT-HUAWEI(config-if-gpon-0/2)# display ont optical-info 3 all
  The ONT optical module information does not exist

GPON-OLT-HUAWEI(config-if-gpon-0/2)# display ont optical-info 3 all
  ------------------------------------------------------------------------------
  ONT   Rx power     Tx power     OLT Rx ONT   Temperature  Voltage      Current
  ID    (dBm)        (dBm)        power(dBm)   (C)          (V)          (mA)
  ------------------------------------------------------------------------------
   2    -5.86        1.90         -0.63        43           3.280        15
  ------------------------------------------------------------------------------
```

Z výpisu 11.2 je patrné, že OLT ztratila spojení se všemi jednotkami. Při opětovném zadání příkazu však byla detekována jedna z připojených jednotek, konkrétně typ HG8245H. Komunikace prostřednictvím této jednotky však nebyla možná. Právě prostřednictvím této jednotky bylo testováno přerušení komunikace, z počítače připojeného k této jednotce byla pomocí příkazu `ping` testována konektivita. Z výpisu

11.3 je patrné přerušení komunikace při zapnutí zdroje rušení, po jeho vypnutí došlo k obnovení komunikace.

Výpis 11.3: Testování konektivity při rušení komunikace.

```
C:\Users\Jan>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=5ms TTL=57
Reply from 8.8.8.8: bytes=32 time=4ms TTL=57
Reply from 8.8.8.8: bytes=32 time=5ms TTL=57
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 8.8.8.8: bytes=32 time=11ms TTL=57
Reply from 8.8.8.8: bytes=32 time=5ms TTL=57
Reply from 8.8.8.8: bytes=32 time=4ms TTL=57

Ping statistics for 8.8.8.8:
    Packets: Sent = 12, Received = 6, Lost = 6 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 11ms, Average = 5ms
```

Velice důležitá je detekce přítomnosti zdroje rušení, případně modifikované koncové jednotky. OLT jednotka Huawei je tento stav schopna detekovat. Pomocí přiřazení tzv. alarm profilu koncovým jednotkám a nastavení, které ze stavů bude profil sledovat je možná detekce různých událostí na ODN.

Při spuštěném zdroji rušení zaznamenala jednotka hned několik událostí. Jednotka v historii alarmů zaznamenala ztrátu spojení s koncovými jednotkami, ztráta spojení byla indikována alarmy upozorňujícími na ztrátovost rámců a upozorněním na možné poškození optického vedení. Tyto alarmy však neindikují přítomnost zdroje rušení nebo modifikované koncové jednotky. Na přítomnost zdroje rušení upozornil alarm s označením *0x2e314021*, tento alarm je pro detekci klíčový. V historii alarmů je také možné najít událost, která indikuje vypnutí zdroje rušení, informace o těchto událostech je uvedena ve výpisu 11.4.

OLT jednotka Huawei umožňuje vypisování alarmů přímo do CLI, způsob možné konfigurace je uveden ve výpisu 11.5. V první části výpisu je povoleno vypisování alarmů do CLI s periodou 60 s, vypisování do konzole je povoleno pro alarm s ID *0x2e314021*[1]. Ve druhé části tohoto výpisu je uveden příklad konfigurace nového profilu, kdy tento nový profil je vytvořen přiřazením volného ID, volitelně lze profil také pojmenovat. Příkazem `alarm filter` je možné v profilu vyfiltrovat alarmy, na které má profil upozorňovat, alarm je nutné vybrat pomocí jeho ID (pro ilustraci byl

[1] Alarm upozorňující na přítomnost zdroje rušení nebo modifikované ONU.

Výpis 11.4: Alarm detekující přítomnost modifikované ONU.

```
GPON-OLT-HUAWEI(config)# display alarm history all
  ALARM 3800 FAULT MAJOR 0x2e314021 EQUIPMENT 2018-05-09 15:08:36+08:00
  ALARM NAME  : There are illegal incursionary rogue ONTs under the port
  SRVEFF      : SA
  PARAMETERS  : FrameID: 0, SlotID: 2, PortID: 3
  DESCRIPTION : There are illegal incursionary rogue ONTs under the port, it will
                interrupt service of other ONT(s)
  CAUSE       : There is illegal incursionary rogue ONT under the port
  ADVICE      : Detect rogue ont manually, and then replace it
  --- END

  ALARM 3806 RECOVERY CLEARED 0x2e324021 EQUIPMENT 2018-05-09 15:13:02+08:00
  ALARM NAME  : The illegal incursionary rogue ONTs under the port have been
                cleared
  SRVEFF      : NSA
  PARAMETERS  : FrameID: 0, SlotID: 2, PortID: 3
  DESCRIPTION : The illegal incursionary rogue ONTs under the port have been
                cleared
  CAUSE       : All illegal incursionary rogue ONTs have been replaced under
                the port
  ADVICE      : No need to deal with it
  --- END
```

vybrán opět alarm *0x2e314021*). Provedené změny v profilu jsou potvrzeny příkazem `commit`. Vytvořený profil je možné přiřadit vybraným ONU, případně všem ONU na zvoleném portu.

Výpis 11.5: Konfigurace alarmů na OLT Huawei.

```
GPON-OLT-HUAWEI(config)# alarm jitter-proof on
GPON-OLT-HUAWEI(config)# alarm jitter-proof 60
GPON-OLT-HUAWEI(config)# alarm alarmlevel critical 0x2e314021

GPON-OLT-HUAWEI(config)# ont-alarm-policy policy-id 1
GPON-OLT-HUAWEI(config-ont-alarm-policy-1)# alarm filter 0x2e314021
GPON-OLT-HUAWEI(config-ont-alarm-policy-1)# commit
GPON-OLT-HUAWEI(config-ont-alarm-policy-1)# quit
GPON-OLT-HUAWEI(config)# interface gpon 0/2
GPON-OLT-HUAWEI(config-if-gpon-0/2)# ont alarm-policy 3 all policy-id 1
```

Spolehlivá ochrana proti tomuto typu útoku v současné době neexistuje. V případě detekce přítomnosti zdroje rušení se může jednat o poruchu některé z koncových jednotek. Tuto skutečnost je možné prověřit příkazem `display ont optical-info`, jednotka s poruchou bude vykazovat nestandardní hodnoty. Pokud se však jedná o jiný zdroj rušení, jednotka dokáže identifikovat pouze port, na kterém se tento zdroj nachází.

Základním předpokladem ochrany proti tomuto typu útoku je fyzická bezpečnost všech instalovaných pasivních optických rozbočovačů. Proveditelnost útoku je závislá především na použitém zdroji záření, zdroj musí vysílat přesně na vlnových délkách,

které jsou použity pro komunikaci v napadené PON. Zdroj musí také disponovat odpovídajícím výkonem.

11.2 Skenování portů

Pro skenování portů OLT jednotek byl využit nástroj Kali Linuxu *zenmap*. Jedná se o grafickou nástavbu nástroje *nmap*, který slouží pro skenování otevřených portů počítačů, serverů, ale i síťových prvků.

Ve výpisu 11.6 je možné vidět výsledky získané pro systém GPON, výpis 11.7 obsahuje výsledky pro systém EPON a výpis 11.8 obsahuje výsledky skenování pro koncovou jednotku Huawei HG8247H.

Z výsledků je patrné, že u obou systémů je povolena služba pro vzdálenou správu Telnet. Pro vzdálenou správu v laboratorním prostředí nepředstavuje používání služby Telnet významné bezpečnostní riziko. Pro nasazení v běžném provozu je však vhodné používat SSH, neboť komunikace probíhá v zašifrované podobě.

Výpis 11.6: Informace zjištěné nástrojem zenmap pro OLT Huawei.

```
Not shown: 998 closed ports

PORT   STATE SERVICE VERSION
22/tcp open  ssh     Dopra Linux sshd 1.5 (protocol 2.0)
| ssh-hostkey:
|_  2048 e1:1b:21:a5:e3:20:09:4f:da:87:c5:40:e3:37:30:79 (RSA)
23/tcp open  telnet  Pocket CMD telnetd

MAC Address: 48:FD:8E:E0:3A:4F (Huawei Technologies)

Operating System: Huawei S9300 switch
Accuracy: 96 %

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Dopra Linux; CPE: cpe:/o:huawei:dopra_linux

TRACEROUTE
HOP RTT     ADDRESS
1   2.44 ms 10.0.0.2
```

11.3 Záplava fiktivními MAC adresami

Tento typ útoku je označován jako MAC flood attack. Útočník se snaží pomocí velkého počtu fiktivních MAC adres zahltit paměť síťového zařízení, typicky CAM tabulku přepínače (Adresovatelná paměť – Content Addressable Memory). Jakmile

Výpis 11.7: Informace zjištěné nástrojem zenmap pro OLT ZyXEL.

