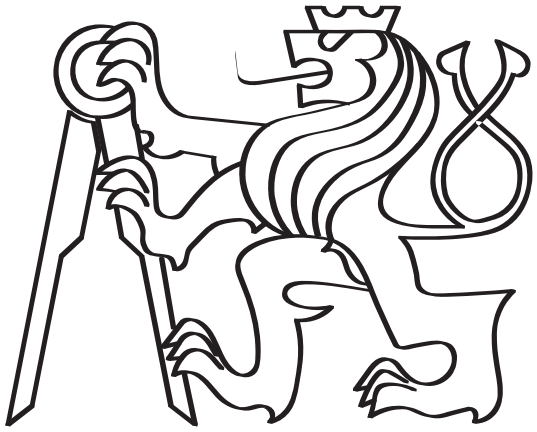
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky



Bakalářská práce

Automatizace konfigurace síťových prvků pomocí Ansible

Miroslav Hudec

Studijní program: Komunikace, multimédia a elektronika
Studijní obor: Síťové a informační technologie
Vedoucí práce: Miloš Kozák

Praha, Březen 2016

Obsah

Zadání projektu

Využijte nástroj Ansible pro automatickou správu sítových prvků. Zaměřte se na síťové prvky od společnosti Mikrotik a rozšiřte nástroj Ansible tak, aby bylo možné konfigurovat základní i pokročilé funkce těchto síťových prvků. Mezi základní funkce patří správa uživatelský účtů, logování a adresace síťových rozhraní. Mezi pokročilé funkce patří správa firewallu, překladu adres a síťových mostů. Navrhněte případy užití, na kterých ukážete funkci implementovaného rozšíření.

Motivace

V důsledku stálého rozvoje dnešních počítačových sítí a zvyšovaní nároků na ně kladených, je často potřeba zavádět do produkčního provozu větší množství nových a výkonějších zařízení. V současnosti bývají tato zařízení konfigurována jedno po druhém, což prodlužuje dobu nutnou pro nastavení a tím samozřejmě zvyšuje náklady na implementaci. Cílem této práce je zefektivnění tohoto postupu navrhnutím řešení, které umožní automatizovanou konfiguraci mnoha zařízení dle zadaných požadavků. Zařízení by tak bylo možné nakonfigurovat během velmi krátké doby a s minimálním úsilím. V rámci této práce se budu věnovat konfiguraci na zařízeních MikroTik.

Úvod

Komunikace mezi lidmi hrála vždy velkou roli. Předávání informací je jedním ze základních předpokladů pro vývoj lidstva. Mnoha významných objevů v historii by nebylo možné dosáhnout bez spolupráce lidí z různých zemí či kontinentů, kterým nejrůznější prostředky komunikace umožnili sdílet získané poznatky či nápady. Dnes si mohou vědecké týmy z celého světa vyměňovat ohromná množství nově získaných dat takřka okamžitě, lidé mohou sledovat dění na opačné straně planety v reálném čase, přátelé si sdělují zážitky prostřednictvím sociálních sítí, multimediálních zpráv. Díky internetu a dnešním chytrým mobilním zařízením máme téměř celé vědění lidstva v kapse, doslova. Tento ohromný pokrok nám umožnil právě vznik počítačových sítí.

Počátky počítačových sítí můžeme sledovat do 60. let 20. století. Tehdy začaly první pokusy s propojením dvou počítačů a výměnou informací mezi nimi. Od té doby ušel vývoj počítačových sítí ohromný kus cesty. Dokonalejší hardware umožnil spolehlivěji přenášet větší množství dat mnohonásobně rychleji. Tyto sítě se také značně rozvinuli co do rozlohy. Oproti tehdejšímu propojení dvou počítačů v sousedních místnostech dosáhly počítačové sítě vskutku globálního rozsahu. Tuto celosvětovou síť jistě všichni známe pod názvem Internet. V současnosti má více než 40% světové populace přístup k této globální síti. V roce 1995 to bylo méně než 1%. Každou minutou navíc přibyde zhruba 500 uživatelů internetu. Nároky na dnešní počítačové sítě navíc stále narůstají. Musejí být schopné přenášet ještě větší objemy dat ještě rychleji, spolehlivě, být bezpečné a odolné proti výpadku. Z těchto skutečností je zřejmé, že aby dnešní sítě udržely s těmito požadavky krok, musí se neustále rozvíjet nejen po stránce rozlohy, ale také výkonu. Tím se v podstatě rozumí nasazování nových síťových prvků, které jsou schopny tyto požadavky ukojit. Právě na usnadnění a urychlení tohoto procesu se zaměřuje tato práce.

