COMPUTER NETWORKS BASED ON VYOS AND CISCO IOS OPERATING SYSTEMS

Denis Jalovecky
Bachelor Degree Programme (3), FEEC BUT
E-mail: xjalov05@vutbr.cz

Supervised by: Aneta Koláčková
E-mail: xkolac15@stud.feec.vutbr.cz

Abstract: This thesis focuses on configurations and issues of network protocols in operating systems of Cisco IOS and VyOS routers. One of the main goals include choosing the most appropriate emulator and installation of this emulator in virtual enviroment. The thesis also describes the properties and differences of protocols and their application in the network operating systems mentioned above.

After learning about possibilities of emulations, two scenarios, in which the protocols were applied and analyzed, were created. These scenarios meet standard of a lab excersise which takes around one and a half hour. The most frequent issues and their solutions are mentioned as well.

Keywords: Cisco, VyOS, networking, internet protocols, firewall

1 ÚVOD

Cieľom tejto práce je poukázať na jednotlivé funkcie smerovačov s operačnými systémami Cisco IOS-XR a VyOS. Poukázať na rozdiely medzi nimi z hľadiska funkčnosti a konfigurácie. Taktiež sa bude zaoberať možnosťami emulácie týchto operačných systémov na hardvéri a vo virtuálnom prostredí pomocou emulačných programov.

Ďalšou časťou bude využitie sieťových protokolov ako OSPF (Open Shortest Path First), BFD (Bidirectional Forwarding Detection), IPv4 (Internet Protocol version 4), IPv6 (Internet Protocol version 6) na fungovanie komunikácie medzi Ciscom IOS-XR (Internetworking Operating System-XR), VyOS a užívateľmi. V dnešnej dobe zohráva významnú úlohu aj bezpečnosť a tak sa práca zaoberá aj zabezpečením sieťovej komunikácie.

Navrhnuté sú dva rôzne scenáre, ktoré sa venujú analýze a problematike použitých sieťových protokolov. Obidva scenáre by mali zodpovedať dĺžke laboratórneho cvičenia o dĺžke cca 1,5 hodiny.

Prvý scenár obsahuje nastavenie IPv6 adries na portoch smerovačov a na užívateľov. Následne konfiguráciu protokolu OSPFv3 (Open Shortest Path First version 3) s priradením smerovačov a užívateľov do oblastí. Posledná časť sa zameriava na protokol BFD, ktorý rýchlejšie zistí, keď spojenie zlyhá.

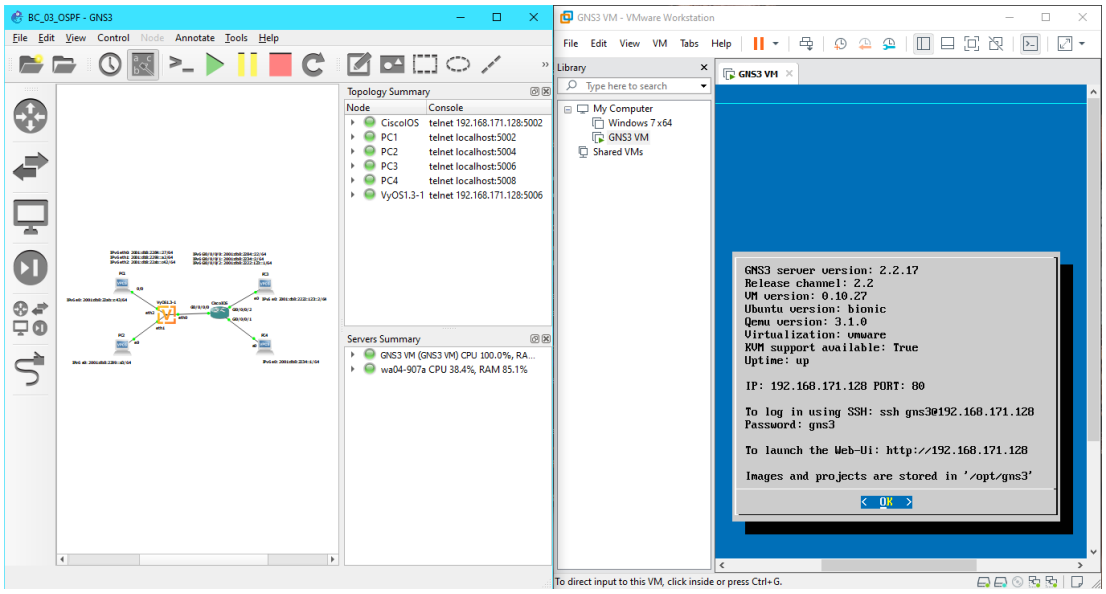
Druhý scenár obsahuje konfiguráciu IPv4 adries pomocou protokolu DHCP (Dynamic Host Configuration Protocol), nastavenie OSPF a konfiguráciu firewallu na VyOS smerovači a filtrovanie paketov na smerovači Cisco IOS.