```
Not shown: 996 closed ports

PORT    STATE SERVICE    VERSION
22/tcp  open  tcpwrapped
23/tcp  open  telnet
|   Help:
|     User name: HELP
|   NCP:
|     User name: DmdT
|   SIPOptions:
|     User name: OPTIONS sip:nm SIP/2.0
|   tn3270:
|     User name:
|_    IBM-3279-4-E
80/tcp  open  http  Allegro RomPager 4.30b3
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=OLT at Fri May 11 17:13:59 2018
| http-methods:
|   Supported Methods: GET HEAD POST PUT
|_  Potentially risky methods: PUT
|_http-server-header: Allegro-Software-RomPager/4.30b3
|_http-title: Web Configurator
443/tcp open  ssl/https

MAC Address: C8:6C:87:06:82:FD (ZyXEL Communications)

Operating System: ZyXEL ES-3024A switch
Accuracy: 96 %

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=23 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE
HOP RTT     ADDRESS
1   2.06 ms 10.0.0.75
```

je tabulka takového přepínače zaplněna, může být znemožněna komunikace oprávněným uživatelům. Závažným důsledkem ovšem je, že funkčnost přepínače je degradována na funkci rozbočovače (hub). Rozbočovač předá signál na všechny své porty, vyjma toho, ze kterého byl signál přijat. Útočník může tímto způsobem odposlouchávat komunikaci, která je tímto napadeným přepínačem zpracovávána.

Útok na OLT jednotky byl vykonán pomocí nástroje Kali Linuxu *macof*. Před provedením útoku byly ještě zkontrolovány počty MAC adres na jednotlivých OLT jednotkách. Na OLT jednotce Huawei je možné počet MAC adres zjistit hned několika způsoby, které jsou uvedeny v následujícím výpisu. Situaci před provedením útoku na OLT Huawei zachycuje výpis 11.9, na OLT ZyXEL situaci zachycuje obrázek 11.5.

Výpis 11.8: Informace zjištěné nástrojem zenmap pro ONU Huawei HG8247H.

```
Not shown: 994 closed ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      Dropbear sshd 2013.62 (protocol 2.0)
23/tcp    open  telnet   Huawei Home Gateway telnetd
53/tcp    open  domain   dnsmasq 2.49
| dns-nsid:
|_  bind.version: dnsmasq-2.49
80/tcp    open  ssl/http
49152/tcp open  upnp     Portable SDK for UPnP 1.6.18
     (Linux 2.6.34.10_sd5115v100_wr4.3; UPnP 1.0)
49153/tcp open  upnp     Portable SDK for UPnP 1.6.18
     (Linux 2.6.34.10_sd5115v100_wr4.3; UPnP 1.0)

MAC Address: C8:8D:83:D5:1D:CB (Huawei Technologies)

Operating System: OpenWrt Kamikaze 8.09 (Linux 2.6.25 - 2.6.26)
Accuracy> 98 %

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 192.168.100.1
```

Výpis 11.9: Výpisy MAC adres před provedením útoku (OLT Huawei).

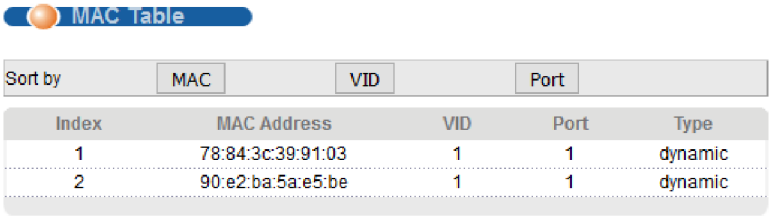
```
GPON-OLT-HUAWEI(config)# display mac-address number

  It will take some time, please wait...
  Number of static MAC configured: 0
  Number of security dynamic binding MAC: 0
  Number of other MAC: 10

GPON-OLT-HUAWEI(config)# display mac-address port 0/2/3
  ------------------------------------------------------------------------
   SRV-P BUNDLE TYPE MAC            MAC TYPE F /S /P   VPI  VCI   VLAN ID
   INDEX INDEX
  ------------------------------------------------------------------------
       9     -  gpon 7884-3c39-9103 dynamic  0 /2 /3   5    230         2
      11     -  gpon 90e2-ba5a-e5be dynamic  0 /2 /3   7    230         2
  ------------------------------------------------------------------------

GPON-OLT-HUAWEI(config-if-gpon-0/2)# display ont mac-count 3 7
 ------------------------------------------------------------------------
  F/S/P                   : 0/2/3
  ONT-ID                  : 7
  ONT MAC count           : 1
 ------------------------------------------------------------------------
```

Nástroj *macof* je možné spustit prostřednictvím terminálu, syntaxe příkazu je uvedena ve výpisu 11.10. Stav po vykonání útoku je možné pozorovat ve výpisu 11.11



Obr. 11.5: Tabulka s MAC adresami před provedením útoku (OLT ZyXEL).

pro OLT Huawei a na obrázku 11.6 pro OLT ZyXEL.

Výpis 11.10: Vykonání útoku za pomoci nástroje macof.

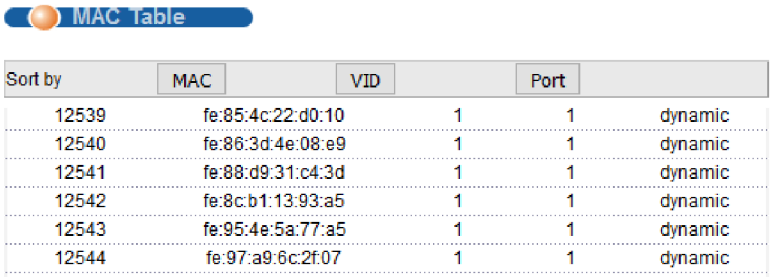
```
root@kali:~# macof -i eth1 -d 10.0.0.2 -n 700000
```

Výpis 11.11: Výpisy MAC adres po provedeném útoku (OLT Huawei).

```
GPON-OLT-HUAWEI(config)# display mac-address number

  It will take some time, please wait...
  Number of static MAC configured: 0
  Number of security dynamic binding MAC: 0
  Number of other MAC: 66007

GPON-OLT-HUAWEI(config-if-gpon-0/2)# display ont mac-count 3 7
 ------------------------------------------------------------------------------
  F/S/P                   : 0/2/3
  ONT-ID                  : 7
  ONT MAC count           : 1035
 ------------------------------------------------------------------------------
```



Obr. 11.6: Tabulka s MAC adresami po provedeném útoku (OLT ZyXEL).

11.3.1 Vyhodnocení útoku

Z předchozích výpisů je patrné, že se paměti obou OLT jednotek nepodařilo zaplnit. Dle údajů výrobců dokáže OLT jednotka Huawei pojmout 512 000 adres a OLT jednotka ZyXEL potom 16 000 MAC adres.

Z podstaty komunikace v pasivních optických sítích je zřejmé, že odposlech komunikace při zahlcení OLT fiktivními MAC adresami nebude na rozdíl od klasického přepínače možný. Jednotka OLT vysílá data všesměrově všem koncovým jednotkám ONU, které zahodí veškeré datové jednotky, které jim nebyly určeny. Postrádá tedy smysl, aby se útočník snažil donutit vysílat všesměrově zařízení, které již v sestupném směru všesměrově vysílá. Mohlo by pouze dojít k zaplnění vyhrazené paměti pro MAC adresy a znemožnění připojení oprávněným uživatelů. Na jednotky OLT je však možné připojit velký počet uživatelů (řádově tisíce), k jejich zahlcení by mohlo dojít při intenzivním DDoS útoku.

11.3.2 Ochrana proti útoku

Ochranou proti tomuto typu útoku je omezení počtu MAC adres, které jednotka dynamicky zaznamenává do své paměti. Konfiguraci tohoto opatření je na OLT jednotce Huawei možné provést hned několika způsoby. Počet MAC adres je možné omezit pro určitý modul OLT jednotky, port, VLAN, případně servisní port. Při omezení počtu MAC adres pro určitý servisní port, dojde k omezení především pro danou jednotku ONU, která daný servisní port využívá. Příklady konfigurace pro výše uvedené varianty jsou uvedeny ve výpisu 11.12.

Výpis 11.12: Možnosti konfigurace omezení počtu MAC adres na OLT Huawei.

