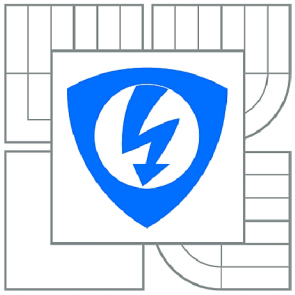
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

OPTICKÝ PŘENOS INFORMACÍ - BEZPEČNOST PŘENOSU

OPTICAL INFORMATION TRANSMISSION - TRANSMISSION SECURITY

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

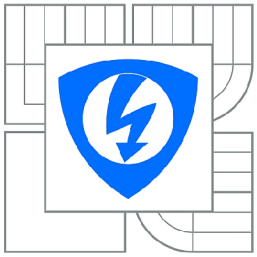
AUTOR PRÁCE — Bc. DÁVID KONDICZ

AUTHOR

VEDOUCÍ PRÁCE — prof. Ing. MILOSLAV FILKA, CSc.

SUPERVISOR

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Dávid Kondicz	***ID:***	98223
Ročník:	2	***Akademický rok:***	2014/2015

NÁZEV TÉMATU:

Optický přenos informací - bezpečnost přenosu

POKYNY PRO VYPRACOVÁNÍ:

Porovnejte bezpečnost optických přenosů s jinými přenosovými médii. Uvažujte provoz v různých prostředích. Zvažte možnosti před rušením, poškozením, výpadky a zaměřte se hlouběji na možnost odposlechu optického vlákna a následné možnosti zabezpečení odposlechu. Práci realizujte na dvou druzích vláken – gradietních a jednovidových a využijte různé spektrum vlnových délek. Zaměřte se i na legislativu, stavební zákon, úmyslné poškození, trestní zákon.

DOPORUČENÁ LITERATURA:

[1] FILKA, M. Optoelektronika pro telekomunikace a informatiku. CENTA, Brno 2009.
[2] FILKA, M. Přenosová média. Skripta laboratoře. VUT FEKT, Brno 2003.
[3] KUCHARSKI, M., DUBSKÝ, P. Měření přenosových parametrů optických vláken, kabelů a tras. Mikrokom, Praha 2001.
[4] Dostalík, M.: Elektrická zařízení v prostředí s nebezpečím výbuchu, FCC PS Brno, Automa 1/2001.
[5] Norma ČSN EN 60079-28 Výbušné atmosféry - Část 28: Ochrana zařízení a přenosových systémů používajících optické záření, Česká státní norma, 10/2007.

Termín zadání:	9.2.2015	***Termín odevzdání:***	26.5.2015

Vedoucí práce: prof. Ing. Miloslav Filka, CSc.
Konzultanti diplomové práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

Prehlásenie

Prehlasujem, že záverečnú diplomovú prácu na tému „Optický přenos informací - bezpečnost přenosu“ som vypracoval samostatne, pod vedením vedúceho diplomovej práce a s použitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej diplomovej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a som si plne vedomí následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia § 152 trestného zákona č. 140/1961 Sb.

V Brne dňa ....

podpis autora

Poďakovanie

Touto cestou chcem vyjadriť poďakovanie, prof. Ing. Miloslavovi Filkovi, CSc., za profesionálne vedenie, odborné rady, cenné a podnetné pripomienky pri vypracovaní diplomovej práce.

V Brne dňa .....

.....

podpis autora

Abstrakt

Predložená práca sa zaoberá problematikou optických prenosov a ich bezpečnosťou. Oboznámime sa s celou škálou možností prenosu informácie, na základe čoho vieme zhodnotiť výhody a nevýhody jednotlivých technológií v porovnaní s optickým prenosom informácie. Na základe získaných informácií sa pokúsime realizovať odpočúvanie optickej komunikácie poskytovateľa káblovej televízie.

Kľúčové slová:

Optický prenos, Rádiové spoje, FSO, LSOH, Odpočúvanie optickej komunikácie

Abstract

The submitted work deals with issues of optical transmissions and its security. We will become familiar with a variety of transferability of information, based on which we can assess the advantages and disadvantages of each technology as compared to optical information transmission. Based on acquired information we will try to implement interception of optical communication of cable TV provider.

Key words:

Optical transmission, Wireless networks, FSO, LSOH, Fiber network tapping

Obsah

Zoznam obrázkov

Zoznam tabuliek

ÚVOD

Nebolo to ešte tak dávno, keď sa tvrdilo, že najbezpečnejším prenosom informácií je optický prenos informácie. Bezpečnosť optického prenosu je relatívny pojem. Úroveň bezpečnosti nezáleží len na spôsobe prenosu informácie, použitej technológii, ale aj na zabezpečení prenosovej trasy. A to ako na fyzickej, tak aj na logickej úrovni. To, že sa informácia prenáša opticky, nemusí znamenať, že sa jedná o 100% garantované spojenie. Práve preto je pri projektovaní siete nutné počítať s ochrannými mechanizmami, ktoré napomôžu k dlhodobému, stabilnému a bezpečnému prevádzkovaniu siete. Pod tieto ochranné mechanizmy patrí aj samotná kruhová topológia, ktorá umožňuje fyzické kruhovanie a prezálohovanie sietí v prípade prerušenia jednotlivých trás.

Diplomová práca je zameraná na fyzické zabezpečenie telekomunikačných okruhov počnúc ich samotnou výstavbou a to pri optických aj bezdrôtových sieťach. Pozornosť upriamujeme na stavebnú legislatívu a právne pozadie v prípade úmyselného poškodenia dátových sietí a verejne prospešných zariadení. V rámci diplomovej práce porovnáme bezpečnosť jednotlivých prenosových systémov, na základe čoho zistíme ich skutočné výhody alebo nevýhody, prípadne oblasti, v ktorých je priestor na zlepšenie jednotlivých parametrov. Porovnáme aj bezpečnosť optického prenosu v nebezpečnom výbušnom aj horľavom prostredí a overíme možnosti ochrany optických vlákien v prípade požiaru.

Diplomová práca sa ďalej zaoberá možnosťami odpočúvania optického prenosu, za pomoci čoho zistíme, ako náročný môže byť takýto úkon a či je vôbec uskutočniteľný mimo laboratórnych podmienok. Pokus vykonáme na lokálnej počítačovej sieti a tiež v skutočnom prostredí káblového operátora na optickej trase, ktorá zabezpečuje distribúciu televízneho signálu k jednotlivým optickým nodom.

Na základe získaných skúseností ohľadom odpočúvania optického prenosu navrhneme ochranné opatrenia a postupy k eliminácii a identifikácii možného zásahu tretej osoby do optickej prenosovej trasy. Tieto skúsenosti sa následne pokúsime využiť v záujme monitorovania a včasnej detekcie možných problémov na optickej prenosovej trase ešte predtým, ako by malo dôjsť k prerušeniu samotného prenosu.

1. Porovnanie prenosových systémov

Prenos dát prostredníctvom optických sietí je výrazne rýchlejší a bezpečnejší ako je tomu v prípade prenosu dát prostredníctvom metalických a rádiových sietí. Je to hlavne z dôvodu, že pri prenose dát v optických sieťach nedochádza k takým útlmom, presluchom medzi vedeniami, alebo rušeniu prenosu zapríčineného elektromagnetickým žiarením z iných zdrojov. Výrazným rozdielom je šírka pásma jednotlivých prenosových systémov a možnosti modulácie signálov. Koaxiálne prenosové systémy podporujú šírku pásma zväčša do 1 GHz, štruktúrovaná kabeláž kategórie 6 približne 200 MHz a kategórie 7 približne 600MHz. Optické vlákna nám ponúkajú šírku pásma, ktoré viacnásobne prekračujú požiadavky dnešnej doby. Jedno vidové optické vlákno je schopné na vzdialenosť 100m preniesť šírku pásma až 5 THz. Prenosová rýchlosť jednotlivých systémov teda záleží od použitej modulácie, šírky prenosového pásma a samotného prostredia v ktorom sa informácie prenášajú.

Bezpečnosť jednotlivých prenosových systémov je rôzna. Určité prednosti vyplývajú už z použitej technológie, ale tie nemusia garantovať bezporuchovosť. V záujme čo najvyššej dostupnosti služieb je nutná implementácia dodatočných ochranných mechanizmov na rôznych úrovniach OSI modelu. V rámci bezpečnosti pred odpočúvaním je na tom najlepšie prenos dát prostredníctvom optických vlákien. Je to hlavne z dôvodu šírenia signálu prostredníctvom fotónov v uzavretom vlákne, v podstate s nulovými emisiami signálu v okolí vodiča.

2. Optický prenos informácií

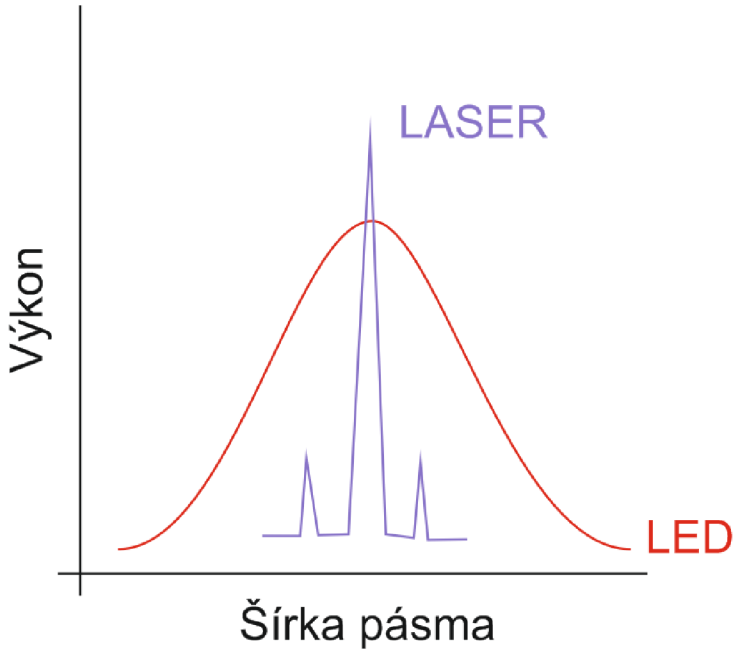
Azda najrozšírenejším spôsobom prenosov informácií, je prenos prostredníctvom optických vedení, optických vlákien. Pri optických prenosoch sa informácia prenáša fotónmi na určitej vlnovej dĺžke v okolitom prostredí, alebo vo svetelnom vodiči. Inými slovami v optickom vlákne.

V tomto prípade sa na prenos informácií využíva vlákno zložené z kremičitého skla SiO2, pričom útlm vlákna záleží hlavne od čistoty použitých materiálov. Takéto vlákna sú uspôsobené na prenos fotónov vo vlnových dĺžkach v rozmedzí približne od 1300 do 1600 nm. Takáto forma konštrukcie jedno vidového kábla nám zaručuje

extrémne rýchly prenos dát v svetelnom vodiči. Toto však ku spoľahlivej funkčnosti nestačí. Bezpečnosť a stabilitu prenosu dosiahneme výlučne kombináciou viacerých prvkov a mechanizmov. V prípade prenosu informácie prostredníctvom optických vlákien je najväčším problémom krehkosť samotného vlákna, čo nám sťažuje samotný proces inštalácie optických vedení. Za uplynulé roky sa situácia v tomto smere zmenila a dnešné optické vedenia je možné už pomerne jednoducho inštalovať. Tento priaznivý stav bol dosiahnutý nástupom nových optických vedení. Jedným z nich sú aj optické vodiče podľa ITU-T odporúčania ITU-T G.657, ktoré sa vyznačujú extrémne nízkym útlmom spôsobeným ohybom vodiča. Bežne je pri vedení tolerovaný ohyb 15 až 5 mm v závislosti od konkrétneho typu. Bežné využitie našli hlavne v prístupových optických sieťach, čo umožňuje ľahšie narábanie a inštaláciu vodičov napríklad v bytových rozvodniach a elektrických šachtách bez nutnosti dodatočnej ochrany. Fyzická ochrana je zabezpečená použitím viacvrstvovej ochrany vlákna a za pomoci ochranného opláštenia. Ochranný plášť okolo jadra zabezpečuje prioritne mechanickú pevnosť a odolnosť samotného kábla a to z dôvodu veľkej krehkosti optických vlákien. Konštrukcia ochranného plášťa môže byť rôzna, vzhľadom na prostredie, v ktorom má byť vedenie použité. Dôležitým faktorom konštrukcie je počet potrebných vlákien pre danú aplikáciu.

Ďalšou možnosťou optického prenosu je optický prenos vo voľnom prostredí. Táto technológia je tiež známa pod označením FSO – Free space optics. Jedná sa o zariadenie, ktoré obsahuje optický prijímač a vysielač, pričom sa vysielaný signál sústreďuje za pomoci šošoviek na určitú vzdialenosť vo voľnom prostredí. Táto technológia nám prináša vyššiu bezpečnosť pri prenose dát, ako je tomu v prípade bežne dostupných WiFi spojení.

Ako zdroj svetla je v oboch prípadoch možné použiť LED, alebo laserovú diódu. Každá z nich má svoje výhody a nevýhody. LED emitory sa vyznačujú nižšiu cenou a ich vlnová dĺžka je v rozmedzí od 850 do 1300nm. Ich nevýhodou je široké pásmo vyžiareného svetla a nižší výkon, čím je znemožnená integrácia viacerých vlnových dĺžok do jedného vlákna.

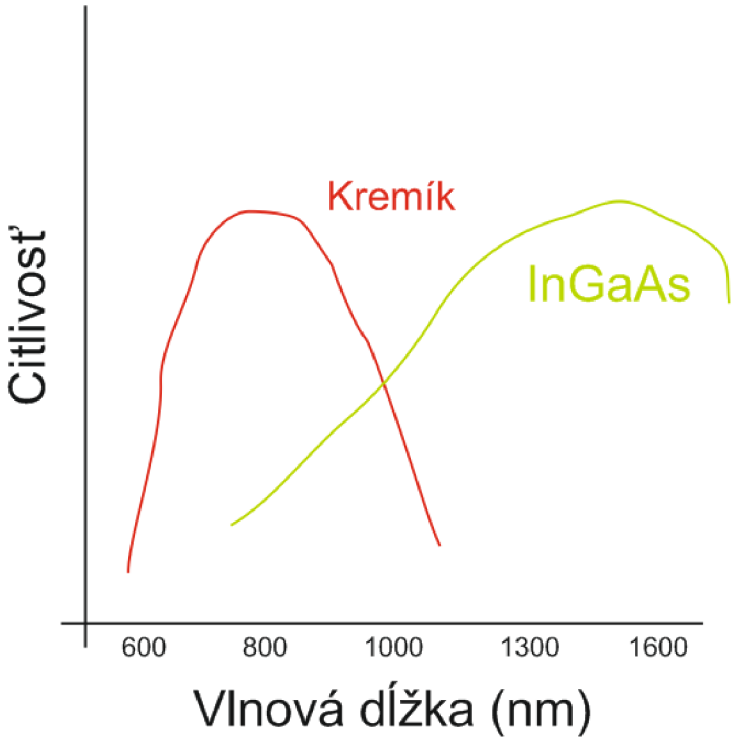


Obr. 2.1: Porovnanie výkonu a spektrálnej šírky pásma LED a laserového emitoru

Tab. 2.1: Porovnanie technických parametrov optických emitorov

Typ	Vlnová dĺžka (nm)	Výkon (dBm)	Frekvencia	Typ opt. vlákna
LED	850 až 1300	Od -30 do -10	<250 MHz	MM
FP Laser	850, 1310 (1280-1330) 1550 (1480-1650)	Od 0 do +10	>10 GHz	MM, SM
DFB Laser	1550 (1480-1650)	Od 0 do +25	>10 GHz	SM
VCSEL	850	Od -10 do 0	>10 GHz	MM

Na príjem svetelného signálu sa používajú foto-diódy alebo foto-detektory, za pomoci čoho prevádzame optický signál späť na elektrický. Na tento účel sa používajú kremíkové fotodiódy. Tie majú najlepšiu citlivosť v rozmedzí okolo 700 až 900 nm. Pre vyššie vlnové dĺžky sa používajú Germániové, alebo InGaAs - indium galium arzenitové detektory.

