elektrorevue
ISSN 1213 - 1539

Rok / Year:	Svazek / Volume:	Číslo / Number:	Jazyk / Language
2018	20	4	CZ

Měření a testování optické trasy a aktivních prvků

Measurement and testing of optical path and active devices

Jakub Frolka, Petr Mlýnek

frolka@feec.vutbr.cz

Fakulta elektrotechniky a komunikačních technologií VUT v Brně

DOI: -

Abstract: The article deals with the assessment of the optical path for the stress testing of the network infrastructure on application layers L4–L7, where the load generator/analyzer is located at Brno University of Technology in Brno and the tested target environment is at Masaryk University in Brno. The article first describes the measurement of the optical path on the physical layer, the application layer and, finally, using Virtual Private Network and Mikrotik devices.

elektrorevue
ISSN 1213 - 1539

Měření a testování optické trasy a aktivních prvků

Jakub Frolka, Petr Mlýnek

Fakulta elektrotechniky a komunikačních technologií VUT v Brně
Email: frolka@feec.vutbr.cz

Abstrakt *– Článek se zabývá posouzením optické trasy pro zátěžové testování síťové infrastruktury na aplikačních vrstvách L4-L7, kdy zátěžový generátor / analyzátor je umístěn na VUT v Brně a testované cílové prostředí je na Masarykově univerzitě v Brně. Článek prvně popisuje měření optické trasy na fyzické vrstvě, dále na aplikační vrstvě a na závěr s využitím Virtual Private Network a zařízení Mikrotik.*

1 Úvod

Z pohledu datových sítí přináší optické systémy vysoce spolehlivé přenosové vlastnosti, jež ve srovnání s ostatními technologiemi (bezdrátové rádiové přenosové technologie) poskytují optické sítě mnohonásobně vyšší přenosové rychlosti a to v řádech desítek až stovek Gb s ohledem na využité technologie, která může být také v řádu tisíců až milionů Kč.

Pro měření fyzické vrstvy budou uvažovány metody: (i) přímá metoda, (ii) měření chromatické disperze, (iii) měření PMD a (iv) měření OTDR. Přímá metoda měření útlumu je základní metoda měření, levnější než ostatní, ale není tak přesná a nezjistí konkrétní body se závadami. Výstupem přímé metody je útlum celé trasy. Měření chromatické disperze umožní sledovat hodnoty chromatické disperze podle přenosové rychlosti systému, který na ní bude provozován dle normy[1]. V případě zjištění rozporu s uvedenými hodnotami, musí být provedeno odstranění nedostatků. Po odstranění těchto nedostatků se musí celé měření opakovat[2].

V poslední kapitole je popsáno testování přenosové rychlosti přes tunel Virtual Private Network (VPN), kdy jedna strana tunelu je zakončena na zařízení Mikrotik. Byla testována přenosová rychlost na několika zařízeních a výsledky byly prezentovány.

2 Metody měření fyzické vrstvy optické trasy

V experimentálním testu bylo provedeno měření optické experimentální trasy, jednalo se o test fyzické vrstvy sítě. Dle norem je využito měření pomocí metody OTDR (Optical time domain reflectometry), měření PMD (polarizační módová disperze) a CD (chromatické disperze). V neposlední řadě je také nutné brát v úvahu přímé měření útlumu optické trasy. Všechna tato měření určí výchozí a také základní parametry o trase, které je nutné sledovat. A díky výsledkům měření je možné pak na tyto trasy nasadit přenosové systémy.

Příkladem výsledků měření CD a PMD může být také určení uložení trasy, kde je viditelné, že část trasy je provedena v závěsu, oproti instalaci v zemi jsou opakovaná měření rozdílná a to z důvodu vlivu okolních jevů na volně instalované vedení. Právě tyto vlivy mohou ovlivnit ve svém důsledku rychlost a kvalitu přenosu.