2 MOŽNOSTI EMULÁCIE

Existuje viacero možností emulácie sieťových prvkov. Jedným zo spôsobov je nahranie obrazu na ľubovoľný hardvér, ktorý podporuje virtualizáciu (stolný počítač, notebook). Ďalším spôsobom je nahranie obrazu smerovačov priamo do programov, ktoré podporujú virtualizácie, t.j. VMWare alebo VirtualBox. Poslednou možnosťou je vytvorenie servera v programe VMware alebo Virtualbox a

pomocou emulačných programov akými sú GNS3 (Graphical Network Simulator-3) alebo EVE-NG (Emulated Virtual Environment-Next Generation), je možné nahrať obrazy smerovačov a následne ich konfigurovať. [1]

Táto práca sa realizuje podľa poslednej možnosti. Najprv je potrebné stiahnuť z oficiálnych stránok program VMware Workstation Pro, ktorý sprostredkúva vytvorenie servera. Následne aj emulátor GNS3, ktorý slúži priamo na virtualizáciu. Na stránkach GNS3 sa nachádza aj server pre VMware, ktorý je taktiež potrebné stiahnuť a otvoriť priamo vo VMware. Nastavenie parametrov je následovné: 4GB RAM a 20GB pamäť na disku. Serveru je automaticky priradená IP adresa 192.168.106.128. Ak je server správne nainštalovaný, po spustení programu GNS3 by sa mala zobraziť pri IP adrese, vyššie spomenutej, zelená bodka. Na obrázku 1 je zobrazený emulátor GNS3 so smerovačmi a užívateľmi na ľavej strane. Na pravej strane sa nachádza server GNS3 VM v programe VMware.



