Implementace vysoké dostupnosti služeb počítačové sítě

Bc. Filip Miškařík

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Filip Miškařík**
Osobní číslo:	**A19794**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**Kombinovaná**
Téma práce:	**Implementace vysoké dostupnosti služeb počítačové sítě**
Téma práce anglicky:	**Implementing High Availability Network Services**

Zásady pro vypracování

1. Prostudujte moderní metody a systémy pro implementaci vysoké dostupnosti základních služeb a protokolů počítačových sítí.
2. Zaměřte se na služby DHCP, DNS, autentizace a autorizace uživatelů a VLAN.
3. Uvažujte rozlehlou počítačovou síť s desítkami až stovkami směrovačů a přepínačů, s existencí více možných cest mezi uzly.
4. Implementujte směrování pomocí dynamických směrovacích protokolů. Redundanci kritických prvků zabezpečte pomocí VRRP.
5. Výslednou implementaci otestujte záměrnými výpadky prvků v reálném provozu.

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

Seznam doporučené literatury:

1. BEIJNUM, Iljitsch van. BGP: Building Reliable Networks with the Border Gateway Protocol. 1st edition. B.m.: O’Reilly Media, 2002.
2. LIU, Cricket a Paul ALBITZ. DNS and BIND. Fifth edition. Sebastopol, CA: O’Reilly Media, 2006. ISBN 978-0-596-10057-5.
3. MOY, John. OSPF: Anatomy of an Internet Routing Protocol. 1st edition. Reading, Mass: Addison-Wesley Professional, 1998. ISBN 978-0-201-63472-3.
4. DROMS, Ralph a Ted LEMON. The Dhcp Handbook. Subsequent edition. Indianapolis, Ind: Sams, 2002. ISBN 978-0-672-32327-0.
5. SRIKANTH, Ayikudy a Adnan Adam ONART. VRRP: Increasing Reliability and Failover with the Virtual Router Redundancy Protocol. 1st edition. Boston: Pearson Education, 2002. ISBN 978-0-201-71500-2.

Vedoucí diplomové práce: **Ing. Tomáš Dulík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **15. ledna 2021**
Termín odevzdání diplomové práce: **17. května 2021**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

prof. Mgr. Roman Jašek, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 17. 5. 2021 Bc. Filip Miškařík, v. r.

ABSTRAKT

Tato diplomová práce se zabývá implementací vysoké dostupnosti služeb počítačové sítě. Teoretická část práce popisuje principy internetu, směrování a směrovacích protokolů používaných pro zajištění vysoké dostupnosti sítě. Praktická část popisuje způsob realizace redundance klíčových síťových prvků v konkrétní telekomunikační síti. Zabývá se také možnostmi zabezpečení sítě a omezení přístupu uživatelů. Součástí jsou ukázky konfiguračních souborů jednotlivých služeb a protokolů.

Klíčová slova: internet, dynamické směrování, DHCP, DNS, VRRP

ABSTRACT

This diploma thesis deals with the implementation of high availability of computer network services. The theoretical part describes the principles of the Internet, routing and routing protocols used to implement high availability of computer networks. The practical part describes how to implement redundancy of key network elements in a particular telecommunications network. It also discusses implementation of some network security aspects. Samples of configuration files of individual services and protocols are included.

Keywords: internet, dynamic routing, DHCP, DNS, VRRP

Za odborné vedení chci poděkovat svému vedoucímu práce Ing. Tomáši Dulíkovi PhD., svému kolegovi Michalu Klimentovi a kolegům ze sdružení UnArt a NFX, z.s.p.o. za umožnění vypracování práce. Také bych zde chtěl poděkovat své rodině a přítelkyni Martině Šimoníkové DiS. za podporu ve studiu a při vypracování této práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Tématem diplomové práce je implementace vysoké dostupnosti služeb počítačové sítě. Téma bylo zvoleno za účelem průzkumu a následné implementace moderních metod a systémů zajišťující služby počítačových sítí. Pojem vysoká dostupnost se ve výpočetní technice používá pro označení časového období, kdy je služba k dispozici. Označovat může také čas, za který systém reagoval na požadavek. Vysokou dostupnost datové sítě v této diplomové práci budeme řešit pro zajištění co nejlepší kvality internetového připojení pro koncového uživatele dané sítě.

Teoretická část práce je věnována popisu jednotlivých služeb pro realizaci telekomunikační sítě v rámci organizací nebo firem, které poskytují svým uživatelům připojení k Internetu. V úvodu teoretické časti je čtenář seznámen s problematikou internetu, jak funguje směrování, a s existencí síťových protokolů. Síťové protokoly jsou rozebrány a rozděleny do skupin: statické a dynamické. Cílem práce je implementovat dynamické směrování, proto je větší míra pozornosti věnována protokolům dynamického směrování. Další kapitoly teoretické části se věnují službám pro přidělování IP adres a pro překládání doménových jmen. Zmiňuji se zde o protokolu OSPF a BGP pro realizaci dynamického směrování a část práce je také věnována autorizaci a autentizaci uživatelů. Cílem je též popsat služby implementující redundanci klíčových prvků sítě pro zajištění minimálních výpadků sítě při nedostupnosti jednoho zařízení. Tento problém nazývá single point of failure – neboli kritické místo výpadku.