Příkladem měření OTDR je zjištění fyzického stavu optické sítě, konkrétně se může jednat o kvalitu provedení svárů či spojek na optické trase či čistotu konektorů. Měření pomocí této technologie je velmi nákladné, ale zákazník získá kompletní přehled o každém metru trasy. Oproti tomu je využita také technologie přímého měření útlumů trasy, která nám řekne pouze její útlum, ale již nenapoví kvalitu jednotlivých úseků.

Zhodnocení ze všech výše uvedených aspektů je jasný přínos optické sítě a to v možnosti využití optické infrastruktury pro datové přenosy a také pronájmy regionálním či národním poskytovatelům komunikačních služeb. Další možností je využití pro efektivního řízení rozvoden či trafostanic, kde může být optický přenosový systém mimo jiné využit jako senzorický systém pro vyhodnocování stavu silnoproudé infrastruktury.

Pro měření byly využity přístroje od firmy EXFO FTB-200 (PMD), FTB-400 (OTDR) a FTB-600 (přímá metoda).

3 Výsledky měření fyzické vrstvy optické trasy

Cílem měření bylo provést měření optické trasy z VUT na MU. V rámci experimentálního testování bylo provedeno měření optické trasy, jednalo se o test fyzické vrstvy sítě. Dle norem bylo využito měření pomocí:

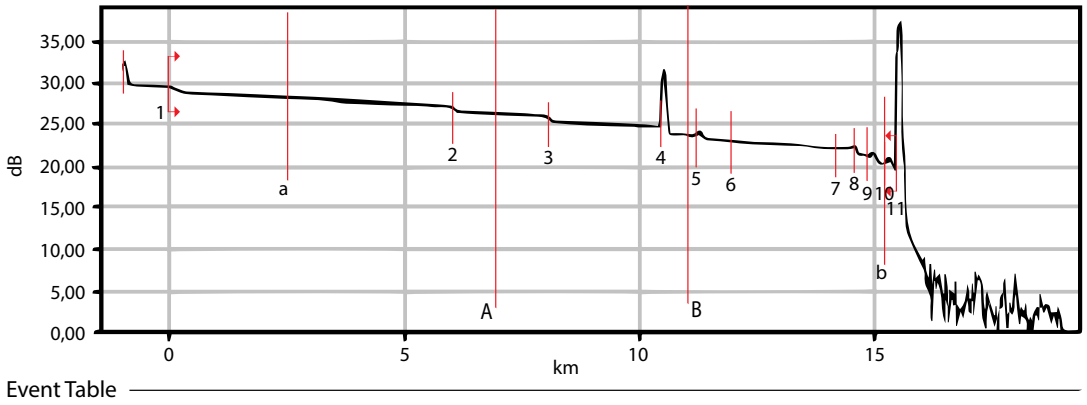
(a) přímé měření útlumu optické trasy,

(b) metody OTDR (Optical time domain reflectometry),

(c) měření CD (chromatická disperze) a PMD (polarizační módová disperze).

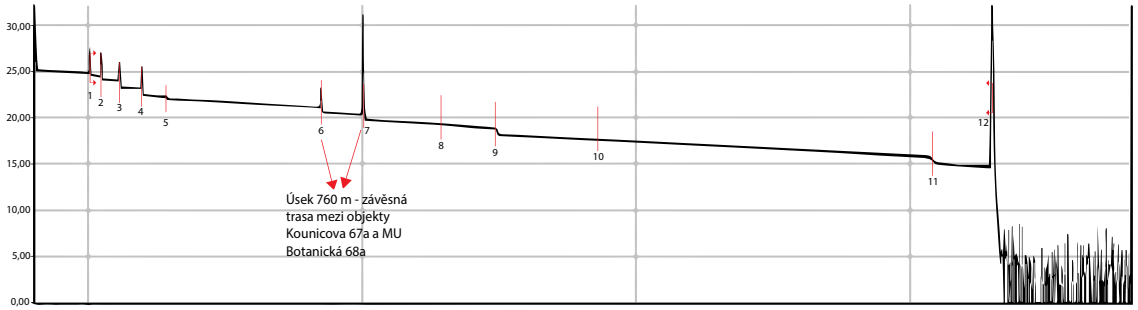
Všechna tato měření určí výchozí a také základní parametry o trase které je nutné sledovat. A díky výsledkům měření, je možné pak na tyto trasy nasadit přenosové systémy.

