UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

BAKALÁŘSKÁ PRÁCE

2017 Ondřej Šanko

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Protokol NetFlow v hybridní infrastruktuře

Ondřej Šanko

Bakalářská práce

2017

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne: 2. 5. 2017 Ondřej Šanko

PODĚKOVÁNÍ

Děkuji vedoucí práce Ing. Soně Neradové, Ph.D. za cenné rady a odborné vedení, které mi poskytla. Také bych chtěl poděkovat své rodině za podporu a trpělivost při studiích.

ANOTACE

Tato práce popisuje propojení virtuální sítě s fyzickým zařízením a nastavení protokolu NetFlow.

V praktické části je, navržena síť v simulačním nástroji GNS3, propojení s fyzickým zařízením od firmy MikroTik a monitorování datové sítě pomocí protokolu NetFlow.

KLÍČOVÁ SLOVA

NetFlow, GNS3, hybridní infrastruktura, virtuální síť, MikroTik

TITLE

Protocol NetFlow in hybrid infrastructure.

ANNOTATION

This work describes link between virtual network and physical device and setting protocol NetFlow.

In the practical part is designed network in simulation tool GNS3, link with physical device from company MikroTik and track with protocol NetFlow.

KEYWORDS

NetFlow, GNS3, hybrid infrastructure, virtual network, MikroTik

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

CLI	Command Line Inteface
FTP	File Transfer Protocol
GNS3	Graphical Network Simulator 3
IOS	Internetwork Operating Systém
ISO/OSI	International Standards Organization / Open System Interconnection
LAN	Local Area Network
LSA	Link-State Advertisement
LSR	Link State Request
LSU	Link State Update
MPLS	Multiprotocol Label Switching
NVRAM	Non-Volatile Random Access Memory
OSPF	Open Shortest Path First
PoE	Power over Ethernet
SPF	Shortest Path First
SSH	Secure Shell
VIRL	Virtual Internet Routing Lab
VPN	Virtual Private Metwork
WAN	Wide Area Network

ÚVOD

Motivací pro měření síťových toků jsou zjištění o tom, jaký druh provozu je v síti, jak probíhá tento provoz a v kterých částech sítě probíhá. Měřením těchto toků získáváme informace potřebné pro správu sítě a síťových služeb, dohledávání problémů a incidentů, plánování rozšíření a optimalizaci sítě. Pro každého síťového administrátora je důležité, aby měl k dispozici nástroje umožňující síť monitorovat a provádět analýzu síťového provozu.

Jedním z nástrojů, který sbírá datové toky a odesílá je na jiné zařízení pro následnou analýzu je protokol Netflow. Standard NetFlow je základní podmínkou pro moderní správu a zabezpečení datové sítě. Tento standard poskytuje síťovým administrátorům podrobný vhled do síťového provozu v jejich infrastruktuře. NetFlow pomáhá při řešení provozních problémů v síti a poskytuje informace důležité pro ochranu sítě před kybernetickými hrozbami.

Cílem bakalářská práce je aplikace protokolu Netflow na navrhnuté infrastruktuře. V teoretické části jsou popsány použité protokoly, zařízení a simulační prostředí. Praktická část podrobně popisuje nasazení protokolu Netflow v simulačním prostředí.

1 SIMULÁTORY SÍŤOVÉHO PROSTŘEDÍ

1.1 Úvod do simulátorů

V dnešní době, kdy technologie a zapojení jsou stále sofistikovanější, si nemůžeme příliš často dovolovat navrhovat, či upravovat, sítě bez předchozího podrobného testování. Problémem při odzkoušení nově navrhnutých topologií bývá rozsáhlost, pro kterou je danou síť téměř nemožné odzkoušet. Tento problém lze efektivně odstranit pomocí simulačních nástrojů, ve kterých lze pohodlně celou topologii sestavit a jednotlivé části odzkoušet aniž bychom zasahovali do reálné sítě a případnými změnami ohrožovali stabilitu celé sítě. Mezi nejznámější simulační nástroje patří například Packet Tracer od společnosti Cisco, který slouží převážně pro výukové účely, VIRL – Virtual Internet Routing Lab od společnosti Cisco, či GNS3 – Graphical Network Simulator 3, který jsem zvolil pro realizaci úlohy v praktické části práce a který je popsán podrobněji v následující kapitole.

1.2 Packet Tracer

Jedná se o simulační nástroj, určený převážně pro studenty síťové akademie a je volně dostupný pro členy Networking Academy od společnosti Cisco. Základním cílem je umožnit studentům získat znalosti síťových technologií v rozsahu kurzů CCNA, CCNAS a CCNP. Je dostupný pro platformy Windows, Linux a Android.

Mezi jeho výhody patří uživatelsky přívětivá instalace a snadné používání všech jeho nástrojů. Mezi nevýhody patří: podpora pouze základních funkcí reálného zařízení, poskytuje jen výsek skutečných funkcionalit reálných zařízení, tím se může stát, že budou odlišné chybové stavy od provozu na reálném zařízení a má omezené možnosti v kryptografii. Další velkou nevýhodou je, že jej nelze propojit s fyzickou sítí, jako je to možné v dalších dvou zmiňovaných nástrojích: VIRL a GNS3.

1.3 Virtual Internet Routing Lab (VIRL)

VIRL je již profesionální nástroj pro simulaci sítí od firmy Cisco. Na rozdíl od Packet Traceru, který nepokrývá celou škálu Cisco technologií s přednastavenými IOSy, VIRL umožňuje pracovat v prostředí, které využívá IOS určený pro reálná zařízení. Nabídka používaných prvků je rozšiřována o nejnovější zařízení firmy Cisco a na rozdíl od GNS3 umožňuje použití směrovačů i přepínačů.

Mezi hlavní výhody tedy patří aktuálnost, technická podpora a možnost propojovat jednotlivé projekty s fyzickou sítí, či propojovat jednotlivé projekty mezi sebou (lze propojit i se sítí v prostředí GNS3).

Mezi nevýhody patří vysoká náročnost na hardware. Jako úplně minimum společnost Cisco uvádí: minimálně 8GB RAM a čtyř-jádrový procesor alokovaný výhradně pro tento simulační nástroj. Hardwarové požadavky se odvíjejí od velikosti a složitosti sítě, kterou chcete simulovat. Další nevýhodou je, že tento software je placený a cena je 200 USD za rok. (VIRL - Virtual Internet Routing Lab, 2017)

1.4 GNS3 – Graphical Network Simulator 3

Jedná se o grafický simulační nástroj s licencí open-source. Emulaci síťových prvků zajišťuje emulátor Dynamips, který je také open-source. Jediné co tento nástroj neposkytuje zdarma, jsou operační systémy jednotlivých zařízení, které si musí uživatel opatřit sám. Je to z důvodů že Dynamips emuluje pouze hardware a nikoli software. GNS3 podporuje zařízení od společnosti Cisco a Juniper.

GNS3 je velmi oblíbený z důvodu, že lze k němu připojit i fyzická zařízení, na rozdíl od Paket Traceru, který propojení do reálného světa neumožňuje. Simulační prostředí GNS3 umožňuje navrhnout síť, kterou připojíme k reálné síti skrze síťovou kartu počítače a testovat chování, či podnikat například útoky na naši simulovanou síť přes reálná fyzická zařízení. Další výhoda je i možnost připojovat další virtuální prvky (osobní počítače, servery) do prostředí GNS3 a to pomocí VirtualBoxu či VMWaru. Velkou nevýhodou je, že tento nástroj umí emulovat pouze směrovače, nikoli přepínače. (Getting Started with GNS3, 2017)

Tento simulační nástroj jsem zvolil pro řešení praktické části.

2 GNS3

GNS3 je nástroj určený pro testování sítí a přípravu na získání síťových certifikací. Propustnost implementovaných směrovačů do GNS3 je 1000 paketů za sekundu, což je několika násobně méně než kolik dosahují reálná zařízení.

2.1 Instalace

Získání instalačního balíčku je na stránce společnosti GNS3 Technologies Inc.[1] a po zaregistrování získáme přístup k tomuto nástroji. Instalační balíček obsahuje vlastní prostředí GNS3, což je pouze grafická nadstavba, která sama o sobě nedokáže simulovat a další nástroje vytvářející simulační prostředí:

- Dynamips – emulátor hardwaru jednotlivých směrovačů.
- Dynagen – textové rozhraní pro Dynamips.
- Qemu – emulátor poskytující hardwarovou a softwarovou virtualizace.
- WinPcap – Windows Packet Capture, knihovna kterou využívá Wireshark.
- Putty – software používaný k připojení ke konzoli směrovačů přes telnet, či SSH.
- Wireshark - nástroj sloužící k zachytávání, či analýze, síťového provozu.

Na oficiálních stránkách GNS3 nalezneme kompletní dokumentaci ke všem doplňkům a k postupu instalace samotného GNS3. (Getting Started with GNS3, 2017)

2.2 IOS pro GNS3

GNS3 neobsahuje ve výchozím stavu obrazy operačních systémů jednotlivých zařízení. Jedna z možností jak je získat, je být zákazníkem společnosti Cisco, a tím získat přístup ke stažení jednotlivých IOS z oficiálních stránek, nebo další možností je, pokud vlastníme směrovač od společnosti Cisco, který je podporován emulačním nástrojem Dynamips, lze stáhnout jeho IOS a nahrát jej do GNS3. GNS3 podporuje následující řady směrovačů: c1700, c2600, c3600, c3700 a c7200. (Gns3 Supported Routers, 2017)

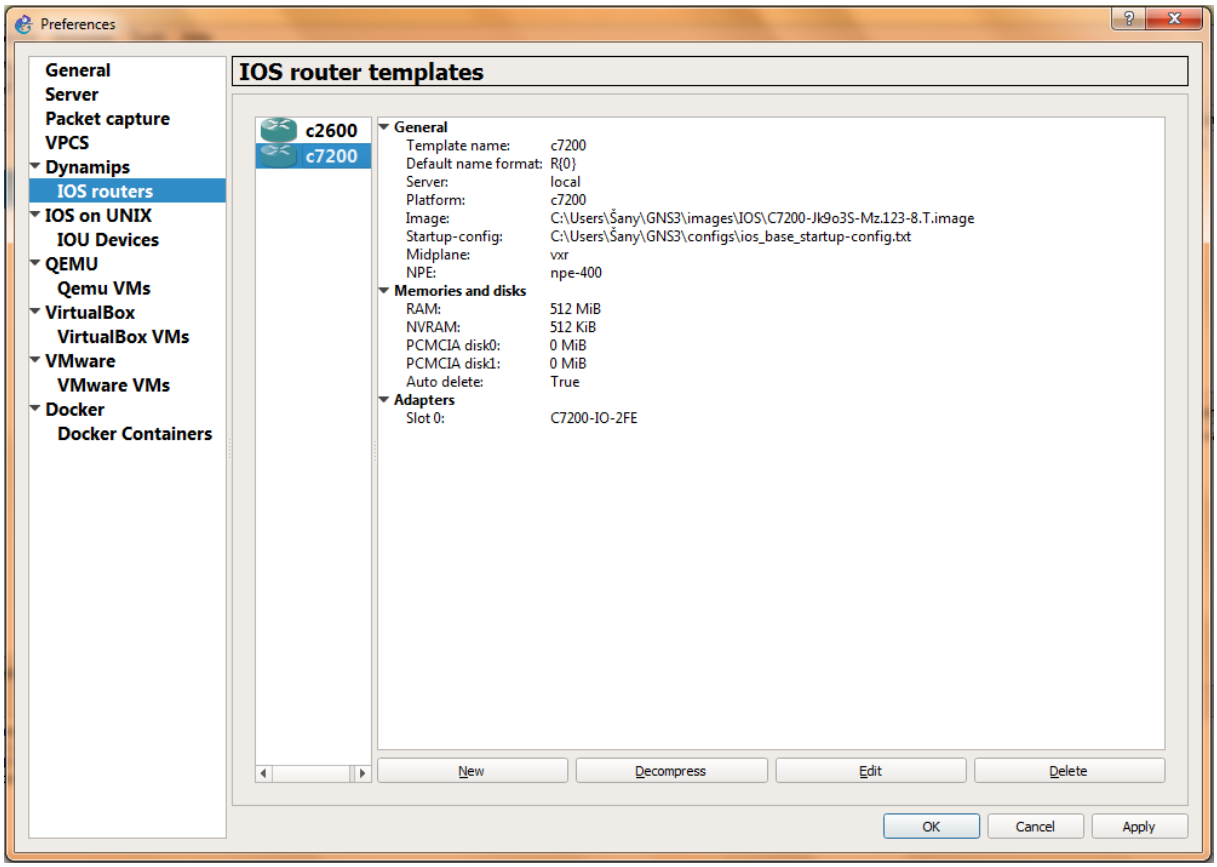
2.3 Přidání směrovače do GNS3

Pokud vlastníme a máme připravený image IOS, je vložení nového směrovače jednoduché.

