Technológia IPv6, jéj bezpečnosť a nasadenie

IPv6 Technology, Security and Deployment

Lukáš Urbančok, Ivan Kovár, David Pala

Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, Nad Stráněmi 4511, 760 05 Zlín, Česká republika

urbancok@fai.utb.cz, ikovar@fai.utb.cz, pala@fai.utb.cz

Abstrakt: Cieľom tohto článku je preskúmať nastupujúcu technológiu IPv6 jéj bezpečnosť a nasadenie pri implementovaní infraštruktúry rozvojové platformy. Praktické laboratórne cvičenie znázorňuje ukážkový postup ako nakonfigurovať IPv4 a IPv6 zariadenia a pripraviť sa na prechod z existujúcej fiktívnej IPv4 na IPv6 sieť pomocou GNS3. Príspevok sa venuje možnostiam zvyšovania bezpečnosti a popisuje hrozby, ktoré ohrozujú IPv6. V záveru článku je popísaná platforma s IPv6 a možnosťami aplikácie SDN (softvérovo definované siete), virtuálnej reality a Internetu vecí.

Kľúčové slová: IPv4, IPv6, SDN, GNS3, počítačové siete, infraštruktúra, laboratórne cvičenie, virtuálni platforma.

Abstract: The aim of this article is to create lab exercises using the IPv6 technology. It also deals with the IPv6 safety implementation and deployment across network infrastructures of development platforms. The main focus of the labs are the advancing IPv6 technology, and exercises can also serve as a procedure to configure the IPv4 and IPv6 devices and prepare to make the transition from the fictitious existing IPv4 to IPv6 network using GNS3. There is also analyzed the IPv6 theoretical foundation of the technology in the paper. There are described increasing security and the threats that endanger IPv6 in the article. In conclusion, the article describes platform with IPv6 applications SDN (Software-defined networking), virtual reality and the IoT.

Keywords: IPv4, IPv6, SDN, GNS3, computer network, infrastructure, labs, virtual platform.

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. 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. 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 korporačných sietí, je potrebné pripraviť sa a dôsledne zvážiť nasadenie nového protokolu, hodnotením nákladov a kritických aplikácií ako technológiami autonómnych vozidiel, riadiacich mechanizmov, virtualizácie, cloud computingu, Internetu vecí. 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. [1]

Cieľom tohto článku je zoznámenie sa s technológiou IPv6 a metódami, ktoré sa používajú pri prechode zo v súčasnosti ešte stále atraktívnejšej IPv4. V článku je analyzovaná technológia IPv6, jéj bezpečnosť a nasadenie. Na základe rozboru hlavičky sa uvažuje o bezpečnosti daného protokolu v porovnaní s predchádzajúcou verziou. Naviac článok skúma bezpečnosť a hrozby protokolu IPv6 a sieťových služieb, ktoré prináša. V prípade zdieľania dát s cloudom, veľkú pravdepodobnosť výskytu tzv. jitter kde prichádzajúce pakety majú kolísajúcu prenosovú rýchlosť a pre niektoré aplikácie (komunikačné platformy s audio vizuálnym vstupom a výstupom) to môže spôsobovať sekanie obrazu prípadne vyžadovať dynamickú šírku pásma. Tieto požiadavky je možné riešiť i technológiou IPv6 nastavením kvality služieb nastavením priorít služieb. Môže byť vyhradená šírka pásma a infraštruktúra je riadená na aplikačnej úrovni.