```
GPON-OLT-HUAWEI(config)# mac-address max-mac-count board 0/2 100

GPON-OLT-HUAWEI(config)# mac-address max-mac-count service-port 11 10

GPON-OLT-HUAWEI(config)# mac-address max-mac-count eth 0/2/3 user-vlan 2 10
```

Omezení bylo nakonfigurováno pro servisní port číslo 11, který je přiřazen k ONU číslo 7 (zde byl připojen útočník). Pro demonstraci byl počet MAC adres omezen na 10, viz výpis 11.13. Ve výpisu 11.14 je poté uveden stav po opětovném vykonání útoku při již aktivovaném omezení.

Omezení počtu MAC adres pro OLT ZyXEL je možné provést pouze pro daný PON port (v tomto případě port číslo 1). Pro demonstraci byl maximální počet MAC adres na tomto portu opět omezen na 10. Konfiguraci je možné provést v nabídce *Advanced Application*, záložce *Switch Advance*, *Port Security*. Provedené nastavení je

Výpis 11.13: Omezení počtu MAC adres na servisním portu OLT Huawei.

```
GPON-OLT-HUAWEI(config)# mac-address max-mac-count service-port 11 10

GPON-OLT-HUAWEI(config)# display mac-address max-mac-count service-port 11
  ---------------------------------------------------------------------------
   SRV-P TYPE  F /S /P  VPI  VCI   VLAN ID FLOWTYPE   FLOWPARA    LEARNABLE
   INDEX                                                         MAC NUMBER
  ---------------------------------------------------------------------------
      11 gpon  0 /2 /3  7    230         2 vlan       2                   10
  ---------------------------------------------------------------------------
  Total: 1
  Note: F--Frame, S--Slot, P--Port,
        A--The MAC address is learned or configured on the aggregation port,
        VPI indicates ONT ID for PON, VCI indicates GEM index for GPON,
        v/e--vlan/encap, pritag--priority-tagged,
        ppp--ppppoe, ip--ipoe, ip4--ipv4oe, ip6--ipv6oe
```

Výpis 11.14: Ověření funkčnosti nakonfigurovaného opatření na OLT Huawei.

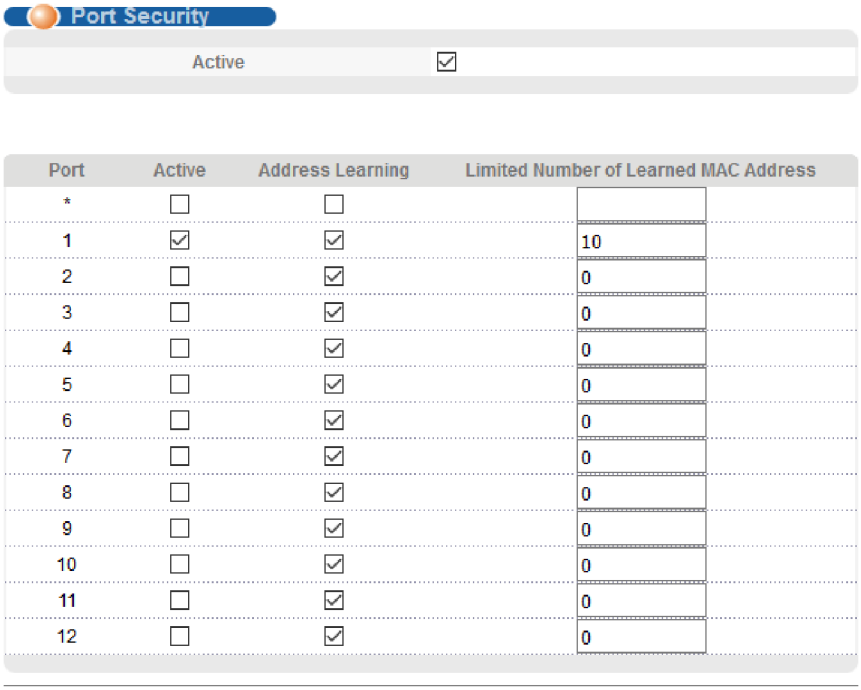
```
GPON-OLT-HUAWEI(config-if-gpon-0/2)# display ont mac-count 3 7
 ---------------------------------------------------------------------------
  F/S/P                   : 0/2/3
  ONT-ID                  : 7
  ONT MAC count           : 10
 ---------------------------------------------------------------------------
```

zobrazeno na obrázku 11.7, obrázek 11.8 zobrazuje tabulku MAC adres po vykonání útoku při aktivním bezpečnostním opatření.

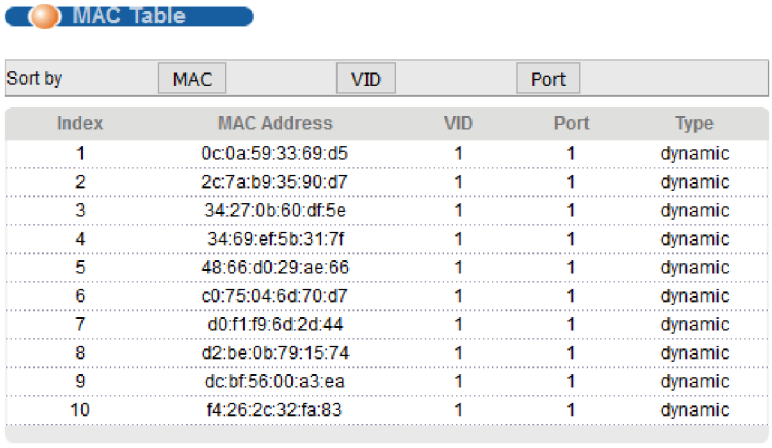
11.4 Shrnutí

Proveditelnost útoku pomocí laserového zdroje se ukázala jako obtížnější, než bylo uvažováno. Pro úspěšné provedení tohoto útoku je třeba vysílat přesně na vlnové délce, na které se uskutečňuje komunikace v dané PON. Laserový zdroj musí být dostatečně výkonný – v PON se komunikace uskutečňuje na vzdálenosti v řádu kilometrů za použití pasivních optických rozbočovačů s vyšším rozbočovacím poměrem.

Důležitá je také fyzická bezpečnost instalovaných prvků ODN. Jednotky OLT bývají zpravidla umístěné v zabezpečených prostorách s ostatními síťovými prvky poskytovatele služeb. Takové prostory bývají zpravidla zabezpečeny bezpečnostním systémem, kamerovým systémem se záznamem a také přístupovým systémem. Narušení bezpečnosti v těchto prostorách poměrně rychle zaznamená dohledové centrum poskytovatele služeb, případně najaté bezpečnostní agentury. Pasivní optické rozbočovače však na takové úrovni zabezpečeny nejsou, nicméně pro provedení tohoto útoku stačí odpojit oprávněnou koncovou jednotku např. v domácnosti a místo ní připojit zdroj rušení. Případný útočník tedy nepotřebuje přístup přímo k pasiv-



Obr. 11.7: Nastavení zabezpečení portu na OLT ZyXEL.



Obr. 11.8: Výpis MAC adres na OLT ZyXEL po nastavení omezení.

nímu optickému rozbočovači. Stejně tak může podrobit koncovou jednotku analýze a případně provést její modifikaci.

V porovnání se standardními přepínači vykazuje systém GPON jisté výhody. Především se jedná o šifrování komunikace (musí být aktivována), koncoví uživatelé tak nemohou zachytit komunikaci síťových protokolů. Nespornou výhodou je také centralizovaná správa celé sítě prostřednictvím jednotky OLT.

12 Závěr

S rozvojem stále nových telekomunikačních služeb bude i nadále pokračovat vývoj v oblasti přístupových sítí, především pak těch optických. Pasivní optické sítě se těší velké oblibě pro svoji vysokou přenosovou rychlost, dosah i možný počet připojených koncových uživatelů. Z hlediska provozních nákladů není nutné zajišťovat napájení pro pasivní optické rozbočovače, infrastruktura od optického linkového zakončení až po koncovou jednotku umístěnou u zákazníka je kompletně pasivní.

První standardy pasivních optických sítí jsou již minulostí, sehrály však zásadní roli pro vývoj svých současných následovníků. Gigabitová pasivní optická síť je jedním z nejúspěšnějších standardů definovaných Mezinárodní telekomunikační unií. Tento standard se dočkal širokého rozšíření po celém světě, ve velkém je nasazován v Severní Americe, Evropě, na Středním východě a Austrálii, kde hraje významnou roli pro přivedení optického vlákna do domovů koncových uživatelů. Předpokládá se, že tento standard bude i nadále dominantní.

Následovníci Gigabitové pasivní optické sítě byli již Mezinárodní telekomunikační unií standardizováni, nicméně zatím nedošlo k tak masivnímu nasazení jako v případě standardu Gigabitové pasivní optické sítě. Lze však předpokládat, že v průběhu příštích let dojde i k rozšíření nejnovějších standardů pasivních optických sítí. Konkurenční standard Ethernetové pasivní optické sítě je rozšířen zejména v Asijských zemích.

V rámci této diplomové práce byl popsán historický vývoj jednotlivých standardů pasivních optických sítí definovaných Mezinárodní telekomunikační unií, dále byla popsána bezpečnost pasivních optických sítí a v neposlední řadě také bezpečnostní rizika spojená s nasazením a provozem těchto sítí.

V rámci praktické části bylo realizováno osazení racku optickým linkovým zakončením dvou odlišných standardů – Gigabitové pasivní optické sítě a Ethernetové pasivní optické sítě, které budou využity pro budoucí testování. Byla realizována optická distribuční síť, která umožňuje variabilně měnit výslednou délku, případně vytvořit hned několik oddělených sítí. Propojením jednotlivých vláken optického kabelu lze dosáhnout maximální délky 24 km. Provedena a popsána byla také základní konfigurace vybraných optických linkových zakončení.

Byla ověřena vybraná bezpečnostní rizika. Jako nejzávažnější se jeví narušení komunikace za pomoci vysílání laserového zdroje. Nerespektování přidělených časových intervalů pro komunikaci kompletně naruší komunikaci v dané optické distribuční síti. Proveditelnost tohoto útoku je však závislá na použitém laserovém zdroji, který musí vysílat na vlnové délce užité pro komunikaci v dané síti, jinak se komunikaci narušit nepodaří. Důležité bude najít efektivní způsob ochrany vůči tomuto způsobu narušení komunikace.