- V horní liště otevřeme rozevírací seznam „Edit“ a klikneme na „Preferences“.

[1] https://www.gns3.com/

- Otevře se okno s nastavením, kde v seznamu po levé straně zvolíme záložku Dynamips a otevřeme IOS routers.
- Klikneme na new v dolní části okna s nastavením.
- Spustí se průvodce, který nás provede celým nastavením.
- Zadáme cestu k připravenému image IOS a dáme „Next“.
- Program převážně sám rozpozná a jaké zařízení jde a před vyplní název a o jakou jde platformu.
- V další kartě se nastavuje velikost RAM (opět program před vyplní převážně sám).
- V následující kartě se nastavují moduly (sériové i ethernetové).
- Na poslední kartě se nastavuje Idle-PC, díky této hodnotě je počítáno v čase, kdy je směrovač nevyužit a Dynamips jej převede ro režimu spánku, jinými slovy je zachována co největší efektivita procesoru.

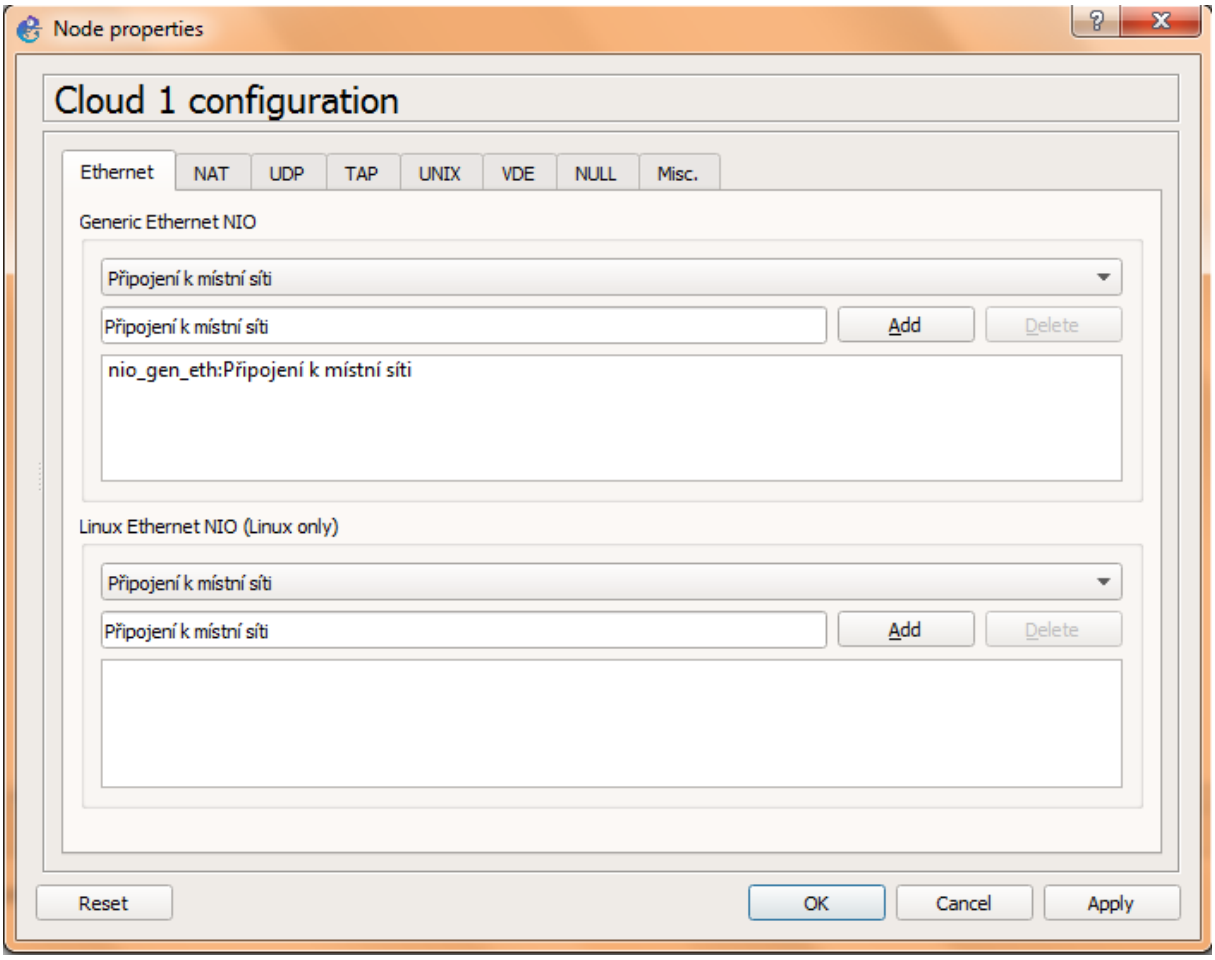


Obrázek 1 – Okno s nastavením směrovačů

Zdroj: vlastní

2.4 Cloud

Jak již bylo zmíněno, GNS3 umí propojovat simulovanou síť s reálnou. Této funkce je dosaženo pomocí funkce Cloud, která vytváří most mezi reálnou a simulovanou sítí. Cloud nalezneme v levém menu pod záložkou „Browse End Devices“. Přetáhneme jej na pracovní plochu, klikneme na něj pravým tlačítkem a zvolíme „Configure“. Otevře se nám okno s nastavením, kde zvolíme, přes jaký síťový adaptér se má spojit s reálnou sítí a klikneme na „Add“ a poté na „Ok“. Se simulovanou sítí se připojí přes kabel, jako bychom spojovali dva směrovače.



Obrázek 2 – Konfigurace funkce Cloud

Zdroj: vlastní

3 SYSTÉM CISCO IOS

Cisco IOS neboli Internetwork Operating System je operační systém běžící na většině zařízeních od společnosti Cisco. Obsluha je založena na příkazové řádce CLI (Command Line Inteface). IOS je uložen v paměti flash (paměť typu NVRAM, která je přepisovatelná a po odpojení a opětovném připojení napájení zůstane její obsah zachován). Existuje mnoho verzí s různými a opravami. Nejnovější verze je označena číslem 15.

Práce v IOS je rozdělena do několika módů. Každý mód nám poskytuje odlišné možnosti nastavení, některé lze i zabezpečit pomocí přihlašovacího jména a hesla. Dále jsou popsány od „nejzákladnějšího“. (Cisco IOS 1 - úvod, 2007)

- Uživatelský mód – do tohoto módu se dostanete okamžitě po připojení do CLI. Funkce tohoto módu jsou omezené, slouží spíše pro ověření nějakých informací.
- Privilegovaný mód – do tohoto módů se dostanete pomocí příkazu *enable*, slouží jako „přechodová“ vrstva do další módů. V tomto módu lze již získávat detailnější informace (IP adresy, údaje o směrovacích protokolech apod.).
- Globální konfigurační mód – do tohoto módů se dostanete pomocí příkazu *configure terminal* (musíte již být v privilegovaném módu), slouží k nastavování funkcí, které ovlivní celý systém.
- Konfigurace rozhraní – do tohoto módů se dostanete pomocí příkazu *interface* a název daného rozhraní (například f0/0 dále, musíte již být v globálním konfiguračním módu). Zde se upravují vlastnosti daného rozhraní.

4 POUŽITÁ ZAŘÍZENÍ

4.1 Cisco c7200

Jedná se o směrovač od společnosti Cisco podporovaný simulačním nástrojem GNS3. Právě tato podpora, je hlavní důvod, proč byl pro tuto práci tento směrovač zvolen. IOS je verze 12.3(8) T. Velikost RAM: 512MiB. NVRAM: 512KiB. Tento směrovač zajišťuje komunikaci mezi serverem a směrovačem od společnosti MikroTik pomocí směrovacího protokolu OSPF, dále monitoruje komunikaci pomocí protokolu NetFlow.

4.2 Mikrotik hAP ac lite (RB952Ui-5ac2nD)

Směrovač od firmy MikroTik, který poskytla pro zhotovení této práce Univerzita Pardubice. Zajišťuje komunikaci mezi směrovačem od společnosti Cisco a koncovým zařízením pomocí protokolu OSPF, dále také monitoruje komunikaci pomocí protokolu NetFlow (Traffic Flow).

Technická specifikace:

- Dual chain wireless 2.4GHz, Single chain wireless 5GHz
- 650MHz CPU, 64MB of RAM
- Five x 10/100Mbps Ethernet ports
- Passive PoE output on port 5
- USB port for 3G/4G modem

Obrázek 3 – MikroTik

Zdroj: vlastní

5 POUŽITÉ PROTOKOLY

V této kapitole jsou teoreticky popsány protokoly, které jsou implementované v praktické části práce.

5.1 OSPF – Open Shortest Path First

OSPF byl vytvořen v roce přibližně v letech 1988-1991 společností IETF. Můžeme jej zařadit do skupiny IGP - Interior Gateway Routing Protocols. Je tedy určen k použití uvnitř autonomního systému.

OSPF patří mezi Link State protokoly. To znamená, že v paměti směrovače je uložena celá topologie sítě označována jako Link State Database (česky nazývaná jako topologická databáze). Nad touto databází probíhá výpočet pomocí SPF algoritmu, který poskytuje výpočty k nalezení nejvýhodnější cesty do jednotlivých sítí. Aby se ušetřilo místo topologické databáze a čas výpočtu SPF algoritmu, lze síť rozdělit do oblastí (area), které jsou na sobě nezávislé (pokud provedeme změnu v síti, spustí se opět SPF algoritmus pouze v oblasti, kterou jsme upravili, nikoli v celé topologii). (LAMMLE, 2015, s. 446)

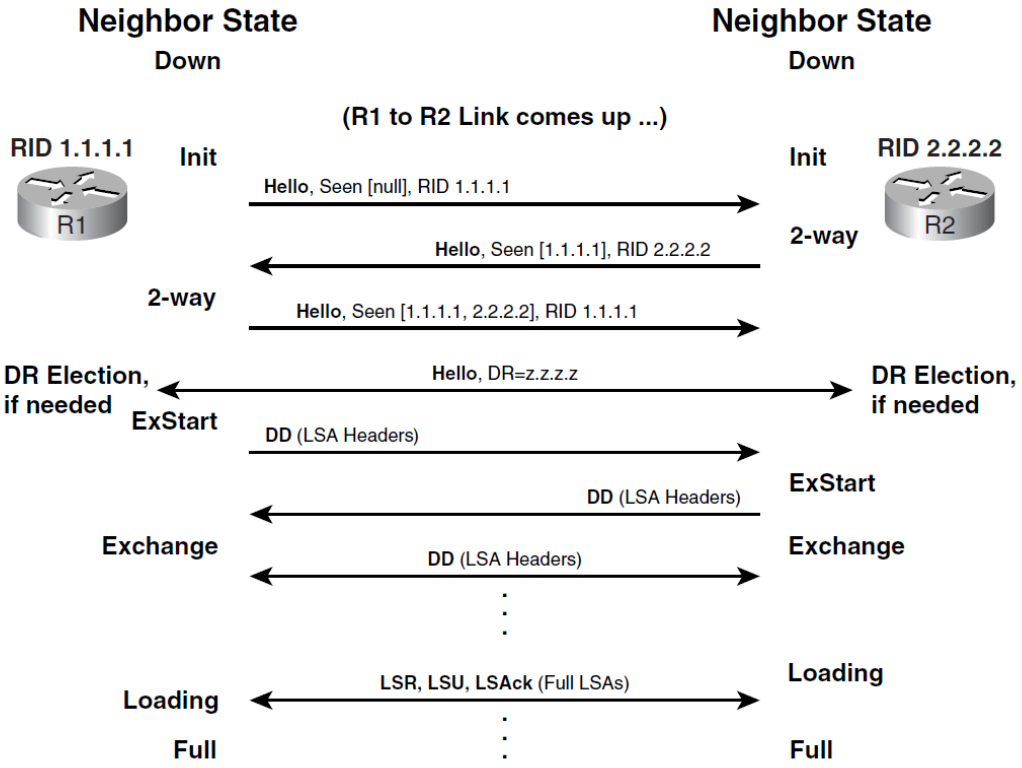
5.1.1 Navázání komunikace

V této podkapitole je popsané chování navázání komunikace pomocí protokolu OSPF.Po nakonfigurování protokolu OSPF se spustí Hello protokol, který začne na rozhraních směrovače posílat Hello pakety. Hello pakety se odesílají periodicky, standardně každých 10 sekund. Pokud dva spojené směrovače se shodují na určitých parametrech (číslo oblasti, typ oblasti, síť a maska sítě, autentizační údaje) pomocí Hello paketů, stávají se takzvanými sousedy (Neighbors).