elektrorevue
ISSN 1213 - 1539



Type	Number	Location/Length (km)	Loss (dB)	Reflection (dB)	Attenuation (dB/km)	Cumul. (dB)
Launch Level		-1,0111		-46,5		
Section		1,0111	0,340		0,336	
Reflective	1	0,0000	0,502	-61,3		0,502
Section		6,0078	1,965		0,327	2,467
Non-Reflective	2	6,0078	0,393			2,860

Obrázek 1: Příklad výstupu měření metody OTDR.



Obrázek 2: Příklad výstupu měření metod CD a PMD.

(a) Přímé měření

Technologie přímého měření útlumů trasy ukázala útlum 8,6 dB a 9,75 dB pro vlnovou délku 1310 nm a 6,48 dB a 5,9 dB pro vlnovou délku 1550 nm (vlákno A a B). Toto měření přineslo pouze informaci o základním útlumu, ale již nenapoví kvalitu jednotlivých úseků. Základní metoda měření, levnější než OTDR. Není tak přesná a nezjistí konkrétní body se závadami.

(b) Metoda OTDR

Výsledkem měření OTDR bylo zjištění fyzického stavu optické sítě, konkrétně kvalita provedení svárů či spojek na optické trase či čistotu konektorů. Měřák na trase vyhodnotil špinavé konektory a útlum spojek, což je zcela běžné na tak členité trase. Na případné přenosy tento fakt nebude mít vliv, je možné dosahovat rychlostí od 1 do 100 Gb/s. Závada na trase by mohla být na 6,0103 km a 8,0291 km, mohlo by se jednat o nedokonalé spojky nebo sváry. Dále na 10,4664 km se jedná o nevyčištěný konektor. Nevyhovující útlumy jednotlivých úseků jsou způsobeny již počátečním útlumem na 6,0103 km. Opět při této délce trasy by tyto chyby neměly mít vliv na přenosovou rychlost. Měření pomocí této technologie je velmi nákladné, ale přineslo kompletní přehled o každém metru trasy.

Příklad výstupů měření lze vidět na obrázku 1.

(c) Měření CD a PMD

Výsledkem měření CD a PMD mimo disperzi je také určení uložení trasy, kde na obrázku 2 je viditelné, že část trasy je provedena v závěsu, oproti instalaci

elektrorevue
ISSN 1213 - 1539

v zemi jsou opakovaná měření rozdílná, a to z důvodu vlivu okolních jevů na volně instalované vedení. Právě tyto vlivy mohou ve svém důsledku ovlivnit rychlost a kvalitu přenosu.

Trasa musí splňovat hodnoty chromatické disperze podle přenosové rychlosti systému, který na ní bude provozován dle normy. V případě zjištění rozporu s uvedenými hodnotami, musí být provedeno odstranění nedostatků. Po odstranění těchto nedostatků se musí celé měření opakovat.

PMD na trase se velmi rychle mění dle okolních podmínek trasy, je třeba zdůraznit, že vliv PMD je až od přenosových rychlostí Gb/s s tím, že na trase, není zcela jasné, jestli bude třeba tyto rychlosti přenášet a zda by mělo PMD vliv na přenos na takovou vzdálenost. Ale pro korektní využití trasy a sledování její kvality je třeba měření disperzí dle norem vždy provést.

Z velmi rozdílných hodnot měření plyne také fakt, že trasa obsahuje závěsný úsek, který by měl být náchylnější na polarizační disperzi, protože na něj působí více vnějších vlivů, něž na zemní trasu.

PMD odhalí:

- Náhodnost výskytu na trase – možno odhalit polarizačním reflektometrem.
- Vliv okolí a aktuálních podmínek může měření značně ovlivnit.