Literatura

[1] ABBAS, H. Saleh a Mark A. GREGORY. The next generation of passive optical networks: A review. In: *Journal of Network and Computer Applications* [online]. Elsevier, 2016, **67**, 53–74 [cit. 13. 3. 2018]. DOI: 10.1016/j.jnca.2016.02.015. ISSN 1084-8045. Dostupné z URL: <https://www-sciencedirect-com.ezproxy.lib.vutbr.cz/science/article/pii/S1084804516000989>.

[2] ABRAMS, M., P. C. BECKER, Y. FUJIMOTO, V. O'BYRNE a D. PIEHLER. FTTP deployments in the United States and Japan – equipment choices and service provider imperatives. In: *Journal of Lightwave Technology* [online]. USA: IEEE, 2005, **23**(1), 236–246 [cit. 28. 10. 2017]. DOI: 10.1109/JLT.2004.840340. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/1377452/>.

[3] ALISON, Diana. Verizon, Calix Deploy Commercial NG-PON2. *Broadband World News* [online]. Broadband World Forum, 30. 1. 2018 [cit. 31. 3. 2018]. Dostupné z URL: <http://www.broadbandworldnews.com/author.asp?section_id=548&doc_id=740105>.

[4] ASIF, Rameez, Paul HAO HU, John MITCHELL, et al. Experimental demonstration of 6-mode division multiplexed NG-PON2: Cost effective 40 Gbit/s/spatial-mode access based on 3D laser inscribed photonic lanterns. In: *Optical Communication (ECOC), 2015 European Conference* [online]. Spain: Viajes el Corte Ingles, VECISA, 2015, 1–3 [cit. 30. 3. 2018]. DOI: 10.1109/ECOC.2015.7341921. ISBN 978-8-4608-1741-3. Dostupné z URL: <http://ieeexplore.ieee.org/document/7341921/>.

[5] BOURG, Kevin, Sergey TEN, Robert WHITMAN, Joe JENSEN a Vanesa DIAZ. The evolution of outside plant architectures driven by network convergence and new PON technologies. In: *Optical Fiber Communications Conference and Exhibition (OFC), 2017* [online]. USA: OSA, 2017, 1–3 [cit. 16. 3. 2018]. ISBN 978-1-9435-8023-1. Dostupné z URL: <http://ieeexplore.ieee.org/document/7936825/>.

[6] CALE, I., A. SALIHOVIC a M. IVEKOVIC. Gigabit Passive Optical Network – GPON. In: *Information Technology Interfaces, 2007. ITI 2007. 29th International Conference* [online]. Croatia: IEEE, 2007, 679–684 [cit. 29. 10. 2017]. DOI: 10.1109/ITI.2007.4283853. ISBN 953-7138-09-7. ISSN 1330-1012. Dostupné z URL: <http://ieeexplore.ieee.org/document/4283853/>.

[7] DRAKULIC, S., M. TORNATORE a G. VERTICALE. Degradation attacks on Passive Optical Networks. In: *Optical Network Design and Modeling (ONDM), 2012 16th International Conference* [online]. IEEE, 2012, 1–6 [cit. 19. 11. 2017]. DOI: 10.1109/ONDM.2012.6210184. ISBN 978-1-4673-1440-4. Dostupné z URL: <http://ieeexplore.ieee.org/document/6210184/>.

[8] EFFENBERGER, Frank J. The XG-PON System: Cost Effective 10 Gb/s Access. In: *Journal of Lightwave Technology* [online]. USA: IEEE, 2011, **29**(4), 403–409 [cit. 4. 2. 2018]. DOI: 10.1109/JLT.2010.2084989. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/5595476/>.

[9] *Federal Information Processing Standards Publication 197. Announcing the Advanced Encryption Standard (AES)* [online]. National Institute of Standards and Technology, 2001. [cit. 8. 12. 2017]. Dostupné z URL: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>.

[10] FILKA, Miloslav. *Optoelektronika pro telekomunikace a informatiku*. 1. vydání. Brno: Miloslav Filka, 2009. 369 s. ISBN 978-80-86785-14-1.

[11] FILKA, Miloslav. *Optické sítě – přednášky* [online]. 2007, poslední aktualizace 30. 11. 2007 [cit. 21. 7. 2017]. Dostupné z URL: <https://www.vutbr.cz/www_base/priloha.php?dpid=24589>.

[12] *About FSAN* [online]. Full Service Access Network. [cit. 1. 10. 2017]. Dostupné z URL: <https://www.fsan.org/>.

[13] GAGNAIRE, Maurice a Sašo STOJANOVSKI. Stream traffic management over an ATM passive optical network. In: *Computer Networks* [online]. Elsevier B.V., 2000, **32**(5), 571–586 [cit. 29. 9. 2017]. DOI: 10.1016/S1389-1286(00)00018-9. ISSN 1389-1286. Dostupné z URL: <http://www.sciencedirect.com.ezproxy.lib.vutbr.cz/science/article/pii/S1389128600000189>.

[14] GIANORDOLI, S., M. RASZTOVITS-WIECH, A. STADLER a R. GRABENHORST. Next generation PON. In: *E & i Elektrotechnik und Informationstechnik* [online]. Vienna: Springer-Verlag, 2006, **123**(3), 78–82 [cit. 11. 11. 2017]. DOI: 10.1007/s00502-006-0320. ISSN 0932-383X. Dostupné z URL: <https://link-springer-com.ezproxy.lib.vutbr.cz/article/10.1007/s00502-006-0320>.

[15] HAJDUCZENIA, Marek, Pedro M. INACIO, Henrique DA SILVA, Mario FREIRE a Paulo MONTEIRO. On EPON security issues. In: *Communications Surveys & Tutorials, IEEE* [online]. USA: IEEE, 2007, **9**(1), 68–83 [cit. 21. 11. 2017]. DOI: 10.1109/COMST.2007.358972. Dostupné z URL: <http://ieeexplore.ieee.org/document/4198187/>.

[16] HAJDUCZENIA, Marek a Henrique J. A. DA SILVA. Next generation PON systems – Current status. In: *Transparent Optical Networks, 2009. ICTON '09. 11th International Conference* [online]. Portugal: IEEE Publishing, 2009, 1–8 [cit. 25. 1. 2018]. DOI: 10.1109/ICTON.2009.5185097. ISBN 978-1-4244-4825-8. ISSN 2162-7339. Dostupné z URL: <http://ieeexplore.ieee.org/document/5185097/>.

[17] HOOD Dave a TROJER Elmar. *Gigabit-capable passive optical networks*. Hoboken, New Jersey: John Wiley & Sons, 2012. 435 s. ISBN 978-0-470-93687-0.

[18] HORVATH, Tomas, Lukas MALINA a Petr MUNSTER. On security in gigabit passive optical networks. In: *Fiber Optics in Access Network (FOAN), 2015 International Workshop* [online]. Brno, Czech Republic: IEEE, 2015, 51–55 [cit. 15. 11. 2017]. DOI: 10.1109/FOAN.2015.7320479. ISBN 978-1-4673-7625-9. ISSN 2378-847X. Dostupné z URL: <http://ieeexplore.ieee.org/document/7320479/>.

[19] CHANCLOU, P., S. GOSSELIN, J. F. PALACIOS, V. L. ALVAREZ a E. ZOUGANELI. Overview of the optical broadband access evolution: a joint article by operators in the IST network of excellence e-Photon/One. In: *Communications Magazine, IEEE* [online]. USA: IEEE, 2006, **44**(8), 29–35 [cit. 9. 11. 2017]. DOI: 10.1109/MCOM.2006.1678106. ISSN 0163-6804. Dostupné z URL: <http://ieeexplore.ieee.org/document/1678106/>.

[20] CHANCLOU, P., Z BELFQIH, B. CHARBONNIER, et al. Access network evolution: optical fibre to the subscribers and impact on the metropolitan and home networks. In: *Comptes Rendus Physique* [online]. Elsevier France-Editions Scientifiques Medicales Elsevier, 2008, **9**(9–10), 935–946 [cit. 10. 11. 2017]. DOI: 10.1016/j.crhy.2008.10.010. ISSN 1631-0705. Dostupné z URL: <http://www.sciencedirect.com.ezproxy.lib.vutbr.cz/science/article/pii/S1631070508001382>.

[21] CHEN, Ling, Stefan DAHLFORT a Dave HOOD. Evolution of PON: 10G-PON and WDM-PON. In: *Communications and Photonics Conference and Exhibition (ACP), 2010 Asia* [online]. China: IEEE Publishing, 2010, 709–711 [cit. 4. 2. 2018]. DOI: 10.1109/ACP.2010.5682701. ISBN 978-1-4244-7111-9. Dostupné z URL: <http://ieeexplore.ieee.org/document/5682701/>.