Obrázek 1: GNS - Prostredie

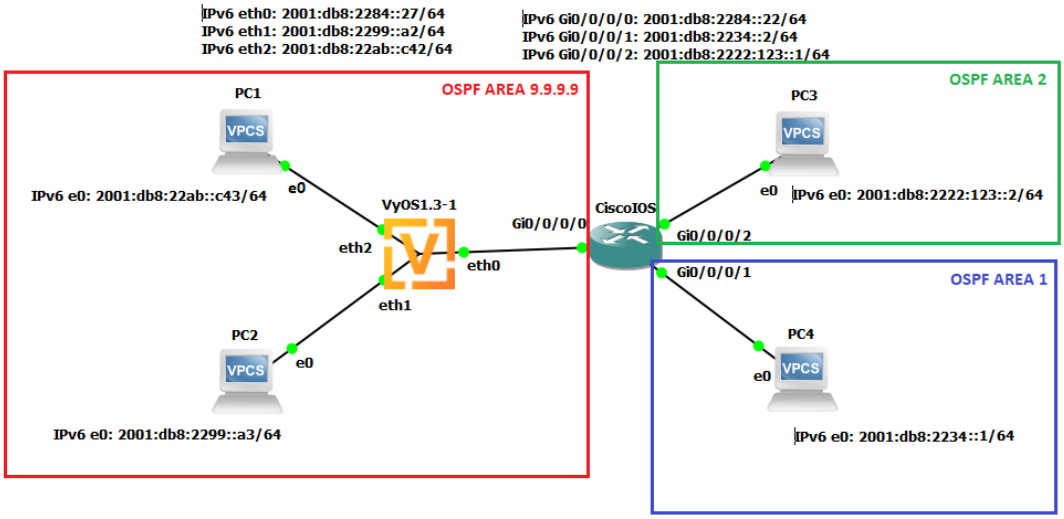
3 SCENÁRE PRE KONFIGURÁCIU

Práca obsahuje 2 scenáre pre laboratórne cvičenia, v ktorých sa využívajú rôzne sieťové protokoly pre prepojenie, zabezpečenie a plynulú komunikáciu. Týmto sa ukáže rozdiel konfigurácií a nastavení medzi smerovačmi Cisco IOS XR a VyOS.

3.1 PRVÝ SCENÁR

V prvom scenári sa najprv konfigurujú IPv6 adresy pomocou vhodne vytvorenej adresnej tabuľky.Priradenie IPv6 adries vidieť na obrázku 2. Medzi smerovačmi Cisco a VyOS je nastavený subinterface, a až na ten sa konfiguruje IPv6 adresa. Pre VyOS router je nutné nastaviť VLAN, ktorá funguje ako subinterface.Tu je možné vidieť zásadný rozdiel medzi konfiguráciami týchto smerovačov.

Ku každému smerovaču sú pripojení dvaja užívatelia (PC). Ďalším krokom je konfigurácia OSPFv3 protokolu, práve táto verzia podporuje IPv6. Na obrázku 2 sú zobrazené oblasti pre konfiguráciu protokolu OSPF, kde je možné vidieť, že Cisco je hraničný smerovač, ktorý prepája 3 vytvorené oblasti. Oblasti v tejto práci sú simulované z dôvodu, že keď dôjde k zmene v sieti, tak OSPF rozposiela LSU (Link State Update) pakety len v rámci jednej oblasti, kde nastala zmena. Týmto sa znižuje zaťaženie siete. [2]



Obrázek 2: OSPF oblasti a IPv6 adresy

Overenie konfigurácie protokolu OSPF na smerovačoch je možné napríklad pomocou príkazu ping. Na obrázku 3 sa overovalo spojenie medzi PC1 a PC4, ktoré bolo úspešné.

```
PC1> 2001:db8:22ab::c43/64

2001:db8:2234::1 icmp6_seq=1 ttl=62 time=69.949 ms
2001:db8:2234::1 icmp6_seq=2 ttl=62 time=6.158 ms
2001:db8:2234::1 icmp6_seq=3 ttl=62 time=5.966 ms
2001:db8:2234::1 icmp6_seq=4 ttl=62 time=6.752 ms
2001:db8:2234::1 icmp6_seq=5 ttl=62 time=6.223 ms
```

Obrázek 3: Overenie konfigurácie

Poslednou experimentálnou súčasťou scenáru je aplikovanie BFD protokolu na protokol OSPF. BFD protokol primárne slúži na veľmi rýchlu detekciu výpadku linky, ale monitoruje aj parametre ako: stratovosť paketov, jitter a latenciu. Informácie posiela ďalším protokolom.

3.2 Druhý scenár

Druhý scenár bude komunikovať pomocou IPv4 adries. Tentokrát sa nevytvára adresný plán manuálne, ale pomocou protokolu DHCP, ktorý bude na oboch smerovačoch. Podobne ako v prvom scenári sa aj tu konfiguruje protokol OSPF, ale verzia 2. Práve táto verzia podporuje IPv4 adresy. Po konfigurácií a pred ďalším nastavovaním je potrebné overiť spojenie medzi smerovačmi a koncovými užívateľmi.

Ďalším krokom je nastavenie firewallu na smerovači VyOS. Firewall slúži napríklad pre povolenie alebo zakázanie protokolu ICMP (Internet Control Message Protocol), do ktorého spadá príkaz ping. Taktiež je možné obmedziť komunikáciu z určitých IP adries a portov. [3]

Cisco smerovač nemá firewall, obmedzenie komunikácie je možné len cez ACL (Access Control Lists-Prístupové zoznamy). Pomocou ACL sa zakáže komunikácia s jedným užívateľom, tu si treba dať pozor, pretože v prípade zmeny IP adresy je potrebné ACL vymazať a nastaviť odznova. Výber práve týchto protokolov použitých v druhom scenári je z dôvodu, že pri ich konfigurácií a nastavovaní je vidieť rozdiely medzi smerovačmi. Po úspešnej konfigurácií sa simuluje troubleshooting (riešenie chýb) pri nastavovaní OSPF alebo DHCP hlavne medzi smerovačmi. Jedná sa o najčastejšie chyby a ich riešenia, pričom sa porovnajú jednotlivé konfigurácie smerovačov.