Druhá časť článku sa venuje možnostiam nahradenia reálnej siete emulačným/simulačným modelom. Na vytvorenie cvičnej úlohy je využitý program GNS3 (Graphical Network Simulator 3). Dané laboratórne cvičenie je zamerané hlavne na nastupujúcu technológiu IPv6. Podobné fiktívne príklady pomáhajú zvyšovať úspešnosť zmeny pred skutočným nasadením, čím sa eliminujú nežiaduce chyby a skryté hrozby. V rámci projektu IGA sa zaoberáme platformou pre prenosné audio vizuálne zariadenia pre projekciu zvuku a obrazu. Danou emuláciou je možné testovať a cvičiť nasadenie infraštruktúry modernej platformy virtuálnej reality, ktorá má vysoké sieťové nároky, na rýchlosť sťahovania a nahrávania dát na cloud, počet senzorov, narastajúci počet užívateľov, neštruktúrovaný obsah, čo práve inovácia SDN s IPv6 rieši. Moderná platforma má vysoké sieťové nároky, na rýchlosť sťahovania a nahrávania dát na cloud. Vývoj a implementácia kvality služieb v rámci pokračovania daného projektu je nevyhnutná. Nakoľko daná platforma pracuje so streamovaným video a audio obsahom, interaktívnymi aplikáciami, ktoré sú citlivé na riadenie a straty paketov. IPv6 má v hlavičke prítomnú identifikáciu tokov paketov, čo pomáha šetriť náklady. [2]

1. Protokol IPv6

IPv6 (Internet Protocol verzia 6) je nová verzia protokolu sieťovej vrstvy, ktorá sa používa pri komunikácii. Správcovia sami nasadzujú protokol kvôli väčšiemu rozsahu adries, rozšíreniu na trhoch a využívaniu jeho možností pri vývoji aplikácií (Internet vecí). *[3]*

Jadro IPv6 je definované v dokumente RFC 2460 (Request for Change) s konceptom paketov, adries, rozdelenie celého rozsahu, ako aj pravidlá a roly koncových staníc a smerovačov. Tieto pravidlá dovoľujú zariadeniam prepínať a smerovať pakety od zdroja naprieč niekoľkými smerovačmi (IPv4 definuje podobný koncept v dokumente RFC 791). Nástup novej IPv6 nie je jednoduchý. Na záver tejto časti je uvedená zhrňujúca tabuľka (*Tab. 1*) s porovnaním IPv4 a IPv6 podľa formátu hlavičky. *[1]*

Tab. 1: Porovnanie technológií IPv4 s IPv6 na základe rozdielu hlavičky. [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 QoS**	Identifikácia tokov paketov na zabepečenie **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 **podsiete naraz**	Pomocou **broadcast** adresy môžu byť adresované uzly určitej **podsiete naraz**

2. Bezpečnosť IPv6

Veľa bezpečnostných rizík asociovaná s IPv4 je spojená aj s novou IPv6. Znamená to, že je potrebné implementovať bezpečnostné mechanizmy a riadiť bezpečnosť oboch sád protokolov. Táto časť analyzuje nové bezpečnostné hrozby pre technológiu IPv6:

2.1. Hrozby IPv6

Nástup IPv6 priniesol v oblasti bezpečnosti 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. Skenery a červy, ktoré fungujú na IPv4 budú fungovať i na IPv6. Problém je i neuvedomenie si prítomnosti IPv6. Nové spôsoby IPv6 útokov implementujú nové metódy útokov ako výsledok manipulácie s paketmi a správami NDP:

- **Protokol objavovania susedov (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). Pri MiTM, útočník vidí všetky poslané pakety. *[5]*

- **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.

- **ICMPv6**

Tento protokol je často použitý v IPv6 ako aj NDP. Manipuláciou tohto protokolu môže útočník spôsobiť 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 hosť si môže pre seba automaticky prideľovať 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 zaria-deniu. Pomocou získaného prístupu cez jednu sadu, si útočník môže upraviť konfi-guráciu tak, ako mu to na jeho účely vyhovuje.