[22] CHEN, Xue, Zhiguo ZHANG a Xintian HU. The evolution trends of PON and key techniques for NG-PON. In: *Information, Communications and Signal Processing (ICICS) 2013 9th International Conference* [online]. Taiwan: IEEE, 2013, 1–6 [cit. 13. 2. 2018]. DOI: 10.1109/ICICS.2013.6782905. ISBN 978-1-4799-0434-1. Dostupné z URL: <http://ieeexplore.ieee.org/document/6782905/>.

[23] CHOI, Byungchul, Jeasung KIM, Eun-mo YEO a Youngil PARK. Detection of failed ONUs in TDM-PON using CDMA coding scheme. In: *14th OptoElectronics and Communications Conference, OECC 2009.* [online]. Austria: IEEE, 2009, 1–2 [cit. 2. 12. 2017]. DOI: 10.1109/OECC.2009.5214905. ISBN 978-1-4244-4102-0. ISSN 2166-8892. Dostupné z URL: <http://ieeexplore.ieee.org/document/5214905/>.

[24] *ITU-T Recommendation G.983.1. Broadband optical access systems based on Passive Optical Networks (PON)* [online]. International Telecommunication Union, 2005. [cit. 19. 7. 2017]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.983.1-200501-I/en>.

[25] *ITU-T Recommendation G.983.3. A broadband optical access system with increased service capability by wavelength allocation* [online]. International Telecommunication Union, 2001. [cit. 29. 9. 2017]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.983.3-200103-I/en>.

[26] *ITU-T Recommendation G.983.4. A broadband optical access system with increased service capability using dynamic bandwidth assignment* [online]. International Telecommunication Union, 2001. [cit. 12. 10. 2017]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.983.4-200111-I/en>.

[27] *ITU-T Recommendation G.984.1. Gigabit-capable passive optical networks (GPON): General characteristics* [online]. International Telecommunication Union, 2008. [cit. 17. 7. 2017]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.984.1-200303-S/en>.

[28] *ITU-T Recommendation G.984.3. Gigabit-capable passive optical networks (GPON): Transmission convergence layer specification* [online]. International Telecommunication Union, 2014. [cit. 5. 11. 2017]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.984.3-201401-I/en>.

[29] *ITU-T Recommendation G.984.5. Gigabit-capable passive optical networks (GPON): Enhancement band* [online]. International Telecommunication Union, 2014. [cit. 12. 2. 2018]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.984.5-201405-I/en>.

[30] *ITU-T Recommendation G.987.1. 10-Gigabit-capable passive optical networks (XG-PON): General requirements* [online]. International Telecommunication Union, 2016. [cit. 22. 1. 2018]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.987.1-201603-I/en>.

[31] *ITU-T Recommendation G.987.3. 10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence layer specification* [online]. International Telecommunication Union, 2014. [cit. 10. 2. 2018]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.987.3-201401-I/en>.

[32] *ITU-T Recommendation G.989.1. 40-Gigabit-capable passive optical networks (NG-PON2): General requirements* [online]. International Telecommunication Union, 2013. [cit. 12. 2. 2018]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.989.1-201303-I/en>.

[33] *ITU-T Recommendation G.989.2. 40-Gigabit-capable passive optical networks (NG-PON2): Physical media dependent (PMD) layer specification* [online]. International Telecommunication Union, 2014. [cit. 19. 2. 2018]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.989.2-201412-I/en>.

[34] *ITU-T Recommendation G.989.3. 40-Gigabit-capable passive optical networks (NG-PON2): Transmission convergence layer specification* [online]. International Telecommunication Union, 2015. [cit. 16. 3. 2018]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.989.3-201510-I/en>.

[35] *ITU-T Series G Supplement 49. Rogue optical network unit (ONU) considerations* [online]. International Telecommunication Union, 2014. [cit. 2. 12. 2017]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.Sup49-201102-I>.

[36] JAIN, S., F. EFFENBERGER, A. SZABO, et al. World's First XG-PON Field Trial. In: *Journal of Lightwave Technology* [online]. USA: IEEE, 2011, **29**(4), 524–528 [cit. 23. 1. 2018]. DOI: 10.1109/JLT.2010.2104313. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/5692799/>.

[37] JAMES, K. A. a S. FISHER. Developments in optical access networks. In: *BT Technology Journal* [online]. Dordrecht: Kluwer Academic Publishers, 2002, **20**(4), 81–90 [cit. 23. 9. 2017]. DOI: 10.1023/A:1021378600830. ISSN 1358-3948. Dostupné z URL: <https://link-springer-com.ezproxy.lib.vutbr.cz/article/10.1023/A%3A1021378600830>.

[38] *Kali Linux: Official Documentation* [online]. Offensive Security, 2018 [cit. 15. 5. 2018]. Dostupné z URL: <https://docs.kali.org/>.

[39] *Kali Linux: Tools Listing* [online]. Offensive Security, 2018 [cit. 15. 5. 2018]. Dostupné z URL: <https://tools.kali.org/tools-listing>.

[40] KAZOVSKY, L. G., S. W. WONG, V. GUDLA, P. T. AFSHAR, S. H. YEN, S. YAMASHITA a Y. YAN. Challenges in next-generation optical access networks. In: *IET Optoelectronics* [online]. 2011, **5**(4), 133–143 [cit. 29. 11. 2017]. DOI: 10.1049/iet-opt.2011.0027. ISSN 17518768. Dostupné z URL: <http://ieeexplore.ieee.org/document/5984711/>.

[41] KHOTIMSKY, Denis A. NG-PON2 Transmission Convergence Layer: A Tutorial. In: *Journal of Lightwave Technology* [online]. USA: IEEE, 2016, **34**(5), 1424–1432 [cit. 14. 3. 2018]. DOI: 10.1109/JLT.2016.2523343. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/7394098/>.

[42] KIM, Kyeong Soo. On the evolution of PON-based FTTH solutions. In: *Information Sciences* [online]. Elsevier, 2003, **149**(1), 21–30 [cit. 23. 10. 2017]. DOI: 10.1016/S0020-0255(02)00241-4. ISSN 0020-0255. Dostupné z URL: <http://www.sciencedirect.com.ezproxy.lib.vutbr.cz/science/article/pii/S0020025502002414>.

[43] LEE, Byung-Tak a Mun-Seob LEE. Remote Fault Detection Method for Time-Slot-Violated Terminal Using Periodic Probing Signal in TDM-PON. In: *Journal of Lightwave Technology* [online]. USA: IEEE, 2009, **27**(16), 3498–3508 [cit. 21. 11. 2017]. DOI: 10.1109/JLT.2008.2011566. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/4815443/>.

[44] MENDONCA, C., M. LIMA a A. TEIXEIRA. Security issues due to reflection in PON physical medium. In: *Transparent Optical Networks (ICTON), 2012 14th International Conference* [online]. Coventry, UK: IEEE, 2012, 1–4 [cit. 18. 11. 2017]. DOI: 10.1109/ICTON.2012.6254487. ISBN 978-1-4673-2228-7. ISSN 2161-2056. Dostupné z URL: <http://ieeexplore.ieee.org/document/6254487/>.

[45] MUCIACCIA, Tommaso, Fabio GARGANO a Vittorio PASSARO. Passive Optical Access Networks: State of the Art and Future Evolution. In: *Photonics* [online]. Basel: MDPI, 2014, **1**(4), 323–346 [cit. 17. 2. 2018]. DOI: 10.3390/photonics1040323. Dostupné z URL: <http://www.mdpi.com/2304-6732/1/4/323>.

[46] MUKHERJEE, Biswanath. *Optical WDM Networks.* Boston: Springer, 2006. 974 s. ISBN 978-0-387-29188-8.