Praktická část práce se věnuje popisu sítě sdružení UnArt, z.s. a NFX, z.s.p.o. Popisuje architektonická řešení sítí s velkým množstvím zařízení. Věnuje se možnostem nasazení služeb DHCP, DNS a VRRP. Dynamické směrování je v síti řešeno prostřednictvím protokolu OSPF pro směrování uvnitř sítě a pro vnější síť je použit protokol BGP (pro připojení do sítě Internetu).

I. TEORETICKÁ ČÁST

1 INTERNET

Internet je síť mezi sebou propojených počítačů, směrovačů, přepínačů, satelitů, kamer, telefonů a mnoha dalších zařízení. Internet umožňuje zařízením mezi sebou komunikovat. Zařízení jsou shlukována do sítí provozovaných různými organizacemi, vládami, univerzitami. Taková infrastruktura nám každý den usnadňuje život. Můžeme díky internetu nakupovat, volat, sdílet svůj život díky sociálním sítím, sledovat přímé přenosy z celého světa, získávat informace o čemkoliv jen chceme. [7]

1.1 Pakety

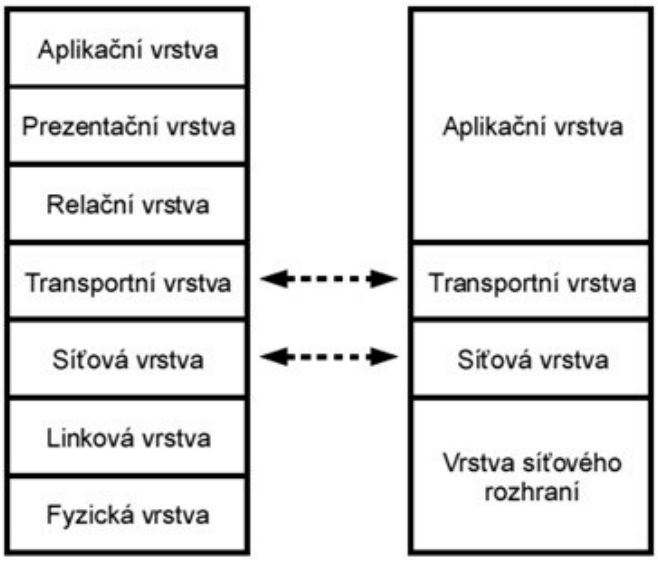
Internetem jsou různě směrovány pakety. Paket je malá část dlouhé zprávy [4]. Pakety slouží k veškeré internetové komunikaci. Díky paketům si můžeme prohlížet internetové stránky, sledovat videa, kontrolovat stav bankovního účtu, pracovat na vzdálených počítačích, a mnoho dalších služeb, jež internet poskytuje. [5]

Již víme, že paket představuje pouze část zprávy. Jelikož každá zpráva je jinak dlouhá, jsou zprávy rozdělovány na části a ty jsou pak transportovány sítí. To znamená, že u odesílatele jsou zprávy rozděleny na pakety a u příjemce opět sestaveny do původní zprávy. [4] Paket může obsahovat informace pro kontrolu chyb, které se využívají při zpětném sestavování zpráv. Pakety můžou mít různé velikosti a struktury v závislosti na základní síťové architektuře. [5]

1.2 Síťové architektury

Rozlišujeme dvě základní architektury: Referenční model ISO/OSI a rodinu protokolů TCP/IP. ISO/OSI není v praxi nasazen a slouží jako model pro demonstrování funkcí sítě. V praxi je nasazen model TCP/IP. Obrázek 1 srovnává přístupy k internetu těchto dvou architektur. Vlevo je znázorněn pohled dle referenčního modelu ISO/OSI, vpravo pak podle modelu TCP/IP. [8]

Model ISO/OSI uvažuje 7 vrstev, kdežto TCP/IP 4 vrstvy. Spodní vrstva modelu TCP/IP, vrstva síťového rozhraní, zahrnuje dvě spodní vrstvy modelu ISO/OSI, a to fyzickou a síťovou vrstvu. Další dvě vrstvy jsou v obou modelech pojaty stejně. Do horní vrstvy modelu TPC/IP jsou zahrnuty vrstvy relační, prezentační a aplikační z modelu ISO/OSI. Funkce jednotlivých vrstev jsou v obou modelech ve velké míře podobné. [9]



Obrázek 1: ISO/OSI vs. TCP/IP [9]

1.3 Směrovače

Aby paket dorazil na správné místo určení a zároveň tím nejvýhodnějším směrem, jsou v síti umístěny směrovače (routery). Routery představují rozhodovací prvky určující trasy paketů. Algoritmy (protokoly), které routery mezi sebou spouští, mají za úkol učit routery k tomu, aby učinily ta správná rozhodnutí a trasy paketů tak byly nejoptimálnější. [5]