- **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. *[5]*

3. Laboratórna úloha nasadenia IPv6 v sieti IPv4

Praktické laboratórne cvičenie znázorňuje ukážkový 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. Laboratórna úloha bola vypracovaná na OS X 10.11.1 s VirtualBoxom a testoval som GNS3 1.4.1 i na W10 a Kali Linux. *[6]*

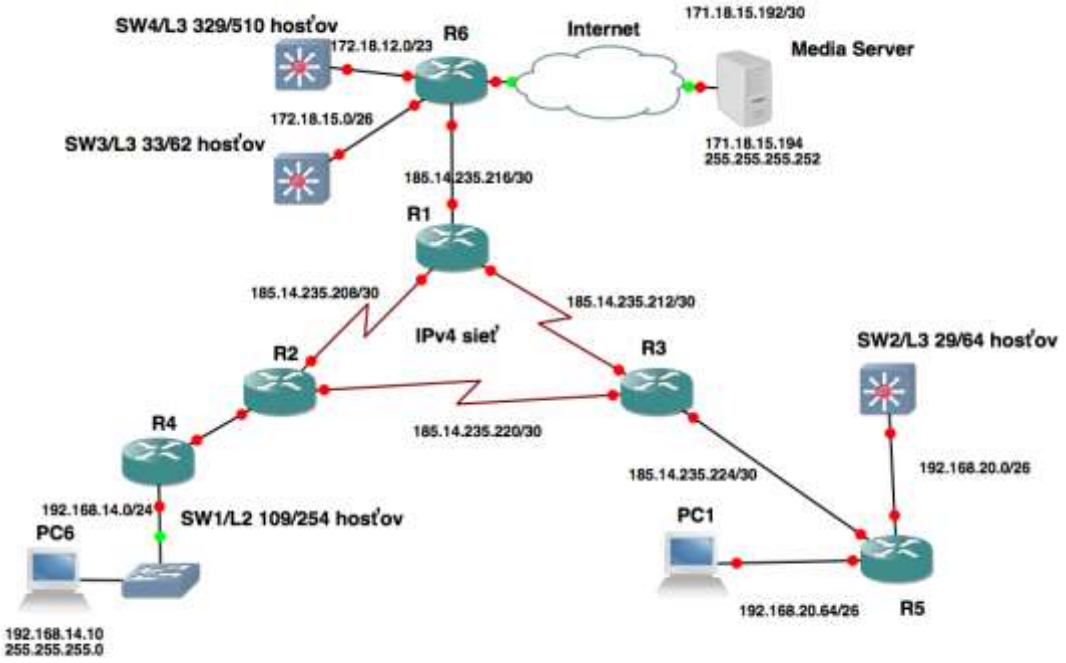
3.1. Plánovanie a management adries

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 adries, nakonfigurovanie smerovačov klasickým IPv4. Management adries je uvedený v tabuľke nižšie, kde boli preIPv6 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 zpätnovazbovým slučkám smerovačov. Pre prístupovú vstvu LAN sietí boli vybraté adresy z fd00:cb20:x::/64. Aby bolo dané cvičenie prehľadnejšie a pochopiteľnejšie, boli vyberané xx pre rozhranie smerovačov. Pre zpätnovazbové slučky (loopback) zariadení boli použité adresy z prefix 2a00:cb20:f::/112. Management adries 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. *[7]*

Pre PC6 je zadaná požiadvka na konfiguráciu pomocou dynamicky pridelenej adresy EUI-64 podľa MAC v oblasti 20. V oblasti 30 je zadaná požiadavka na priraďovanie adries 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. *[8]*