[47] NESSET, Derek. NG-PON2 Technology and Standards. *Journal of Lightwave Technology* [online]. USA: IEEE, 2015, **33**(5), 1136-1143 [cit. 4. 3. 2018]. DOI: 10.1109/JLT.2015.2389115. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/7005437/>.

[48] NESSET, Derek. PON roadmap [invited]. *Journal of Optical Communications and Networking, IEEE/OSA* [online]. USA: IEEE, 2017, **9**(1), A71-A76 [cit. 16. 3. 2018]. DOI: 10.1364/JOCN.9.000A71. ISSN 1943-0620. Dostupné z URL: <http://ieeexplore.ieee.org/document/7830264/>.

[49] Nokia Siemens Networks. *Surpass hiX R2.0: Operation Manual CLI.* Nokia Siemens Networks, © 2007–2008.

[50] PETERKA, Jiří. *Principy počítačových sítí, modul 10: ATM* [online]. 1997, [cit. 16. 9. 2017]. Dostupné z URL: <http://www.earchiv.cz/i_pri.php3#10>.

[51] PETERKA, Jiří. *WDM – revoluce v optice* [online]. 2000, [cit. 29. 9. 2017]. Dostupné z URL: <http://www.earchiv.cz/b00/b1200006.php3>.

[52] PHILLIPS, A. J., J. M. SENIOR, P. J. VETTER, M. O. van DENVENTER, M. VALVO a R. MERCINELLI. Reliability of SuperPON Systems. In: *6 th IEE Conference* [online]. Edinburg: IET, 1998, 219–223 [cit. 17. 10 .2017]. DOI: 10.1049/cp:19980045. ISBN 0-85296-700-4. ISSN 0537-9989. Dostupné z URL: <http://ieeexplore.ieee.org/document/675168/>.

[53] VAN DER PLAS, G., R. SMETS, B. SUARD a W. VERBIEST. Demonstration of an ATM-based passive optical network in the FTTH trial on Bermuda. In: *Global Telecommunications Conference, 1995. GLOBECOM '95. IEEE* [online]. Singapore: IEEE, 1995, **2**, 988–992 [cit. 24. 10. 2017]. DOI: 10.1109/GLOCOM.1995.502553. ISBN 0-7803-2509-5. Dostupné z URL: <http://ieeexplore.ieee.org/document/502553/>.

[54] RINGOOT, E., N. JANSSENS, A. TASSENT, J. ANGELOUPOULOS, C. BLONDIA a P. VETTER. Demonstration of dynamic medium access control for APON and SuperPON. In: *Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE* [online]. USA: IEEE, 2001, **3**, 1570–1574 [cit. 21. 9. 2017]. DOI: 10.1109/GLOCOM.2001.965844. ISBN 0-7803-7206-9. Dostupné z URL: <http://ieeexplore.ieee.org/document/965844/>.

[55] SAKAUE, Y., K. TAGUCHI, K. HARA, et al. Demonstration of NG-PON2 coexisting with other systems on same ODN by using WDM filter with low power penalty of under 1.0 dB. In: *European Conference on Optical Communication, ECOC* [online]. Germany: IEEE, 2016, 923–925 [cit. 30. 3. 2018]. ISBN 9783800742745. Dostupné z URL: <http://ieeexplore.ieee.org/document/7767767/>.

[56] SHUMATE, P. W. Fiber-to-the-Home: 1977–2007. In: *Journal of Lightwave Technology* [online]. USA: IEEE, 2008, **26**(9), 1093–1103 [cit. 13. 11. 2017]. DOI: 10.1109/JLT.2008.923601. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/4542893/>.

[57] SCHLITTER, Pavel. *Optické přístupové sítě* [online]. 2004, [cit. 17. 7. 2017]. Dostupné z URL: <http://access.feld.cvut.cz/view.php?cisloclanku=2004072807>.

[58] SIVALINGAM, Krishna M. a Suresh SUBRAMANIAM. *Emerging Optical Network Technologies: Architectures, Protocols and Performance*. Boston: Springer, 2005. 449 s. ISBN 0-387-22584-6.

[59] SUGIE, Toshihiko a Hirotaka NAKAMURA. Recent advances in access networks and their components technologies. In: *International Conference on Microwave and Photonics (ICMAP), 2015* [online]. India: IEEE, 2015, 1–2 [cit. 16. 3. 2018]. DOI: 10.1109/ICMAP.2015.7408735. ISBN 978-1-4673-6897-1. Dostupné z URL: <http://ieeexplore.ieee.org/document/7408735/>.

[60] SÝKORA, Jiří. *Princip WDM* [online]. 2004, [cit. 31. 10. 2017]. Dostupné z URL: <http://access.fel.cvut.cz/view.php?cisloclanku=2004072805>.

[61] THOMAS, S. a D. WAGNER. Insecurity in ATM-based passive optical networks. In: *Communications, 2002. ICC 2002. IEEE International Conference* [online]. USA: IEEE, 2002, **5**, 2803–2805 [cit. 7. 11. 2017]. DOI: 10.1109/ICC.2002.997353. ISBN 0-7803-7400-2. Dostupné z URL: <http://ieeexplore.ieee.org/document/997353/>.

[62] Úřad vlády České republiky. *Digitální Česko v. 2.0, Cesta k digitální ekonomice* [online]. 2013, [cit. 13. 7. 2017]. Dostupné z URL: <https://www.vlada.cz/assets/media-centrum/aktualne/Digitalni-Cesko-v--2-0_120320.pdf>.

[63] VAN DE VOORDE, Ingrid a Gert VAN DER PLAS. Full service optical access networks: ATM transport on passive optical networks. In: *IEEE Communications Magazine* [online]. USA: IEEE, 1997, **35**(4), 70–75 [cit. 8. 10. 2017]. DOI: 10.1109/35.570721. ISSN 0163-6804. Dostupné z URL: <http://ieeexplore.ieee.org/document/570721/>.

[64] VAN VEEN, D., W. PÖHLMANN, J. GALARO, et al. System demonstration of a time and wavelength-set division multiplexing PON. In: *IET Conference Publications* [online]. UK: IEEE, 2013, **2013**(622), 564–566 [cit. 30. 3. 2018]. DOI: 10.1049/cp.2013.1461. ISBN 9781849197595. Dostupné z URL: <http://ieeexplore.ieee.org/document/6647654/>.

[65] WEIS, Erik, Rainer HOLZL, Dirk BREUER a Christoph LANGE. GPON FTTH trial – lessons learned. In: *Communications and Photonics Conference and Exhibition (ACP), 2009 Asia* [online]. Shanghai, China: IEEE, 2009, 1–7 [cit. 19. 11. 2017]. DOI: 10.1364/ACP.2009.TuBB2. ISBN 978-1-55752-877-3. ISSN 2162-1098. Dostupné z URL: <http://ieeexplore.ieee.org/document/5405442/>.

[66] ZHONGWEI, Sun, Ma YANING, Guo QINGRUI a Sun FENGJIE. Security mechanism for distribution automation using EPON. In: *Network Infrastructure and Digital Content, 2009. IC-NIDC 2009. IEEE International Conference* [online]. Beijing, China: IEEE, 2009, 581–585 [cit. 28. 11. 2017]. DOI: 10.1109/ICNIDC.2009.5360954. ISBN 978-1-4244-4898-2. ISSN 2374-0272. Dostupné z URL: <http://ieeexplore.ieee.org/document/5360954/>.

Seznam symbolů, veličin a zkratek

10GEPON 10 Gigabitová Ethernetová pasivní optická síť – 10 Gigabit Ethernet Passive Optical Network

ACTS Pokročilé komunikační technologie a služby – Advanced Communication Technologies and Services

ADSL Asymetrická digitální účastnická linka – Asymetric Digital Subscriber Line

AES Standard pokročilého šifrování – Advanced Encryption Standard

AON Aktivní optická síť – Active Optical Network

APC Konektor s šikmou kontaktní plochou – Angled Polish Connector

APD Lavinová fotodioda – Avalanche Photodiode

APON Pasivní optická síť založená na technologii ATM – ATM Passive Optical Network

ASCII Americký standardní kód pro výměnu informací – American Standard Code for Information Interchange

ASU Účastnická jednotka technologie ATM – ATM Subscriber Unit

ATM Asynchronní přenosová technologie – Asynchronous Transfer Mode

AWG Vlnovod s mřížkovým uspořádáním – Array Wavelength Gratings

BER Bitová chybovost – Bit Error Ratio

B-ISDN Širokopásmové ISDN – Broadband ISDN

BPON Širokopásmová pasivní optická síť – Broadband Passive Optical Network

CAM Adresovatelná paměť – Content Addressable Memory

CATV Kabelová televize – Cable Television

CE Koexistenční prvek – Coexistence Element

CDMA Kódový multiplex – Code Division Multiple Access