3.1 Zhodnocení měření na fyzické vrstvě

Měřená trasa je v praxi spíše využívána jako páteřní síť městem. Nevýhodou měřené trasy je to, že je příliš členitá, tzn. je složena z více kabelových úseků. Trasa by byla schopna přenášet rychlosti od 1 Gb/s do 100 Gb/s (což dokazuje test na aplikační vrstvě). Tyto rychlosti je možné násobit s využitím trasy A i B.

Dále je možné využít i multiplexování signálu, vytvoření více kanálů přenosu na základě vlnového multiplexu CWDM případně DWDM. To znamená, že rychlosti je možné násobit, ale u této délky trasy je to nevyužitelné a zbytečně drahé.

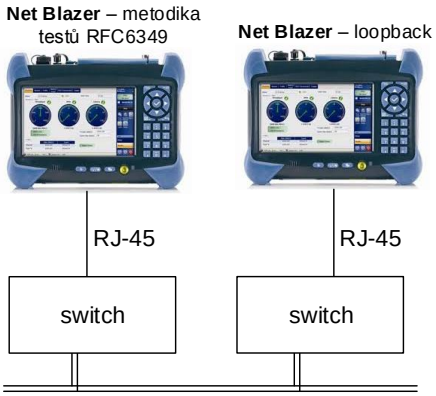
Fyzické parametry trasy vyplývají z měření, kdy byl proměřen celkový útlum trasy A a B. A dále byla trasa proměřena reflektometrickou metodou. Trasa je v pořádku, bez problémů zvládne desítky Gbit/s (což dokazuje test na aplikační vrstvě). Na trase se vyskytují zcela běžné závady, které nemají vliv na komunikaci.

3.2 Měření na aplikační vrstvě

Měření proběhlo s testery NetBlazer a dle metodiky RFC 6349, které používají TCP spolehlivý protokol [3], dle zapojení na obrázku 3.

Použité optické rozhraní testeru má 1 Gbit/s na fyzické vrstvě, to je limitujícím faktorem. Výsledky měření jsou následující:

- 0,9389 Gbit/s (rychlost na linkové vrstvě, blízká aplikační)
- 0,181 ms
- 0 % ztrátovost



Obrázek 3: Schéma zapojení.

4 Měření přenosové rychlosti VPN

Z důvodu plánované spolupráce s MU byl proveden průzkum možností, jak nejjednodušším způsobem lokality propojit. Jednou z uvažovaných variant bylo využití VPN (Virtual Private Network) tunelu. Z důvodu zájmu využití zařízení Spirent Avalanche vlastněného VUT pro generování provozu na pozadí infrastruktury virtualizovaného prostředí, byl zájem o zabezpečený VPN tunel přenášející i informace linkové vrstvy OSI modelu. Byla zkoumána možnost využití OpenVPN. Jelikož na vstupu experimentální sítě VUT je umístěno zařízení Mikrotik, bylo testováno jeho použití jako VPN klienta. První měření přenosové rychlosti bylo provedeno přes veřejnou síť a bylo dosaženo rychlosti pouze 8 Mbit/s. Následně bylo hledáno limitující místo, které se po zkoumání ukázalo být právě zařízením Mikrotik. Bylo provedeno měření přenosové rychlosti pro několik modelů zařízení Mikrotik. Výsledky měření jsou uvedeny v tabulce 2.

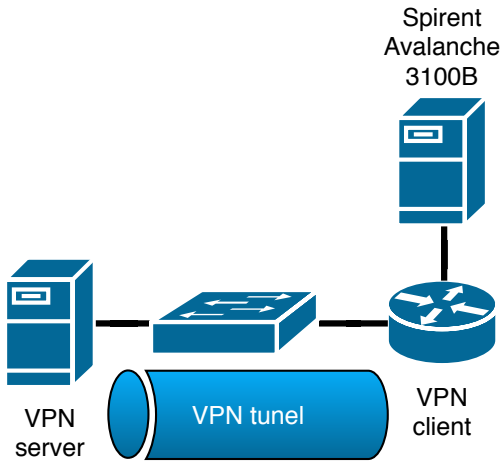
4.1 Laboratorní prostředí

Pro experimentální měření přenosové rychlosti zařízení Mikrotik bylo použito zapojení dle blokového schématu uvedeném na obrázku 4.