Toto ale ke správné funkčnosti nestačí. Aby si směrovače začaly přeposílat informace o topologii sítě, je potřeba, aby se směrovače staly takzvanými přilehlými (Adjacent). Poté, co se stanou sousedy, si začnou směrovače posílat Database Description Packet. Uvnitř je obsažen návrh náhodného sekvenčního čísla SEQ, které je používáno pro další komunikaci. Směrovač, který má vyšší Router ID je zvolen jako Master a bude sekvenční číslo pro další komunikaci používat (druhý směrovač je označován jako Slave).

Dále nastane další přeposílaní Database Description Packet (Master zahajuje další komunikaci), ve kterých si nyní předávají informace o svých topologických databází. Tyto pakety jsou číslovány od určeného sekvenčního čísla. Dochází k porovnání s vlastní databází, a pokud zjistí, že nějaké informace jsou zastaralé, nebo dokonce chybí, zažádá o ně pomocí

paketu Link State Request (LSR). Na něj soused odpoví pomocí paketu Link State Update (LSU), který obsahuje požadované informace ve formě Link State Advertisement (LSA). Následuje potvrzení o přijetí informací pomocí paketu Link State Acknowledgement. Pokud nedojde k potvrzení, je po uplynutí určitého času LSU odeslán znovu. Pokud topologické databáze všech směrovačů jsou stejné, stávají se přilehlými (Adjacent). V případě změny (přidání, nebo odebrání směrovače) se proces opakuje. (LAMMLE, 2015, s. 466)



Obrázek 4 – OSPF - navázání komunikace

Zdroj: (INFRAWORLD, 2011)

5.1.2 Směrovací tabulka

Cílem každého směrovacího protokolu je naplnění směrovací tabulky. Všechny potřebné informace se nacházejí v topologické databázi. Lze jej interpretovat jako graf, kde směrovače jsou vrcholy a cesty hrany. Každá hrana má vlastní cenu (cost), která slouží jako metrika protokolu OSPF. Pokud jsou všechny potřebné informace k dispozici, proběhne algoritmus SPF (jinak označován jako Dijkstrův algoritmus). Cílem algoritmu je odstranit smyčky a získat nejvýhodnější cestu do každé sítě.

Z celé vypočtené cesty se využije adresa nejbližšího směrovače, na který bude sloužit k provozu do cílové sítě. Dále se do směrovací tabulky uloží sumární cena této cesty. Pokud

se najde více cest ze stejnou cenou, zaleží pak na nastavení směrovače, zda bude používat pouze jednu preferovanou cestu, nebo zda bude rovnoměrně dělit zátěž do všech cest.

Vypočet SPF algoritmu je poměrně náročný na směrovač. Je proto potřeba zajistit aby probíhal v co možná nejdelších intervalech (například se vyhnout nestabilním linkám a podobně). (LAMMLE, 2015, s. 451)

5.1.3 Metrika

Každý směrovací protokol využívá nějaké kritérium, podle kterého určuje, jaká cesta je do dané sítě nejvýhodnější.

V případě protokolu OSPF se využívá již zmiňovaná cena (cost). Jedná se o číslo v rozsahu od 1 až do 65535, které je přiřazené ke každému rozhraní směrovače. Čím menší číslo, tím má cesta lepší metriku a bude preferovanější před ostatními. Obecně je cena přiřazena automaticky. V tomto případě je spočtena z šířky pásma (bandwidth) pomocí vztahu:

- cena = 100 000 000 / bandwidth (bps)

Cenu lze samozřejmě přidělit i ručně.

5.1.4 Typy oblastí

- Backbone area – vždy pojmenována jako Area 0, slouží k propojení ostatních oblastí,
- stub area – nepřímá cesty z ostatních autonomních systémů (AS), pro směrování mimo AS se použije defaultní cesta,
- totally stubby area – nepřímá sumární cesty mimo jeho oblast, je Cisco proprietární,
- not-so-stubby area – podobné jako stub area, ale importuje některé externí cesty typu 7 LSA paketu.

5.1.5 Typy směrovačů

- Area Border Router – má rozhraní ve více oblastech, pro každou oblast má vlastní Link State tabulku připojuje oblasti do backbone oblasti,
- Autonomous System Border Router – má rozhraní ve více autonomních systémech,
- Internal Router – běžný, pouze v jedné oblasti,
- Backbone Router - alespoň jedno rozhraní v Area 0.

Dále lze směrovače z pohledu přilehlosti (Adjacent) rozdělit na:

- Designated Router (DR) – aby se omezila režie provozu na síti, je v broadcast síti jeden směrovač určen jako pověřený směrovač (DR), kdy každý další směrovač navazuje vztah přilehlosti pouze s tímto směrovačem,
- Backup Designated Router (BDR) – stejná funkce jako výše zmiňovaný, pouze funguje jako záložní. (LAMMLE, 2015, s. 449)

5.2 FTP – File Transfer Protokol

FTP je síťový protokol, používaný k přenosu souborů ze serveru na klienta pomocí počítačové sítě. Je postaven na architektuře klient-server. Využívá protokol TCP z rodiny TCP/IP. Je nezávislý na operačním systému.

Využívá porty TCP/20 a TCP/21. Port 21 slouží k přenosu příkazů na server, které uživatel zadává. Port 20 slouží výhradně pro přenos dat (v případě pasivního režimu komunikace může výt využit jiný port). Přenos dat je 8 bitový. Může být textový, kdy dochází ke konverzi konci řádků, či binární, kdy ke konverzi nedochází vůbec. (KABELOVÁ a DOSTÁLEK, 2012, s. 345)

Architektura protokolu FTP využívá 2 kanály:

- Příkazový kanál – je využívaný k zasílání požadavků na server, např. stažení souboru.
- Datový kanál – je určen k přenášení požadovaných dat. U datového kanálu se může role serveru a klienta obrátit. Z tohoto důvodu rozeznáváme dva režimy komunikace a to aktivní a pasivní.

5.2.1 Aktivní režim komunikace

Jedná se o „běžný“ režim komunikace, který je nejčastěji používaný. Lze tuto volbu změnit, ale málokterý klient tuto volbu poskytuje. V tomto režimu se při otevření datového proudu vymění role mezi klientem a serverem. Nyní si popíšeme průběh tohoto režimu komunikace.

- Klient zažádá o port správu volných portů na lokálním počítači.
- Po přidělení naváže komunikaci se serverem pomocí TCP spojení s portem 21. Je vytvořen příkazový kanál.

Nyní máme připravený příkazový kanál, po kterém můžeme posílat příkazy na server. Dále je popsané vytvoření datového proudu. Například pokud bychom chtěli výpis adresáře ze serveru na klienta.

- Klientovi je přidělen volný port na lokálním počítači (větší než 1023).
- Klient odešle šest desítkových čísel obsahujících jeho IP adresu a přidělený port na server.
- Server se spojí protokolem TCP s klientem pomocí IP adresy a portu, kterou mu zaslal klient.
- Je vytvořen datový proud, přes který je možné odeslat požadavek (výpis adresáře).
- Pokud vše proběhne úspěšně, je ukončení přenosu signalizováno příkazovým kanálem.
- Uživatel může zadat další příkaz.

Server nám tedy navazuje komunikaci s klientem, jejich role jakoby se navzájem prohodili. Toto řešení může mnohdy vadit, pokud například chceme síť chránit pomocí filtrace na přístupovém směrovači. Z tohoto důvodu existuje pasivní režim komunikace. (KABELOVÁ a DOSTÁLEK, 2012, s. 348)

5.2.2 Pasivní režim komunikace

Jak již bylo zmíněno, u aktivního režimu nám může vadit, že datový kanál je navázán ze strany serveru. Tento problém je odstraněn díky pasivnímu režimu, kde klient navazuje jak příkazový kanál, tak datový kanál. Role tedy zůstávají zachovány. Dále je popsané vytvoření datového kanálu (příkazový kanál se chová stejně, jako v případu aktivního režimu).

- Klient požádá server o alokaci portu.
- Server odpoví šesticí čísel (První čtyři jsou IP adresa a další dvě jsou port).
- Klient naváže na tuto IP adresu a port spojení pro datový kanál.

V tomto případě není použit port 20 pro datový kanál. (KABELOVÁ a DOSTÁLEK, 2012, s. 350)

5.2.3 Anonymní FTP

Anonymní FTP servery jsou určeny zejména pro webové servery, kdy není potřeba autentizace klienta. Slouží na stahování souborů pro uživatele, kteří jej navštíví (například informace o nějaké organizaci). Obvykle se anonymní FTP servery používají pouze pro čtení

souborů. Převážně se na anonymní FTP servery bez problémů přistupuje pomocí internetových prohlížečů.

Protokol FTP původně s anonymními servery nepočítal, takže i anonymní uživatelé zadávají jméno a heslo. Zpravidla se pro jméno používá „ftp“ a pro heslo je po uživateli vyžadována e-mailová adresa (ta většinou slouží provozovateli FTP serveru k vytváření statistik přístupu na server). (KABELOVÁ a DOSTÁLEK, 2012, s. 358)

5.2.4 Bezpečnost

Pokud budeme hodnotit úroveň bezpečnosti, tak na tom není FTP nejlépe. Nastavuje se zde *login* a *heslo,* ale tyto údaje nejsou nijak šifrované, lze je tedy bez problému odposlechnout a dostat se na daný FTP server. Proto je v dnešní době dostupný FTPS – SSH File Transfer Protokol, který funguje obdobně, ale nezajišťuje autentizaci jako klasické FTP, ale místo toho využívá protokol SSH, který umožňuje přihlášení a šifrování dat. (CompleteFTP User's Guide, [b. r.])

5.3 NetFlow

NetFlow je otevřený protokol vyvinutý společností Cisco. NetFlow je monitorovací nástroj poskytující podrobný přehled o provozu sítě, pracující na bázi IP Toku. Vytváří nám „prostředí“ kde administrátor má prostředky potřebné k porozumění jaký, kde, který, kdy a jak síťový provoz plyne. Díky tomuto lze síť daleko lépe spravovat a snižuje možnost výpadků, či jiných chyb v síti. Spojené s tím jsou i menší náklady, poněvadž dokážeme efektivněji využívat síť s méně výkonnými zařízeními.