V první kapitole vysvětlena podstata činnosti počítačových sítí a jejich rozdělení. Dále je zde uveden princip činnosti základních síťových prvků a jejich uplatnění v síti, výčet základních používaných protokolů a standardů a vysvětlení referenčního modelu ISO OSI a TCP/IP.

Druhá kapitola pojednává o současném postupu při implementaci nových síťových prvků a navrhuje možné zefektivnění tohoto postupu...

Třetí kapitola popisuje technické prostředky pro automatizaci konfigurace síťových prvků, konkrétně na zařízeních společnosti MikroTik...

Čtvrtá kapitola – praktická ukázka, use-case...

Pátá kapitola ...

V závěru této práce ...

1 Počítačové sítě

Počítačová síť neboli datová síť, je telekomunikační síť, která umožňuje počítačům vyměňovat si data. Zařízení v počítačové síti si vyměňují data prostřednictvím datových okruhů (angl. data link). Tyto okruhy jsou realizovány pomocí metalického nebo optického kabelu, či bezdrátovou technologií. Zařízení, která vysílají, přijímají nebo směrují data, označujeme jako síťové uzly. Takovýmto uzlem je například osobní počítač, chytrý telefon, server či síťový prvek. Základními předpoklady pro funkčnost počítačové sítě jsou:

- Zařízení vysílající nebo přijímající data
- Přenosové médium
- Protokol nebo sada protokolů

1.1 Typy počítačových sítí

Počítačové sítě lze rozdělit podle mnoha kritérií. Nejčastějším způsobem klasifikace je dělení podle rozlehlosti sítě. Sítě pak můžeme dělit na:

- **Lokální sítě** – LAN (Local Area Network) – Sítě pokrývající malé území, většinou v rámci domácnosti či budovy.
- **Metropolitní sítě** – MAN (Metropilotan Area Network) – Sítě pokrývající území v rámci například města, spojující více budov. Typickým příkladem jsou kampusové sítě.
- **Rozsáhlé sítě** – WAN (Wide Area Network) – Sítě spojující velká geografická území. Typickým příkladem takovéto sítě je Internet.

1.2 Referenční modely

Motivací pro vytvoření referenčního modelu (RM) je poskytnutí základů pro vytvoření norem pro účely propojování systémů. Na základě takového modelu je pak možné abstrahovat nejrůznější úkony a prvky síťové komunikace do určitých vrstev. Díky této abstrakci je poté snazší vytvářet standardy a popisovat všeobecné principy síťové architektury. Každá vrstva má za úkol převzít data z vyšší vrstvy, vhodně je upravit pro nižší vrstvu a naopak.

1.2.1 Referenční model ISO/OSI

V rámci snahy o standardizaci počítačových sítí vypracovala organizace ISO v roce 1984 Referenční model ISO/OSI a přijala ho jako normu ISO 7498. Tento model se používá jako názorný příklad řešení komunikace v počítačových a telekomunikačních sítí. Jedná se o vrstevnatý model, ve kterém má každá vrstva svoji úlohu. RM OSI pracuje se sedmi vrstvami:

1. **Fyzická vrstva** – angl. physical layer. Fyzická vrstva popisuje všechny elektrické a fyzikální vlastnosti zařízení. Jejím účelem je vytvoření, udržení a ukončení fyzického spoje mezi dvěma nebo více systémy. Na této vrstvě se řeší přizpůsobení vysílaného signálu přenosovému médiu (kódování, modulace, multiplexace), standardizace rozhraní, parametry používaných médií, specifikace konektorů apod.
2. **Spojová (linková) vrstva** – angl. data link layer. Poskytuje spojení mezi dvěma sousedními systémy. Uspořádává data z fyzické vrstvy do logických celků, které se označují jako rámce (angl. frame). Tyto rámce jsou opatřeny zdrojovou a cílovou fyzickou adresou, známou jako MAC adresa (Media Access Control). Tuto adresu má každé zařízení na světě unikátní a je dána výrobcem daného zařízení.

3. **Síťová vrstva** – angl. network layer. Stará se o směrování v síti a o logické síťové adresování. Poskytuje spojení mezi systémy, které spolu přímo nesousedí a zajišťuje přenos dat různé délky od zdroje k příjemci skrze jednu nebo více vzájemně propojených sítí. Pro jednoznačné označení jednotlivých sítí a zařízení v nich se používají IP adresy. Logické celky dat přenášené na této vrstvě se označují jako pakety (angl. packet). Tato vrstva se primárně snaží najít nejvýhodnější cestu mezi koncovými body, avšak nezaručuje, že přenášená data dorazí v pořádku a nezměněna. Typickým protokolem pracujícím na této vrstvě je IP protokol.