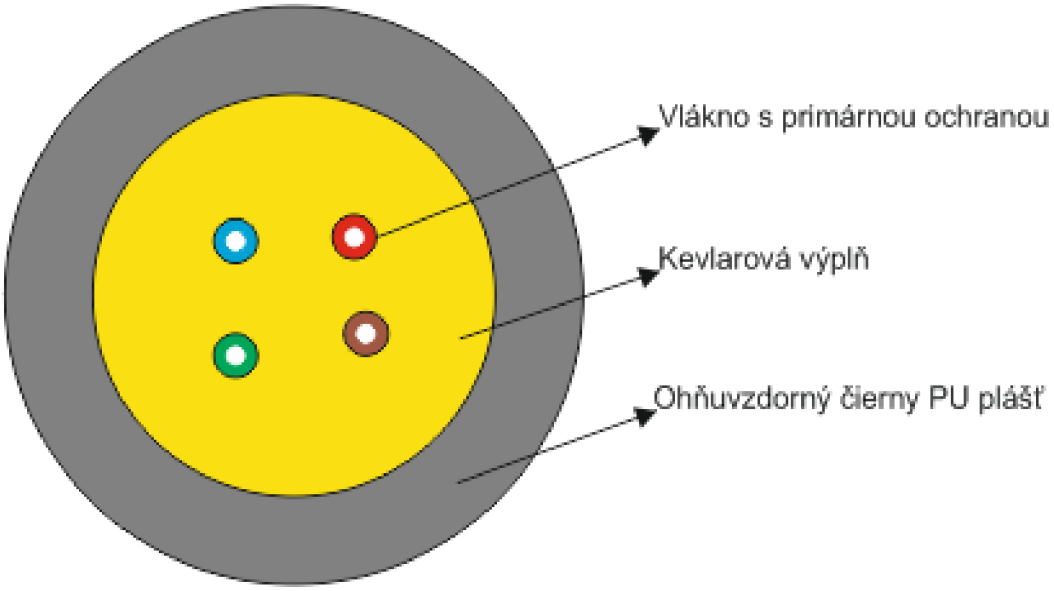


Obr. 2.2: Porovnanie citlivosti foto detektorov vzhľadom na vlnovú dĺžku.

Prenášanie fotónov nesprevádza elektromagnetické pole, čo je dôvodom, že prenášané informácie mimo trasy alebo vedenia nie je možné odsledovať. Výhodou optického prenosu informácií je, že nie je nutné vynakladať veľkú námahu na zabezpečenie a utajenie prenášanej informácie komunikačným kanálom. Toto nemôžeme povedať pri prenose informácie rádiovým prostredím, kde vysielané informácie môže prijať ktokoľvek, v rámci smerovosti rádiového spojenia. V tomto prípade je nutné zabezpečiť utajenie informácie ešte pred samotným odvysielaním do okolitého prostredia, pričom účastník, ktorému je informácia zaslaná, musí byť schopný prenesenú informáciu odtajiť.

2.1 Vnútorné optické vedenia

Používajú sa na optické prenosy v rámci objektov a vyznačujú sa jednoduchšou konštrukciou za účelom ľahkého narábania a inštalácie, pričom majú odolať pri bežnom použití v kancelárskych a domácich podmienkach. V drvivej väčšine sa jedná o vertikálne vedenia v bytových domoch. Ich konštrukcia len minimálne odoláva mechanickému namáhaniu a preto je nutné tieto káble umiestniť do líšt, alebo podľa konštrukcie kábla do mikrotrubičiek. Pre tieto účely sa najčastejšie využívajú drop káble, ktoré sú určené na pripojenie koncového užívateľa k pripojovaciemu bodu umiestneného zväčša v tej istej budove. Tieto káble majú však minimálnu mechanickú odolnosť a sú stavané skôr na záťaž v ťahu. Aj z tohto dôvodu majú optické drop káble pod nehorľavým plášťom hustejšiu kevlarovú výplň.



Obr 2.3: Konštrukcia Samsung drop optického kábla SM9/125

Drop káble sa vyznačujú výbornou ohybnosťou a nízkym polomerom ohybu. Je to vďaka tomu, že sa jedná o optické vlákna typu G.657.

Ďalšou z možností pre vnútorné inštalácie je použitie mikrokáblov alebo káblových zväzkov. Mikrokáble majú ešte menšiu úroveň ochrany a preto ich použitie

je možné výlučne v kombinácii s mikrotrubičkami. Toto riešenie je veľmi rozšírené pri poskytovaní služieb FTTH prostredníctvom pasívnej G(e)PON siete. Mikrotrubičky pri uvedenom riešení uľahčujú a zjednodušujú celkovú inštaláciu. V prvom kroku sa inštaluje samotná mikrotrubička bez osadeného vlákna. Následne keď je osadená, zafukuje sa do nej mikrokábel za pomoci čoho nám mikrokábel vyústi priamo v byte účastníka. Mikrotrubičky sa vyrábajú z tvrdeného plastu a neslúžia len ako ochrana pred mechanickým poškodením vlákien a káblov, ale uľahčujú aj samotnú inštaláciu. Bežne sa využívajú v panelových domoch pri budovaní prístupových sietí typu FTTH – „Fiber to the Home“. V takomto prípade sa k bytom jednotlivých potenciálnych užívateľov privedú z prípojného miesta telekomunikačného operátora prázdne mikrotrubičny, do ktorých sa v prípade potreby zafúkne zväzok optických káblov, alebo len samotné vlákno. Z hľadiska poskytovania telekomunikačných služieb koncovým užívateľom prostredníctvom optických sietí, je takáto forma mechanickej ochrany základom pre zabezpečenie bezpečného a spoľahlivého optického prenosu.

V poslednej dobe stále viac naberajú na popularite špeciálne pred konektorované káblové systémy napríklad od výrobcu Riser, ktoré sa konštrukčne snažia napodobniť riešenie mikrokábla v kombinácii s mikrotrubičkou. Riser ponúka 12 alebo 24 vláknové predkonektorované káble s tvrdeným ochranným plášťom, ktorý sa dá v mieste potrebnom na zriadenie účastníka jednoducho narezať. Týmto spôsobom docielime, že nie je nutné inštalovať mikrotrubičky pre každého účastníka, ale stačí natiahnuť toto vedenie vertikálne na najvyššie poschodie obytného domu s dostatočnou rezervou.

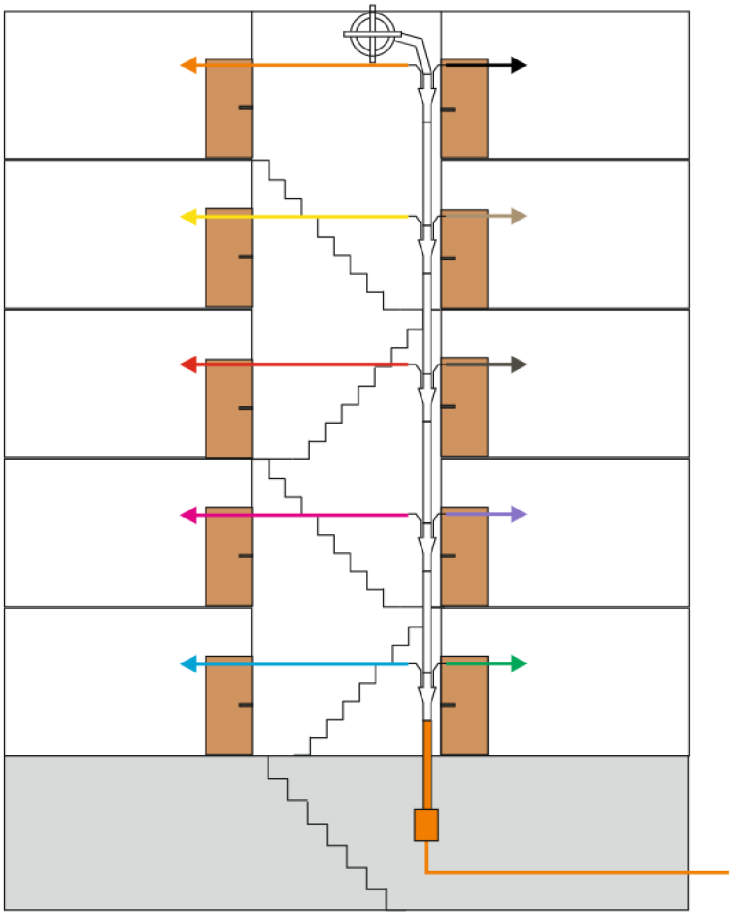
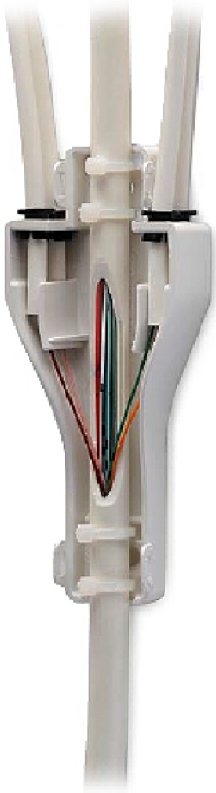


Schéma zapojenia Riser 12vl v obytnom dome



Odbočka horizontálna

Obr. 2.4: Riešenie vertikálnych rozvodov technológiou Riser

Vzhľadom na použitú technológiu môžeme konštatovať, že sa jedná o bezpečnú technológiu, ktorá je pripravená na stopercentnú penetráciu.

2.2 Vzdušné optické vedenia

Základným rozdielom vonkajších optických vedení oproti vnútorným, z hľadiska bezpečnosti a spoľahlivosti dlhodobej prevádzky, je ich odolnosť proti UV žiareniu. Táto vlastnosť vonkajších, hlavne nadzemných vedení rázne predlžuje ich životnosť. Ďalšou významnou vlastnosťou vonkajších vedení je ich mechanická odolnosť voči poveternostným podmienkach, ako sú námraza, vietor, vysoké teploty a podobne. Tieto vlastnosti sú zabezpečené za pomoci použitia špeciálnych materiálov akými sú napríklad kevlar, gél a sadze na zvýšenie odolností proti UV žiareniu. Okrem

poveternostných podmienok je veľkým problémom napríklad inštalácia vedení naprieč korún stromov, kde sa po čase vplyvom vetra a samotných konárov stromov, vedenia poškodzujú. Vysoká odolnosť káblov sa zabezpečuje tiež vďaka polyetylénu a jeho kombinácii s rôznymi katalyzátormi, čím sa dá regulovať ich odolnosť voči UV žiareniu a mechanická pevnosť.

Vzdušné optické siete sa využívajú na vysokorýchlostný prenos signálov v rámci chrbticovej siete, ale ponúkajú aj možnosti pripájania koncových užívateľov, čo je aj z dôvodu vlastností optických vlákien sťažujúcim faktorom. Na pripojenie koncových užívateľov je nutná inštalácia vodotesných hrncových spojok, kde sa hlavné vedenie preruší, pasívne rozbočí a prevarí s vláknom, ktoré vedie k účastníkovi.

Z hľadiska bezpečnosti je nutné podotknúť dodržanie ochranných pásiem od iných inžinierskych sietí a dodržanie minimálnej výšky vedenia nad zemou. Z hľadiska bezpečnosti prenosu dát je úroveň bezpečnosti rovnaká ako je to v prípade iných optických sietí. Úroveň spoľahlivosti, stability a časovej dostupnosti služieb v rámci vzdušných sietí je ovplyvnená faktom, že vedenia sú namáhané a zaťažované vonkajšími vplyvmi.

Najväčším problémom vzdušných vedení je fakt, že od roku 2004 je výstavba vzdušných sietí v intraviláne miest a obcí zakázaná.

2.3 Zemné optické vedenia

V prípade podzemných optických vedení je situácia o niečo iná z dôvodu, že podzemné vedenia môžu byť rozličného typu a môžu byť uložené viacerými spôsobmi. Je nutné si uvedomiť, aké služby budú prevádzkované cez dané vedenie a aké škody spôsobí prípadný výpadok služby. V dôsledku toho je nutné myslieť na ochranu vedenia ešte pred zahájením stavby.

Bežnou ochranou pred poškodením podzemných vedení je podľa STN uloženie výstražnej fólie približne 20 až 30 centimetrov nad samotné vedenia, ktorý je do úrovne výstražnej fólie zakopaný piesočnou zemou. V prípade náročnejších aplikácií sa hlavne v zastavaných územiach alebo na miestach s väčším výskytom inžinierskych sietí, požívajú ochranné platne, ktoré upozorňujú pri výkopoch v blízkosti vedení, že sa tam

v bezprostrednej blízkosti nachádza telekomunikačné, alebo iné vedenie. Na rozdiel od výstražnej fólie zabezpečia dodatočnú mechanickú ochranu vedenia pri rozkopávke.

Obr. 2.5: Vzor výstražnej fólie

Obr. 2.6: Vzor ochrannej plate

V extrémnych prípadoch sa používajú betónové káblové žľaby, ktoré zabezpečujú najvyššiu úroveň ochrany vedenia pred poškodením, ktoré môžu vzniknúť

dôsledkom výkopových prác. V prípade poškodenia je možné jednotlivé elementy ľahko vymeniť. Uvádzaná forma ochrany vedenia je finančne veľmi nákladná aj z dôvodu, že do žľabov sa nepokladá priamo vedenie, ale najprv sa uloží chránička, ktorá zabezpečuje lepšiu manipuláciu s optickým vedením po zahrnutí káblového žľabu. Následne je do chráničky možné kedykoľvek zafúknuť optické káble požadovaných parametrov. Zabezpečenie telekomunikačného vedenia takýmito prostriedkami sa používa hlavne v miestach, kde sa následne po udusaní stavia cestná komunikácia alebo aj pozdĺž železničných tratí . Obdobné riešenia sa obľubou využívajú vo väčších mestách, kde sa takéto káblové kanály prenajímajú od mesta za účelom rýchlejšej a menej deštruktívnej výstavby podzemných inžinierskych sietí.

Obr. 2.7: Betónový káblový žľab

V dávnejších dobách sa takáto úroveň ochrany optického vedenia zabezpečila pokládkou pálených tehál tesne nad optické vedenia. Takúto formu ochrany vedenia používali aj slovenské telekomunikácie na svojich diaľkových optických trasách. Významným ochranným faktorom v extraviláne je popri spomenutých ochranných prvkoch aj hĺbka uloženého vedenia.

Často krát sa stáva, že sa pri výkope vedenie nepoškodí úplne, ale len čiastočne. Buď dôjde k poškodeniu chráničky alebo obalu optického kábla. Pokiaľ dôjde k poškodeniu vlákien, miesto poškodenia môžeme s veľkou presnosťou zistiť pomocou zariadenia OTDR. V prípade, že ku poškodeniu vlákna nedošlo, poškodená chránička sa lokalizuje za pomoci detekčného plynu.

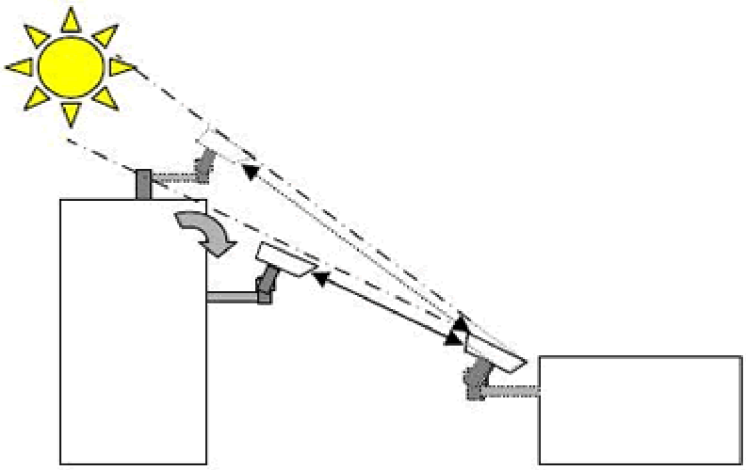
K bezpečnosti a stabilite prenášaných informácií prostredníctvom optických sietí prispieva popri konfigurácii aktívnych prvkov aj spôsob vedenia alebo uloženia optických káblov. Preto môžeme jednoznačne určiť, že najvyššiu mieru stability a zabezpečenia prenosu pred výpadkami nám poskytnú podzemné optické siete. Tie sa po legálnej výstavbe stávajú verejnou komunikačnou sieťou a sú legislatívne chránené. „Osoba, ktorá úmyselne poškodzuje alebo ohrozuje prevádzku všeobecne prospešného zariadenia podľa § 286 Trestného zákona číslo 300/2005 Zbierky zákonov v znení zákona číslo 576/2009 Zbierky zákonov sa dopúšťa trestného činu a môže byť potrestaný odňatím slobody na štyri roky až osem rokov.