5.3.1 IP Tok

Každý paket, který je předáván pomocí směrovače, či přepínače, je zkoumán pro několik atributů. Tyto atributy jsou identifikátorem daného paketu (v anglčtině zvané IP packet identity, nebo také fingerprint) a určují, zda je paket unikátní, nebo podobný jiným paketům. Klasicky je IP Tok založen na pěti, nebo až na sedmi, atributy. Níže jsou popsané atributy IP paketů, které používá protokol NetFlow.

- Zdrojová IP adresa.
- Cílová IP adresa.
- Zdrojový port.
- Cílový port.
- Typ protokolu třetí síťové vrstvy.

- Požadavky protokolů vyšších vrstev (Class of Service, CoS).
- Rozhraní směrovače, nebo přepínače.

Všechny pakety, které mají stejné atributy (zdrojovou/cílovou IP adresou, zdrojový/cílový port, protokol, a požadavky daných protokolů (CoS)) jsou seskupeny v tok dat a poté jsou tyto pakety a bajty zaznamenány. Tato metoda snímání je škálovatelná, poněvadž jsou tyto data ve velkém množství ukládány do NetFlow databáze, známé jako NetFlow cache. Tyto informace jsou velice užitečné pro porozumění, jak se síť chová. (Introduction to Cisco IOS NetFlow, 2012)

Zde jsou uvedeny příklady co, nám která informace poskytne:

- Zdrojová adresa nám umožňuje zjistit, odkud pramení daný provoz.
- Cílová adresa nám říká pro koho je určen.
- Porty nám charakterizují aplikaci využívající provoz.
- Požadavky protokolů (CoS) zkoumá prioritu provozu.
- Jak je síť zatížena nějakým rozhraním určitého zařízení.
- Zaznamenané pakety a bajty ukazují rozsah provozu dané sítě.

5.3.2 NetFlow collector

Existují dvě hlavní metody jak přistoupit k datům, které NetFlow zaznamenal. První možnost je pomocí příkazového řádku (Command Line Inteface, CLI). Tento způsob se využívá v okamžiku, kdy potřebujeme okamžitý přístup k datům na daném zařízení. NetFlow CLI je často využíván pro řešení chyb a problémů (troubleshoot).

Další možnost je exportovat data na server zvaný „NetFlow collector“. NetFlow collector má primárně za úkol analyzovat příchozí tok dat a vytvářet ze zjištěných dat zprávy a statistiky, které dále slouží pro administrátora, či pro další výpočty a analýzy. NetFlow zasílá tyto data na server periodicky. Obecně se tedy NetFlow cache plní nějakým tokem dat. Dále software ve směrovači (či přepínači) prohledává tuto cache a hledá tok dat, který je ukončený, nebo „prošlý“ a tento tok je exportován na server, kde běží NetFlow collector. Tok dat je ukončený pokud skončí daná komunikace. Zjednodušeně, lze celý proces popsat takto:

- NetFlow se nastaví pro zaznamenávání komunikace do NeFlow cache.
- Nastaví se NetFlow export pro zasílání dat na collector.
- V NetFlow cache se hledají uzavřené toky dat.

- Přibližně mezi třiceti až padesáti jsou „toky“ dat „svázány“ dohromady a typicky jsou v UDP datagramu v jednom z formátů, které NetFlow podporuje, odeslány na server, kde běží NetFlow collector.
- NetFlow collector nakonec vytváří ze získaných dat zprávy a grafy buď v přítomném čase, či statistiky za nějaký uplynulý čas.

Tok dat je připraven k exportu, pokud je neaktivní určitý čas (není získán žádný nový paket), nebo pokud je aktivní déle než časovač běžící uvnitř protokolu NetFlow (například dlouhé stahování z FTP serveru), nebo pokud je ukončený (TCP flag). Časovač, který určuje zda je tok dat neaktivní bývá nastaven na 15 sekund, a časovač určující, že je aktivní příliš dlouho bývá nastaven na 30 minut. Oba časovače lze samozřejmě v případě potřeby upravit. (NetFlow Services Solutions Guide, 2012)

5.3.3 Formát exportujících dat

V předchozí kapitole je zmíněno, že NetFlow odesílá data pomocí UDP v nějakém formátu na server, kde běží collector. Tyto formáty podporuje NetFlow ve čtyřech verzích. Jsou to:

- Verze 1
- Verze 5
- Verze 7
- Verze 8

Verze 2 až 4 nebyli nikdy uvedeny. Nejpoužívanějším je verze 5, kterou si podrobněji popíšeme.

Odesílaný datagram obsahuje hlavičku a záznamovou část. Hlavička obsahuje informace jako: sekvenční číslo, číslo záznamu a čas, kdy byl systém inicializován (SysUptime). Hlavička nám tedy říká základní informace o datagramu, nikoliv informace, které jsme monitorovali pomocí NetFlow. Záznamová část obsahuje infromace jako: IP adresy (zdrojová/cílová) port a směrovací informace. Tato část nám říká informace, kvůli kterým existuje protokol NetFlow. (NetFlow Export Datagram Format, 2012)

Níže je popsané co obsahují a kolik to celkově z dané části zabírá místa.

Tabulka 1: Hlavička exportovaného datagramu

Bajt	Obsah	Popisek
0-1	Verze	Číslo verze, ve kterém exportér odesílá data.
2-3	Číslo	Číslo datové toku, který odeslán v tomto paketu.
4-7	SysUptime	Čas kdy byl systém inicializován.
8-11	unix_secs	Aktuální počet sekund 0000 UTC 1970.
12-15	unix_nsecs	Zbytkový čas 0000 UTC 1970 v nanosekundách.
16-19	flow_sequence	Čítač všech datových toků.
20	engine_type	Typ flow-switching engine.
21	engine_id	Číslo slotu flow-switching engine.
22-23	Sampling_interval	První 2 bity obsahují mód vzorkování, zbytek obsahuje hodnotu vzorkovacího intervalu.

Zdroj: zpracováno dle (CISCO,2007)

Tabulka 2: Záznamová část exportovaného datagramu

Bajt	Obsah	Popisek
0-3	srcaddr	Zdrojová IP adresa.
4-7	dstaddr	Cílová IP adresa.
8-11	nexthop	IP adresa dalšího směrovače.
12-13	input	SNMP index vstupního rozhraní.
14-15	output	SNMP index výstupního rozhraní.
16-19	dPkts	Paket z daného toku dat.
20-23	dOctets	Celkový součet bajtů třetí síťové vrstvy, který obsahuje daný paket z toku dat.
24-27	First	SysUptime na začátku daného toku dat.
28-31	Last	SysUptime v čase kdy příjde poslední paket daného toku dat.
32-33	srcport	Zdrojový TCP/UDP port, nebo jeho ekvivalent.
34-35	dstport	Cílový TCP/UDP port, nebo jeho ekvivalent.
36	pad1	Nepoužívaný (nultý) bajt.
37	tcp_flag	Kumulativní OR z TCP flag.
38	prot	Typ IP protokolu (například: TCP = 6; UDP = 17)
39	tos	IP type of service (ToS)
40-41	src_as	Zdrojové číslo autonomního systému.
42-43	dst_as	Cílové číslo autonomního systému.
44	src_mask	Prefix masky zdrojové adresy.
45	dst_mask	Prefix masky cílové adresy.
46-47	pad2	Nepoužívaný (nultý) bajt.

Zdroj: zpracováno dle (CISCO,2007)

5.3.4 Podporované rozraní, enkapsulace a protokoly

NetFlow podporuje IPv4 směrovací provoz přes širokou škálu všech možných enkapsulací arozhraní na daném zařízení. Od verze 12.3(7)T a vyšší podporuje také IPv6. Mezi podporované protokoly patří Frame Relay, Asynchronous Transfer Mode, Inter-Switch Link, 802.1q, Muti-link Point to Point Protocol, General Routing Encapsulation, Layer 2 Tunneling Protocol, Multi-protocol Label Switching VPNs a IP sec Tunnels.

V případě tunelu NetFlow může být nakonfigurován na rozhraní, kde tunel končí. NeFlow také podporuje sub-interface. Pokud je NetFlow nastavený na „hlavním“ rozhraní potom všechny sub-interface budou svázány a započítány pod monitorování. NetFlow může být efektivně využit i v MPLS sítích. Obecný přístup NetFlow může být nastaven pro monitorování provozu od uživatelské stránky vstupující do MPLS sítě přes VPN. (NetFlow Services Solutions Guide, 2012)

5.3.5 Implementace protokolu NetFlow

Protokol NetFlow je typicky implementován na „centrální“ straně, odkud nám plyne veškerý, pro nás důležitý provoz. Samozřejmě záleží na složitosti topologie a umístění collectoru, který slouží i jako databáze monitorovaných datových toků.

Obecné se dnes využívají dvě architektury zapojení. Tradičně obstarávají monitorování a exportování směrovače, na kterých máme puštěný i normální provoz sítě. Řešení je to snadné a může se zdát i ekonomicky výhodné. Bohužel však výpočet NetFlow statistik, je poměrně náročná činnost uvedeme-li fakt, že nám na daných směrovačích běží i normální provoz. Tudíž ve středních a velkých firmách je potřeba poměrně drahých zařízení, aby nedocházelo k velkým odezvám.

Další možnost je pořídit takzvané pasivní sondy, které se napojí mezi směrovače na linku, kterou chceme monitorovat. Toto řešení nám odstraňuje veškeré nevýhody předchozí architektury. Je to z důvodu, že směrovače již nic nepočítají (o protokolu NetFlow nemusí vůbec vědět). Vše obstarává pasivní sonda, která monitoruje daný provoz (pouze monitoruje, nijak nezasahuje, proto pasivní) a exportuje data dedikovanou linkou přímo na collector. (NetFlow Services Solutions Guide, 2007)

V praktické části se zaměříme na první možnost a to zapojení kdy protokol NetFlow běží na směrovači a data exportuje na collector.

5.3.6 Aplikace pro správu NetFlow

Existuje velké množství různých aplikací pro správu protokolu NetFlow, buď přímo od společností Cisco, či třetích komerčních stran, nebo volně stažitelné a použitelné pro nekomerční využití. Jsou mezi nimi někdy i poměrně velké rozdíly, záleží k čemu konkrétně nám má náš collector sloužit. Nyní si popíšeme základní otázky, které by nás měly zajímat při volbě vhodné aplikace.

- Kvůli čemu jsme se rozhodli využívat protokol NetFlow? (bezpečnost, zátěž daného provozu, analýza a sběr dat apod.)
- Je pro nás stěžejnější analýza v reálném čase, či sběr dat za určitý čas?
- Na kterém operačním systému collectot poběží?
- V jakém rozsahu bude implementace protokolu NetFlow?
- Kolik a jestli vůbec jste ochotni platit za daný software?
- Pokud nám již běží nějaký collector, je vhodné ho měnit za jiný? (Introduction to Cisco IOS NetFlow, 2007)

Toto jsou základní otázky, které by si měl každý správce, který chce zprovoznit NetFlow collector, klást. Dále si popíšeme dva představitele a to Real-time NetFlow Analyzer od společnosti SolarWinds, NetFlow Analyzer od společnosti ManageEngine.

Real-time NetFlow Analyzer

Jedná se o software od společnosti SolarWinds. Jedná se o americkou nadnárodní společnost sídlící v Austinu ve státě Texas. Založena byla v roce 1999. Zaměřují se převážně síťové služby a to z pohledu IT správy. Vyvíjí převážně software určený k monitorování sítě, usnadnění správy sítě, sledovaní prostředků a výkonu sítě apod. V České republice se nachází také jedna z jejich poboček a to konkrétně v Brně, kde je zaměstnáno více jak 300 zaměstnanců. (Network Management news, events, jobs and awards, [b. r.])