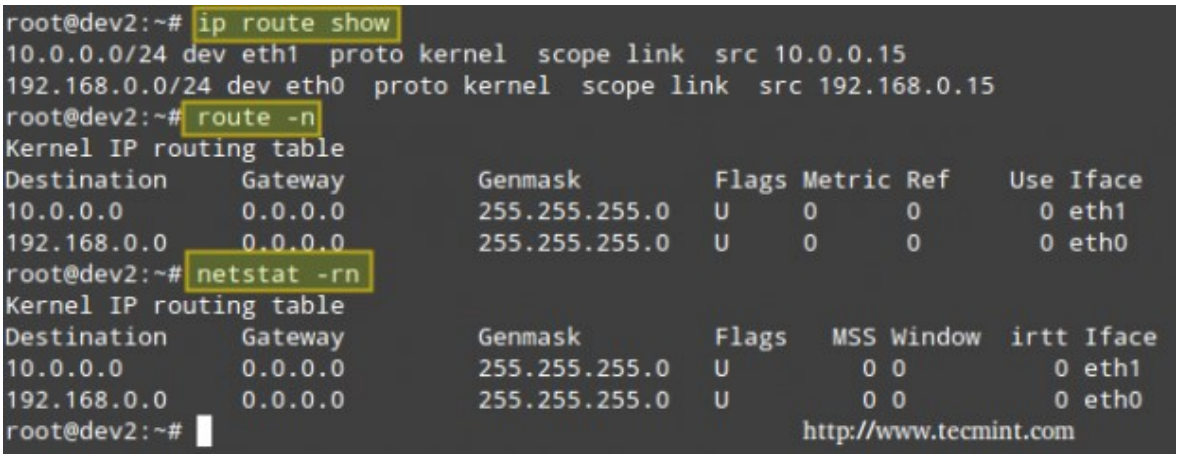
Směrovače jsou optimalizovány pro oblast jejich použití. Směrovač umístěn na páteřním bodu sítě bude mnohem výkonnější (předávají pakety rychlostí několika gigabitů za sekundu), než směrovač umístěn v bodu koncovém. Propojení jednotlivých sítí k sítím jiných poskytovatelů je řešeno většinou hraničními směrovači používající směrovací protokol BGP. Hraniční směrovače jsou též využívány pro stanovení priorit provozu pomocí Quality of Service (QoS). [6]

1.3.1 Směrovací tabulky

Směrovací protokoly TCP/IP zjišťují dosažitelné prefixy (předpony) IP adres a pro každou předponu určují next-hop (následující) směrovač. Jak se mění síť, linky postupně zanikají a vznikají nové, musí směrovací protokoly neustále přehodnocovat dosažitelnost prefixu IP adresy. Proces hledání nového následujícího směrovače se nazývá konvergence. Většinou je preferencí používat takové směrovací protokoly, které mají dobu konvergence nejkratší.

Každý směrovací protokol však bojuje s velikostí sítě. Ta totiž dobu konvergence prodlužuje. Směrovací protokoly ukládají výsledky své práce do tzv. směrovací tabulky.

Směrovací tabulka směrovači udává, kam dál předávat pakety. Pro každý paket je prohledána směrovací tabulka, kdy je cílová IP adresa paketu použita jako vyhledávací klíč. Směrovací tabulka vrátí IP adresu následujícího směrovače, kam má být paket odeslán.



Obrázek 2: Směrovací tabulka [10]

Obrázek 2 ukazuje příklady směrovací tabulky. Tato konkrétně pochází z linuxového prostředí. Obrázek ukazuje několik variant výpisu podle použitého příkazu terminálu. Ve všech třech variantách výpisu je v prvním sloupci zobrazena cílová síť. Podle tohoto parametru se porovnává cílová IP adresa paketu, jak je již výše zmíněno. [10]

1.4 Směrování

Směrování slouží k učení směrovačů správně se rozhodovat. Směrovací protokol je sada definovaných pravidel používaných směrovačem ke komunikaci mezi zdrojem a cílem. Není jejich úkolem dopravovat informace od zdroje k cíli, avšak pouze aktualizovat směrovací tabulku. Určují způsob vzájemné komunikace dvou směrovačů. Směrování umožňuje síti vybrat trasy mezi libovolnými dvěma body počítačové sítě. [11]

Rozlišujeme dva základní druhy směrovaní: statické a dynamické.