CIR Minimální garantovaná přenosová rychlost – Commited Information Rate

CLI Příkazový řádek – Command Line Interface

CT Ukončení kanálu – Channel Termination

CWDM Hrubý vlnový multiplex – Coarse Wavelength Division Multiplex

DBA Dynamické přidělení šířky pásma – Dynamic Bandwidth Assignment

DBRu Zpráva o přidělení šířky pásma ve vzestupném směru – Dynamic Bandwidth Report upstream

DFB Laser s rozloženou zpětnou vazbou – Distributed Feedback Laser

DHCP Protokol pro automatické přidělování IP adres – Dynamic Host Configuration Protocol

DoS Odepření služby – Denial of Service

DDoS Distribuovaný DoS útok – Distributed Denial of Service

DHCP Protokol pro automatickou konfiguraci IP adres – Dynamic Host Configuration Protocol

DWDM Hustý vlnový multiplex – Dense Wavelength Division Multiplex

EDFA Erbiem dotovaný vláknový zesilovač – Erbium Doped Fibre Amplifier

EFM Ethernet na první míli – Ethernet in the First Mile

EPON Ethernetová pasivní optická síť – Ethernet Passive Optical Network

FEC Samoopravný kód – Forward Error Correction

FER Chybovost rámců – Frame Error Rate

FDM Frekvenční multiplex – Frequency Division Multiplex

FSAN Síť plného přístupu ke službám – Full Service Access Network

FTP Protokol pro přenos souborů – File Transfer Protocol

FTTA Vlákno do antény – Fiber To The Antenna

FTTB Vlákno do budovy – Fiber To The Building

FTTC Vlákno do uzlu – Fiber To The Curb

FTTH Vlákno do domu – Fiber To The Home

FTTO Vlákno do kanceláře – Fiber To The Office

FTTx Vlákno do... – Fiber To The...

GEM Metoda zapouzdření GPON sítí – GPON Encapsulation Method

GPON Gigabitová pasivní optická síť – Gigabit Passive Optical Network

GTC Přenosová vrstva standardu GPON – GPON Transmission Convergence

HEC Korekční kód hlavičky – Header Error Correction

HFC Hybridní opticko-koaxiální vedení – Hybrid Fiber-Coax

ICTP Protokol pro ukončení interních kanálů – Inter-Channel-Termination Protocol

IEEE Institut elektrotechnického a elektronického inženýrství – Institute of Electrical and Electronics Engineers

IoT Internet věcí – Internet of Things

IP Internet Protocol

IPsec Zabezpečený IP protokol – IP Security

ISDN Digitální síť integrovaných služeb – Integrated Services Digital Network

ITU Mezinárodní telekomunikační unie – International Telecommunication Union

KEK Klíč sloužící k zabezpečení přenášeného klíče – Key Encryption Key

LAN Lokální síť – Local Area Network

LRE Ethernet s dlouhým dosahem – Long Reach Ethernet

MAC Řízení přístupu na médium – Medium Access Control

MCF	Optické vlákno obsahující více jader – Multi Core Fiber
MIC	Kontrola integrity zpráv – Message Integrity Check
MitM	„Člověk uprostřed“ – Man in the Middle
NG-PON	Síť PON nové generace – Next Generation PON
NTP	Protokol pro synchronizaci času – Network Time Protocol
OAN	Optická přístupová síť – Optical Access Network
ODN	Optická distribuční síť – Optical Distribution Network
OFDM	Ortogonální multiplex s frekvenčním dělením – Orthogonal Frequency Division Multiplex
OFDR	Optická reflektometrie ve frekvenční oblasti – Optical Frequency Domain Reflectometry
OLT	Optické linkové zakončení – Optical Link Termination
OMCI	Optické síťové řídicí a kontrolní rozhraní – Optical Network Unit Management and Control Interface
ONT	Optické síťové zakončení – Optical Network Termination
ONU	Optická síťová jednotka – Optical Network Unit
OTDR	Optická reflektometrie v časové oblasti – Optical Time Domain Reflectometry
PC	Konektor s kolmou kontaktní plochou – Polished Connector
PCBd	Kontrolní blok fyzické vrstvy v sestupném směru – Physical Control Block downstream
PDU	Protokolová datová jednotka – Protocol Data Unit
PIN	Polovodičová dioda – Positive Instrinsic Negative
PIR	Špičková přenosová rychlost – Peak Information Rate
PLANET	Fotonová lokální síť – Photonic Local Access Network
PLOAM	Provoz, správa a údržba fyzické vrstvy – Physical Layer Operation, Administration and Maintenance
PLOu	Režijní část zprávy pro vzestupný směr – Physical Layer Overhead upstream
PON	Pasivní optická síť – Passive Optical Network
POTS	Klasická telefonie – Plain Old Telephone Service
PtP	Komunikace typu bod-bod – Point-to-Point
QoS	Kvalita služeb – Quality of Services
SFP	Zásuvný konektorový modul – Small Form-factor Pluggable
SDH	Synchronní digitální hierarchie – Synchronous Digital Hierarchy
SDM	Prostorové oddělení – Space Division Multiplex
SDN	Softwarově definovaná síť – Software Defined Network
SN	Sériové číslo – Serial Number
SNR	Odstup signálu od šumu – Signal-to-noise ratio

SOA	Polovodičový optický zesilovač – Semiconductor Optical Amplifier
SSH	Zabezpečený protokol SSH – Secure Shell
SSL	Vrstva zabezpečených soketů – Secure Sockets Layer
SMTP	Protokol pro přenos elektronické pošty – Simple Mail Transfer Protocol
T-CONT	Přenosový kontejner – Transmission Container
TCP	Spojově orientovaný protokol – Transmission Control Protocol
TDM	Časový multiplex – Time Division Multiplex
TDMA	Časový multiplex s vícenásobným přístupem – Time Division Multiple Access
TWDM	Časový a vlnový multiplex – Time and Wavelength Division Multiplex
ToS	Odcizení služby – Theft of Service
TPON	Telefonie prostřednictvím PON – Telephony over PON
UPC	Konektor s kolmou kontaktní plochou – Polish Connector
USB	Univerzální sériová sběrnice – Universal Serial Bus
VDSL	Vysokorychlostní DSL – Very High Speed DSL
VLAN	Virtuální lokální síť – Virtual Local Area Network
VoD	Video na vyžádání – Video on Demand
VoIP	Přenos hlasu přes Internet protokol – Voice over Internet Protocol
VPN	Virtuální privátní síť – Virtual Private Network
WAN	Rozlehlá síť – Wide Area Network
WDM	Vlnový multiplex – Wavelength Division Multiplex
xDSL	xDigital Subscriber Line
X-GEM	Metoda zapouzdření XG-PON sítí – XG-PON Encapsulation Method
XG-PON	X Gigabitová pasivní optická síť – X Gigabit Passive Optical Network
XGS-PON	10 Gigabitová symetrická PON – 10 Gb/s Symmetrical PON
XGTC	Konvergence přenosu XG-PON – XG-PON Transmission Convergence

Seznam příloh

A Konfigurace OLT jednotky Huawei

V rámci prvotní konfigurace OLT je třeba aktivovat osazené GPON moduly (označené jako H806GPBD). Po jejich aktivaci se jejich stav změní na `Normal`. Výpis osazených modulů v šasi jednotky spolu s příkazem potřebným k jejich aktivaci obsahuje výpis A.1.

Následuje definování portu pro uplink, v tomto případě je jako uplink využíván port číslo *1* umístěný v modulu *0/8*. Příklad konfigurace tohoto portu je uveden ve výpisu A.2.

V rámci popisu konfigurace OLT jednotky Huawei, který je obsahem podkapitoly 10.2 na straně 84, je často využívána VLAN s číslem 2. Způsob konfigurace VLAN je uveden ve výpisu A.3. Po vytvoření VLAN číslo 2 je tato VLAN přidána na uplinkový port, tímto dojde k předávání značkovaných rámců i mimo OLT jednotku. V posledním kroku výpisu je dané VLAN přiřazena IP adresa.

Výpis A.1: Výpis modulů osazených v šasi OLT Huawei.