V porovnaní legislatívnej ochrany optickej prenosovej siete s rádiovou sieťou sa situácia mení. Na rozdiel od podzemných optických sietí, pri rádiových sieťach nie je možné zriadenie ochranných pásiem. Jediné zabezpečenie pred rušením je koordinácia vlastných frekvencií, čo zabezpečí vydanie individuálneho povolenia, čím má operátor výhradné právo na využitie danej frekvencie na danom spoji. Negarantuje to však náhodné ani úmyselné rušenia inými operátormi, ktoré sa ťažko odhaľujú a ešte ťažšie dokazujú. Za masívne nasadenie rádiových spojov môžu hlavne nízke obstarávacie náklady a možnosť ich rýchleho nasadenia.

2.4 Optický prenos informácií vo voľnom prostredí

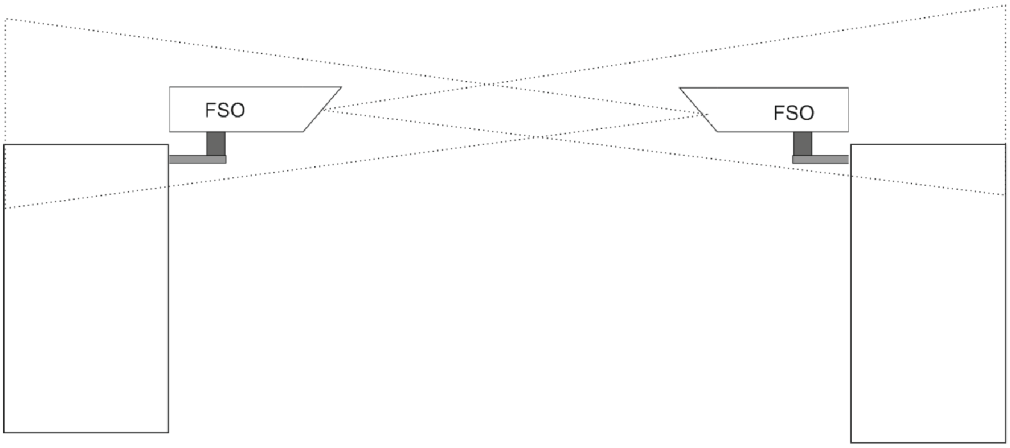
Medzi optickú formu komunikácie zahŕňame aj prenos informácií cez laserové spoje, ktoré poznáme pod názvom „Free Space Optics“. Táto technológia je v dnešnej dobe už na ústupe a používa sa skôr pri veľmi špecifických aplikáciách alebo tam, kde nie sú kladené veľké požiadavky na časovú dostupnosť spojenia hlavne vplyvom poveternostných podmienok. Nasadzujú sa hlavne v miestach, kde sú nelicencované pásma preplnené a použitie licencovaného pásma je neefektívne. Technológia FSO „Free space optics“, sa zakladá na smerovosti optického lúča, zväčša o vlnovej dĺžke na

rozhraní viditeľného spektra vo voľnom prostredí. Zariadenia FSO majú uspôsobený výkon aj rozptyl optického lúča na základe vzdialenosti, na ktorú je daný spoj požadovaný. Táto technológia sa vyznačuje vysokou úrovňou bezpečnosti prenosu dát, nakoľko sa na prenos využíva smerový lúč zväčša o vlnovej dĺžke 785 nm a práve úzka smerovosť zabezpečuje vysokú bezpečnosti prenosu a to z dôvodu, že potenciálny útočník musí byť schopný detekovať prenosový signál v danej úzkej trase. Nevýhodou uvedeného spôsobu optického prenosu je časté rušenie poveternostnými podmienkami, znečisťovaním šošoviek a slnečným žiarením v prípade, že jednotlivé strany spoja mali významný výškový rozdiel.



Obr. 2.8: Rušenie optického prenosu vplyvom slnečného žiarenia

Okrem toho tiež môže vzniknúť riziko odchytu niektorého z lúčov tesne pri jednom zo zariadení. Daný lúč je možné externým detektorom a sústavou šošoviek prijať a následne analyzovať prenášané informácie, ktoré prenosovým kanálom nie sú nijako dodatočne šifrované, alebo inak chránené.



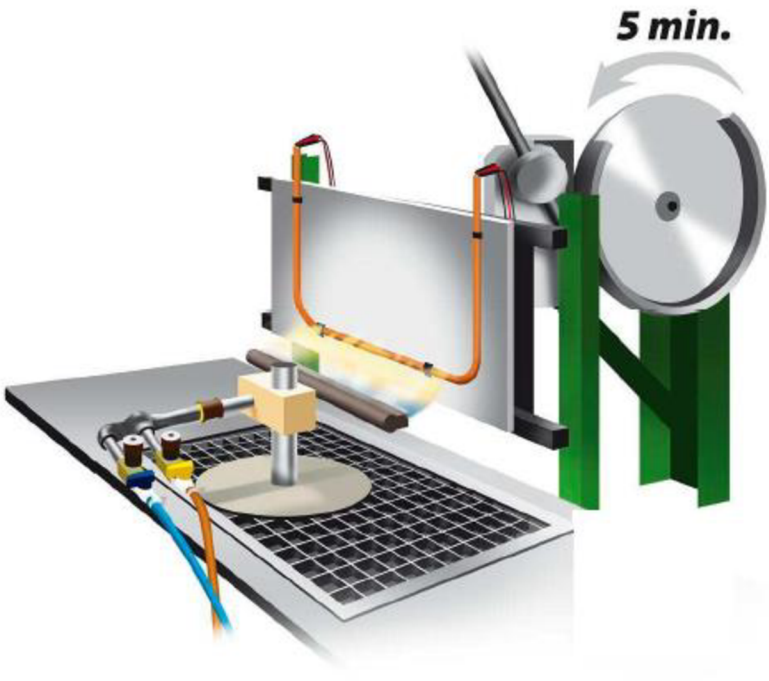
Obr. 2.9: Rozptyl svetelného lúča pri použití technológie FSO

Na základe uvedených informácií môžeme usúdiť, že za účelom odpočúvania komunikácie prenosového kanálu je vo väčšine prípadov nutný prístup k vedeniu, alebo zariadeniu prostredníctvom ktorého sa požadované informácie prenášajú.

2.5 Optický prenos informácií v prostrediach s nebezpečenstvom výbuchu

V prípade inštalácie optických rozvodov do budov je nutné zvažovať aj požiarno-bezpečnostné predpisy. Tieto môžu okrem iného stanoviť aj druh použitého kábla, aj opláštenia. V prípade objektov ako sú parkoviská, hotely a kancelárske priestory, je nutné pri výstavbe rátať s použitím káblov, ktorých plášť je vyrobený z bez halogénových, takzvaných LSOH - Low smoke zero halogen materiálov. Bez halogénový plášť LSOH podľa STN-IEC 60332-1 má zabrániť šíreniu plameňa, má nízku hustotu dymu pri horení, ale samotné optické vlákna nijakým spôsobom pred následkami ohňa neochráni. Slúži hlavne ako prevencia na zníženie následkov požiaru.

Pre signalizačné optické káble do výbušného a horľavého prostredia je nutné použiť špeciálne, na to uspôsobené káble, ktoré garantujú minimálnu dobu funkčnosti aj v prípade vystavenia priamemu ohňu. Vlastnosti káblov na tento účel sú definované normou STN EN 50200 a STN EN 50362.



Obr. 2.10: Princíp skúšobnej metódy vodičov

Pri tomto princípe skúšobnej metódy je vzorka kábla umiestnená na platňu, na ktorú v nepravidelných intervaloch pôsobia mechanické rázy, pričom na vzorku kábla pôsobíme otvoreným plameňom o konštantnej teploty 842°C. Vzorka kábla je pritom pripojená na skúšobný elektronický obvod. Počas skúšky nemôže dôjsť k prerušeniu komunikácie a v prípade metalických vedení ani ku skratu medzi vodičmi.

Použitie optických prenosových systémov vo výbušnom prostredí stanovuje norma IEC EN 60079-28. Vo výbušných prostrediach vzniká riziko vznietenia, ktoré môže byť spôsobené hlavne zdrojmi svetelného signálu ako napríklad lasery a LED diódy. Existujú štyri možné mechanizmy vznietenia:

- Optické vyžarovanie je absorbované povrchom, čím za určitých podmienok môže dôjsť k dosiahnutiu teploty, ktorá spôsobí vznietenie okolitého výbušného prostredia.
- Vznietenie teplom u objemu plynu, pokiaľ je vlnová dĺžka a výkon svetelného signálu zhodná u absorpčným rozsahom plynu.
- Vznietenie fotochemickou cestou v dôsledku svetelného rozkladu molekúl kyslíku žiarením v ultrafialových vlnových dĺžkach.

- Priamym rozkladom plynu v ohnisku spôsobeného silným prúdom laseru, za vzniku plazmy a rázovej vlny.

Napriek spomenutým možnostiam je pravdepodobnosť vznietenia výbušného plynu spôsobeného optickým prenosom cez optický kábel veľmi nepravdepodobná. V záujme ochrany pred výbuchom je možné použiť nasledovné techniky:

- Zabezpečiť zdroj svetelného signálu s vlastnou bezpečnou úrovňou čo znamená viditeľné vyžarovanie, alebo infračervené vyžarovanie, ktoré nie je schopné dodať dostatočnú energiu pre vznietenie danej výbušnej atmosféry.
- Chránené optické vyžarovanie, ktoré vyžaduje, aby zariadenie bolo uzatvorené vo vnútrajšku optického vlákna, alebo iného prenosového média za predpokladu, že vyžarovanie nemôže z uzatvoreného prostredia unikať.
- Blokovanie optického vyžarovania pri prerušení optického vlákna, ktoré je nutné použiť, keď vyžarovanie nemá vlastnú bezpečnú úroveň a je zabezpečená blokovaním, ktoré pri poruche ochrany zapôsobí v čase podstatne kratšom ako je doba potrebná na vznietenie.

Bezpečné optické výkony a intenzitu pre nebezpečné prostredia sú stanovené v tabuľke 2.2.

Tab. 2.2: Bezpečné hodnoty optického výkonu a intenzity pre nebezpečné priestory

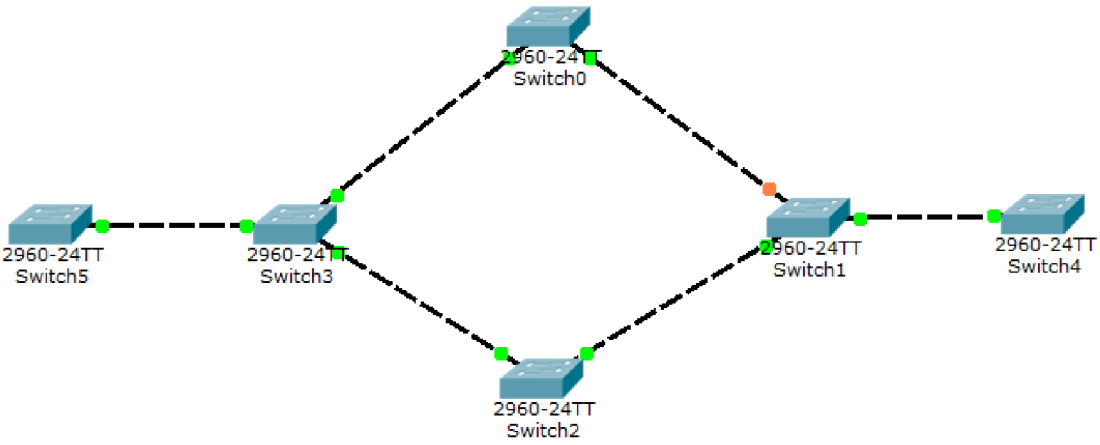
Skupina zariadení	I	IIA	IIA	IIB	IIC	
Teplotná trieda		T3	T4	T4	T4	T6
Teplotná trieda °C	≤ 150	≤ 200	≤ 135	≤ 135	≤ 135	≤ 85
Výkon (mW)	150	150	35	35	35	15
Intenzita(mW/mm2)	20a	20a	5	5	5	5

2.6 Bezpečnosť optického prenosu informácií

Prenos informácií prostredníctvom vedení sa javí za veľmi spoľahlivý spôsob prenosu informácií. Vysoká spoľahlivosť je docielená dodržaním viacerých krokov a predpisov, ktoré začínajú ešte pred samotnou výstavbou optickej siete. V záujme zabezpečenia čo najdlhšej životnosti a vzhľadom k možnostiam a požiadavkám, je možné rozdeliť optické siete na vnútorné, vonkajšie a zemné optické vedenia.

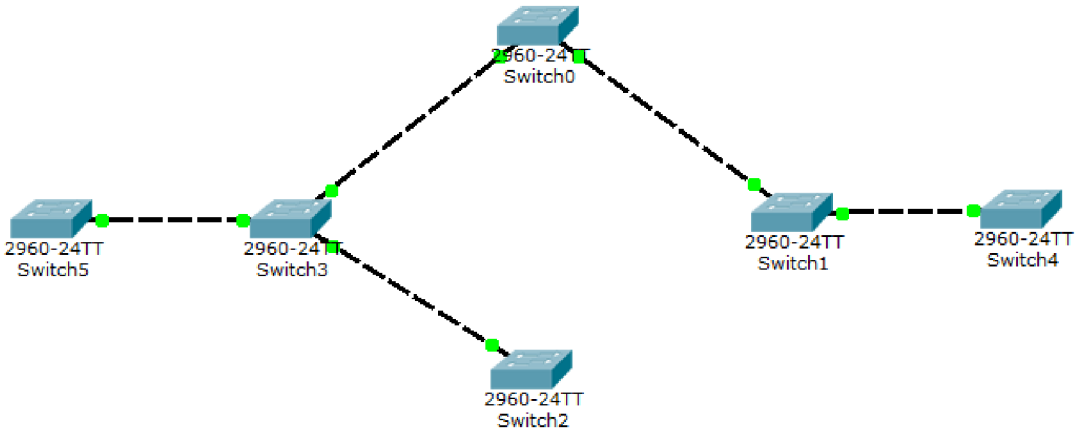
Možnosti vedenia trasy, ako aj jej výstavby v rámci územného konania určuje a schvaľuje stavebný úrad. Ten na základe rozsahu projektu určuje možnosti inštalácie vedení, alebo možnosti rozkopávky vzhľadom na existujúce inžinierske siete. Práve z dôvodu stavebného konania je nutné oboznámiť prevádzkovateľov inžinierskych sietí o zámere výstavby novej optickej siete, na základe čoho sa vykoná zameranie a vytýčenie hlavne podzemných sietí. Pri výstavbe nových sietí je nutné rešpektovať už jestvujúce siete a dodržiavať ochranné pásma medzi nimi ako aj predpísanú hĺbku v prípade podzemných sietí. Stavebné konania môžu extrémne predĺžiť proces výstavby optických sietí a to hlavne v prípade vysokej hustoty inžinierskych sietí na plánovanej trase novej siete, ale práve tento krok prispieva k zabezpečeniu bezporuchovej prevádzky telekomunikačných sietí. Hlavný prínos je v informovanosti prevádzkovateľa sietí o plánovaných výstavbách v rámci trasy vedení, čím je možné zamedziť poškodeniu vedení, ešte pred samotným zahájením stavby. Momentom kolaudácie stavby a jeho odovzdania do užívania. Telekomunikačné siete sú považované za verejnoprospešné zariadenia a páchatelia sa v prípade poškodenia dopúšťajú trestného činu, čo väčšinu ľudí odrádza od podobného konania, prípadne nelegálnej výstavbe vedení.