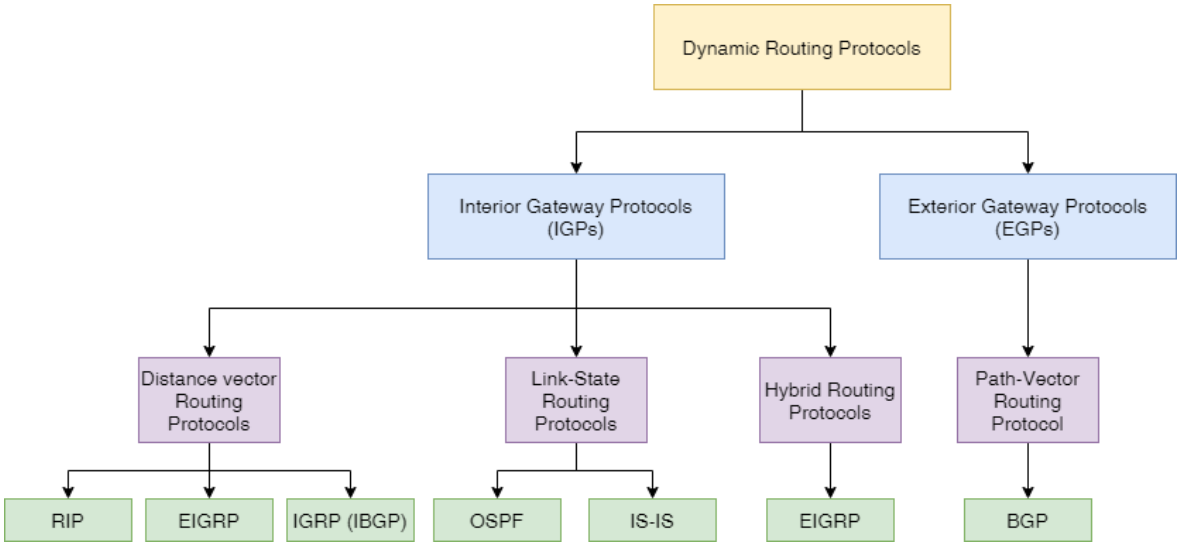
1.4.1 Statické směrování

Statické směrování je neadaptivní směrování, které nemění směrovací tabulku. Pouze správce sítě může ručně změnit směrovací tabulku zařízení. [20] Pro statické směrování lze použít levnější směrovače, jelikož není potřeba mít výkonný procesor pro zpracování směrování. Statické směrování je bezpečnější, protože pouze správce sítě může povolit

směrování do konkrétních sítí. Na druhé straně je pak náročné ručně vytvořit a následně udržovat směrovací tabulku pro velkou síť čili každému směrovači v síti. Náročné je i předávání sítě novému správci, jelikož musí získat dokonalý přehled o síti, aby byl schopen přidat záznam do směrovací tabulky. Statické směrování nijak nekomunikuje mezi sousedními směrovači, nevyžaduje proto žádnou přenosovou kapacitu ani spolehlivost linek mezi směrovači. [21]

1.4.2 Dynamické směrování

Dynamické směrování je síťová technika, při které je poskytováno optimální směrování dat. Při použití dynamického směrování je směrovačům umožněno vybrat cesty podle změn rozložení sítě v reálním čase. Další výhodou dynamického směrování je výměna informací o změně topologie sítě. Směrovačům je umožněno mezi sebou komunikovat a vyměňovat si informace o těchto změnách. S tím souvisí i menší administrativní režie a lepší škálovatelnost sítě. [13]



Obrázek 3: Dělení dynamických směrovacích protokolů [12] [73]

Dynamické směrování používá několik směrovacích protokolů. Každý k tomuto úkolu přistupuje jinak. Obrázek 3 je schématem rozdělení dynamických směrovacích protokolů podle techniky. Je potřeba si definovat pojem autonomní systém, zkráceně AS. Lze jej definovat jako skupinu sítí, které jsou řízeny jedinou administrativní entitou. Takovou entitou může být místní poskytovatel služeb, mezinárodní podnik, univerzita a další podobné instituce. Pro směrování uvnitř AS se použijí protokoly vnitřní (Interior Gateway Protocols), a pro výměnu informací mezi dvěma AS se použijí protokoly vnější (Exterior Gateway Protocols), viz Obrázek 3 druhý řádek. To je základní rozdělení dynamických směrovacích protokolů. [12]

Interní směrovací protokoly tedy řeší politiku směrování paketu uvnitř autonomního systému. Dále se dělí na protokoly Distance Vector a Link State.

Distance Vector protokoly zakládají svá rozhodnutí na nejlepší cestě k danému cíli na základě vzdálenosti. Vzdálenost se obvykle měří jako počet přeskoků – „hopů“, tj. počet směrovačů, kterými paket projde na cestě od zdroje k cíli. Trasa, která do cíle čítá nejméně hopů, je považována za nejlepší cestu. Metrikou pro výpočet vzdálenosti mezi prvky ale může být i jiný parametr, např. zpoždění, ztracené pakety atd. [14]

Algoritmus protokolů Distance Vector je známý jako starý směrovací algoritmus ARPANET, též jako Bellman-Fordův algoritmus. Princip spočívá v tom, že směrovač přenáší svůj vektor vzdálenosti každému ze svých přímo připojených sousedů. Každý soused si ukládá poslední přijatý vektor od svého souseda. K přepočtu vektoru vzdálenosti dochází když:

- směrovač přijme od souseda jiné informace, než měl doposud,
- došlo k přerušení spojení se sousedem. [17]

Mezi protokoly, které jsou zástupci Vector distance přístupu, patří RIP a IGRP (podrobněji budou rozebrány v následujících kapitolách). [14]

Link State protokoly, také známe pod názvem Shortest-Path-First protokoly (protokoly nejkratší cesty), mají úplný obrázek topologie sítě. Proto znají celou síť lépe než distance vector protokoly. Na každém směrovači s povoleným Link State směrováním jsou vytvořeny tři samostatné tabulky. Jedna tabulka slouží k uchovávání informací o přímo připojených sousedech. Další tabulka uchovává topologii všech připojených sítí a poslední tabulka je skutečná směrovací tabulka. Protokoly Link State odesílají informace o přímo připojených linkách na všechny směrovače v síti. [14] Výměny informací mezi jednotlivými prvky jsou nazvané Link State Advertisement – LSA. [15]

Výpočet nejkratší cesty probíhá následujícím způsobem. Chceme-li nalézt nejkratší cestu mezi prvky, musí každý uzel spustit Dijkstrův algoritmus. Tento algoritmus prochází následující kroky.

1. Zvolí se uzel, který je poté považován za kořenový uzel stromu. Vytvoří se strom s jediným uzlem a stanoví se celková cena každého uzlu na určitou hodnotu na základě informací z Link State databáze spojení.