4. **Transportní vrstva** – angl. transport layer. Účelem této vrstvy je zajistit přenos dat mezi koncovými uzly v požadované kvalitě. Na této vrstvě pracují dva ze základních protokolů na dnešních počítačových sítích: TCP – spojově orientovaný a UDP – nespojově orientovaný. Datové celky na této vrstvě se pak označují jako segmenty (angl. segment).

5. **Relační vrstva** – angl. session layer. Cílem této vrstvy je v podstatě organizovat a synchronizovat dialog s relačním vrstvou vzdáleného systému. Má za úkol sestavit, udržet a případně ukončit relaci, v níž jsou data posílána. Umožňuje také obnovení ztraceného spojení a oznamování výjimečných stavů. Velmi důležitým pojmem souvisejícím s touto vrstvou je port. Vzhledem k tomu, že jedno zařízení může v tentýž okamžik vést mnoho relací, je potřeba tyto jednotlivé komunikace nějakým způsobem odlišit. Právě k tomuto účelu existují porty.

6. **Prezentační vrstva** – angl. pressentaion layer. Tato vrstva má za úkol upravit data do podoby vhodné pro použití libovolnou aplikací. Mezi nejdůležitější funkce této vrstvy patří komprimace dat nebo šifrování. Vrstva se především zabývá strukturou dat, nikoliv jejich významem.

7. **Aplikační vrstva** – angl. application layer. Vrstva, se kterou interaguje uživatel. Jejím hlavním účelem tak je získávat od uživatele data a naopak uživateli data zobrazovat či jinak prezentovat.

1.2.2 Referenční model TCP/IP

Jelikož RM OSI je pro praktické využití mnohdy příliš složitý, často se využívá také modelu TCP/IP. Tento model je odvozen od protokolové sady TCP/IP, která je základem celosvětové počítačové sítě – Internetu. Oproti modelu OSI se skládá pouze ze 4 vrstev. Aplikační, prezentační a relační vrstva OSI modelu je zde sloučena do jedné – aplikační vrstvy. Podobně vrstva spojová a fyzická jsou sloučeny do vrstvy spojové.

1.3 Protokoly

Síťový protokol je sada pravidel či standardů, podle které se řídí komunikace mezi dvěma nebo více zařízeními v síti. Jedná se o jeden z nezbytných předpokladů pro uskutečnění komunikace jako takové. Tato pravidla definují syntaxi, sémantiku a synchronizaci komunikace. Zjednodušeně se dá říct, že protokol určuje, kdy která strana vysílá a přijímá, jakou strukturu musí přenášená zpráva mít a jaký je její význam. Tyto standardy umožňují, aby si různá zařízení od různých výrobců v síti „rozuměla“. Vzhledem k velkému množství typů komunikace v počítačové síti není možné ani výhodné, aby každý typ popisoval jen jeden protokol. Proto existuje celá řada protokolů, které navzájem spolupracují a řídí komunikaci většinou v rámci jedné vrstvy RM OSI či TCP/IP.

1.3.1 Ethernet

Tento protokol byl komerčně představen v roce 1980 a roku 1983 byl standardizován jako IEEE 802.3. Postupem času nahradil konkurenční protokoly a stal se de facto jediným protokolem spojové (druhé) vrstvy ISO modelu v lokálních sítích (LAN). Zařazení tohoto protokolu do druhé vrstvy (L2) však může být poněkud zavádějící, neboť tento protokol popisuje i parametry spadající do první, fyzické vrstvy (L1). Ve svých počátcích využíval jako sdíleného média koaxiálních kabelů, dnes se však používají kabely s kroucenou dvoulinkou či optické kabely.

Systémy komunikující po Ethernetu rozdělují přenášená data do menších celků, označovaných jako rámce. Velikost takového rámce je standardně 64 - 1518 bytů. Každý rámec obsahuje zdrojovou a cílovou MAC adresu, značku dle standardu 802.1Q (tzv. 802.1Q tag), označení typu rámce, přenášená data a kontrolní součet.

1.3.2 IP protokol

IP neboli Internet Protocol, je protokolem pracujícím na síťové vrstvě OSI modelu (L3). Jeho hlavním účelem je směrování, tedy určit jakým způsobem budou data přenášena za hranicemi lokální sítě. Byl představen roku 1974 a v současnosti existuje ve dvou verzích, IP verze 4 (IPv4) a verze 6 (IPv6).