```
GPON-OLT-HUAWEI> enable
GPON-OLT-HUAWEI# config
GPON-OLT-HUAWEI(config)# display board 0
  ------------------------------------------------------------------------
  SlotID  BoardName  Status           SubType0 SubType1    Online/Offline
  ------------------------------------------------------------------------
  0
  1
  2       H806GPBD   Auto_find
  3
  4       H806GPBD   Auto_find
  5
  6       H802SCUN   Standby_normal
  7       H802SCUN   Active_normal
  8       H801GICF   Normal
  9       H801X2CS   Normal
  10
  11
  12
  ------------------------------------------------------------------------

GPON-OLT-HUAWEI(config)# board confirm 0/2
  0 frame 2 slot board confirms successfully

GPON-OLT-HUAWEI(config)# board confirm 0/4
  0 frame 4 slot board confirms successfully
```

Výpis A.2: Konfigurace uplinkového portu.

```
GPON-OLT-HUAWEI(config)# interface giu 0/8
GPON-OLT-HUAWEI(config-if-giu-0/8)# network-role 1 uplink
```

Výpis A.3: Konfigurace VLAN.

```
GPON-OLT-HUAWEI(config)# vlan 2 smart
GPON-OLT-HUAWEI(config)# port vlan 2 0/8 1
GPON-OLT-HUAWEI(config)# interface vlanif 2
GPON-OLT-HUAWEI(config-if-vlanif2)# ip address 10.0.0.2 255.255.255.0
```

Dále jsou v rámci této přílohy vloženy výpisy z OLT jednotky Huawei. Výpis A.4 obsahuje přehled připojených koncových jednotek, výpis A.5 obsahuje podrobné informace vybrané jednotky ONU. Informace o připojených jednotkách ONU k OLT Huawei jsou umístěny v tabulkách B.1, B.2 a B.3.

Výpis A.4: Připojené jednotky ONU.

```
GPON-OLT-HUAWEI(config-if-gpon-0/2)# display ont info 3 all
  ------------------------------------------------------------------------------
  F/S/P  ONT        SN          Control   Run      Config   Match    Protect
         ID                     flag      state    state    state    side
  ------------------------------------------------------------------------------
  0/2/3   0   48575443D51DCB84  active    online   normal   match    no
  0/2/3   1   4857544371FDCF76  active    online   normal   match    no
  0/2/3   2   485754438009FE75  active    online   normal   match    no
  0/2/3   3   485754437E8E5975  active    online   normal   match    no
  0/2/3   4   485754438A755082  active    online   normal   match    no
  0/2/3   5   485754438A762C82  active    online   normal   match    no
  0/2/3   6   485754438A763682  active    online   normal   match    no
  0/2/3   7   485754438A764082  active    online   normal   match    no
  ------------------------------------------------------------------------------
  F/S/P   ONT-ID   Description
  ------------------------------------------------------------------------------
  0/2/3     0      ONU-0230
  0/2/3     1      ONU-0231
  0/2/3     2      ONU-0232
  0/2/3     3      ONU-0233
  0/2/3     4      ONU-0234
  0/2/3     5      ONU-0235
  0/2/3     6      ONU-0236
  0/2/3     7      ONU-0237
  ------------------------------------------------------------------------------
  In port 0/2/3 , the total of ONTs are: 8, online: 8
```

Výpis A.5: Podrobné informace o jednotce ONU.

```
GPON-OLT-HUAWEI(config-if-gpon-0/2)# display ont info 3 0
  ------------------------------------------------------------------------------
  F/S/P                   : 0/2/3
  ONT-ID                  : 0
  Control flag            : active
  Run state               : online
  Config state            : normal
  Match state             : match
  DBA type                : SR
  ONT distance(m)         : 20011
  ONT battery state       : holding state
  Memory occupation       : 64%
  CPU occupation          : 1%
  Temperature             : 50(C)
  Authentic type          : SN-auth
  SN                      : 48575443D51DCB84 (HWTC-71FDCF76)
  Management mode         : OMCI
  Software work mode      : normal
  Isolation state         : normal
  ONT IP 0 address/mask   : 10.0.0.230/24
  Description             : ONU-0230
  Last down cause         : -
  Last up time            : 2018-04-16 19:15:41+08:00
  Last down time          : -
  Last dying gasp time    : -
  ONT online duration     : 1 day(s), 21 hour(s), 56 minute(s), 4 second(s)
  Type C support          : Not support
  Interoperability-mode   : ITU-T
  ------------------------------------------------------------------------------
  Line profile ID      : 5
  Line profile name    : GPON
  ------------------------------------------------------------------------------
  <T-CONT   0>           DBA Profile-ID:1
  <T-CONT   4>           DBA Profile-ID:12
  <Gem Index 230>
  ------------------------------------------------------------------------------
  Mapping   VLAN  Priority  Port  Port  Bundle  Flow  Transparent
  index                     type  ID    ID      CAR
  ------------------------------------------------------------------------------
     0       2       -         -    -      -       -         -
  ------------------------------------------------------------------------------
  Service profile ID   : 2
  Service profile name : HG8247H
  ------------------------------------------------------------------------------
  Port-type     Port-number              Port-type     Port-number
  ------------------------------------------------------------------------------
  POTS          adaptive                 VDSL          0
  ETH           adaptive                 TDM           0
  CATV          adaptive                 MOCA          0
  ------------------------------------------------------------------------------
  Port   Port Service-type Index S-VLAN S-PRI C-VLAN C-PRI ENCAP      S-PRI
  type   ID                                                          POLICY
  ------------------------------------------------------------------------------
  ETH    1    Translation  1     2      -     2      -     -          -
  ------------------------------------------------------------------------------
```

B Informace o připojených jednotkách ONU

Tab. B.1: Přehled připojených jednotek ONU.

Frame	Slot	Port	ONU ID	Typ ONU	SN	Popis
0	2	3	0	HG8247H	48575443D51DCB84	ONU-0230
			1	HG8247H	4857544371FDCF76	ONU-0231
			2	HG8245H	485754438009FE75	ONU-0232
			3	HG8245H	485754437E8E5975	ONU-0233
			4	HG8310M	485754438A755082	ONU-0234
			5	HG8310M	485754438A762C82	ONU-0235
			6	HG8310M	485754438A763682	ONU-0236
			7	HG8310M	485754438A764082	ONU-0237

Tab. B.2: Profily připojených ONU.

ONU ID	DBA profil	Lineprofile	GEM port	VLAN	Srvprofile	Service port
0	1000-Mbps	GPON	230	2	HG8247H	4
1	1000-Mbps				HG8247H	5
2	1000-Mbps				HG8245H	6
3	1000-Mbps				HG8245H	7
4	1000-Mbps				HG8310M	8
5	1000-Mbps				HG8310M	9
6	1000-Mbps				HG8310M	10
7	1000-Mbps				HG8310M	11

Tab. B.3: Další parametry připojených ONU.

ONU ID	Traffic table (ID)	IP adresa	Maska	Brána	DNS
0	1000-Mbps (11)	10.0.0.230	255.255.255.0	10.0.0.30	8.8.8.8
1	1000-Mbps (11)	10.0.0.231			
2	100-Mbps (10)	10.0.0.232			
3	100-Mbps (10)	10.0.0.233			
4	50-Mbps (9)	–			
5	50-Mbps (9)	–			
6	50-Mbps (9)	–			
7	50-Mbps (9)	–			

C Obsah přiloženého CD

- `/` ..... kořenový adresář přiloženého CD
  - `DP Bezpečnostní rizika PON.pdf` ..... elektronická verze práce
  - `LaTeX` ..... zdrojové soubory DP ze systému LaTeX
    - `cli` ..... zdrojové soubory výpisů
    - `fonty` ..... fonty jednotného vizuálního stylu VUT
    - `grafy` ..... zdrojové soubory grafů
    - `loga` ..... loga školy a fakulty
    - `obrazky` ..... obrázky použité v práci ve formátech jpg, png a pdf
    - `odn` ..... zdrojové soubory protokolu
    - `pdf` ..... pdf stránky generované informačním systémem
    - `tabulky` ..... zdrojové soubory tabulek
    - `text` ..... zdrojové textové soubory
    - `DP Bezpečnostní rizika PON.tex` ..... hlavní soubor pro sazbu DP
    - `thesis.sty` ..... modifikovaný balíček pro sazbu DP
  - `Obrázky` ..... fotodokumentace optické distribuční sítě
  - `Protokol.pdf` ..... protokol o provedeném měření
  - `Visio` ..... zdrojové soubory obrázků ve formátu vsdx