2. Dále je vybrán jeden uzel z uzlů, které nejsou ve stromové struktuře, a který je nejblíž kořenu stromu a přidá se do struktury stromu. Tím se tvar stromu změní.
3. Po přidání dalšího uzlu do stromu je potřeba aktualizovat náklady na všechny uzly, které zatím nejsou součástí stromu, jelikož se mohly změnit jejich cesty.
4. Opakují se kroky 2 a 3 dokud nejsou do stromu zařazeny všechny uzly. [16]

Mezi příklady směrovacích protokolů Link State můžeme zařadit OSPF (Open Shortest Path First) a IS-IS (Intermediate System to Intermediate System – směrovací protokol, který určuje v síti nejkratší cestu pro paket). Existují i protokoly, které jsou v tomto směru považovány za hybridní. To znamená, že využívají vlastností obou přístupů dynamického vnitřního směrování. Za takový protokol bývá v některých zdrojích označen EIGRP (Enhanced Interior Gateway Routing Protocol). [14]

Pro přehledné srovnání obou přístupů je zpracována Tabulka 1.

Distance Vector	**Link State**
požadovaná šířka pásma je menší, kvůli lokálnímu sdílení, malých paketech a žádnému zaplavování sítě pakety	požadovaná šířka pásma je větší, kvůli zaplavování sítě pakety a posílání velkých link state paketů
lokální znalost sítě na základě informací získaných od sousedů	znalost celé sítě
Belmann-Fordův algoritmus	Dijkstrův algoritmus
méně provozu	více provozu
pomaleji konverguje – dobré zprávy se šíří rychle, špatné pomalu	rychleji konverguje
vzniká problém počítaní do nekonečna	nevzniká problém počítání do nekonečna [93]
problém se vznikajícími smyčkami – budou zde pořád	pouze přechodné smyčky
RIP, IGRP	OSPF, IS-IS

Tabulka 1: Porovnání přístupů k vnitřnímu dynamickému směrování [17]

Druhou skupinou protokolů podřazenou dynamickému směrování jsou protokoly externí – EGPs (Exterior Gateway Protocols). Externí neboli vnější směrovací protokoly[1] se používají pro výměnu informací mezi autonomními systémy. Informace předané mezi autonomními systémy se nazývá informace o dosažitelnosti. Tyto informace dávají přehled o dosažitelnosti konkrétního autonomního systému. Nejčastěji je dnes za zástupce této skupiny označován protokol BGP (Border Gateway Protocol). Předchůdcem BGP byl EGP, který byl definován 80. letech minulého století. [18][19]

Dva autonomní systémy, které spolu chtějí komunikovat, musí používat stejný vnější směrovací protokol. Proto je správce sítě většinou při výběru omezen na použití protokolu, který používá druhá strana. Jak je již výše zmíněno, dnes se nejčastěji používá protokol BGP. [19]

Schéma obrázku č. 3 zařazuje protokol BGP do skupiny Path Vector směrovacích protokolů. Path Vector protokoly nespoléhají na náklady na dosažení daného cíle pro zjištění, zdali je cesta dostupná bez smyčky nebo ne. Místo toho se protokoly Path Vector spoléhají na analýzu cesty k dosažení cíle, aby se určilo, jestli je cesta dostupná bez smyčky či nikoliv. Path Vector protokoly zaručují cesty bez smyček tím, že zaznamenají každý přeskok směrovací informace (advertisement) když prochází sítí. Směrovače si postupně předávají informace, že mají dostupnou linku do dané sítě. Pokud se pokusí jeden ze směrovačů předat dalšímu směrovači informaci o tom, že zná cestu do dané sítě, ale ten již cestu do dané sítě zná, zamítne přijetí této informace do své směrovací tabulky. Tím se zabrání vzniku smyčky v síti. [22]

1.5 VLAN

Virtual Local Area Network je síť vytvořena z jedné nebo více lokálních (místních) sítí. Umožňuje sloučit skupinu zařízení z více lokálních sítí do jedné logické sítě. Vznikne virtuální LAN, která je spravována stejně jako fyzická síť. VLAN se staly důležité, jelikož složitost sítě začala překračovat kapacitu typických místních sítí LAN. [49] LAN původně připojovala skupinu místních počítačů a přidružených zařízení k serveru pomocí fyzických kabelů. Připojení nemusí být řešeno pouze pomocí kabelu (Ethernet), ale i bezdrátově. Kombinací obou připojení je řešena většina sítí. V průběhu času společnosti rostly, zvyšovaly se nároky a byla potřeba lepší flexibility a škálovatelnost. VLAN obcházejí

[1] Někdy označovány jako protokoly vnější brány.

fyzická omezení LAN prostřednictvím své virtuální povahy, což přináší možnost snadnější škálovatelnosti a segmentování sítě pro zvýšení bezpečnostních opatření a snížení latence. Neznamená to však, že zařízení nebudou propojeny fyzicky vůbec. Fyzické propojení zůstává mezi jednotlivými prvky. Není však potřeba pro jinou síť na stejných prvcích realizovat další fyzické propojení. [50]