S IP protokolem úzce souvisí pojem IP adresa. Jedná se o logickou numerickou značku přiřazenou každému zařízení v síti. IP adresa verze 4 se skládá ze čtyř oktetů, tedy 32 bitů a nejčastěji se zapisuje v decimálním tvaru, např. 192.168.1.1. Teoreticky nám tento adresní prostor poskytuje 2^{32}, tedy 4 294 967 296 adres, přičemž některé dílčí rozsahy jsou vyhrazeny pro konkrétní účely. Tento rozsah se při návrhu IPv4 protokolu jevil jako naprosto dostačující, avšak s ohromným rozmachem internetu se ukázalo, že tomu tak není. Z tohoto důvodu byl vyvinut protokol IPv6, v němž mají adresy 128 bitů namísto 32. To poskytuje adresní prostor 2^{128}, tedy přibližně $3,4{*}10^{38}$ adres. Ačkoliv se předpokládalo, že přechod na IPv6 se bude v roce 2008 blížit do finální fáze, většina výrobců zařízení a poskytovatelů internetu s její implementací teprve začínala.

Datové celky na L3 se označují jako pakety. Každý paket se skládá z hlavičky a přenášených dat. Hlavička pak obsahuje především zdrojovou a cílovou IP adresu spolu s mnoha dalšími identifikátory daného paketu. Na základě informací obsažených v hlavičce jsou pakety přenášeny do cílového uzlu metodou best-effort, tedy nejlepší snahou. Protokol IP není schopen zaručit, že vyslaná zpráva dorazí na místo určení.

1.3.3 TCP/IP protokol

Transmission Control Protocol byl představen spolu s protokolem IP. Na rozdíl od IP je tento protokol spojově orientovaný a jeho hlavním posláním je zaručit, že vyslaná data dorazí do cílového uzlu a ve správném pořadí. Jedná se o protokol transportní vrstvy (L4) a velmi úzce spolupracuje s protokolem IP. O těchto dvou protokolech se proto často mluví jako o protokolové sadě TCP/IP (angl. TCP/IP suite). TCP umožňuje dvěma zařízením vytvořit mezi sebou spojení, ve kterém je možné obousměrně posílat data. V případě, že se některá data cestou ztratí nebo poškodí, tento protokol zajistí jejich opakované vyslání. Díky TCP je také možné rozeznat mezi sebou jednotlivé typy komunikace prostřednictvím zdrojových a cílových portů. Datové celky přenášené na této vrstvě označujeme jako segmenty. Hlavička každého segmentu obsahuje mimo jiné číslo sekvence, které určuje, v jakém pořadí byly segmenty vyslány. V paketově orientované síti se totiž může stát, že vyslaný segment může do cílového uzlu dorazit dříve, než předchozí vyslaný segment.

1.4 Síťové prvky

Síťové prvky jsou fyzická zařízení, jejichž primárním účelem je přenos dat mezi koncovými uzly. Mezi tato zařízení patří zejména: směrovače, přepínače, rozbočovače, síťové mosty, modemy, bezdrátové přístupové body, firewally a další.

Způsob, jakým jsou tato zařízení v síti propojena, označujeme jako síťovou topologii. Topologii můžeme rozdělit na fyzickou a logickou, přičemž fyzická topologie popisuje, jak jsou zařízení mezi sebou fyzicky propojena, laicky řečeno odkud a kam vedou kabely. Naproti tomu logická topologie určuje, kudy mohou být v síti přenášena data. Právě rozdělením fyzické a logické topologie sítě můžeme docílit vyšší robustnosti a odolnosti sítě. Dojde-li například k poruše na jednom zařízení nebo k poškození kabelu, můžeme změnit logickou topologii sítě a zaručit tak, že se data i navzdory poruše dostanou do cílového uzlu. Tuto změnu přitom nemusí vykonat administrátor sítě ručně, protože mnohá zařízení jsou schopna za pomoci speciálních protokolů měnit logickou topologii automaticky dle potřeby. Jádro dnešních sítí tvoří zejména přepínače a směrovače.

1.4.1 Přepínač (Switch)

Přepínač neboli switche, je síťově zařízení pracující na L2, tedy spojové vrstvě. Jedná se většinou o zařízení s více porty, kdy je ke každému portu připojeno koncové zařízení. Úkolem switche je pak předávat příchozí ethernetové rámce na příslušný port podle cílové MAC adresy. Switch si vede tabulku, ve které přiřazuje adresy zařízení připojených ke konkrétním portům.