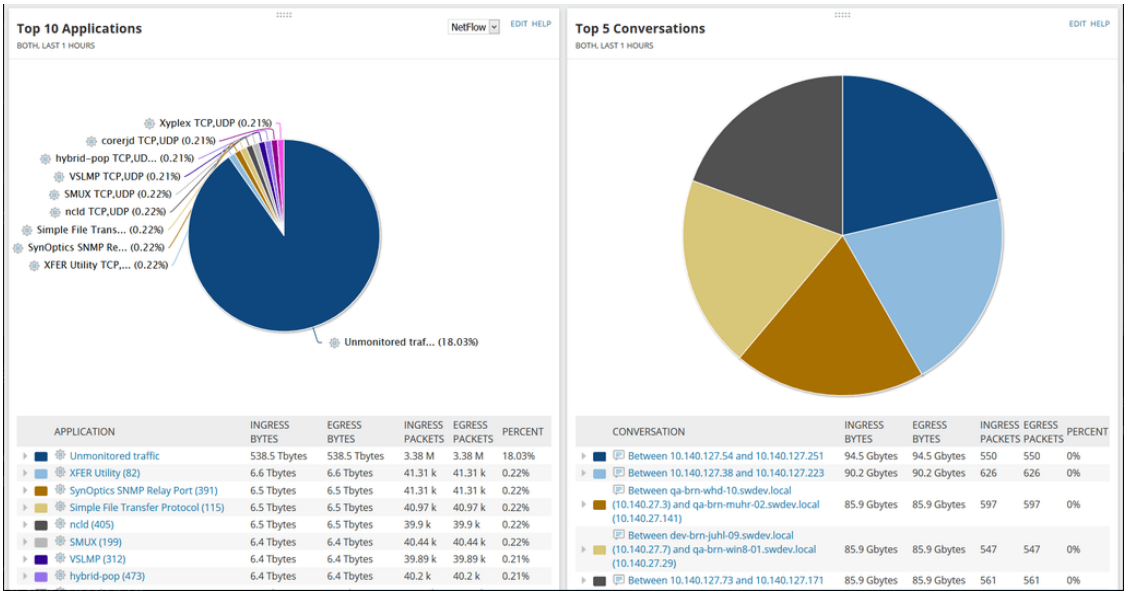
Real-time NetFlow Analyzer je software určený analýze provozu sítě v reálném čase. Jak již bylo zmíněno, jedná se o NetFlow collector, tudíž data sbírá z toku dat, které mu zasílá NetFlow exportér. Společnost SolarWinds nabízí na svých stránkách placenou i neplacenou verzi. (FREE Real-Time NetFlow Analyzer, [b. r.])

Placená verze se jmenuje Network Bandwidth Analyzer Pack, která kromě sledování toku dat nabízí také službu pro vyšetřování a sledování neočekávaných toků dat, filtry pro určité typy dat uvnitř daného toku, službu pro získávání notifikací a „poplašných“ zpráv, možnost vidět

„kro po kroku“ provoz kolem určitého zařízení, možnost integrovat so SolarWinds Orion (software pro sumarizaci dat s více aplikací najednou), možnost sledovat podrobněji odezvu, dostupnost a výkon jednotlivých síťových zažízení. (Network Bandwidth Analyzer – Bandwidth Monitor, [b. r.])

Neplacená verze, neboli zmíněný Real-time NetFlow Analyzer obsahuje pouze sběr toků dat z NetFlow exportéru a ty různě filtrovat, či si je nechat vykreslit v úhledných grafech, nebo tabulkách. Ačkoli pro to tento software není preferován, lze si samozřejmě nechat vypsat statistiky za určitý čas. Lze v něm pohodlně sledovat, kde má síť největší zátěž a co nám ji způsobuje.

Mezi podporované platformy patří pouze Microsoft Windows Server 2008 R2 a novější. Využívá se ve firmách využívající SMB (Server Message Block). (FREE Real-Time NetFlow Analyzer, [b. r.])



Obrázek 5 – Ukázka Real-time NetFlow Analyzer

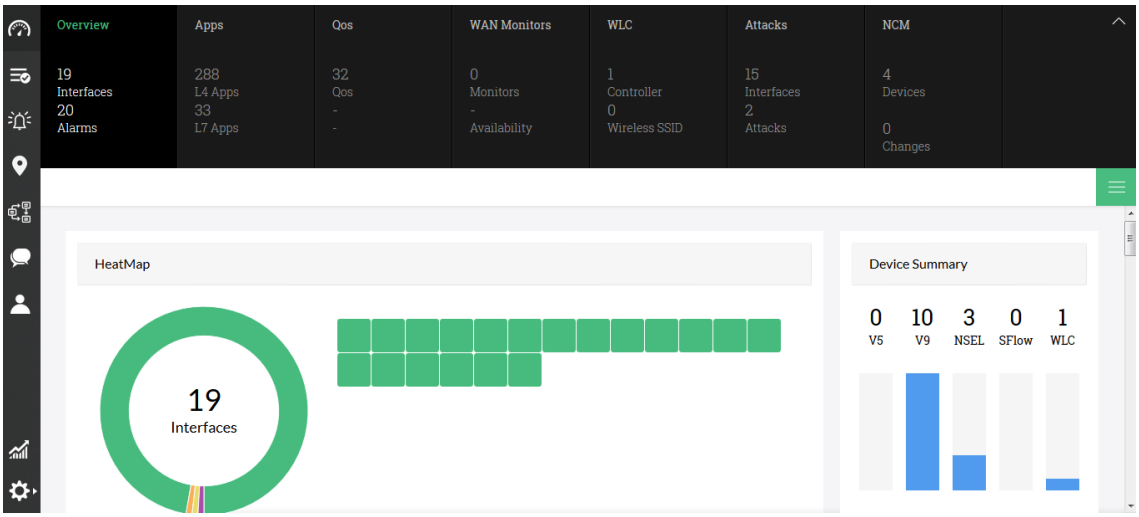
Zdroj: (SOLARWINDS,2017)

NetFlow Analyzer

Tento software vytvořil ManageEngine. ManageEngine je část společnosti Zoho zabývající se IT správou. Zaměřují se na vývoj aplikací usnadňující IT správu. Mají již přes 90 různých produktů, které pomáhají IT specialistům po celém světě. Společnost vznikla v roce 1996 jako AdventNet se zaměřením na správu sítí. V roce 2003 se firma přejmenovala na Zoho corporation a vznikl samostatný oddíl pro vývoj aplikací se zaměřením na správu IT se jménem ManageEngine. (ManageEngine - About Us, [b. r.])

NetFlow Analyzer je nástroj pro analýzu provozu na dané síti, využívající datových toků, poskytující vidět data v reálném čase. Stejně jako předchozí produkt, i tento získává data z protokolu NetFlow a poté je zpracovává do grafů, či tabulek, které dále slouží administrátorovi k různým potřebám (sledování provozu, vyšetřování chyb, zvyšování výkonu apod.).

Tento nástroj je nabízen ve třech verzích. A to Essential, Distributed a Free. Essential a Distributed jsou placené verze. Essential je doporučený pro malé a středně velké firmy. Na rozdíl od Distributed, který využívaný jen velkými firmami je trochu omezený. Omezení se týkají hlavně počtu rozhraní, kde Essential má povolené až 5 000 rozhraních, zatímco Distributed je má neomezené. Další omezení se týkají možností monitorování a bezpečnostních analýz, které si však lze dokoupit formou Add-on. Free verze je na tom nejhůře, dokáže monitorovat pouze dvě rozhraní a poskytuje pouze základní možností monitorování. Je určen tedy k vyzkoušení tohoto nástroje, nebo pro domácí využití. (Network Bandwidth Monitoring, [b. r.])



Obrázek 6 – Ukázka NetFlow Analyzer

Zdroj: online demo (NETFLOWANALYZER,2017)

5.3.7 Nevýhody

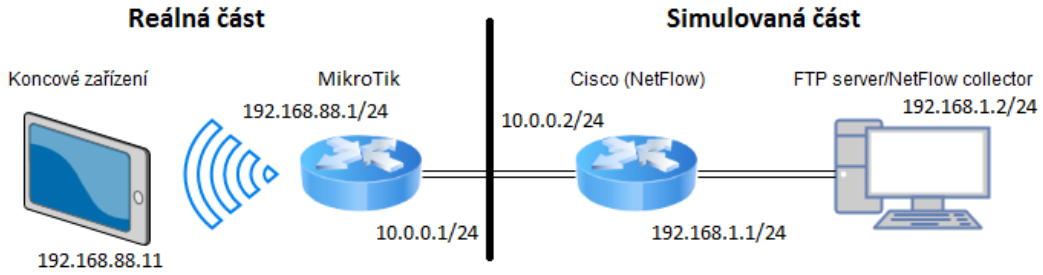
Mezi nevýhody může patřit občasná náročnost zařízení, či výjimečná ztráta dat. Jelikož NetFlow exportér využívá UDP k zasílání datagramů, je jistá šance, že datagram bude ztracen. Je to z důvodu, že okamžitě po odeslání exportérem jej exportér zahodí (aby se mohl věnovat dalším datagramům) aniž by se nějak dozvěděl, zda byl datagram úspěšně doručen.

6 PRAKTICKÁ ČÁST

V této kapitole popisuje jednotlivé kroky k vytvoření testované sítě. Podrobně jsou zde popsány postupy konfigurace jednotlivých částí, počínaje topologií sítě v GNS3, konfigurace jednotlivých zařízení a nastavení jednotlivých protokolů sledování komunikace pomocí protokolu NetFlow.

6.1 Topologie sítě

Topologie vytvořena pro tuto laboratorní úlohu je velmi jednoduchá. Zahrnuje dva směrovače, jeden server a koncové zařízení. Směrovač od společnosti Cisco a server je simulován v simulačním nástroji GNS3. Na tomto Cisco zařízení poběží i protokol NetFlow. Na serveru běží operační systém Windows 10 a bude na něm nakonfigurován FTP server a NetFlow collector. Směrovač od společnosti MikroTik a koncové zařízení jsou již reálná zařízení. O komunikaci se postará směrovací protokol OSPF, který v našem případě postačí nakonfigurovat jako single area (pouze jedna oblast).



Obrázek 7 – Topologie

Zdroj: vlastní pomocí online návrháře (DRAW.IO)

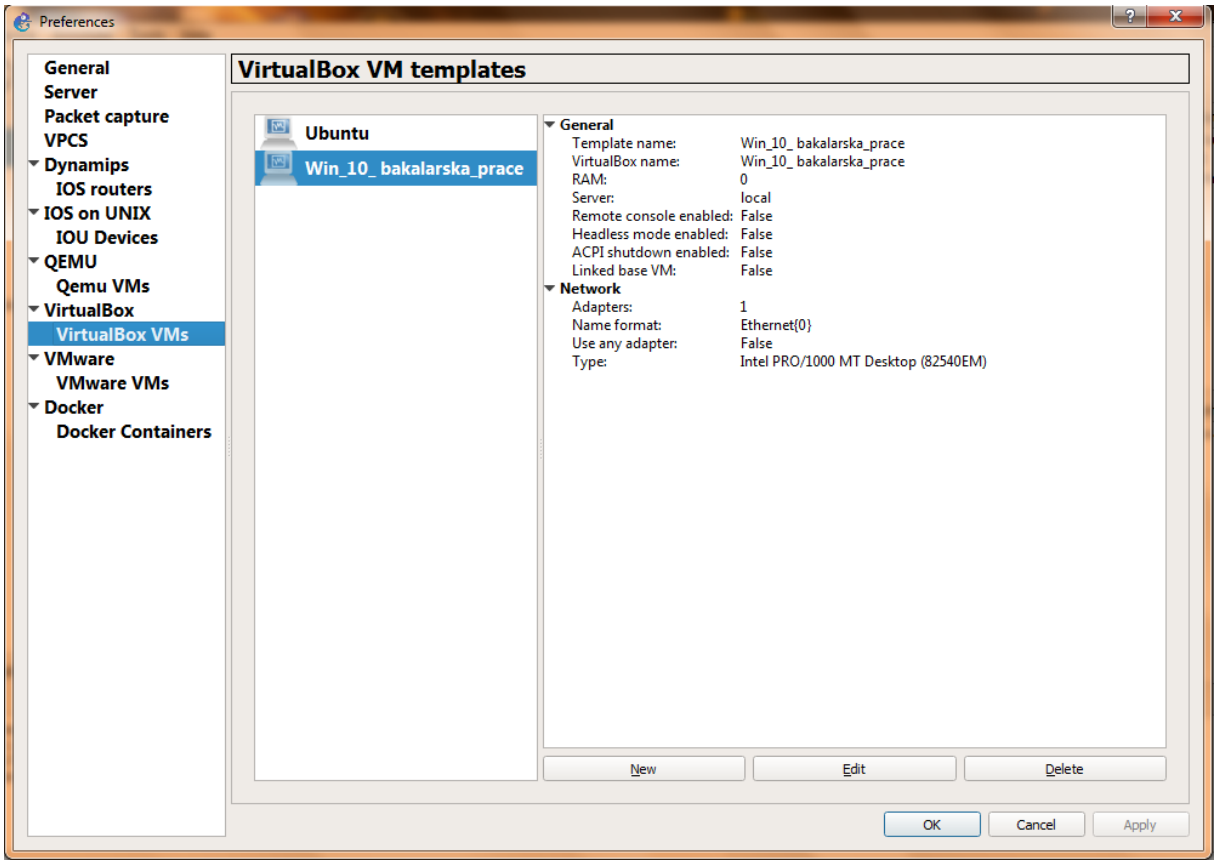
6.2 Zapojení v prostředí GNS3

Jak naistalovat GNS3 a přidat do něj zařízení je již popsané v kapitole věnované tomuto nástroji. V této podkapitole je popsané jak s tímto nástrojem pracovat, aby bylo možné vytvořit navrhnutou topologii.