VLAN nejsou náročné na výkon zařízení, na kterých jsou realizovány. Je to dáno tím, že pro komunikaci mezi dvěma zařízeními ve VLAN postačuje přepínač, dokud není potřeba posílat data mimo danou VLAN. Umožňuje to pak síti VLAN spravovat zvýšené množství dat, protože přepínače mají sice méně funkcí než směrovače, ale podstatně i menší potřebný výpočetní výkon (směrovače v síti způsobují úzká hrdla). Jelikož VLAN nepotřebují předávat informace přes směrovač pro komunikaci s ostatními zařízeními v síti, je redukována latence sítě. VLAN lze konfigurovat a přiřadit na základě podmínek portu, protokolu či podsítě, což přináší flexibilitu při potřebě změnit návrh sítě. VLAN také umožňují být konfigurovány bez omezení na fyzické připojení, vzdálenost druhého zařízení. Mohou být vytvořeny pro pracovní skupiny nacházející se v různých patrech či budovách. [50]

VLAN jsou v síti označeny číslem – VLAN ID. Rozsah, ve kterém je možné VLAN ID přiřadit je 1–4094. Například na přepínači přiřadíme portu číslo VLAN. Přepínač pak umožňuje odesílat data mezi různými porty označenými stejným VLAN ID. Za určitých podmínek je možné ke každému portu přiřadit více VLAN ID a jedno VLAN ID může být přiřazeno více portům. Existují tři typy VLAN sítí. [50]

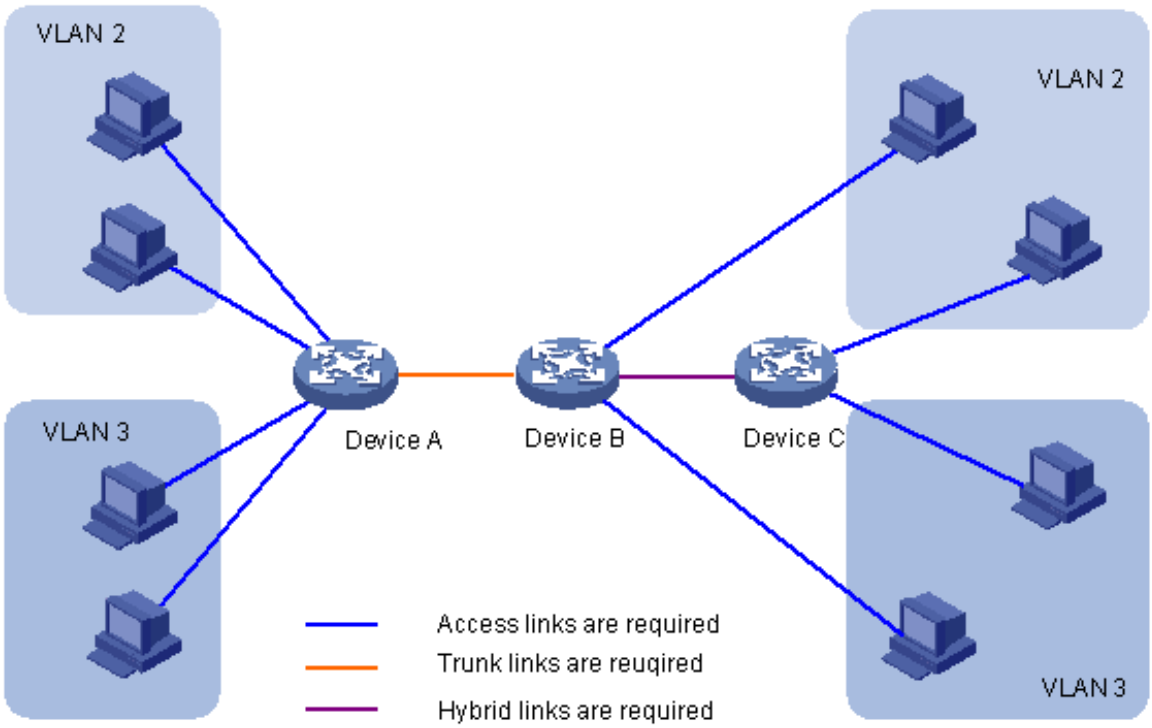
1.5.1 Port-Based VLAN

Prvním je Port-Based VLAN – na základě portu. Jak je již výše popsáno, k portu lze přiřadit číslo VLAN. Zařízení zapojená k tomuto portu budou patřit do stejné sítě, jak je VLAN nakonfigurována. Typ připojení může být typu Access, Trunk nebo Hybrid. Pokud je připojení portu typu Access, znamená to, že patří pouze jedné VLAN a odesílá provoz neoznačený (untagged). Takový port se většinou používá pro připojení koncového zařízení, které nedokáže identifikovat pakety označené VLAN, nebo se používají tehdy, když není potřeba oddělovat různé členy VLAN. [51]

Port typu Trunk nese více VLAN sítí. Realizuje jejich příjem a odesílání provozu. Provoz odeslán skrz trunk port se nazývá označený (tagged). Většinou jsou porty typu trunk mezi dvěma síťovými zařízeními typu přepínač, popř. směrovač. To lze vidět na obrázku č. 4 mezi

zařízeními Device A a Device B. Zde konkrétně musí port přenést provoz z VLAN 2 a VLAN 3. [51]

Hybridní port umožňuje provoz některých VLAN projít skrze sebe jako označený, jiným jako neoznačený. Hybridní porty se ve většině případů konfigurují tam, kde není jisté, jaký provoz bude podporován. Obrázek 4 ukazuje, že jsou porty mezi zařízeními Device B a Device C nakonfigurovány jako hybridní, aby provoz na zařízení Device C přicházel provoz neoznačený.[51]