Přepínače nahradili v sítích dnes již zastaralé rozbočovače neboli Huby. Ty se od switchů lišily především v tom, že si nevedly tabulku adres připojených zařízení, ale pouze rozesílaly příchozí rámce na všechny porty s výjimkou příchozího. To velmi zvyšovalo provoz v síti. Představme si, že máme 10 osobních počítačů připojených prostřednictvím rozbočovače. Bude-li chtít počítač č. 1 komunikovat s počítačem č. 2, veškerá jejich komunikace v obou směrech bude zároveň odesílána na počítače č. 3-č. 10. Ty pak tato data v lepším případě zahodí, protože jim nejsou určena, v horším případě to umožňuje potenciálnímu útočníkovi odposlouchávat tuto komunikaci.

Toto „zbytečné“ kopírování dat navíc velmi negativně ovlivňuje propustnost sítě. Všechny koncové stanice propojené pomocí hubu tvoří tzv. kolizní doménu. Pokud chce daná stanice vysílat na sdíleném médiu, musí nejdříve naslouchat, je-li médium volné – tedy zda na něm právě nevysílá jiná stanice. V důsledku konečné rychlosti šíření elektromagnetické vlny v médiu však může nastat situace, že stanice začne vysílat krátký okamžik po tom, co začala vysílat jiná stanice a dojde tak ke kolizi. O vzniku této kolize jsou stanice informovány speciálním signálem, po kterém počkají náhodnou dobu, než začnou znovu vysílat. Oproti tomu v sítích, které používají switche, tvoří kolizní doménu vždy jeden port switche a zařízení k němu připojené. Tato metoda se označuje jako mikrosegmentace a zabraňuje vzniku kolizí. Moderní switche navíc podporují řadu pokročilých funkcí, jako je tvorba virtuálních lokálních sítí (VLAN – Virtual LAN), prioritizaci daného typu provozu a v neposlední řadě umožňují zabránit neoprávněným uživatelům v připojení do sítě.

1.4.2 Směrovač (Router)

Směrovač je síťové zařízení, jehož úkolem je směrovat provoz mezi vícero sítěmi. Oproti přepínači pracuje pouze s IP adresami, jedná se tedy o L3 zařízení. Router se většinou nachází na okraji lokální sítě a zpracovává data, která jsou určena k odeslání mimo lokální síť, nebo naopak do ní.

Router bývá na odchozí straně připojen k jednomu nebo více dalším routerům. Zde je důležité zmínit, že každý port routeru má vlastní IP adresu a porty sousedních routerů, kterými jsou propojeny, se musí nacházet ve stejné podsíti neboli subnetu.

IP adresu můžeme rozdělit na část síťovou a hostovskou. Všechny stanice (angl. hosts) v rámci jedné sítě mají společnou síťovou část IP adresy. Aby bylo možné určit, kde je hranice mezi těmito dvěma částmi adresy, používá se síťová maska (angl. network mask). Ta je stejně jako IP adresa tvořena čtyřmi oktety, tedy 32 bity. Provedením bitové operace AND mezi IP adresou a síťovou maskou dostaneme adresu sítě:

IP adresa 192.168.1.100: 1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 1 1 0 0 1 0 0 Síťová maska 255.255.255.0: 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0 Adresa sítě 192.168.1.0: 1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 0 0 0 0 0

Právě na základě síťové adresy router rozhodne, kam daný paket vyslat. Spadá-li cílová adresa paketu do definovaného adresního rozsahu, je paket odeslán na odpovídající další zařízení. V případě, že router nemá konkrétně definovaný rozsah, do kterého daná adresa spadá, využije výchozího záznamu, který se označuje jako výchozí brána. Tento proces se nazývá směrování a údaje podle kterých se router rozhoduje jsou obsaženy ve směrovací tabulce. Ta může být nastavená staticky administrátorem sítě, nebo dynamicky pomocí směrovacích protokolů jako je RIP, OSPF, IGRP, BGP či další.

Reference

[1] Ansible Docs. Developing modules. http://docs.ansible.com/ansible/developing_modules.html, 2016. [Online].

[2] Ansible Docs. Intro to playbooks. http://docs.ansible.com/ansible/playbooks_intro.html, 2016. [Online].

[3] Ansible Docs. Introduction to ad-hoc commands. http://docs.ansible.com/ansible/intro_adhoc.html, 2016. [Online].

[4] Lorin Hochstein. *Ansible: Up and Running*. O'Reilly Media, Inc., May 2015.

[5] MikroTik Wiki. Manual:api - mikrotik wiki. http://wiki.mikrotik.com/wiki/Manual:API. [Online].

[6] MikroTik Wiki. Manual:winbox - mikrotik wiki. http://wiki.mikrotik.com/wiki/Manual:Winbox. [Online].

[7] Wikipedia. Api — wikipedia, the free encyclopedia. https://cs.wikipedia.org/wiki/API, 2016. [Online].