4 ZÁVER

V tejto práci bol vypracovaný spôsob, kde sa používali programy GNS3 a VMWare, pomocou ktorých sa vytváralo virtuálne prostredie pre smerovače Cisco a VyOS. Program VMware slúžil na vytvorenie virtuálneho servera a GNS3 priamo na emuláciu. Pri inštalácií daných programov si treba dávať pozor na verzie programov a verziu servera na VMware. Pri odlišných verziách smerovače nefungujú ako by mali. Napríklad pri vydaní novej verzie GNS3 nebola vydaná nová verzia práve pre server, VyOS smerovač mal problémy s ukladaním konfigurácie. Pri reštarte smerovača sa celá konfigurácia stratila. Ďalšie možné problémy a ich riešenia sú popísané v bakalárskej práci.

V prvom scenári bolo zahrnuté vytvorenie adresného plánu IPv6 adries a následné nastavenie na rozhrania smerovača, kde medzi smerovačmi bol použitý subinterface. Protokol OSPFv3 bol natavený pre komunikáciu koncových užívateľov a protokol BFD pre rýchlu detekciu zlyhania spojenia a monitorovania parametrov siete.

V druhom scenári bol využitý protokol IPv4. Tentokrát sa nevytváral manuálne adresný plán, ale vytvoril ho protokol DHCP aplikovaný na oboch smerovačoch. V tomto scenári sa použil OSPFv2 protokol, ktorý funguje výhradne len pri IPv4 adresách. Po overení fungujúceho spojenia medzi užívateľmi sa konfiguroval firewall na smerovači VyOS a ACL na smerovači Cisco. Po konfigurácií sa simuloval troubleshooting spojený s protokolmi IPv4, OSPF, ACL a Firewallu.

Pri realizovaní vytvorených scenárov bolo vidieť aké sú konfigurácie smerovačov rozličné. Či už pri nastavovaní IP adries, kde na Cisco smerovači sa najprv treba dostať na rozhranie a až potom nastaviť IP adresu, u VyOS je to možné jedným príkazom. Podobné rozdiely boli aj pri nastavovaní OSPF. Ďalším dôležitým rozdielom bol práve subinterface a jeho konfigurácia. U smerovača Cisco bolo nastavenie jednoduchšie. Porty routra Cisco treba zapínať po konfigurácií, VyOS ich zapne automaticky. VyOS má funkciu zabezpečenia systému (firewall), pričom na Ciscu je možný len ACL. Okrem tejto funkcionality s firewallom som nenarazil na zásadný rozdiel, ktorý by jeden z operačných systémov uprednostňoval pred iným. Je tým myslená napríklad nefunkčnosť protokolov (OSPF, BFD) pri virtualizácií OS v emulátoroch. V konečnom dôsledku to zavisí len na rozhodnutí užívateľa a jeho preferencií, ktorý sieťový operačný systém si vyberie.

REFERENCE

[1] CBT Nuggets. CBT Nuggets [online]. Copyright ©. [cit. 11.3.2021] Dostupné z URL: https://www.cbtnuggets.com/blog/career/career-progression/5-best-network-simulators-for-cisco-exams-ccna-ccnp-and-ccie>.

[2] OSPF protokol [online]. Copyright © [cit. 9.03.2021]. Dostupné z URL: http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html.

[3] VyOS 1.4.x (sagitta) documentation. [online]. Copyright © [cit. 10.03.2021]. Dostupné z URL: https://docs.vyos.io/en/latest/configuration/firewall/index.html DE, b-Quadrat, 2004, s. 131-145, ISBN 3-933609-02-X.