Jako první importujeme do GNS3 virtuální stroj, který bude reprezentovat server, který bude fungovat jako FTP server a NetFlow collector.

- V horní liště vybereme rozevírací seznam „Edit“ a zvolíme možnost „Preferences“.
- V nově otevřeném okně v levém seznamu záložku „VirtualBox VMs“.

- Kliknutím na tlačítko „New“ se otevře okno, kde máme možnost vybrat nějaký virtuální stroj vytvořený nástrojem VirtualBox.
- Po vybrání uzavřeme okno tlačítkem „Finish“.



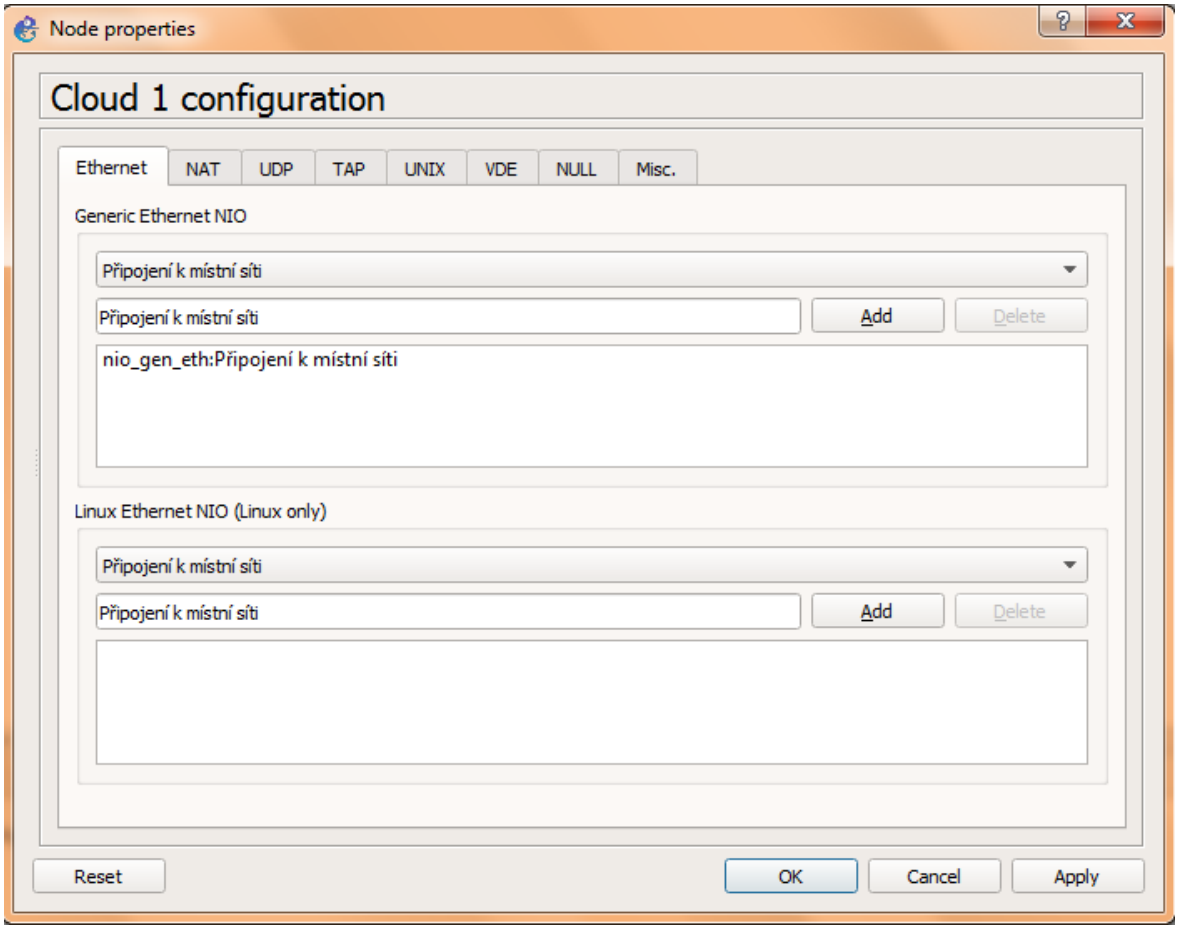
Obrázek 8 – Konfigurační okno, VirtualBox

Zdroj: vlastní

Nyní již je virtuální stroj k dispozici a lze jej nalézt v záložce „End Devices“. Nyní již lze bez problémů vytvořit navrhovanou topologii.

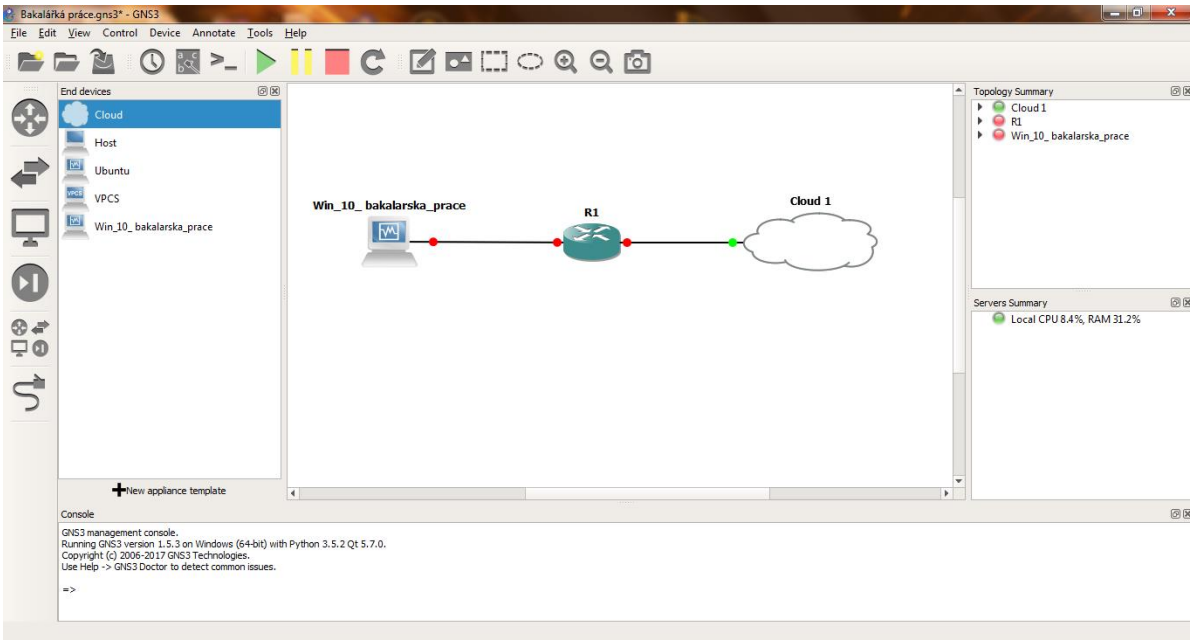
- V levé části obrazovky vybereme záložku „Routers“ a pomocí „drag and drop“ přesuneme vybraný směrovač na pracovní plochu.
- Stejně tak učiníme s našim virtuálním strojem, který nalezneme v záložce „End Devices“.
- Nakonec vložíme nástroj „Cloud“, díky kterému se lze připojit k reálné síti. Ten se nachází taktéž v záložce „End Devices“.
- Pravým kliknutím na „Cloud“ se otevře rozevírací seznam, kde se nachází možnost „Configure“. Otevře se konfigurační okno (viz Obrázek 9), kde zvolíme síťové rozhraní, přes které se GNS3 propojí do reálné sítě. Přidáme jej tlačítkem „Add“ a okno uzavřeme tlačítkem „Ok“.

- Dále klikneme na záložku „Add a link“. Nyní lze jednotlivé zařízení propojit, podle navrhnuté topologie (viz Obrázek 10). Kliknutím na zařízení se otevře seznam rozhraní, ke kterým lze připojit propojovací „kabel“.



Obrázek 9 – Konfigurace Cloud

Zdroj: vlastní



Obrázek 10 – Ukázka zapojení v nástroji GNS3

Zdroj: vlastní

6.3 Konfigurace OSPF

V této podkapitole se nachází postup konfigurace protokolu OSPF na směrovači od společností Cisco a na směrovači od společnosti MikroTik. Jako první je popsána konfigurace směrovače od společnosti Cisco v simulačním nástroji GNS3.

Nejdříve je potřeba zvolit vhodnou adresaci pro jednotlivé rozhraní.

Tabulka 3: Adresovací tabulka

Směrovač/rozhraní	Adresa sítě	IP adresa rozhraní	Maska sítě
MikroTik/WiFi	192.168.88.0	192.168.88.1	255.255.255.0
MikroTik/LAN 3	10.0.0.0	10.0.0.1	255.255.255.0
Cisco/f0/0	10.0.0.0	10.0.0.2	255.255.255.0
Cisco/f0/1	192.168.1.0	192.168.1.1	255.255.255.0
Server	192.168.1.0	192.168.1.2	255.255.255.0
Koncové zařízení	192.168.88.0	192.168.88.11	255.255.255.0

Zdroj: vlastní

Následuje konfigurace v simulačním nástroji GNS3.

- Nejdříve je potřeba zapnout simulaci. Ta se zapíná pomocí tlačítka znázorňující zelenou šipku s názvem „Start all devices“.

- Po úspěšném startu stačí dvakrát poklepat na směrovač, který chceme konfigurovat, a otevře se Putty, který se rovnou připojí ke směrovači, a zobrazí CLI.

Jako první se musí nakonfigurovat IP adresy na jednotlivé rozhraní (viz Tabulka2). Následuje ukázka jak toho docílit.

```
R1#configure terminal
R1(config)#interface f0/0
R1(config-if)#ip address 10.0.0.2 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
```

Stejným způsobem se konfigurují všechny rozhraní týkající se této laboratorní úlohy.