Jako VPN server byl použit server s následujícími parametry:

- procesor: Intel® Xeon® E5-2603 v4 @ 1,7 GHz, 15MB cache, 6 jader, RAM: 32GB, NIC: 1 GbE,
- OS: Linux Ubuntu 18.04.1 LTS, 64bit, kernel: 4.15.0-29-generic,
- OpenVPN server 2.4.4-2, Apache 2.4.29.

elektrorevue
ISSN 1213 - 1539



Obrázek 4: Zapojení v laboratoři.

Tabulka 1 obsahuje parametry vybraných zařízení mikrotik, které byly použity pro měření přenosové rychlosti VPN. Obsahuje zástupce přepínače, domácího wifi směrovače a několika dalších směrovačů. Pouze modely RB1100AHx2 a CCR1016-12S-1S+ mají vícejádrové procesory.

Tabulka 1: Parametry testovaných zařízení Mikrotik.

Model	**Procesor**		**Cena**
	Frekvence [MHz]	Počet jader	Kč
CRS226-24G-2S+	400	1	6 358
RB493G	680	1	4 378
RB941-2nD	650	1	483
RB1200	680	1	7 678
RB1100AHx2	1 066	2	7 678
CCR1016-12S-1S+	1 200	16	16 390

4.2 OpenVPN

OpenVPN patří mezi volně dostupný software, který umožňuje vytvořit šifrovaný VPN tunel mezi dvěmi sítěmi. Pro šifrování využívá OpenSSL knihovny a proto podporuje veškeré šifrovací algoritmy, které tato knihovna nabízí [4]. VPN server umožňuje vytvořit tunel, který může být v jednom ze dvou režimů a to tunel síťové vrstvy (IP) a tunel linkové vrstvy (ethernet) OSI/ISO modelu. Také lze nastavit typ protokolu pro přenos dat, jsou to protokoly UDP a TCP. V článcích [5] a [6] autoři provedli výkonnostní srovnání využití TCP a UDP protokolu a srovnání IP tunelu OpenVPN a OpenSSH. Označili protokol UDP a tunel OpenSSH jako lépe využívající linku. V tomto článku se zabýváme tunelem linkové vrstvy, který bývá také označován jako v režimu bridge. Zařízení Mikrotik ve stávající verzi RouterOS, podporuje OpenVPN tunel pouze přes protokol TCP.

Testovaná zařízení Mikrotik pro OpenVPN tunel podporují následující šifry:

- AES128, AES192, AES256,
- Blowfish128.

Konfigurace OpenVPN serveru použitá pro testování je uvedena na ukázce nastavení 1:

```
port 40060
proto tcp-server
dev tap
up "/etc/openvpn/up.sh br0 ens192"
server-bridge 10.10.1.1 255.255.255.0
                        10.10.1.10 10.10.1.100

ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh.pem

cipher AES-128-CBC
auth SHA1

keepalive 10 120
persist-key
persist-tun
log  /etc/openvpn/openvpn.log
verb 3
```

Ukázka nastavení 1: Konfigurace OpenVPN serveru.

4.3 Měřící zařízení Spirent Avalanche 3100B

Zařízení Spirent Avalanche, které je zobrazeno na obrázku 5, je využíváno k bezpečnostnímu a výkonnostnímu testování síťových infrastruktur. Díky funkci simulace serveru umožňuje testovat klientská zařízení, ale umí simulovat také i stranu klientů a tudíž je možné testovat i serverová zařízení. Je tedy využíván jako generátor síťového provozu. Umožňuje generovat síťový provoz dle referenčního modelu ISO / OSI na 4-7 vrstvě. Výsledky testování jsou uvedeny v přehledných grafech a detailních informacích o průběhu testů [7].

Obrázek 5: Spirent Avalanche 3100B.