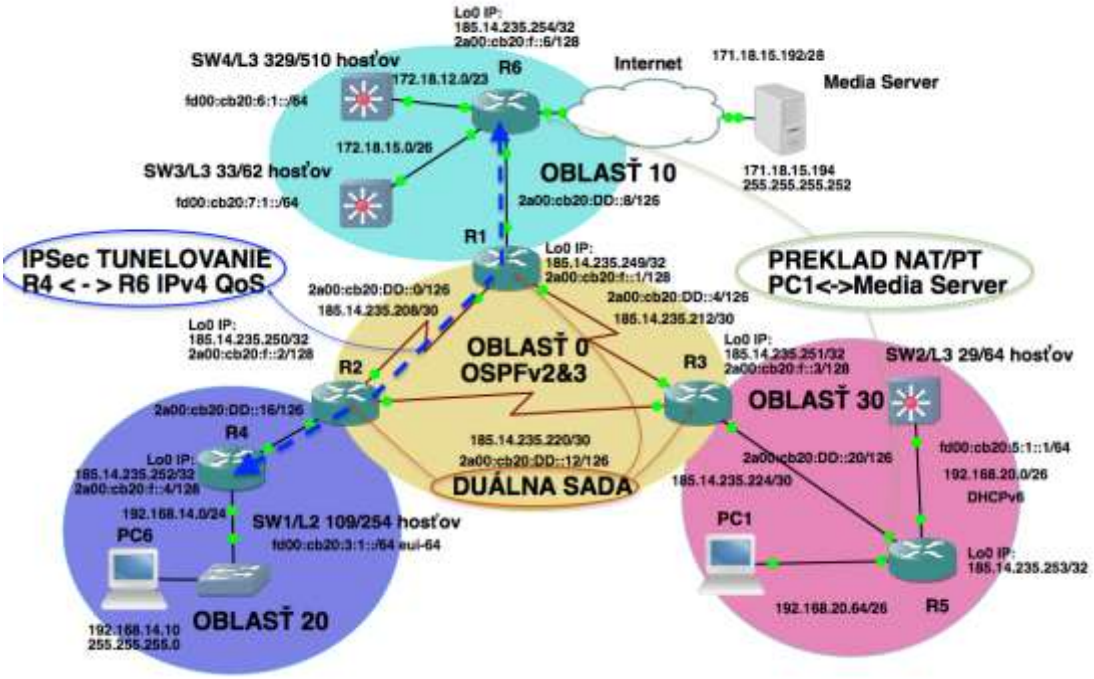
3.2. Topológia zákazníckej siete

V článku bola vytvorená laboratórna úloha, ktorá má za cieľ zoznámiť sa s návrhom a riešením migrácie z IPv4 na IPv6. Na *Obr. 1* nižšie je znázornená topológia IPv4 siete zákazníka, ktorá zabezpečuje dostupnosť všetkých zariadení. 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. 1: 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. 2: Topológia IPv4 siete s podporou IPv6 [autor]

3.3. Adresovanie na úrovni sieťovej vrstvy

Na základe požiadaviek zákazníka, bola navrhnutá adresácia IPv4 a IPv6. Každé zariadenie obsahuje i zpätnovazbovú slučku, využitú v smerovacích protokoloch a tunelovaní, čo rieši výpadok na fyzickej vrstve.

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

3.4. Konfigurácia sieťových zariadení

Konfigurácie a zdrojové kódy zodpovedajúcim zariadeniam sú dostupné v elektronickej podobe autora. Dané konfigurácie a sú testované a ladené pomocou *show debug* príkazov. Po nastavení základnej konfigurácie prístupu a hesiel systému. Nasleduje nastavenie tretej vrstvy 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 rozhraniam. V poslednom kroku je nastavovaný *DHCP* server, *IPSec* tunel a *NAT-PT* preklad. *[8][9]*

Tab. 3: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]

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

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} adries, automatická konfigurácia na zariadenia, zjednodušenie formátu hlavičky s dodatočnou možnosťou rozšírenia – mobilita (pohyb bez nutnosti reinicializácie spojenia), smerovanie, kvalita služieb (identifikácia dátových tokov) a bezpečnosť (autentifikácia a šifrovanie medzi hosťami v sieti*). [4]*

Koncové stanice (virtuálna a rozšírená realita, inteligentné telefóny, hodinky, laptopy, zariadenia IoT a iné), ale hlavne aktívne prvky (prepínače, smerovače, Firewally, VPN koncentrátory a pod.) využívajú na komunikáciu známe protokoly (stovky) modelu TCP/IP za účelom smerovania, mapovania adries či využitia aplikácií koncových staníc. Sieťový administrátori a inžinieri hľadajú neustále spôsoby ako vylepšovať výkonnosť siete, skúmať správanie a testovať komplexné prostredie zákazníka sieťovej štruktúry, aby zvyšovali poskytovanú hodnotu.*[9]*