Okrem legislatívnej ochrany siete sa pred poškodením používa niekoľko ochranných mechanizmov. Tie sa zväčša aplikujú v prípade prenosu cez manažovateľné prepínače alebo prostredníctvom SDH zariadení. V prípade najrozšírenejších paketových sietí sa siete kruhujú už na prístupovej vrstve za pomoci protokolov STP a RSTP. Tieto protokoly umožňujú nahradenie poškodenej prenosovej trasy inou funkčnou trasou, zväčša bez zníženia prenosovej rýchlosti. Bežný scenár môžeme vidieť na obrázku 2.11.



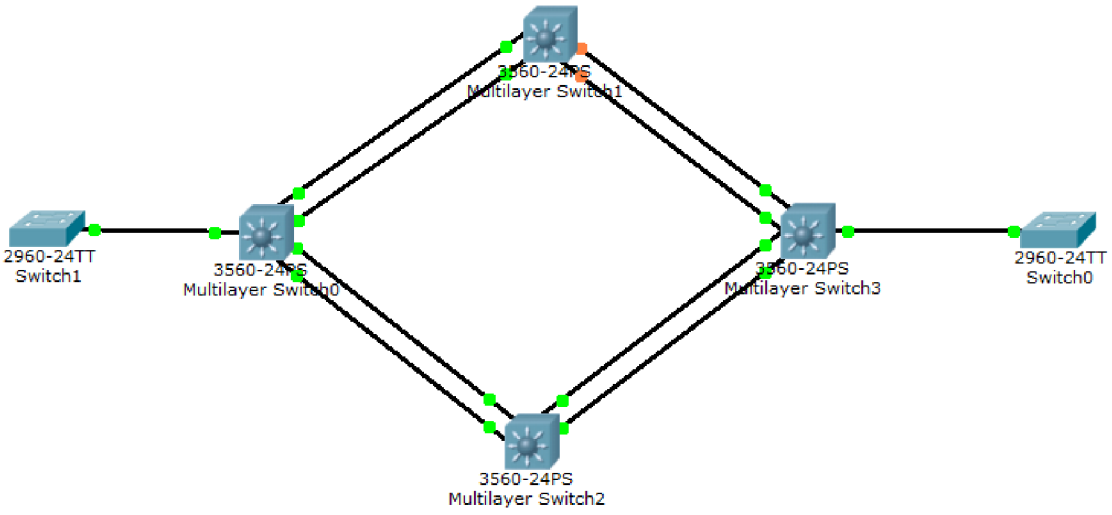
Obr. 2.11: Kruhové zapojenie prepínačov s režimom STP

V prípade kruhového zapojenia jeden z prepínačov buď automaticky, alebo manuálne zastaví jedno rozhranie, aby sa nezacyklovala sieť. Toto rozhranie je však v režime načúvania a keď sa primárna trasa preruší, tak prepínač uvoľní blokované rozhranie. Blokované rozhranie je na obrázku označené oranžovou farbou. Konvergencia uvedenej zálohy však nie je najrýchlejšia a záleží od časovačov nastavených v prepínačoch.



Obr. 2.12: Konvergencia siete pri prerušení primárneho vedenia

Obrázok 2.12 znázorňuje oživenie blokovaného rozhrania v prípade výpadku hlavnej linky. Ďalšou z možností zálohovania liniek na prístupovej úrovni je možnosť použitia protokolov LAGP a PAGP, v skratke link aggregation protokol, alebo port aggregation protokol. Tieto protokoly prioritne slúžia na rozdeľovanie záťaže medzi jednotlivé rozhrania, vďaka čomu nám poskytujú možnosť automatickej zálohy v prípade poškodenia jedného z fyzickým spojení medzi prepínačmi. Pri použití protokolov PAGP a LAGP nie je možné kruhovanie sietí. Slúžia výlučne na prepojenie dvoch zariadení za pomoci dvoch až ôsmich fyzických rozhraní, pričom všetky rozhrania musia byť úplne rovnako nastavené a musia byť úplne rovnako v jednej skupine. Pri použití týchto protokolov je možné docieliť extrémne rýchlu konvergenciu v prípade poruchy jednej z liniek. Doba konvergencie sa tu pohybuje rádovo v milisekundách. PAGP a LAGP je možné nasadiť aj v kruhovaných sieťach a to prioritne za účelom zvýšenia prenosových kapacít. Scenár použitia protokolov PAGP alebo LAGP je znázornený na obrázku 2.13



Obr. 2.13: Kruhové zapojenie prepínačov s režimom STP v kombinácii s LAGP/PAGP

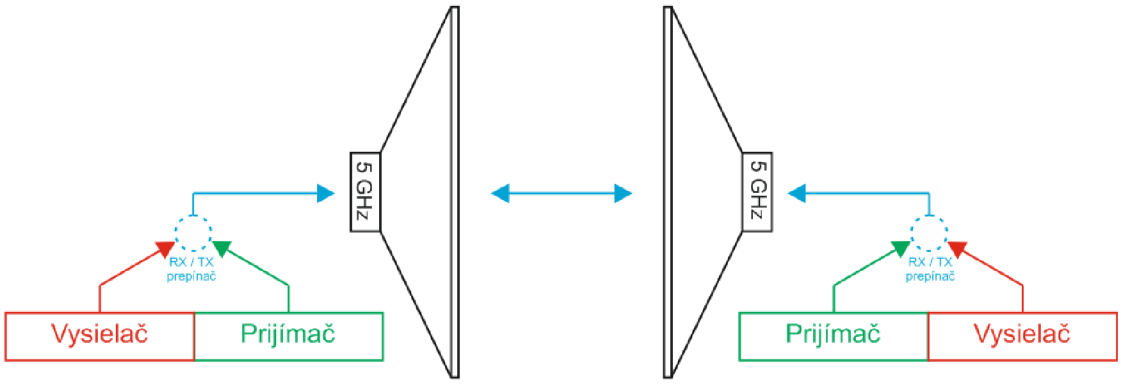
Toto riešenie neposkytuje vyššiu rýchlosť konvergencie, tá je rovnaká ako je tomu v prípade použitia STP.

3. Bezkáblový a káblový prenos informácií

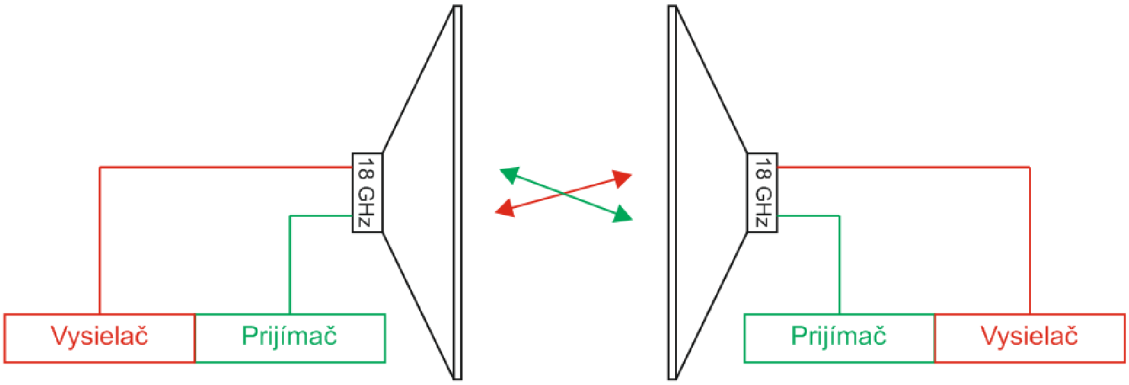
Ďalším veľmi obľúbeným a využívaným spôsobom prenosu informácií je bezdrôtový rádiový prenos informácií, ktorý je zabezpečený elektromagnetickým vlnením na určitých frekvenciách s určitou smerovosťou.

Výber frekvencie je na základe konkrétnych požiadaviek na prenosovú kapacitu a vzdialenosť, na ktorú majú byť informácie prenášané. V prvom rade sa stanovuje požadovaná dostupnosť spoja v roku pri určitej prenosovej kapacite. V prípade náročných aplikácií sa volia frekvenčné pásma, s nižším útlmom rádiových vĺn voči molekulám vody alebo kyslíka. Určité frekvenčné pásma totiž reagujú s čiastočkami vody a kyslíku v prostredí, čím vzniká nežiaduci útlm. Pásma, pre ktoré je tento jav charakteristický sú určené zväčša ako voľné, nelicencované pásma. Vzhľadom na náročnosť spojenia je možné rádiové prenosové systémy využívať v takzvaných voľných licencovaných alebo nelicencovaných pásmach.

Voľné pásma sú určené na menej náročné aplikácie, kde sa nevyžaduje vyhradenosť prenosového pásma na konkrétny spoj. Využívanie voľných pasiem je na základe všeobecného oprávnenia vydaného regulátorom. Na základe toho sú stanovené jednotné pravidlá a obmedzenia, ktoré umožňujú uvedené pásma využívať. Najčastejšie sa využíva pásmo 2400MHz, 5500-5700MHz, 10 GHZ (pre ČR), 24 GHz a 60+ GHz. Najväčším obmedzením voľných pásiem sú interferencie od iných zariadení často využívajúcich frekvenčný kanál a nízke vyžiariteľné výkony rádiokomunikačných zariadení, ktoré sú práve stanovené všeobecným oprávnením regulátora. Na základe vplývajúcich faktorov sa v uvedených pásmach využíva takzvaná polo duplexná komunikácia v spojení s nižšie stavovou moduláciou, čo spôsobuje vyššie, až nestabilné odozvy. Obrovskou výhodou je nízka cena zariadení určených pre tieto pásma a schopnosť fungovať obojsmerne na jednej frekvencii.



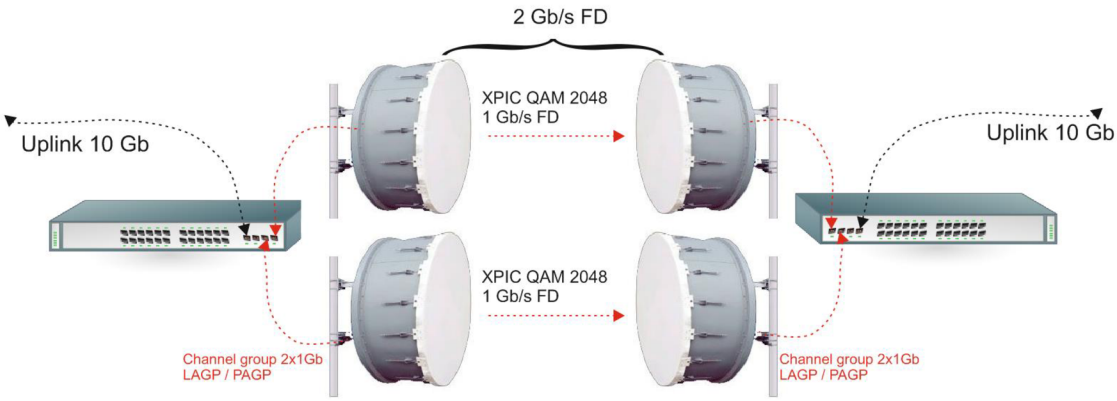
Obr. 3.1: Polo duplexný bezdrôtový prenos



Obr. 3.2: Plne duplexný bezdrôtový prenos

Licencované pásma sú určené na náročnejšie aplikácie. Jedná sa o rozličné frekvenčné pásma, ktoré vyčlenil regulátor na základe plánu využitia frekvenčného spektra. V týchto pásmach je možné vysielať a prevádzkovať bezdrôtové spoje výlučne prostredníctvom individuálneho oprávnenia. Významom oprávnenia je vzájomná koordinácia jednotlivých rádiokomunikačných zariadení, aby nemohlo dôjsť k vzájomnému rušeniu. Vďaka tomu sa výskyt interferencií a rušenia eliminuje na minimum čo umožní nasadenie vysokokapacitných prenosových systémov s vysokou úrovňou stability a spoľahlivosti. Vo väčšine prípadov sa jedná o plne duplexné, obojsmerné prenosové systémy, vďaka čomu sa dosahuje odozva na úrovni optických a metalických sietí. Dnešné bezdrôtové prenosové systémy bez akýchkoľvek problémov dosahujú prenosové rýchlosti cez 1,2 Gb/s a chybovosť 10E-12. Pre zvýšenie prenosovej kapacity je možné spájanie prenosových kanálov, prípadne komunikácia na viacerých polarizáciách prostredníctvom technológie MIMO alebo XPIX. V prípade, že by uvádzané kapacity nepostačovali, je možné spájanie viacerých xpic spojov do jednej

prenosovej skupiny. Toto sa dá docieliť na vrstve L2 alebo L3 OSI/ISO za pomoci manažovateľných prepínačov vďaka protokolom PAGP alebo LACP. Port agregation protokol zabezpečuje rozloženie záťaže medzi viaceré fyzické rozhrania na prepínači.



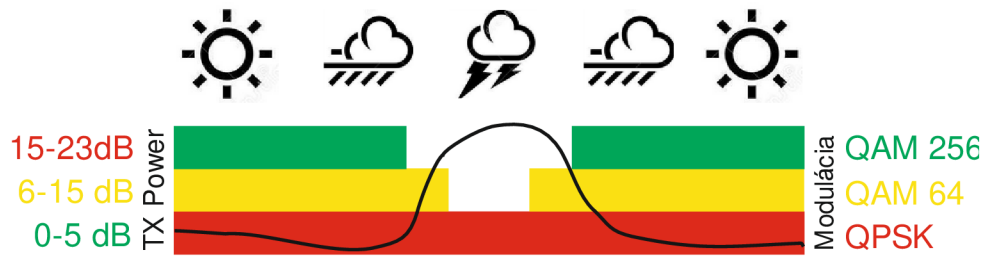
Obr. 3.3: Zálohovanie rárioveho spoja protokolom PAGP/PAGP

Bežným scenárom je, keď sa uplinkový port o rýchlosti 10 GB/s rozdelí na viac portov o rýchlosti 1 Gb/s. Tieto porty sa následne konfigurujú ako člen channel groupu. Fyzické rozhrania začlenené do channel groupu musia mať rovnakú prenosovú rýchlosť, ako aj rovnaké nastavenie duplexu rozhraní. Využívanie rozdelenia záťaže za pomoci protokolu PAGP alebo LACP, prináša viaceré výhody. Najväčším prínosom je rýchla redundancia v prípade výpadku niektorého z prepojov medzi prepínačmi. Detekcia výpadku je riešená na úrovni L1 OSI/ISO na základe detekcie stavu fyzického rozhrania, L2 OSI/ISO na základe ARP/MAC požiadaviek a odpovedí, alebo na L3 OSI/ISO za pomoci testovania dostupnosti IP adresy rozhraní.

Jednotlivé prenosové systémy ponúkajú rozličné bezpečnostné mechanizmy. Okrem nutnosti utajenia komunikácie je v rámci rádiového prenosu nutné počítať s viacerými faktormi, ktoré môžu ovplyvniť bezpečnosť a stabilitu prenosu. Veľké problémy spôsobujú úniky na rádiovej trase. Tieto úniky sú bežne spôsobované meniacimi sa poveternostnými podmienkami, námrazou na anténach alebo vtáctvom. Preto je nutné dohliadať a sledovať situáciu už v momente návrhu a plánovania rádiového spoja. Úniky na rádiovom spoji narastajú hlavne pri zvyšujúcej sa vzdialenosti a frekvencii, na ktorej má byť spoj prevádzkovaný. Predísť únikom je možné dobrou kombináciou použitých antén s dostatočným ziskom a dostatočným výstupným výkonom rádiového zariadenia, čím je možné dosiahnuť určitú rezervu na

trase. Pri narastajúcej vzdialenosti je nutné rátať aj s vyššou rezervou, ktorá je nutná na prekonanie útlmov spôsobených napríklad búrkovým dažďom a podobne.