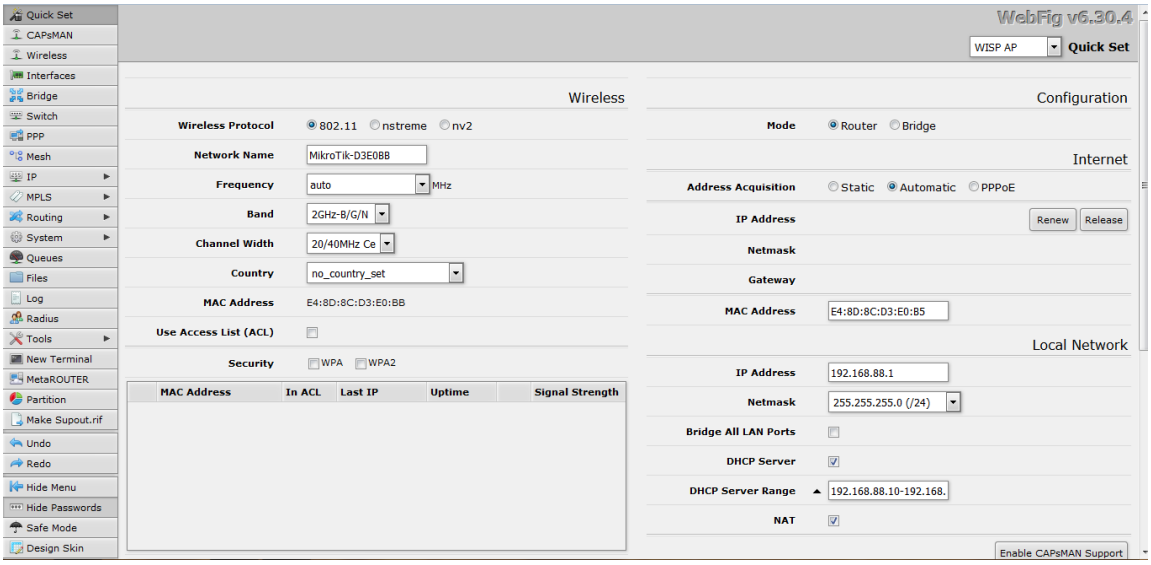
Po nakonfigurování rozhraní je již vše připraveno ke konfiguraci směrovacího protokolu OSPF. Níže je uvedena ukázka konfigurace protokolu OSPF v rámci jedné arei.

```
R1#configure terminal
R1(config)#router ospf 1
R1(config-router)#network 10.0.0.0 0.0.0.3 area 0
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# exit
```

Nyní již stačí uložit běžící konfiguraci a lze nastavení tohoto směrovače opustit. Následující podkapitoly se k tomuto směrovači vrátí, a to při konfiguraci protokolu NetFlow. Níže je popsána ukázka uložení běžící konfigurace.

```
R1# copy running-config startup-config
```

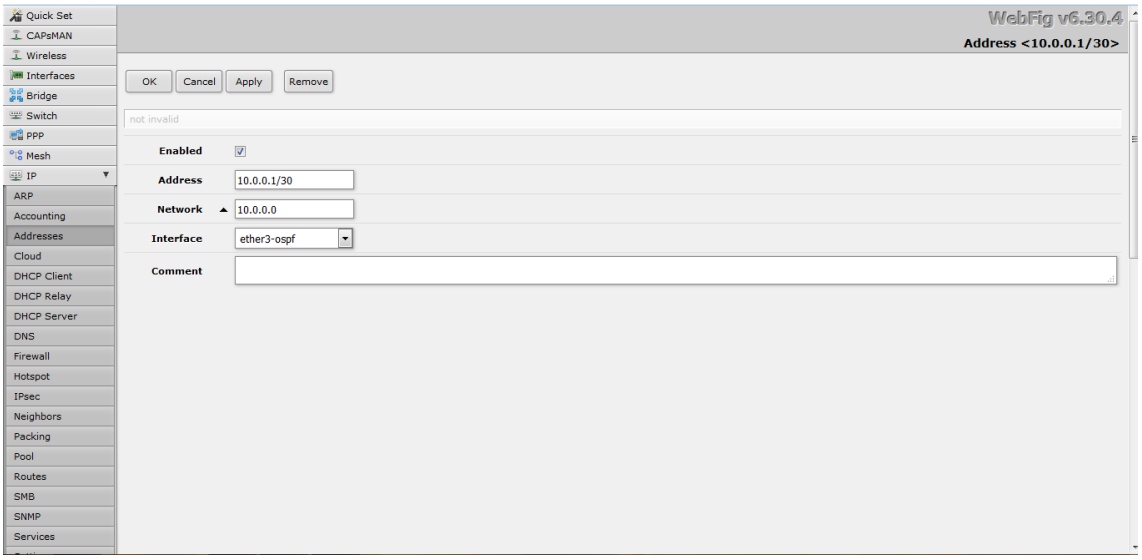
Po úspěšné konfiguraci směrovače od společností Cisco je potřeba nakonfigurovat směrovač od společnosti MikroTik. MikroTik využívá ke spravování grafické rozhraní, které může na první pohled vypadat poněkud chaoticky (viz Obrázek 11).



Obrázek 11 – Ukázka grafického rozhraní – MikroTik

Zdroj: vlastní

Nejdříve je potřeba nastavit adresu rozhraní. To nalezneme v menu na levé straně s názvem „IP“. Rozevře se seznam, kde zvolíme „Addresses“. Otevře se seznam již nastavených IP adres a k nim přiřazené rozhraní. Zvolíme tlačítko „Add New“. Vyplníme podle adresovací tabulky (viz tabulka 3) a potvrdíme tlačítkem „Apply“.



Obrázek 12 – Ukázka nastavení IP adresy – MikroTik

Zdroj: vlastní

Konfiguraci směrovacího protokolu OSPF nalezneme v menu pod záložkou „Routing“. Zobrazí se okno s několika kartami. V našem případě jsou důležité karty: „Interfaces“, „Instances“ „Network“ a „Area“.

- Rozevřeme kartu „Area“ a klikneme na tlačítko „Add“. Otevře se okno, které vyplníme podle potřeb (V našem případě ID: 0.0.0.0).
- Dále zvolíme „Network“ a klineme na tlačítko „Add“, otevře se okno a vyplníme adresami sítí, do kterých chceme mít přístup pomocí protokolu OSPF (10.0.0.0 a 192.168.88.0).
- Karta „Interfaces“ se vyplní automaticky podle zadaných sítí v „Network“. Lze vyplnit i ručně v případě chyby.
- V kartě „Instances“ se nachází „default“, který můžeme nechat jak je a jen jej spustit.

Tato konfigurace je postačující k navázání komunikace pomocí protokolu OSPF. Komunikaci lze ověřit buď v konfiguračním okně MikroTiku, v záložce OSPF, kde zvolíme „Neigbors“ a zde uvidíme sousedící směrovač, či v CLI směrovače od společnosti Cisco, kde zadáme příkaz: `show ip ospd neigbors.` Po zadání příkazu se vypíše seznam sousedů.

6.4 Konfigurace FTP

FTP server běží ve virtualizovaném prostředí na operačním systému Windows 10 od společnosti Microsoft. Následuje postup konfigurace.

- Otevřeme okno s názvem „Funkce systému Windows“ a povolíme server FTP.
- Dále otevřeme „Nástroje pro správu“ a vybereme „Správa informačních služeb“.
- Otevře se další okno, kde po levé stráně vybereme pravým tlačítkem „Stránky“ a klikneme na vložit FTP stránku.
- Otevře se průvodce, který nás provede celým procesem.

Podrobný návod v angličtině je k dispozici zde[2].

6.5 Konfigurace protokolu NetFlow a nastavení NetFlow collector

Zde je popsán postup konfigurace protokolu NetFlow a instalace, včetně konfigurace, NetFlow collectoru.

[2] http://www.windowscentral.com/how-set-and-manage-ftp-server-windows-10

Nejdříve je popsaná konfigurace protokolu NetFlow ve směrovači od společnosti Cisco. Otevřeme CLI směrovače pomocí Putty a přihlásíme se do globálního konfiguračního módu. Následuje sekvence příkazů.

```
R1(config)#ip flow-export destination 192.168.1.2 2055

R1(config)#ip flow-export version 5
```

2055 označuje port, na kterém collector příjme zasílané datové toky. Dále se připojíme na rozhraní směrovače, které chceme monitorovat (v tomto případě f0/0). Zadáme následující příkaz.

```
R1(config-if)#ip flow ingress
```

Toto pro základní konfiguraci protokolu NetFlow stačí. Následující část podkapitoly je věnovaná konfiguraci protokolu NetFlow (Traffic flow) ve směrovači MikroTik.

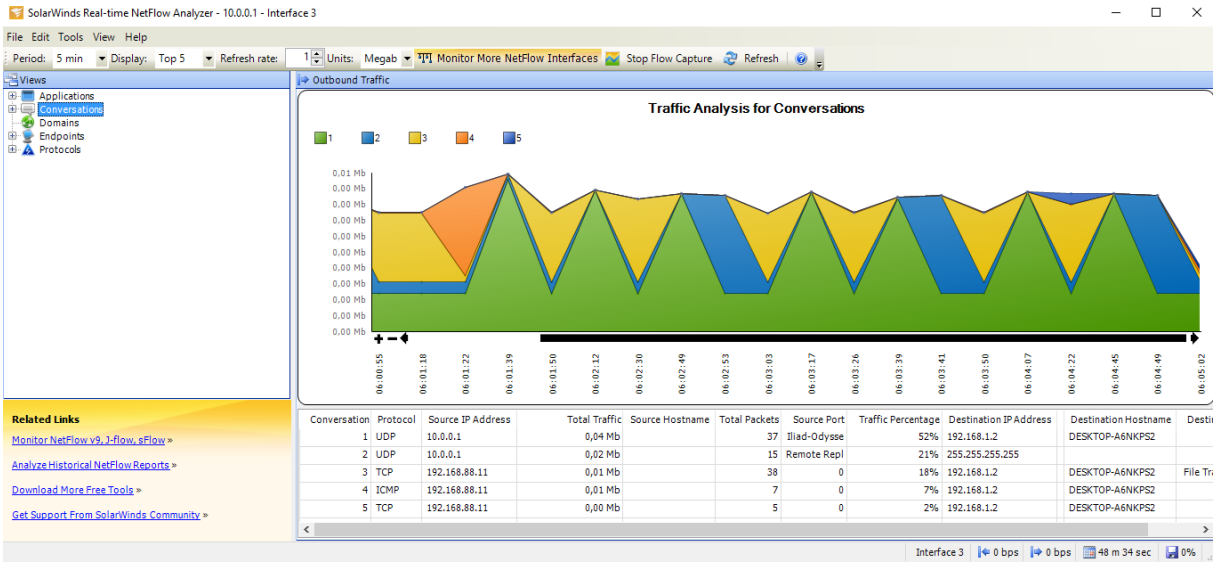
- Otevřeme záložku IP a zvolíme možnost „Traffic flow“.
- Otevře se okno, kde zvolíme rozhraní, které chceme monitorovat.
- Dále zvolíme tlačítko „Target“, kde napíšeme cílovou IP adresu, kam se mají data exportovat (192.168.1.2).
- Potvrdíme tlačítkem „Ok“.
- Nakonec zaškrtneme „Enable“ a původní okno zavřeme.

Nyní již je nastavený protokol NetFlow na obou směrovačích. Poslední část podkapitoly je zaměřena na konfiguraci NetFlow collectoru.

Zvolil jsem jako collector výše popsaný Real-time NetFlow Analyzer od společnosti SolarWinds. Z oficiálních stránek (13) lze stáhnou kompletní instalační balíček, který obsahuje vše potřebné. Instalace je snadná, v případě potřeby lze navštívit technickou podporu.

Po spuštění, se otevře okno s automaticky načtenými rozhraními, na kterých běží protokol NetFlow (v případě chyby, lze přidat ručně). Vybereme rozhraní, které chceme sledovat

a klikneme na tlačítko „Start capture“. Otevře se prostředí NetFlow Analyzeru, kde vidíme monitorovanou komunikaci v reálném čase (viz Obrázek 12).



Obrázek 13 – Ukázka NetFlow Analyzer

Zdroj: vlastní

V levém okně „Views“ můžeme filtrovat výstup na obrazovku podle různých kritérií. Pokud klikneme na záložku „Conversations“ otevře se graf proběhlé komunikace a pod ní tabulka s výpisem proběhlých dat (viz Obrázek 13). Z tabulky lze přehledně vyčíst odkud, a kam daný tok dat probíhal a jaký protokol zde byl využit. Je zde také zaznamenané kolik celkové paketů zde proběhlo a na kolik procent byla linka využita apod.