Náplňou tohto článku bolo preskúmať protokol IPv6. Vychádzala z formátu hlavičky a RFC dokumentov. Ďalej bola analyzovaná bezpečnosť IPv6, autentifikácia, sieťové služby ako smerovanie a kvalita služieb. Praktická časť sa smerovala k vytvoreniu laboratórnej úlohy v aplikácií GNS3, kde sú nakonfigurované zariadenia pre funkčnosť s protokolom IPv6. V *Tab 3* sú exportované konfigurácie a zdrojové kódy zodpovedajúcim zariadeniam. V rámci projektu IGA je riešená moderná platforma pro prenosné audio vizuálne zariadenia pre projekciu zvuku a obrazu, ktorá má v prípade zdieľania dát s cloudom, veľkú pravdepodobnosť výskytu tzv. jitter kde prichádzajúce pakety majú kolísajúcu prenosovú rýchlosť a pre platformu to môže spôsobovať sekanie obrazu prípadne dynamickú šírku pásma. GNS3 je skvelý nástroj na testovanie sieťovej infraštruktúry platformy pre rozvoj chorých v sociálnych centrách, školách s využitím asistenčných technológií a virtuálnej reality. Tieto požiadavky je možné riešiť i technológiou IPv6 nastavením kvality služieb pre uprednostnenie aplikácie v platforme. Môžu jej byť definovaná priority a vyhradená šírka pásma a daná infraštruktúra je riadená cloudom na úrovni aplikačnej vrstvy. Kvalita služieb (QoS) v rámci lokálnej siete nasadenej platformy rieši obmedzenia rýchlosti. Avšak v prípade nasadenia veľkého množstva virtuálnej reality, je potrebné riešiť lokálne zdieľané úložisko. [10]

IPv6 prináša veľa výhod i v kombinácií s nastupujúcimi inteligentnými aplikáciami virtuálnej a rozšírenej reality, cloud computingu a Internetu vecí. Tieto aplikácie obsahujú automatizáciu, škálovateľnost v adresácii, pružnosť v agregácii premávky a zmien v infraštruktúre podľa potrieb aplikácií. Podľa moderného prístupu sa javí spojenie prístupu softwarovo definovaných sietí (SDN) a technológie IPv6 ako možné riešenie sieťovej architektúry, ktorá by bola schopná splniť požiadavky kladené Priemyslom 4.0. V ďalšom nadväzujúcom článku v rámci IGA projektu bude riešená moderná platforma virtuálnej reality, ktorá má vysoké sieťové nároky, na rýchlosť sťahovania a nahrávania dát na cloud, počet senzorov, narastajúci počet užívateľov, neštruktúrovaný obsah, čo práve inovácia SDN s IPv6 rieši. [11]

Poďakovanie

Článok bol spracovaný v rámci projektu IGA Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky za podpory IGA / FAI / 2017/024.

Zoznam použitej literatúry

[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] Cisco Networking Academy Course Catalog, [Online]. [cit. 2016-9-28]. Dostupné z : *http://www.cisco.com/web/learning/netacad/course_catalog/CCNAexploration*

[7] GNS3 | *Graphical Network Simulator*. [Online]. [cit. 2016-9-28]. Dostupné z: http://www.gns3.net/.

[8] Urbančok, Lukáš. *Technologie IPv6, její bezpečnost a simulace sítí s využitím GNS3*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2016, 100 s. diplomová práce (Ing.). Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav počítačových a komunikačních system, Vedoucí práce Korbel, Jiří. Dostupné také z: *https://portal.utb.cz/wps/portalurlid=prohlizeni-prace=43440*

[9] 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.

[10] BARKER, Keith a Scott MORRIS. *CCNA security 640-554 official cert guide. Indianapolis,* IN: CISCO Press, 2013. ISBN 1587204460.

[11] C. W. Tseng, S. J. Chen, Y. T. Yang, L. D. Chou, C. K. Shieh and S. W. Huang, "IPv6 operations and deployment scenarios over SDN," *Network Operations and Management Symposium (APNOMS), 2014 16th Asia-Pacific*, Hsinchu, 2014, pp. 1-6. DOI: 10.1109/APNOMS.2014.6996530