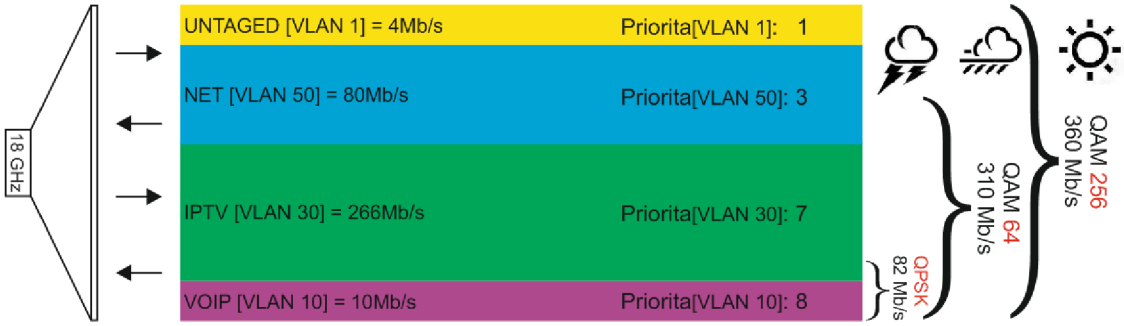
Vysoký výkon a veľký zisk antén nemusí byť riešením v každej situácii. Pre čo najväčší zisk antén je nutné použiť rozmernejšie antény, ktorých inštalácia je obtiažna a často to ani nie je z tohto dôvodu možné. Antény sa zväčša inštalujú na telekomunikačné stožiare, ktoré sú limitované celkovou náveternou plochou a v prípade použitia rozmerných antén to ide na úkor celkovej využiteľnosti telekomunikačného stožiaru. Kompenzovať stratu spôsobenú nižším ziskom antény je možné zvýšením vysielacieho výkonu rádiového zariadenia, čo však znamená vyššie prevádzkové náklady, nakoľko navýšenie vysielacieho výkonu o +3dB znamená zhruba dvojnásobný poplatok za užívanie frekvencie v licencovanom pásme. Preto je už novšími zariadeniami podporovaná funkcia ATPC a ACM.



Obr. 3.4: Znázornenie funkcie ATPC a ACM vplyvom poveternostných podmienok

Funkcia ATPC slúži na automatickú reguláciu výstupného výkonu na dorovnanie únikov rádiovej trasy. Zariadenie s takouto funkciou dokáže zvýšiť výstupný výkon zariadenia len v prípade, ak je to nutné. V prípade, že na trase vznikol útlm väčší, než dokáže kompenzovať funkciou ATPC, prichádza možnosť zníženia kódovania a modulácie. V tomto prípade však musíme zvážiť charakter prenášaných informácií a jednotlivú komunikáciu ešte ošetriť priorizáciou za pomoci QOS. Priorizáciu jednotlivých služieb je možné vykonať priamo na prenosových, rádiokomunikačných zariadeniach na základe presne definovaných kritérií.

Na obrázku 3.5 je znázornená funkcia priorizácie jednotlivej komunikácie cez rádiokomunikačný kanál. Jedná sa o situáciu, keď je jednotlivá komunikácia členená do rozdielnych VLANov. VLAN 10 slúži pre služby VOIP, VLAN 30 slúži pre služby IPTV a VLAN 50 slúži pre internetové služby.



Obr. 3.5: Priorizácia služieb pri bezdrôtovom prenose

Z obrázku vidieť, že vplyvom počasia dochádza ku zmene prenosovej kapacity rádiokomunikačného spoja. Vďaka priorizácii však môžeme určiť, ktorá služba má vypadnúť ako posledná a tiež aj to, že z kapacity ktorej služby je možné uberať pri miernejších poklesoch celkovej prenosovej kapacity spoja. Služba s najvyššou prioritou je najčastejšie hlasová služba, ktorá je náročná na výkyvy v prenosovej kapacite, ako aj na samotnú odozvu. Kapacitné nároky na hlasové služby sú našťastie minimálne vďaka čomu je služby prevádzkyschopná aj za tých najhorších podmienok. Väčší problém je so službami digitálnej televízie, ktorá je z kapacitného hľadiska extrémne náročná. Práve vďaka priorizácii je možné docieliť to, aby nedochádzalo k výpadkom v prípade zhoršeného počasia, ale aj v prípade, že by malo dôjsť k nadmernému vyťažovaniu celkovej prenosovej kapacity prostredníctvom inej VLANy.

Znížením prenosových stavov modulácie získame zvýšenú citlivosť na strane prijímača, ale v tomto prípade to už ide na úkor prenosovej rýchlosti rádiového spoja.

Obr. 3.6: Inštalácia smerových antén Andrew priemeru 120cm pre pásmo 13 GHz.

3.1 Prenos informácií cez metalické vedenia

Situácia je o niečo lepšia v prípade prenosu informácii cez metalické vedenia. Jedná sa o bezpečnejšiu formu prenášania informácií, nakoľko sa informácia zasiela medzi vysielačom a prijímačom prostredníctvom uzatvoreného komunikačného kanála, za pomoci symetrického alebo nesymetrického vedenia. Tu však vzhľadom na charakter prenosu informácií vzniká prechodom elektrónov vo vedení elektromagnetické pole, čo môže spôsobiť emisiu prenášaných informácií do okolitého prostredia, pričom úroveň, rozsah a dosah emisií záleží podľa výkonu a frekvencie prenášaného signálu vo vodiči. Najčastejšou formou takejto emisie informácií sú poškodené komunikačné vedenie, zatečené, alebo poškodené konektory a to hlavne pri nadzemných sieťach. V tomto prípade sa poškodené vedenie môže chovať aj ako anténa a spôsobí nie len možný únik informácií, ale aj zarušenie ostatných komunikačných kanálov v okolí. Najlepšiu ochranu proti presluchom poskytujú nesymetrické koaxiálne vedenia. Samotnú ochranu zabezpečuje ich konštrukcia, nakoľko opláštenie, ktoré môže byť viacvrstvové, zabraňuje prenikaniu prenášaného signálu mimo vedenie. V prípade poškodeného

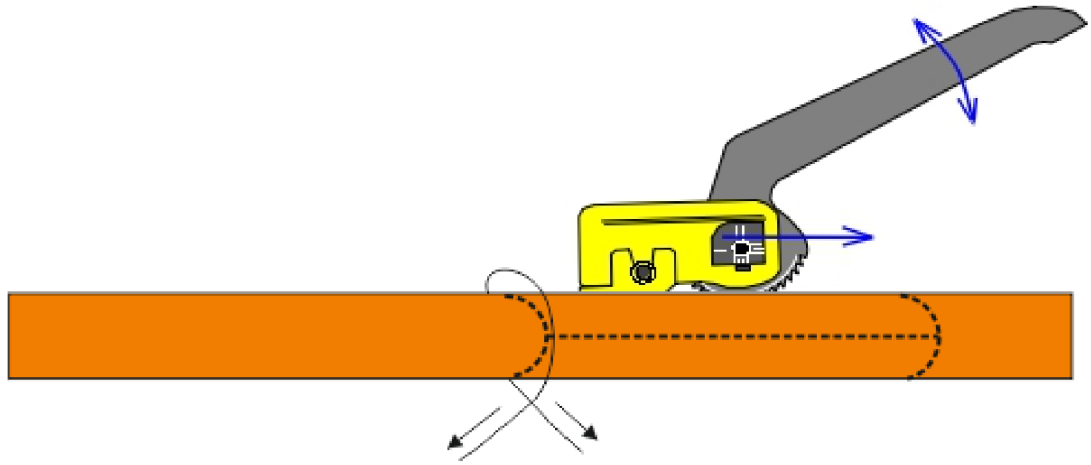
nadzemného alebo podzemného optického vedenia sa takáto forma zarušenia alebo úniku informácií nemôže stať.

4. Možnosti odpočúvania optického prenosu

V prípade, že máme snahu odpočúvať reálnu prevádzku vo vedeniach podzemnej, ale inak situovanej siete, bude nutné zabezpečiť fyzický prístup k samotným optickým vláknam. Vysoká úroveň bezpečnosti optických sietí je práve z toho dôvodu, že samotný spôsob prenášania informácií prostredníctvom optických vlákien neumožňuje prenesené dáta zachytiť inak, než fyzickým prístupom k prenosovému médiu a to doslova. Zabezpečenie fyzického prístupu k podzemnej, alebo vzdušnej sieti nemusí byť ľahká úloha a to aj z toho dôvodu, že väčšina podzemných aj nadzemných inžinierskych sietí je vedených v takzvaných zelených pásmach, ktoré sú majetkom miest a obcí a sú zväčša situované medzi zástavbami a pozemnými komunikáciami, čím sú pred očami mnohých ľudí. Takáto situácia len celý proces sťažuje, nakoľko pre realizáciu je nutné mať stabilný prístup k vláknam, aby bolo možné aplikovať prípravky určené na zachytávanie komunikácie, ktorá sa prenáša vláknom.

V tomto prípade narážame na jednu z prvých legislatívnych prekážok, nakoľko pre realizáciu výkopov je nutné rozkopávkové povolenie a často aj súhlas mesta na zvláštne užívanie verejného priestranstva. Okrem toho, že tieto úkony sú spoplatnené, automaticky evidujú staviteľa, čím je samotný pokus sťažený, alebo úplne znemožnený. V rámci stavebného konania sa naďalej vyžaduje predloženie súhlasných vyjadrení od prevádzkovateľov inžinierskych sietí a to hlavne z dôvodu, aby pri plánovaných prácach nemohlo dôjsť k poškodeniu jestvujúcich podzemných sietí a tým ich obmedziť. Teoretickou možnosťou ako sa vyhnúť podobným konaniam a neupozorniť na danú činnosť, je uskutočnenie a vykonanie pokusov o prístup k vedeniam na odľahlých miestach, alebo na súkromných pozemkoch, cez ktoré dané telekomunikačné vedenia prechádzajú. Tu sa však často stáva, že pri výkopoch mohli byť uložené aj chráničky, alebo vedenia iných operátorov a tým pádom nie je možné jednotlivé vedenia a chráničky rozoznať.

Po zabezpečení fyzického prístupu k vedeniu sa s najväčšou pravdepodobnosťou nedostaneme priamo k optickému vedeniu, ale len ku chráničke, ktorej úlohou je optický kábel chrániť pred poškodením počas výkopových prác. Práve preto, keď sa chceme dostať ku samotnému káblu, musíme plášť chráničky zrezať pozdĺžnym rezačom na DHPE rúry alebo mikrotrubičky. Tento úkon je náročný a vyžaduje si špeciálne náradie, ktoré nespôsobí poškodenie optických vlákien. Náradie sa nasledovne líši vzhľadom na priemer, hrúbku a typ chráničky. Narezanie chráničky, v ktorej je už zafúknuté vlákno znázorňuje obrázok 4.1.



Obr. 4.1: Pozdĺžny rezač na chráničky HDPE

Po tomto kroku môže nastať ďalší problém. HDPE rúry ako aj multirúry môžu byť natlakované. Uzatvorená chránička, ktorá je permanentne pod zvýšeným tlakom vzduchu, ktorý slúži hlavne ako detektor, či daná trasa nie je poškodená. Táto forma kontroly je jednoduchá a reaguje okamžite na poškodenie, ktoré spôsobí únik vzduchu, alebo zníženie tlaku. Najčastejšie sa tlakujú chráničky, v ktorých sa ešte nenachádza žiadne vedenie, nakoľko sa pri výstavbe sietí zvyknú pokladať aj rezervné chráničky. Tie môžu slúžiť na neskoršiu rezervu, ale aj na sondovanie siete, za účelom presnejšieho zamerania.

Poškodenie, ktoré spôsobí únik tlaku môže byť spôsobené aj neúmyselne a to napríklad pri realizácii iných výkopových prác. Často sa stáva, že takéto neúmyselné

poškodenie chráničky, často aj bez viditeľného poškodenia, stavitelia nenahlásia operátorovi, ktorému tým následne pri zafukovaní optických káblov vznikajú problémy spôsobené únikom tlaku. Takéto poruchy na trase sa následne zisťujú za pomoci detekčného plynu.

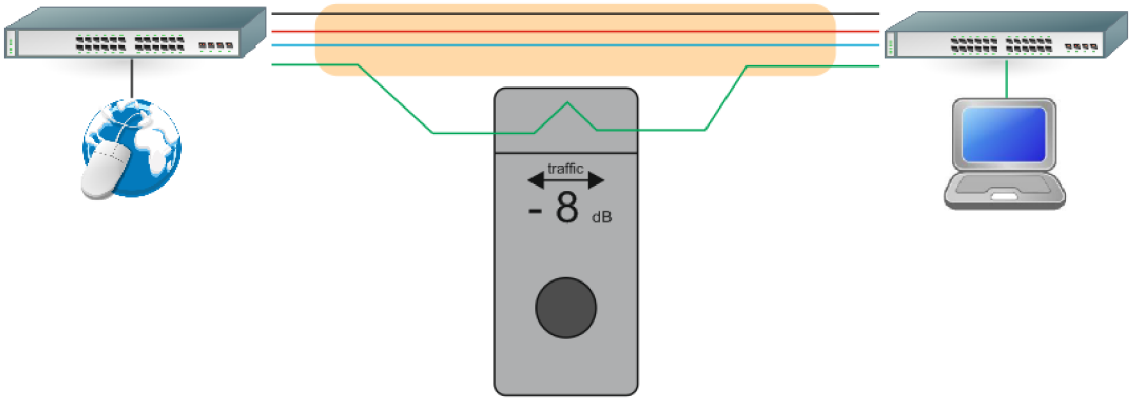
Po sprístupnení optického kábla musí dôjsť k oplášteniu sekundárnej a primárnej ochrany, následne k očisteniu konkrétnych vlákien. Tento úkon je tiež náročný a to z dôvodu, že je nutné roztvoriť pozdĺžne optický kábel, ktorý je okrem iného aj pod prevádzkou. V tomto prípade je nutné tiež použiť špeciálne odizolovacie nástroje, ktoré sú rozdielne vzhľadom na typ optického kábla. Tieto nástroje sú však bežne dostupné pod názvom fiber cable stripper. Týmto to však ešte nekončí, nakoľko vo optickom kábli sú samotné vlákna členené to takzvaných bufferov a to väčšinou po 12 vlákien. V prípade viacvláknových vedení to extrémne komplikuje situáciu. Roztvorenie buffra je azda najnebezpečnejšia časť prípravy. Práve v tomto kroku je najväčšia pravdepodobnosť poškodenia vlákien.

Na základe vyššie uvedených informácií môžeme jednoznačne konštatovať, že odpočúvanie optickej komunikácie nie je vôbec jednoduchá vec. V záujme realizácie odpočúvania treba preklenúť hneď niekoľko prekážok, z ktorých drvivá väčšina pokus ešte viac sťažia, alebo úplne znemožnia. Ale aj napriek tomu sú verejne dostupné informácie o tom, že niektorým vládam sa podarilo odpočúvať prenos informácií v optických vláknach pod zemským povrchom, ale aj optické vedenia na dne morí a oceánov. Je to dôkaz o tom, že odpočúvanie optického prenosu informácií je veľmi reálna a aktuálna vec. V momente keď ich vykonávajú vládne organizácie, okamžite odpadávajú legislatívne a stavebné bariéry.

4.1 Aktívne odpočúvanie optického prenosu

V prípade, že sa chceme pokúsiť o reálne odpočúvanie optického prenosu cez optické vlákno, máme hneď niekoľko možností. Záleží to hlavne od charakteru komunikácie a podľa použitej prenosovej technológie. Rozhodujúcim faktorom je charakter odpočúvanej siete, napríklad distribúcia televízneho signálu určeného pre HFC sieť, alebo duplexný dátový prenos medzi prepínačmi. Vzhľadom na použitú technológiu sa využívajú v sieťach rozdielne modulácie optického signálu, rôzne úrovne a vlnové dĺžky. Z hľadiska odpočúvania je pre nás najvýhodnejšie a jednoduchšie odpočúvať optickú prevádzku simplexného televízneho signálu napríklad s amplitúdovou moduláciou o vlnovej dĺžky 1310 nm, než dátovú prevádzku v paketových sieťach napríklad medzi prepínačmi, ktoré bežne využívajú aj menšie optické výkony.