Obrázek 4: Ukázková síť Port-Based VLAN [51]

1.5.2 Protocol-Based VLAN

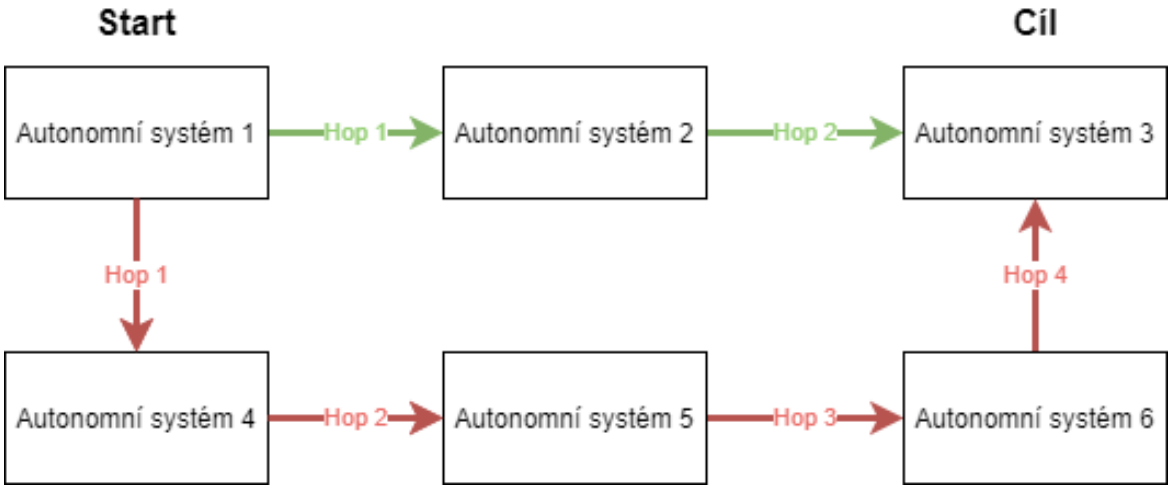
VLAN založená na protokolu přiřazuje příchozí pakety různým VLAN na základě jejich typů protokolů a formátu zapouzdření. Je to možné provádět pouze na hybrid portech, kde se zpracovávají neoznačené pakety. Přiřazují se dostupné typy síťových služeb k VLAN a usnadňují správu a údržbu sítě. VLAN založená na protokolu má jednu nebo více šablon protokolu. Šablona protokolu definuje typ protokolu a formát zapouzdření. Každá šablona má jedinečný index a všechny šablony ve VLAN mají stejné VLAN ID. [52]

1.5.3 MAC-Based VLAN

VLAN založená na MAC umožňuje příchozím neoznačeným paketům přidělit VLAN a tím klasifikovat provoz v závislosti na zdrojové adrese paketu. Mapování adresy MAC na VLAN je definováno konfigurací mapování položky do MAC na VLAN tabulky. Když na přepínač dorazí neoznačené pakety a v tabulce MAC na VLAN existují nějaké záznamy, vyhledá se zdrojová MAC adresa paketu. Pokud je nalezen záznam souhlasící se zdrojovou adresou paketu, je paketu přiřazeno odpovídající VLAN ID. Je-li paket již označen, pokračuje jeho zpracování ověřením přiřazeného VLAN ID podle tabulky. Pokud záznamy souhlasí, paket je postoupen dále přes přepínač. Pokud nesouhlasí, je zahozen. [53]

2 BGP

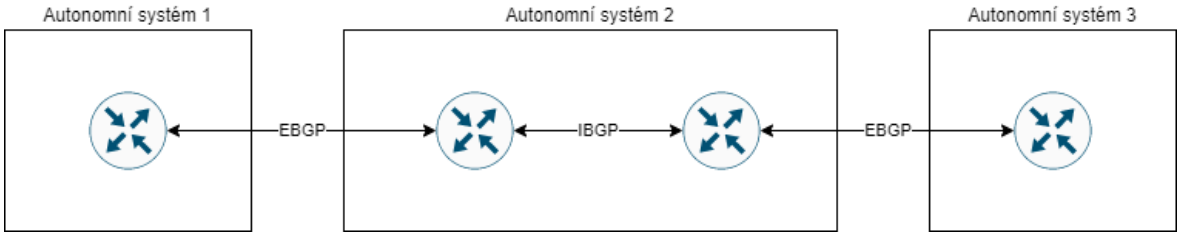
Border Gateway Protocol neboli BGP je protokol, díky kterému funguje internet. Border Gateway Protocol neboli BGP je standardizovaný protokol pro výměnu informací o směrování a dosažitelnosti mezi autonomními systémy. Autonomní systém reprezentuje množinu prefixů IP adres pod kontrolou určitého subjektu s jasně definovanou směrovací politikou. Celý internet je rozdělen na desítky tisíc autonomních systémů. [70]