4.4 Metoda měření

Na VPN serveru byl nainstalován webový server Apache, který poskytoval kopii webové stránky VUT. Na klientském zařízení Mikrotik byl nastaven VPN tunel v módu

elektrorevue
ISSN 1213 - 1539

Tabulka 2: Výsledky měření přenosové rychlosti OpenVPN na zařízeních Mikrotik.

	AES128		**AES256**		**Blowfish128**	
	Vytíž. CPU VPN serveru	**Rychlost**	**Vytíž. CPU VPN serveru**	**Rychlost**	**Vytíž. CPU VPN serveru**	**Rychlost**
Model	[%]	[Mb/s]	[%]	[Mb/s]	[%]	[Mb/s]
CRS226-24G-2S+	4	8	3	6,7	5	5,8
RB493G	11	35	14	30,4	21	33,4
RB941-2nD	9	28,5	8	20,4	13	27,7
RB1200	27	85,9	25	77,3	50	84,5
RB1100AHx2	32	93,1	31	83	52	96,3
CCR1016-12S-1S+	33	102,5	33	102,5	61	102

bridge ve kterém byl zapojen i Spirent Avalanche. Avalanche sloužil jako generátor síťového provozu klientů, kdy byly generovány HTTP GET požadavky na soubor index.html o velikosti 68 kB. Průběh testu byl nastaven tak, aby postupně vzrůstal počet klientů do maximálního počtu, kdy přenášený provoz byl bezeztrátový. U jedno jádrových zařízení docházelo u maximální přenosové rychlosti ke kolísání přenosu z důvodu vytížení procesoru na maximum a postupnému vyřizování uložených požadavků v mezipaměti. Vytížení procesoru na těchto zařízení bylo rozloženo 70-75% služba OpenVPN a zbytek ostatní režie zařízení. Nastavení testů bylo upravováno dokud nebyla nalezena hranice maximální přenosové rychlosti, kdy nedocházelo ke kolísání rychlosti přenosu. U modelů RB1100AHx2 a CCR1016-12S-1S+ bylo plně vytíženo jedno jádro službou OpenVPN a ostatní režie na jiných jádrech.

Z podporovaných šifer AES byla testována varianta o délce 128 a 256 bitů, pro každou testovanou šifru bylo provedeno 5 měření a výsledné průměrné hodnoty byly uvedeny do tabulky 2. V této tabulce také najdeme hodnotu vytížení jednoho jádra procesoru na VPN serveru. Přenosové rychlosti u testovaných šifer se na zařízení Mikrotik liší v řádku jednotek Mb/s, rozdíly jsou pak na vytížení procesoru na VPN serveru. Jak je z tabulky 2 patrné, tak maximální přenosová rychlost přes tunel OpenVPN na zařízeních Mikrotik je přibližně 100 Mb/s, pokud se jedná výkonný směrovač, který má vícejádrový procesor. Kromě modelu RB941-2nD, který má rozhraní podporující pouze rychlost 100 Mb/s, měla všechna ostatní zařízení rychlost 1 Gb/s. Velká ztráta přenosové rychlosti, která je způsobena využíváním OpenVPN je způsobena šifrováním veškeré komunikace, která je řešena softwarově a tím úzce spojena i s nedostatečným výkonem procesoru na zařízeních Mikrotik. U modelů, které mají více jader procesoru, docházelo k využívání pouze jednoho jádra procesoru pro OpenVPN a proto jsou výsledky nižší než by mohly být při využití více jader procesoru. Jedním z možných řešeních jak snížit nároky na výpočetní výkon zařízení by mohla být implementace hardwarové akcelerace šifrování přímo do procesoru, jak je tomu u tunelu IPsec [8], a nová implementace podporující využití více jader procesoru.