V prípade paketového prenosu na prístupovej sieti, kde sú cez vlákno prenášané dáta len občas, napríklad cez pracovné dni, aj to len v pracovnej dobe, môžeme využiť čas mimo prevádzkových hodín na inštaláciu zariadenia vďaka čomu zahájime útok typu man in the middle „muž uprostred“. Túto formu útoku je možné využiť v prípade, že je dostatok času na prerušenie optického prepojenia medzi sieťou a odpočúvaným subjektom, z pravidla medzi smerovačom a prepínačom, ku ktorému je odpočúvaná stanica pripojená. Dôležitým krokom je zistiť, že aké vlnové dĺžky sú optickým vodičom prenášané. Následne je nutné zistiť smer dát vo vlákne, ako aj druh optického vysielača na vlákne. Bežné vlnové dĺžky sú 1550 nm pri duplexnom spojení. Môže sa však stať, že obojsmerná komunikácia prebieha len v jednom vlákne. V tom prípade musíme zistiť prítomnosť minimálne dvoch vlnových dĺžok, každú z iného smeru nakoľko sa jedná o WDM technológiu, ktorá štandardne využíva vlnové dĺžky 1310 a 1550 nm v jednom vlákne. Na zistenie týchto parametrov je možné použiť elektronické zariadenie, ktoré sa primárne používa na včasné odstraňovanie porúch na optických trasách. Jedným z nich je aj JW3306B Fiber identifier, ktorý je schopný detekovať prevádzku ako aj smer prenosu dát vláknom na rôznych vlnových dĺžkach, to aj v prípade, že vlákno nie je očistené od primárnej ochrany. Bežné zapojenie a použitie zariadenia fiber identifier je na obrázku 4.2.



Obr. 4.2: Zapojenie zariadenia fiber identifier

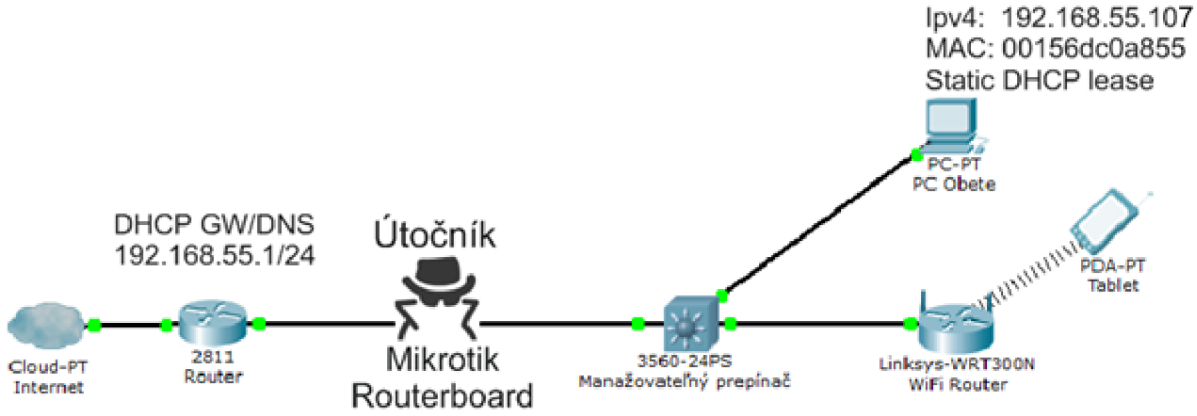
Po zmeraní prevádzky a smeru prenosu signálu je možné vedenie v bode merania prerušiť a nainštalovať zariadenie, ktoré umožňuje analýzu prevádzky, jeho záznam alebo zrkadlenie sieťovej prevádzky. V tomto prípade je možné použiť aj takzvaný L7 Proxy firewall, ktorý umožní podstrčenie falošného SSL certifikátu pri pokuse o otvorenie zabezpečenej stránky. Takýmto spôsobom vieme obmedziť funkčnosť pôvodného DHCP serveru, ba dokonca spustiť vlastný DHCP server v odpočúvanom segmente siete a zmeniť napríklad konfiguráciu DNS serverov jednotlivým staniciam prostredníctvom nového DHCP serveru. Pre výkonnejšie prostredia je alternatíva inštalácie viacvrstvového prepínača ideálne s podporou netflowu alebo wiresharku, ktorý okrem iného umožňuje aj zrkadlenie portov pre ďalší záznam a spracovávanie.

Takáto forma odpočúvania prevádzky je však ľahko odhaliteľná aj z dôvodu, že pridané aktívne zariadenie spôsobí oneskorenie prenosu dát alebo znemožní funkčnosť niektorých protokolov cez dané vlákno. Odhalenie takéhoto pokusu je tiež možné konfiguráciou SNMP Trap správ, ktoré sú následne zaslané sieťovými zariadeniami v momente dočasného, alebo úplného prerušenia fyzického spojenia na optickej linke. Musíme podotknúť, že tento spôsob je použiteľný len v prípade použitia jednej, maximálne dvoch vlnových dĺžok vo vlákne prostredníctvom technológie WDM.

Pri pokuse o uskutočnenie útoku „Man in the Middle“ sme použili zariadenie Mikrotik CCR1036, ktorý podporuje optické moduly vďaka rozhraniu SFP+ až do rýchlosti až 10 Gb/s. Jedná sa o router s plnou podporou premosťovania rozhraní,

podporou IPV4, IPV6, Firewalling a mnoho ďalších. Vďaka možnostiam, ktoré nám poskytuje Mikrotik Router OS dokážeme filtrovať prevádzku a spustiť vlastné služby DNS, DHCP servera a to všetko bez nutnosti zmien v konfigurácii koncových počítačov.

Za účelom demonštrácie možností sme si stanovili úlohu krádeže prihlasovacích údajov na facebookový účet potenciálnej obete. Topológia a parametre siete sú uvedené na obrázku 4.3.



Obr. 4.3: Topológia pokusnej siete pre demonštrovanie útoku „Man in the Middle“

Podľa obrázku vidíme, že v lokálnej sieti sa využíva rozsah 192.168.55.0/24, ktorý je spravovaný za pomoci DHCP serveru, ktorý je prevádzkovaný na hlavnom smerovači. IP adresa hlavného smerovača je 192.168.55.1 a tvorí hlavnú bránu do siete internet. Okrem hlavnej brány, ktorá zabezpečuje internet prekladom adries NAT, je na smerovači prevádzkovaný rekurzívny DNS server. To znamená, že stanice v lokálnej sieti môžu mať nastavenú IP adresu primárneho DNS serveru práve IP adresu hlavného smerovača. DHCP server však môže staniciam prideľovať aj rozdielnu IP adresu DNS serverov. Veľkej obľube sa v súčasnosti tešia DNS servery Googlu s adresou 8.8.8.8 a 8.8.4.4. Práve zmenou týchto parametrov vieme docieliť presmerovanie webovej stránky na nami vytvorenú falošnú stránku, ktorá bude navrhnutá tak, že po vyplnení prihlasovacích informácií do prihlasovacích okienok ich obsah zapíše do súboru alebo obratom pošle do mailu.

V prvom kroku je nutné analyzovať prevádzku v rámci lokálnej siete, pomocou čoho zistíme parametre DHCP serveru, použité rozsahy a tiež MAC adresy. Na analýzu prevádzky je možné využiť samotný Mikrotik Routerboard, bez nutnosti špeciálnych zariadení. Na zapojenie samotného Mikrotik Routerboardu sú potrebné len dve fyzické rozhrania, ktoré budú zaradené do jedného virtuálneho premostenia, inými slovami do jedného Bridge rozhrania. Na vytvorenie bridge rozhrania použijeme v Mikrotiku nasledujúci príkaz:

```
[admin@MikroTik] /interface bridge> add
```

Pre overenie nastavenie môžeme použiť príkaz Print, ktorý nám vráti výstup nastavenia.

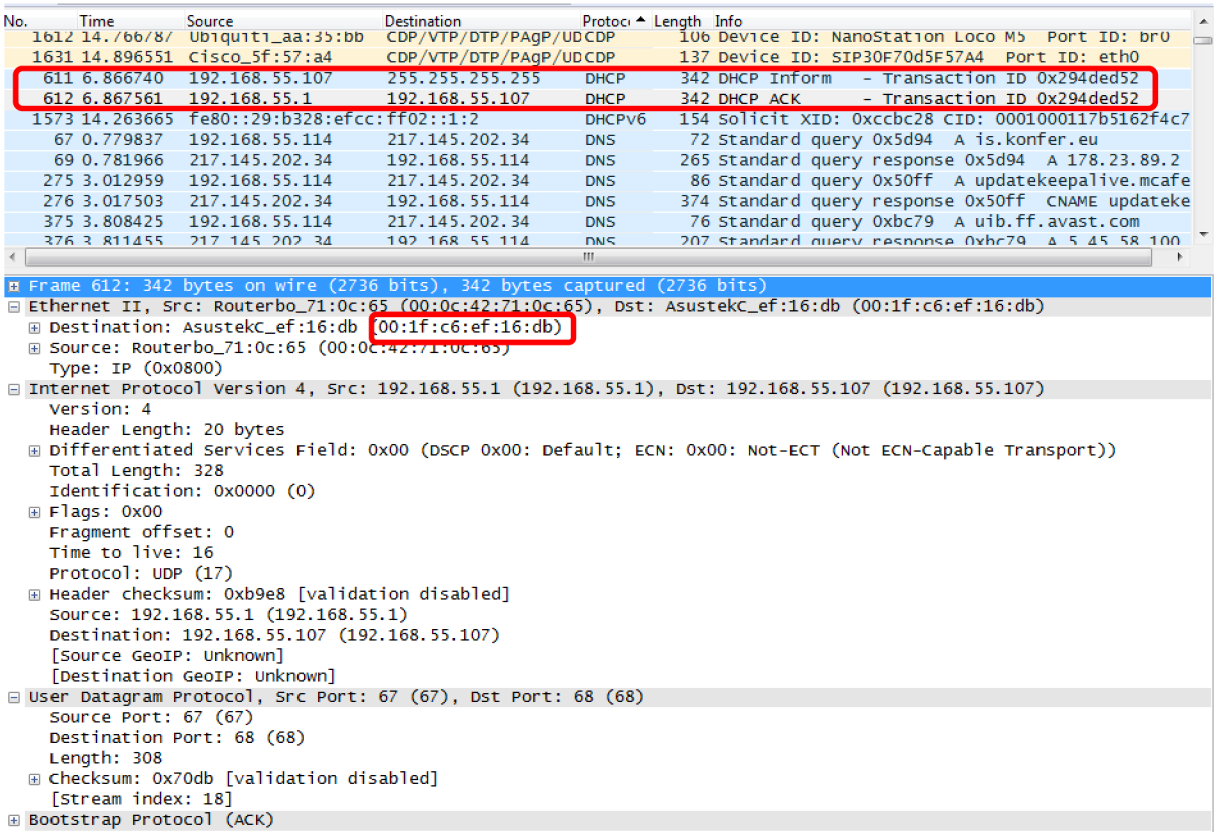
```
[admin@MikroTik] /interface bridge> print
Flags: X - disabled, R - running
 0  R name="bridge1" mtu=1500 l2mtu=65535 arp=enabled
      mac-address=00:00:00:00:00:00 protocol-mode=none priority=0x8000
      auto-mac=yes admin-mac=00:00:00:00:00:00 max-message-age=20s
      forward-delay=15s transmit-hold-count=6 ageing-time=5m
```

Pre zaradenie rozhraní do vytvoreného bridgu použijeme nasledovným príkaz:

```
[admin@MikroTik] /interface bridge port> add bridge=bridge1
interface=ether1
[admin@MikroTik] /interface bridge port> add bridge=bridge1
interface=ether2
[admin@MikroTik] /interface bridge port> print
Flags: X - disabled, I - inactive, D - dynamic
#    INTERFACE            BRIDGE            PRIORITY PATH-COST
ether1                    bridge1           0x80     10
ether2                    bridge1           0x80     10
```

Zaradením fyzických rozhraní do bridgu sa sledovacie zariadenie stáva transparentným zariadením a pri vypnutej funkcii Neighbor, ktorý je kompatibilný s protokolom CDP – Cisco discovery protokol je náš smerovač úplne neviditeľný. Služba neighbor slúži na komunikáciu prostredníctvom broadcastu a rozširuje informácie o zariadení akými sú typ zariadenia, výrobca, verzia OS a rozhranie, z ktorého sa všesmerové správy vysielajú. Po vykonaní základných nastavení je na rade analýza prevádzky. Analýzu môžeme vykonávať priamo prostredníctvom Mikrotik Routerboardu, bez nutnosti špeciálnych prídavných zariadení. Na tento účel použijeme službu Packet sniffer, ktorá slúži na zachytávanie hlavičiek paketov do súboru. V službe Packet sniffer je nutné nastaviť ako sledované rozhranie Bridge1.

Na hlbšiu analýzu zaznamenaného súboru je následne možné použiť externý softvér napríklad Wireshark. Pomocou Wiresharku sa vieme upriamiť na získanie informácií o používaných rozsahoch a rozanalyzovať komunikáciu jednotlivých staníc, vďaka čomu získame ich IP adresy a MAC adresy zároveň. Analýza prideľovania IP adresy stanici obete je na obrátku 4.4.



Obr. 4.4: Odchytenie DHCP komunikácie stanice obete

Na základe analýzy sme zistili, že stanica obete s IP 192.168.55.107 má fyzickú adresu 00:1f:c6:ef:16:db. Táto informácia je pre nás kľúčová, z dôvodu nasledovného nastavenia podvrhnutého DHCP serveru. Vďaka získanej fyzickej adrese a IP adrese obete, vieme vytvoriť statický Leas a obeť bude mať v lokálnej sieti aj naďalej rovnakú IP adresu, čím nebudú znefunkčnené služby lokálnej siete.