Conversation	Protocol	Source IP Address	Destination IP Address	Total Traffic	Source Hostname	Total Packets	Source Port	Destination Port	Traffic Percentage	De
5	UDP	10.0.0.1	255.255.255.255	0,02 Mb		15	Remote Repl	0	0,02%	
3	OSPF	10.0.0.1	224.0.0.5	0,10 Mb		185	0	0	0,1%	
1	TCP	192.168.88.11	192.168.1.2	56,05 Mb		4702	0	49697	64%	DE
2	TCP	192.168.88.11	192.168.1.2	30,77 Mb		2582	0	49696	35%	DE
4	UDP	10.0.0.1	192.168.1.2	0,03 Mb		27	Iliad-Odysse	0	0,04%	DE

Obrázek 14 – Tabulka zachycené komunikace

Zdroj: vlastní

Na obrázku 14 je zachycen okamžik, kdy na FTP server (IP adresa: 192.168.1.2) byla z koncového zařízení (IP adresa: 192.168.88.11) zasílána data. Lze zde vyčíst: jaký protokol byl využit, odkud a kam směroval provoz, celkovou velikost, počet paketů a procentuální vytížení na kolik procent daný tok dat využil monitorovaný port.

ZÁVĚR

Cílem práce bylo zachytávat a kontrolovat datový tok pomocí protokolu Netflow na navrhnuté síťové infrastruktuře. Síťová infrastruktura obsahovala dvě LAN sítě, WAN síť a FTP server. Prvních pět kapitol bylo věnováno hlavně teorii, na kterou navázala praktická část.

Pro praktickou ukázku byl zvolen simulační nástroj GNS3, který podporuje připojení k reálné síti. Uvnitř prostředí GNS3 byl naistalován server, virtualizovaný pomocí VirtualBoxu, s operačním systémem Windows 10. Na serveru byla umístěna aplikace FTP server a NetFlow kolektor. Dále zde byl použit směrovač od společnosti Cisco, který byl spojen s reálným zařízením od společnosti MikroTik. Na tomto směrovači byl nakonfigurován směrovací protokol OSPF a protokol NetFlow, který odesílal data na kolektor.

Reálná část byla vytvořena z již zmiňovaného směrovače od společnosti MikroTik a koncového zařízení. Na směrovači byl nakonfigurován směrovací protokol OSPF a nastaven protokol NetFlow (Traffic Flow). Pomocí reálného rozhraní hostujícího počítače, na kterém bylo implementováno prostředí GNS3, byl MikroTik propojen se simulovanou sítí. Koncové zařízení vytvořilo konektivitu pomocí Wi-Fi k MikroTiku.

Výsledkem bylo, že koncové zařízení mělo schopnost se připojit na FTP server běžící v simulačním prostředí GNS3 a pracovat zde se soubory (stahovat, mazat, či nahrávat nové). Tyto operace byly monitorovány pomocí protokolu NetFlow, který zachytával komunikaci směřující z koncového zařízení na FTP server a zasílal jej na kolektor běžící na serveru. Pomocí kolektoru byla data vyfiltrována a vypsána (viz Obrázek 13). Ze získaných údajů bylo možné vypozorovat několik následujících údajů: odkud, a kam daná síťová komunikace proudila, jaký byl použitý protokol, jakým způsobem vytížil měřenou linku, kolik paketů bylo celkově odesláno v rámci jednoho IP toku. Monitorování síťových toků lze provozovat jak na směrovači od společnosti Cisco, tak na směrovači od společnosti MikroTik.

POUŽITÁ LITERATURA

1. **BOMBAL, David.** Windows Installation. [online]. 2017 [cit. 2017-04-20]. Dostupné z: https://www.gns3.com/support/docs/quick-start-guide-for-windows-us
2. **Cisco Systems, Inc**. Cisco VIRL. [online]. [cit. 2017-04-20] Dostupné z: http://virl.cisco.com/work/
3. **Cisco Systems, Inc**. Introduction to Cisco IOS NetFlow. [online]. 2012 [cit. 2017-04-20]. Dostupné z: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html
4. **Cisco Systems, Inc**. NetFlow Services Solutions Guide. [online]. [cit. 2017-04-20]. Dostupné z: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html#wp1031628
5. **Cisco Systems, Inc**. NetFlow Export Datagram Format. [online]. 2007 [cit. 2017-04-20]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/net_mgmt/netflow_collection_engine/3-6/user/guide/format.html
6. **Draw.io**. [online]. [cit. 2017-04-20]. Dostupné z: https://www.draw.io/
7. **EnterpriseDT.** CompleteFTP User's Guide. [online]. [cit. 2017-04-20] Dostupné z: http://enterprisedt.com/products/completeftp/doc/guide/index.html
8. **GRYGAREK, Petr.** Směrovací protokol OSPF. [online]. [cit. 2017-04-20]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html
9. **KABELOVÁ, Alena, DOSTÁLEK, Libor.** Velký průvodce protokoly TCP/IP a systémem DNS. Vyd. Brno: Computer Press, 2012, ISBN 978-80-251-2236-5.
10. **LAMMLE, Todd**. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.
11. **ManageEngine**. About us. [online]. [cit. 2017-04-20]. Dostupné z: https://www.manageengine.com/company.html
12. **ManageEngine**. Editions Comparison. [online]. [cit. 2017-04-20]. Dostupné z: https://www.manageengine.com/products/netflow/netflow-analyzer-editions.html

13. **ManageEngine**. NetFlow Analyzer. [online]. [cit. 2017-04-20]. Dostupné z: http://demo.netflowanalyzer.com/apiclient/ember/index.jsp#/Home/Dashboard/NFA/NFADB.traffic
14. **SAMURAJ**. Cisco IOS 1 – úvod. [online]. 2007 [cit. 2017-04-20]. Dostupné z: http://www.security-portal.cz/clanky/cisco-ios-1-%C3%BAvod-p%C5%99%C3%ADkaz-show
15. **SolarWinds**. SolarWinds: Delivering Unexpected Simplicity. [online]. [cit. 2017-04-20]. Dostupné z: http://www.solarwinds.com/company/home
16. **SolarWinds**. Real-Time NetFlow Analyzer. [online]. [cit. 2017-04-20]. Dostupné z: http://www.solarwinds.com/free-tools/real-time-netflow-analyzer
17. **SolarWinds**. Network Bandwidth Analyzer Pack. [online]. [cit. 2017-04-20]. Dostupné z: http://www.solarwinds.com/network-bandwidth-analyzer-pack
18. **WAQAZ, Azam.** GNS3 Supported Routers IOS Image list. [online]. 2016 [cit. 2017-04-20]. Dostupné z: http://w7cloud.com/gns3-supported-routers-ios/

PŘÍLOHY

Příloha A – *Konfigurační soubor směrovače od společnosti Cisco*

```
Current configuration : 1114 bytes
!
version 12.3
service timestamps debug datetime
msec
service timestamps log datetime
msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip subnet-zero
no ip icmp rate-limit unreachable
!
ip tcp synwait-time 5
no ip domain lookup
!
ip cef
ip ips po max-events 100
no ftp-server write-enable
!
interface FastEthernet0/0
 ip address 10.0.0.2 255.255.255.0
 ip route-cache flow
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 ip address 192.168.1.1
255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area
0
!
ip classless
ip flow-export version 5
ip flow-export destination
192.168.1.2 2055
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
! end
```

Příloha B – *Konfigurační soubor směrovače od společnosti MikroTik*

```
# jan/02/1970 21:50:28 by RouterOS 6.30.4
# software id = 17MK-HPYT
#
/interface bridge
add admin-mac=E4:8D:8C:D3:E0:B6 auto-mac=no name=bridge-local
add name=loopback
/interface ethernet
set [ find default-name=ether1 ] name=ether1-gateway
set [ find default-name=ether2 ] name=ether2-master-local
set [ find default-name=ether3 ] auto-negotiation=no name=ether3-ospf
set [ find default-name=ether4 ] name=ether4-pomoc
set [ find default-name=ether5 ] master-port=ether2-master-local name=\
    ether5-slave-local
/interface wireless
set [ find default-name=wlan1 ] band=2ghz-b/g/n channel-width=20/40mhz-Ce \
    disabled=no distance=indoors frequency=auto l2mtu=1600 mode=ap-bridge \
    rx-chains=0,1 ssid=MikroTik-D3E0BB tx-chains=0,1 wireless-protocol=802.11
set [ find default-name=wlan2 ] band=5ghz-a/n/ac channel-width=20/40mhz-Ce \
    disabled=no distance=indoors frequency=auto l2mtu=1600 mode=ap-bridge \
    ssid=MikroTik-D3E0BB wireless-protocol=802.11
/ip neighbor discovery
set ether1-gateway discover=no
/ip ipsec proposal
set [ find default=yes ] disabled=yes
/ip pool
add name=default-dhcp ranges=192.168.88.15-192.168.88.254
/ip dhcp-server
add address-pool=default-dhcp interface=bridge-local name=default
/routing ospf instance
set [ find default=yes ] name="ospf 1" router-id=1.1.1.1
/interface bridge port
add bridge=bridge-local interface=ether2-master-local
add bridge=bridge-local interface=wlan1
add bridge=bridge-local interface=wlan2
```

```
/ip address
add address=192.168.88.1/24 comment="default configuration" interface=\
    bridge-local network=192.168.88.0
add address=10.0.0.1/24 interface=ether3-ospf network=10.0.0.0
add address=192.168.168.1/24 interface=loopback network=192.168.168.0
add address=200.0.0.0/24 interface=ether1-gateway network=200.0.0.0
/ip dhcp-client
add    comment="default    configuration"    dhcp-options=hostname,clientid
interface=\
    ether1-gateway
/ip dhcp-server network
add address=192.168.88.0/24 comment="default configuration" gateway=\
    192.168.88.1
/ip dns
set allow-remote-requests=yes
/ip dns static
add address=10.0.0.1 name=router
/ip firewall filter
add chain=input comment="default configuration" disabled=yes protocol=icmp
add chain=input comment="default configuration" connection-state=\
    established,related disabled=yes
add action=drop chain=input comment="default configuration" disabled=yes \
    in-interface=ether1-gateway
add action=fasttrack-connection chain=forward comment="default configuration"
\
    connection-state=established,related disabled=yes
add chain=forward comment="default configuration" connection-state=\
    established,related disabled=yes
add action=drop chain=forward comment="default configuration" \
    connection-state=invalid disabled=yes
add action=drop chain=forward comment="default configuration" \
    connection-nat-state=!dstnat connection-state=new disabled=yes \
    in-interface=ether1-gateway
/ip firewall nat
add action=masquerade chain=srcnat comment="default configuration" disabled=\
    yes out-interface=ether3-ospf
/ip ipsec policy
set 0 disabled=yes
/ip route
```

```
add disabled=yes distance=1 dst-address=192.168.1.0/24 gateway=10.0.0.2
/ip traffic-flow
set enabled=yes interfaces=ether3-ospf
/ip traffic-flow target
add address=192.168.1.2:2055 version=5
/ip upnp
set show-dummy-rule=no
/routing ospf network
add area=backbone network=10.0.0.0/24
add area=backbone network=192.168.88.0/24
add area=backbone network=192.168.168.0/24
/system logging
add topics=ospf
/system routerboard settings
set cpu-frequency=650MHz protected-routerboot=disabled
/tool mac-server
set [ find default=yes ] disabled=yes
add interface=ether2-master-local
add interface=ether3-ospf
add interface=ether4-pomoc
add interface=ether5-slave-local
add interface=wlan1
add interface=wlan2
add interface=bridge-local
/tool mac-server mac-winbox
set [ find default=yes ] disabled=yes
add interface=ether2-master-local
add interface=ether3-ospf
add interface=ether4-pomoc
add interface=ether5-slave-local
add interface=wlan1
add interface=wlan2
add interface=bridge-local
/tool romon port
add
```