5 Závěr

Článek představil měření základních parametrů optické trasy až po metody měření komplexního přehledu o každém metru optické trasy. Měření ukázalo velmi členitou trasu složenou z několika kabelových úseků. V neposlední řadě ukázalo část optické trasy v závěsu, který je náchylný na polarizační disperzi, jelikož na něj působí vnější vlivy a jednak tento úsek představuje vyšší riziko pro dosažení spolehlivosti a dostupnosti (větrné podmínky, pád stromů atd). Měření na aplikační vrstvě bez koncových prvků ukázalo rychlosti jednotky až 100 Gbit/s. S uvažováním koncových prvků, konkrétně Mikrotik a různých druhů zabezpečení, byly ukázány výrazné degradace přenosových rychlostí. Využití OpenVPN tunelu a jeho šifrování komunikace se ukázalo jako výpočetně náročné pro zařízení Mikrotik. I pro nejvýkonnější více jádrový testovaný Mikrotik byla maximální přenosová rychlost pouze 102 Mb/s, to bylo způsobeno využitím pouze jednoho jádra procesoru. K navýšení přenosové rychlosti by mohlo dojít až v případě, kdyby implementace OpenVPN na zařízeních Mikrotik umožňovala využití více jader procesoru. U jednojádrových zařízení jsou uvedené přenosové rychlosti maximální možné a v praxi budou nižší, kvůli povaze zařízení Mikrotik, kdy plní více funkcí např. NAT (Network Address Translation), směrování atp. Pokud se bude jednat o nenáročné nebo domácí použití vyžadující nižších přenosových rychlostí, bude nejvýhodnějším z testovaných zařízením Mikrotik model RB941-2nD, kvůli jeho nízké doporučené ceně a podobným přenosovým rychlostem jako u dražších modelů. Pokud jsou vyžadovány vysoké přenosové rychlosti je výhodnější využít klasický server, který bude dosahovat lepších výsledků než zařízení Mikrotik.

Literatura

[1] ČUČKA, M.; ŠALÍK, P.; RÓKA, R.; MÜNSTER, P.; FILKA, M. *Simulation Models of Pulse Generator for OTDR in Matlab and VPIphotonics.* In The 2018 41st International Conference on Telecommunications and Signal Processing (TSP). 2018. s. 179-183. ISBN: 978-1-5386-4695-3.

elektrorevue ISSN 1213 - 1539

[2] ČUČKA,M.; MÜNSTER, P.; KOČÍ, L.; HORVÁTH, T.; FILKA, M.; VOJTĚCH, J. *Transmission of high power sensor system and DWDM data system in one optical fiber.* Journal of Communications Software and Systems, 2016, roč. 12, č. 4, s. 190-194. ISSN: 1845-6421.

[3] *RFC 6349 - Framework for TCP Throughput Testing.* [online] [cit. 2018-08-20] Dostupné z: `https://tools.ietf.org/html/rfc6349`

[4] *Openvpn. Openvpn24ManPage – OpenVPN Community* [online] [cit. 2018-08-20] Dostupné z: `https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage`

[5] COONJAH, Irfaan, Pierre Clarel CATHERINE a K. M. S. SOYJAUDAH. *Experimental performance comparison between TCP vs UDP tunnel using OpenVPN.* In: Computing, Communication and Security (ICCCS), 2015 International Conference on [online]. IEEE, 2015, s. 1-5 [cit. 2018-08-20]. DOI: 10.1109/CCCS.2015.7374133.

[6] COONJAH, Irfaan, Pierre Clarel CATHERINE a K. M. S. SOYJAUDAH. *Performance evaluation and analysis of layer 3 tunneling between OpenSSH and OpenVPN in a wide area network environment.* In: Computing, Communication and Security (ICCCS), 2015 International Conference on [online]. IEEE, 2015, s. 1-4 [cit. 2018-08-20]. DOI: 10.1109/CCCS.2015.7374130.

[7] *SPIRENT AVALANCHE 3100B, 2011. In: Spirent* [online]. [cit. 2018-08-20]. Dostupné z: `https://www.infopoint-security.de/medien/spirent_avalanche_3100_datasheet.pdf`

[8] "Manual:IP/Ipsec - Hardware acceleration - Mikrotik Wiki. [online] [cit. 2018-08-20] Dostupné z: `https://wiki.mikrotik.com/wiki/Manual:IP/IPsec`