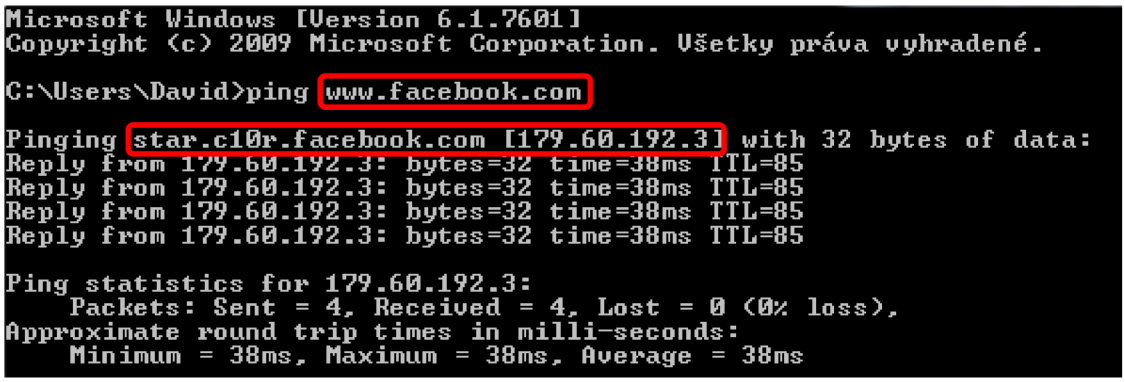
Prvým vážnejším krokom v útoku je odstrihnutie DHCP komunikácie zo smerovača k účastníkom. To zabezpečíme za pomoci nasledovnej konfigurácii priamo vo filtrácii na rozhraní premostenia Bridge1, ktoré prioritne blokuje porty 67 a 68 UDP.

```
/interface bridge filter

add action=log chain=input comment="Zaznam o blokovani DHCP na
192.168.55.0/24" disabled=no dst-address=255.255.255.255/32 ip-
protocol=udp log-prefix="Originalne DHCP-Bloknute" mac-protocol=ip
src-address=192.168.55.0/24 src-port=67-68

add action=drop chain=input comment="Blokovani DHCP na
192.168.55.0/24"    disabled=no dst-address=255.255.255.255/32 ip-
protocol=udp mac-protocol=   ip src-address=192.168.55.0/24 src-
port=67-68
```

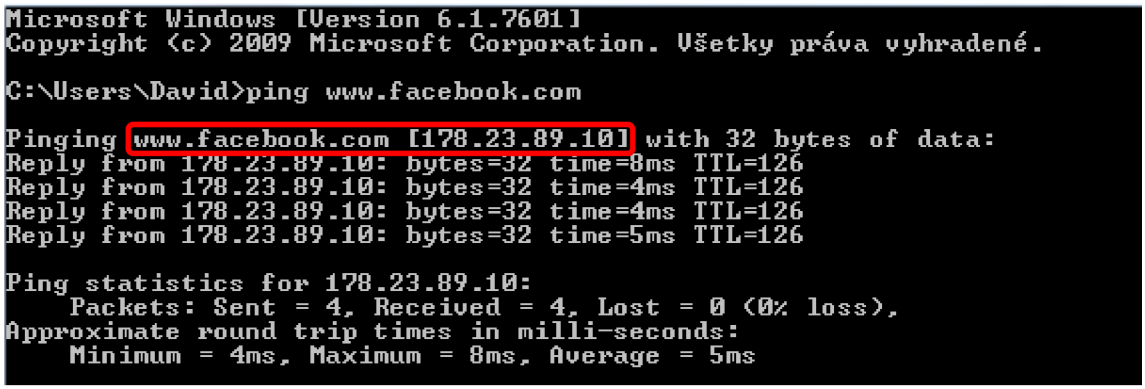
Po uplatnení tejto konfigurácie je možné spustiť služby vlastného DHCP serveru so zmenou IP adresou primárneho DNS serveru. Smerovanie môžeme uskutočniť na samotný Mikrotik routerboard, v ktorom si nastavíme statický doménový záznam pre akúkoľvek IP adresu, na ktorej môže byť prevádzkovaná falošná prihlasovacia stránka na Facebook. Konfiguráciu statického DNS záznamu môžeme vykonať nasledovne:

```
[admin@MikroTik] ip dns static> add name www.facebook.com
address=178.23.89.10
```

Tento príkaz spôsobí, že dotaz smerujúci na www.facebook.com bude presmerovaný na webový server s IP adresou 178.23.89.10.



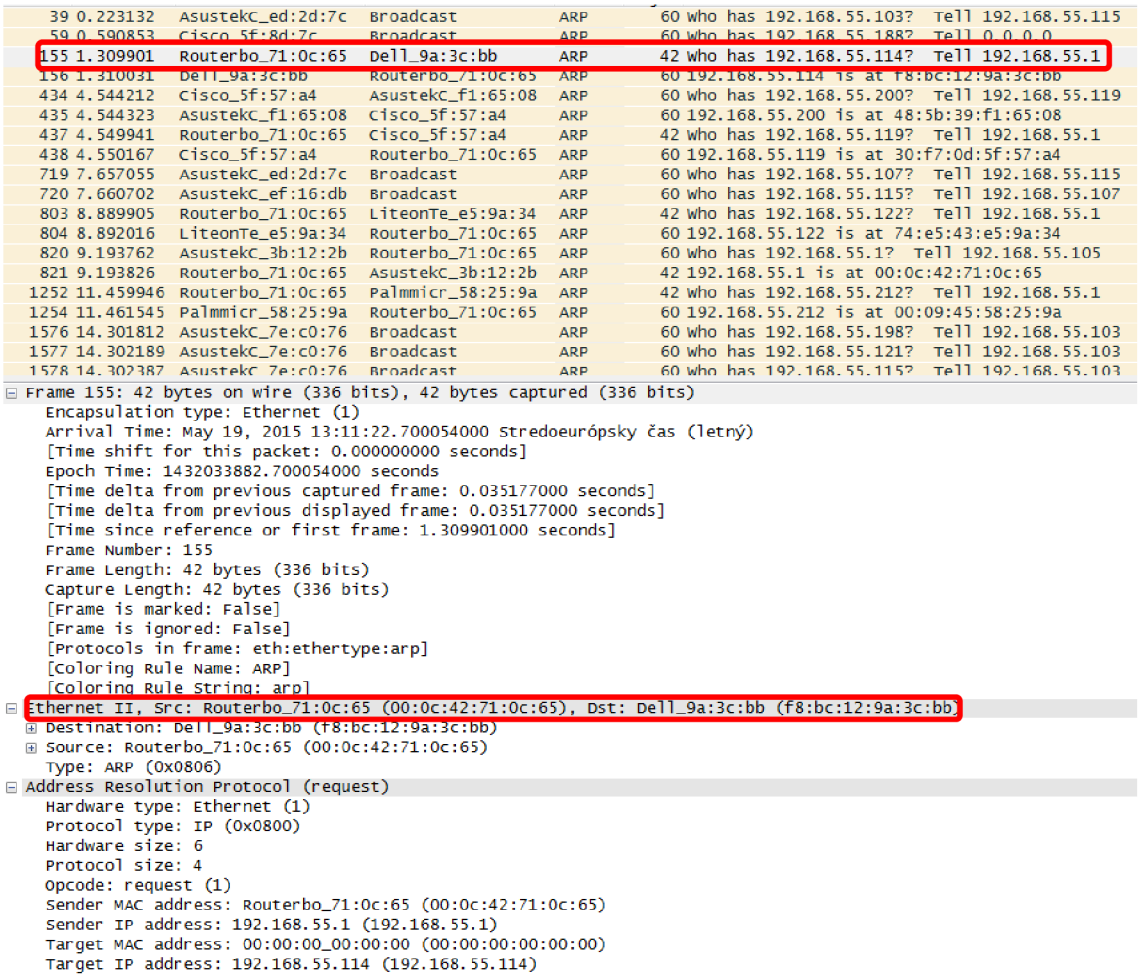
Obr. 4.5: Ping na www.facebook.com pred zadaním statického DNS záznamu



Obr. 4.6: Ping na www.facebook po zadaní statického DNS záznamu

Na obrázku 4.6 je jednoznačne vidieť, že dotaz www.facebook.com preložil na IP adresu nášho webového serveru, ktorý má okrem iného aj výrazne kratšiu odozvu. Zmena sa však neprejavila okamžite. Štandardne je nutné počkať na vypršanie časovačov s operačnom systéme. Premazanie časovačov nastane aj po reštarte počítača, alebo po obnovení prevádzky sieťovej karty.

Za pomoci analýzy zachytených dát máme krásny prehľad aj o staniciach, ktoré majú v lokálnej statickú konfiguráciu IP adresy. IP adresy a fyzické adresy takýchto staníc vidíme na základe komunikácie a analýzy ARP protokolu, ktorý je viditeľný na obrázku 4.7.



Obr. 4.7: Analýza ARP paketov vo firemnej sieti

V lokálnej firemnej sieti sa jedná väčšinou o zariadenia ako tlačiarne alebo dochádzkové terminály. V prípade, že by sa jednalo statickú konfiguráciu IP adries v počítači obete, nič ešte nie je stratené. Presmerovanie DNS komunikácie je bez problémov možné za pomoci pravidiel vo firewale. Konfigurácia pre

```
/ ip firewall nat
add chain=dstnat action=dst-nat to-addresses=192.168.55.2 to-ports=53
protocol=tcp dst-port=53

add chain=dstnat action=dst-nat to-addresses=192.168.55.2 to-ports=53
protocol=udp dst-port=53
```

IP adresa 192.168.55.2 môže byť ako dočasná adresa útočníka. Vďaka tejto konfigurácii docielime toho, že všetka komunikácia smerovaná na akýkoľvek DNS server od účastníkov skrz naše zariadenie bude presmerovaná na interný DNS server

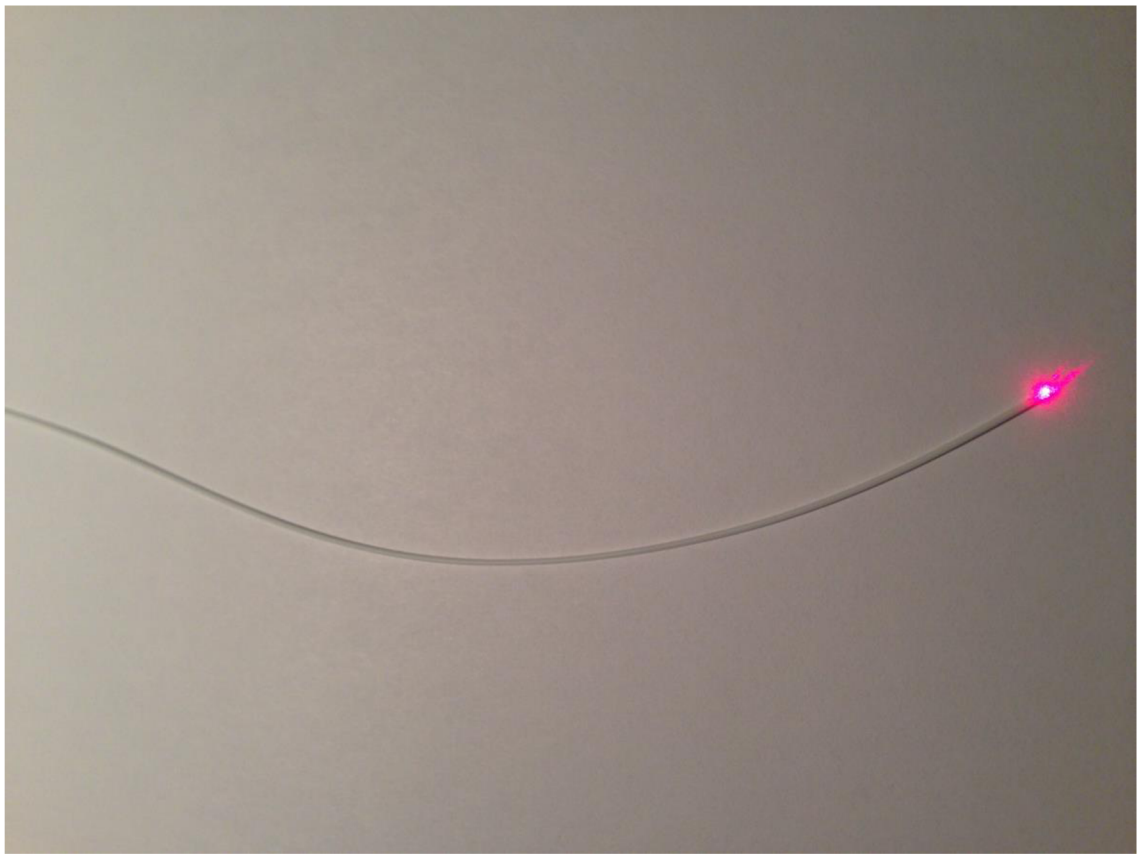
útočníka, v ktorom budú zmenené statické záznamy podľa potreby útočníka. Takáto forma presmerovania DNS serverov je bežná aj vo firemných sieťach a to hlavne za účelom filtrácie a obmedzovania webových stránok. V prípade, že správca chce uplatniť obmedzenia webových stránok len určitým užívateľom, je možné týchto užívateľov zadať do takzvaných address listov, čím sa zjednoduší správa pravidiel v smerovačoch.

Na základe vyššie uvedených informácií sme dokázali, že v prípade prístupu k vláknu je reálne možné aplikovať útok typu „Man in the Middle“. Tento druh útoku je však možné použiť aj pri prenosoch informácie prostredníctvom metalických sietí.

4.2 Pasívne odpočúvanie optického prenosu.

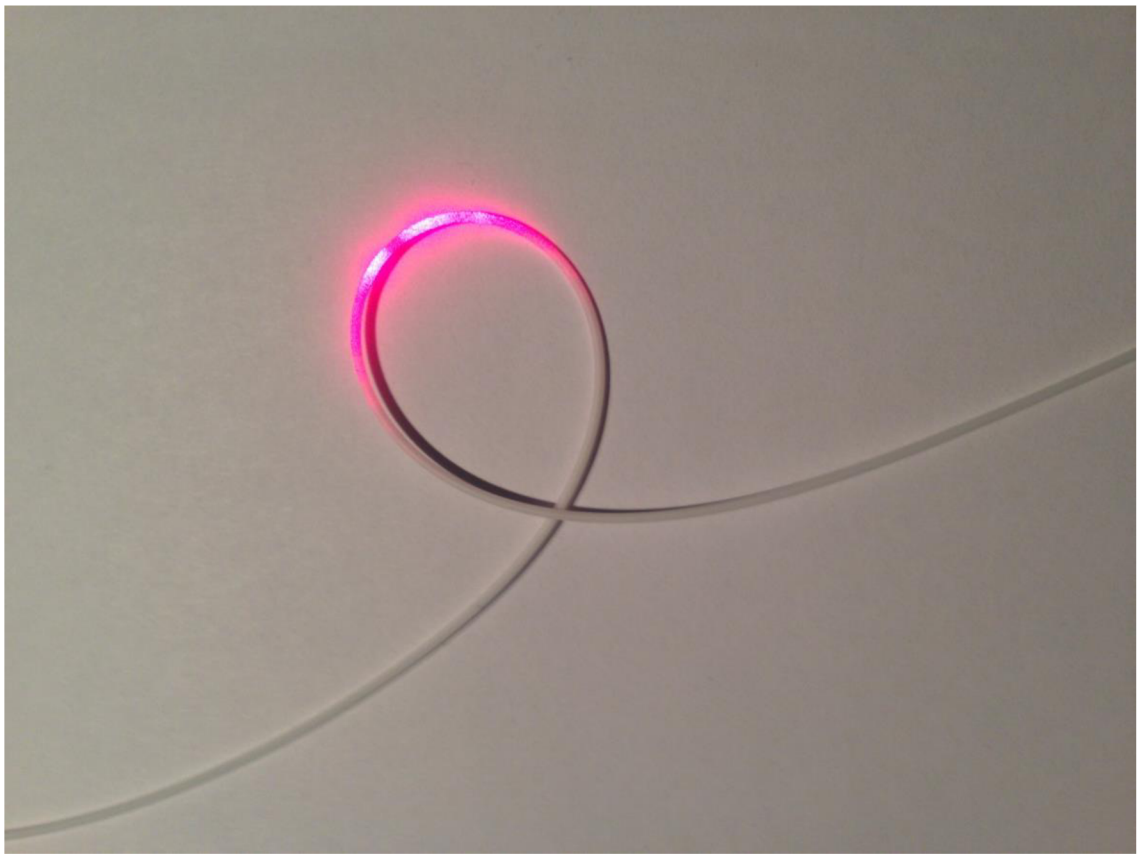
Ďalšou z možností odpočúvania optického prenosu vo vlákne je sledovanie emisných fotónov za pomoci externého detektoru. Tento spôsob je extrémne náročný, avšak nevyžaduje prerušenie optického vlákna. Okrem toho umožňuje výlučne detekciu a sledovanie komunikácie skrz vlákno. Za pomoci detekčného zariadenia zachytávame fotóny mimo jadra optického vlákna. Úroveň svetelného signálu mimo jadra vodiča je pri narovnanom optickom vlákne veľmi nízka, až nemerateľná a jeho hodnota záleží hlavne na vysielacom výkone signálového lasera. Takýto svetelný signál môže byť detekovateľný hlavne v prípade, že vlákno, ktorým tento lúč prechádza, ohneme. Ohyb spôsobí odraz svetelného lúča mimo jadra svetelného vodiča. Tento jav môžeme pozorovať v prípade, že na svetelný vodič v osi pripojíme viditeľný zdroj svetla, napríklad laserový emitor na vlnovej dĺžke 650nm. Na obrázku 4.8 je jasne viditeľné, že zmenšujúcim sa polomerom ohybu narastá úroveň svetla a to hlavne v miestach najväčšieho ohybu. Za účelom pokusu sme použili pigtail s jedno vidovým optickým vlákno G.657 - 9/125 μm s primárnou ochranou. Aj napriek ponechanej primárnej ochrane je únik svetla mimo jadra svetelného vodiča výrazný.

Obrázok 4.8 znázorňuje šírenie svetla optickým vláknom, ktoré je bez výraznejšieho ohybu. Vychádzajúci svetelný lúč je viditeľný len na konci svetelného vodiča.



Obr. 4.8: Vedenie svetla optickým vodičom bez výraznejších ohybov

Na obrázku č. 4.9 sme svetelný vodič ohli, pričom pri zmenšení polomeru ohybu je už voľným okom badateľné svetlo, ktoré opustilo jadro svetelného vodiča v miestach s najväčším ohybom. V prípade opláštеného optického vodiča je únik svetla výrazne vyšší. Pokiaľ by ani to nepostačovalo, je možné ohnuté vlákno obrúsiť napríklad veľmi jemnou brúsnou pastou, ba dokonca so zubnou pastou, ktorá bola k vláknu najjemnejšia. V miestach, kde sa takýto postup aplikuje sa zmenší priemer vodiča a zvýši sa jeho útlm. Dôsledkom toho je, že sa vo väčšine prípadov optické vlákno zlomilo, buď počas brúsenia, alebo počas pokusov o meranie uniknutého svetla.



Obr. 4.9: Vedenie svetla optickým vodičom s výraznejších ohybov

Je všeobecne známym faktom, že ohybom vlákna zvyšujeme útlm vedenia. Hlavným faktorom je pritom polomer ohybu a vlnová dĺžka svetla. Preto musíme dbať na to, aby nebol spôsobený príliš veľký útlm spôsobený malým polomerom ohybu. V extrémnom prípade môžeme spôsobiť aj zlomenie vlákna. Z tohto dôvodu je dôležité uvedený úkon vykonať pri čo najvyššej okolitej teplote a s čo najvyššou opatrnosťou. Tabuľka 4.1 znázorňuje útlm vlákna vzhľadom na priemer ohybu a vlnovú dĺžku.

Tab. 4.1: Útlm vlákna G.657 vzhľadom na vlnovú dĺžku a priemer ohybu

	Polomer závitu12mm		**Polomer závitu30mm**	
Vlnová dĺžka	**1 Závit**	**2 Závity**	**1 Závit**	**2 Závity**
1310 nm	0,6 dB	1,9 dB	0,01 dB	0,03 dB
1550nm	3,4 dB	7,9 dB	0,04 dB	0,09 dB

Na základe tabuľky je jednoznačne vidieť, že zvyšujúcou sa vlnovou dĺžkou nám narastá útlm vedenia v miestach ohybu a to vo výraznej miere.

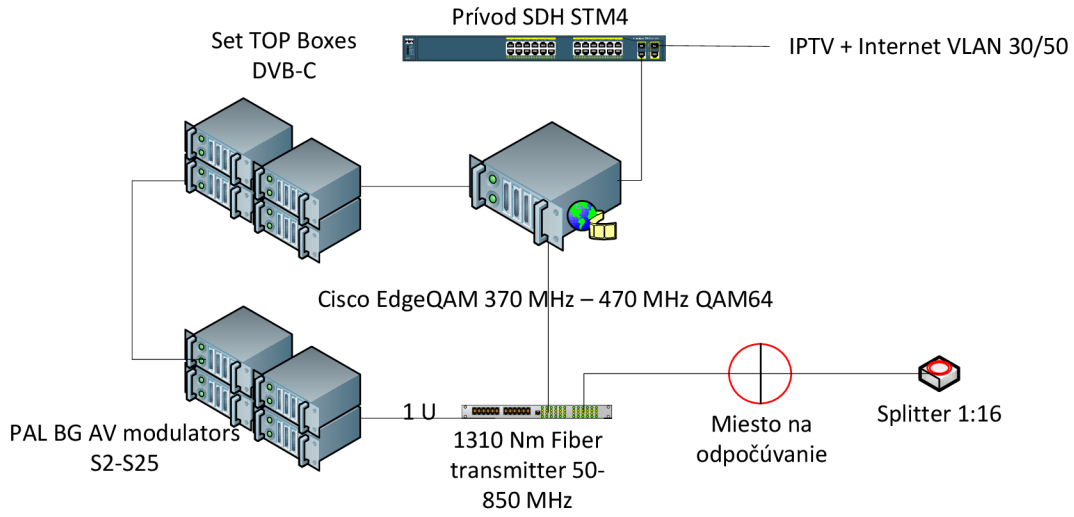
Vyššia úroveň svetla v mieste ohybu nám umožňuje jednoduchšiu detekciu a prípadné odpočúvanie optického prenosu. Takýto pokus môže byť ľahko odhalený a to hlavne v prípade, že na trase sú zariadenia schopné identifikovať úroveň a tým pádom aj pokles optického signálu. Ohyby za účelom odpočúvania komunikácie je teda nutné robiť so zreteľom na možný spôsobený útlm na trase, na základe čoho prevádzkovateľ okruhu dostane podozrenie na poškodený optický transciever, alebo poškodené vedenie. Preveriť vedenie je pritom veľmi jednoduché. Slúži na to zariadenie OTDR, ktoré vykoná optickú reflexometriu a s veľmi veľkou presnosťou určí miesto, v ktorom došlo ku zvýšeniu útlmu, čím sa odhalí miesto pokusu o odpočúvanie.

V záujme predísť podobnému problému je možnosť dosvietiť vlákno nižšie od miesta, v ktorom nastal útlm. V tomto prípade je nutné použiť zdroj svetla o rovnakej vlnovej dĺžky akým je prenášaný signál v optickom vlákne.

Na základe vyššie uvedených informácií bol vykonaný pokus o reálne odpočúvanie komunikácie v optickom vlákne. Ako zdroj signálu sme použili prevodník z RF 75 Ohm na optiku o vlnovej dĺžke 1310 nm s laserom DBF so vstupným rozsahom 50-850 MHz a amplitúdovou moduláciou. Túto vlnovú dĺžku sme volili aj z toho dôvodu, že má nižší útlm v prípade ohybu vlákna v mieste detekcie optickej komunikácie. Signál bol nasledovne šírený jednovidovým optickým vláknom do optického nodu, ktorej úloha je spätná konverzia optického signálu na RF signál o impedancii 75 Ohm.

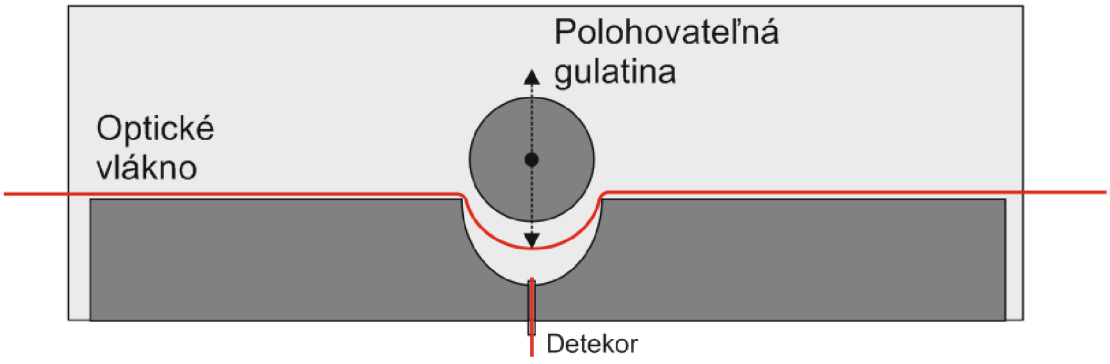
Ako vstupný signál sme použili jeden multiplex o šírke pásme 8MHz na frekvencii 370 MHz. Multiplex bol štandardu DVB-C a použili sme moduláciu QAM64. Vstupná úroveň RF signálu bola 95 dBuVm, MER: >39, BER>10^{-9}. Hodnoty boli namerané DVB-C QAM analyzátorom na koaxiálnom vstupe optického prevodníku. Jednalo sa o jeden multiplex z digitálnej káblovej televízie. Zdroj signálu sme volili zámerne a to z dôvodu charakteru služby, nakoľko sa jedná o jednosmerný spôsob komunikácie, ktorý je QAM analyzátorom po prevedení na RF signál dobre merateľný. V záujme snahy o väčší úspech pokusu sme použili výkonnejší optický prevodník, ktorého výstupný výkon bol až na úrovni 17 dB, vďaka čomu sme dosiahli v mieste ohybu vládna dostatočne silný optický signál.

Na obrázku 4.10 vidíme zapojenie jednotlivých zariadení vrátane miesta kde sme pokus o odpočúvanie vykonali.



Obr. 4.10: Zapojenie optického vysielača s vyznačením najvhodnejšieho miesta na odpočúvanie optického prenosu

Na pokus o odpočúvanie komunikácie sme v domácich podmienkach použili prípravok viditeľný na obrázku 4.11



Obr. 4.11: Prípravok na odpočúvanie optického prenosu

Optické vlákno, prostredníctvom ktorého je vykonaný prenos musíme v jednom bode ohnúť. Na tento účel nám môže slúžiť guľatý predmet a drážka, na ktorú vláknom vyvíjame tlak. V mieste ohybu je nutné dané vlákno očistiť, v záujme čo najlepšieho

šírenia svetla. Uprostred drážky je nutné vsunúť zalomené optické vlákno a následne ho prisunúť čo najbližšie k miestu ohybu vlákna, ktoré chceme odpočúvať. Celý úkon je nutné vykonať v odtienenom prípravku.

Vykonaný pokus v domácich podmienkach priniesol svoj úspech. Získaný signál bol síce na prahovej úrovni citlivosti, ale miestami sme dosahovali hodnoty, pri ktorých by bolo možné na obrazovke vidieť prenášaný obsah. Úroveň takto získaného signálu bola v rozmedzí 35 až 45 dBuV pričom šum samotného optického prijímača bol na úrovni 28 dBuV. Modulačná chybovosť MER 19 až 24, bitová chybovosť BER 10^{-2} až 10^{-4} pred opravou. Výsledok síce nie je najlepší, ale dokazuje skutočnú možnosť odpočúvania optickej komunikácie a to aj bez prerušenia optického vlákna. Treba len dbať na vysokú úroveň mechanického prevedenia prípravku, a na zvýšenú teplotu okolia v čase ohybu vlákna z dôvodu veľmi vysokej krehkosti optických vlákien.

Záver

Na základe vykonaných meraní a pokusov môžeme tvrdiť, že optický prenos informácií nie je najbezpečnejším spôsobom prenosu, ale úroveň zabezpečenia vyplývajúca z mechanickej konštrukcie vedení je dostatočná. Riziko odpočúvania následného zneužitia dát plynie hlavne z toho dôvodu, že optické dáta prenášané optickými vláknami telekomunikačných operátorov nie sú šifrované ako celok. Je to aj z dôvodu veľkej výkonnostnej náročnosti vzhľadom na prenosové kapacity poskytované optickými sieťami. Na rozdiel od optických prenosov je väčšina informácií prenášaných rádiovým prostredím šifrovaná, alebo inak ošetrená voči zneužitiu a neoprávnenému pripojeniu k rádiovej sieti. V rámci rádiových prenosov však vzniká problém, že prenášané informácie môže nenápadne zachytávať potenciálny útočník bez vynaloženia väčšej snahy. Následne zachytené informácie sa môže pokúsiť dešifrovať, pričom pravdepodobnosť dešifrovania prenášanej informácie vzduchom narastá v prípade použitia slabšieho šifrovacieho algoritmu a kľučov. Jedna z foriem ochrany prenášaných informácií optickými vláknami je fyzická ochrana vlákien. Máme na mysli ochranu za pomoci chráničiek a ich následné uloženie pod zemským povrchom, ideálne v súlade so stavebnou legislatívou. Tým je sťažený nielen samotný fyzický prístup k vláknam, ale aj výstavba v súlade so stavebným zákonom vzniká sieť vo verejnom záujme.

Súčasťou práce bolo overenie možností odpočúvania prenosu informácií prostredníctvom optických sietí. Možnosť odpočúvania sa však výrazne líši vzhľadom na charakter prevádzkovaných služieb vo vláknach a situáciu mení aj rozhodnutie, či sa má jednať o sledovanie prevádzky, alebo o potenciálny útok na vybratú obeť. Práca priblížila niekoľko možností odpočúvania s konkrétnym postupom. V jednom prípade sa jednalo o krádež prihlasovacích údajov a v druhom prípade sme sa pokúsili o sledovanie televízneho signálu v sieti káblového operátora. Na tento pokus sme využili hlavnú stanicu káblového operátora a zamerali sme sa na odpočúvanie digitálnych televíznych staníc. Pokus sme realizovali za pomoci optického prevodníku so zvýšeným optickým výkonom o úrovni viac než 16 dB na vlnovej dĺžke 1310 nm. Pravdepodobne to bol hlavný faktor, ktorý nám pokus o odpočúvanie uľahčil. Pri pokuse sa nám niekoľko krát podarilo dosiahnuť hodnoty, za pomoci ktorých by aspoň na krátku dobu bolo možné prenášaný digitálny televízny signál sledovať. Pri pokusoch sme tiež zistili, že prípravok, ktorý by mal slúžiť na odpočúvania optického prenosu vo

vlákne, musí byť veľmi precízny. Pri viacerých pokusoch sa nám podarilo odpočúvané vlákno poškodiť do takej miery že sa vlákno následne zlomilo. Ďalším problémom bolo, že intenzita takto odchyteného svetelného signálu bola aj napriek veľkému výkonu optického vysielača extrémne nízka ba až na prahu citlivosti.

Na základe vyššie uvedených výsledkov môžeme jednoznačne stanoviť, že odpočúvanie opticky prenášanej informácie nie je nemožné. Vyžaduje si veľkú precíznosť a vysokú úroveň technického prevedenia prípravku na odpočúvanie. V oboch prípadoch odpočúvania bolo nutné optické vodiče buď ohnúť, alebo úplne prerušiť. Z tohto dôvodu je možné takéto pokusy v prípade monitorovania intenzity svetelného signálu odhaliť dobrou konfiguráciou pohľadového systému, ktorý na prípadné prerušenia vedenia, alebo zmenu úrovne optického signálu upozorní operátora dohľadového centra.

Tieto prekážky však v prípade záujmu odpočúvania subjektov napríklad vládnymi organizáciami nespôsobujú žiaden problém. Z toho dôvodu je dôležité citlivé informácie prenášať šifrovanými komunikačnými kanálmi, čím minimálne sťažíme úlohu osobám a organizáciám, ktoré sa o odpočúvanie snažia, alebo sa ho reálne aj dopúšťajú.

Použitá literatúra

[1] FILKA, M. Optoelektronika pro telekomunikace a informatiku. CENTA, Brno 2009.

[2] FILKA, M. Přenosová média. Skripta laboratoře. VUT FEKT, Brno 2003.

[3] KUCHARSKI, M., DUBSKÝ, P. Měření přenosových parametru optických vláken, kabelu a tras. Mikrokom, Praha 2001.

[4] Norma CSN EN 60079-28 Výbušné atmosféry - Část 28: Ochrana zařízení a přenosových systému používajících optické záření, Česká státní norma, 10/2007.

[5] Dostalík, M.: Elektrická zařízení v prostředí s nebezpečím výbuchu, FCC PS Brno, Automa 1/2001

[6] Thomas, M. *Zabezpečení počítačových sítí bez předchozích znalostí.* CP Books, ISBN 80-251-0417-6, ČR, 2005

[7] Wendell, O. *Směrování a přepínání sítí.* Computer Press, ISBN 978-80-251-2520-5, ČR, 2010

[8] SOSINSKY, B. *Mistrovství - Počítačové sítě*. Computer Press, ISBN 9788025133637, ČR, 2010

[9] Internetový portál Mikrotik [online]
Dostupný na URL: <http://www.mikrotik.com/>

[10] RACOM – Informace o mikrovlnných rádiových spojoch. Dostupný z http://www.racom.eu