Obrázek 5: Zjednodušené schéma BGP

Obrázek 5 zobrazuje jednoduché schéma výběru nejlepší cesty od odesílatele k cíli. Na obrázku je pro jednoduchost pouze pár autonomních systémů. V reálu se jedná o desítky tisíc autonomních systémů a struktura internetu se neustále mění. Vznikají nové trasy, routery nebo autonomní systémy, jiné zanikají. Z tohoto důvodu musí být autonomní systém informován o nových a zrušených trasách. To je realizováno pomocí TPC/IP připojení mezi sousedními systémy za účelem sdílení informací o směrování. Je zde však problém, že autonomní systémy nejsou strukturálně stejné. Navíc se nemusí jeden systém chovat přátelsky vůči druhému systému. Je to dáno tím, že na trhu tyto autonomní systémy proti sobě vystupují jako konkurenti. Autonomní systémy totiž většinou provozují ISP nebo jiné organizace, ke kterým patří univerzity, vládní agentury, vědecké firmy apod. Proto je potřeba zvážit průchod přes autonomní systém, jelikož některé společnosti si mohou za průchod cizích dat svojí sítí účtovat poplatky. Oficiální autonomní systém musí mít registrované číslo autonomního systému, tzv. ASN. Tato čísla jsou přidělována autoritou IANA (Internet Assigned Numbers Authority) regionálním internetovým registrům (RIR). Tato čísla jsou pak rozdělována jednotlivým ISP a ostatním sítím. ASN je formátu 16bitového čísla od 1 do

65 534 a 32bitového čísla od 131 072 do 4 294 967 294. Aktuálně je používáno přibližně 70 000 čísel. [23] [71]



Obrázek 6: EBGP vs. IBGP

Protokol BGP má dvě verze: Externí (EBGP) a Interní (IBGP). Rozdíl mezi nimi znázorňuje obrázek č. 6, ze kterého vyplývá, že interní verze protokolu BGP se používá uvnitř autonomních sítí, kdežto externí verze propojuje tyto sítě mezi sebou. [23]

2.1 Princip BGP

Protokol BGP používá pro výměnu směrovacích informací mezi autonomními systémy hraniční směrovače (border gateways). Z toho vychází i název Border Gateway Protocol. Pomocí BGP si jednotlivé AS sdělují informace o sítích v jednotlivých AS, o trasách vedoucích k jednotlivým sítím. Protokol BGP používá graf propojení AS, místo propojení směrovačů a sítí, jako to dělá například OSPF. Graf slouží pro vyhledávání cest mezi různými sítěmi v různých autonomních systémech. Cesta (AS PATH) k dané sítí je symbolizována posloupností čísel autonomních systémů, přes které se do sítě dá dostat. Protokol BGP nedisponuje jednoznačnou metrikou, podle které by mohla být vyhodnocována nejkratší cesta do cílové sítě. Provoz je totiž mezi startovní a cílovou sítí veden přes cizí AS, o kterých nemusí mít kompletní informace z důvodů nejrůznějších politik a obchodních podmínek provozovatelů autonomních systémů. Faktory, jenž je po cestě nutné respektovat, vytváří tzv. směrovací politiku (routing policy). Směrovací politika může určovat vstupní a výstupní linky tranzitního provozu naším AS, zdroje a cíle provozu, které můžou přes náš AS procházet. [72]

Cesta od počáteční do cílové sítě nesmí obsahovat smyčku. S tím se BGP vypořádává pomocí principů Path-Vector popsaných v kapitole 1.4.2. Path-Vector je posloupností čísel autonomních systémů, přes které trasa prochází. Jelikož cesta nemůže obsahovat smyčku, může být číslo každého AS ve vektoru pouze jednou. Pokud je možnost, že by mělo být číslo AS v trase víckrát, je tato část trasy zahozena. Tyto principy se využívají také pro výpočet nejkratší cesty do jednotlivých sítí. Za nejkratší cestu bude označena cesta s nejmenším

počtem čísel autonomních systémů. Výměna směrovacích informací (routing updates) probíhá pouze mezi sousedními směrovači (peer směrovače). Za BGP směrovač je označen pouze hraniční směrovač AS. Každý BGP směrovač dostane ručně přiřazený sousední směrovač, se kterým bude moci komunikovat. Jakmile je navázána komunikace mezi sousedy, dojde ke kompletní výměně směrovacích informací, které oba mají. Poté jsou již prováděny pouze inkrementální výměny. Směrovače si mezi sebou testují dostupnost prostřednictvím tzv. keepalive zpráv (běžně v intervalu jedné minuty). Pokud se soused směrovače stane nedostupným, odstraní všechny trasy vedoucí skrz nedostupného souseda a dá tuto informaci vědět dalšímu svému sousedovi. [72]

2.2 Typy zpráv BGP

V protokolu BGP jsou čtyři typy zpráv: OPEN, UPDATE, KEEPALIVE, NOTIFICATION. Zpráva typu OPEN slouží směrovačům při vytváření spojení mezi sebou. Prostřednictvím těchto zpráv se směrovače domlouvají na preferované verzi protokolu, vyměňují si informace o AS, do nějž patří apod. Zpráva UPDATE přenáší směrovací informace. Je složena z několika IP adres, které říkají, jaké AS jsou přes něj dostupné. Zpráva dále může obsahovat atributy přiřazené k cestám. Je zde dále sekce Withdrawn routes s informacemi o již nepoužitelných cestách, jež si má směrovač odstranit ze své směrovací tabulky. KEEPALIVE zpráva je již výše zmíněna. Zpráva NOTIFICATION indikuje chybu v činnosti BGP. Když dojde k odeslání této zprávy, je ukončeno spojení mezi dvě sousedy. [72]

2.3 Nebezpečí BGP

BGP protokol může být pro internet nebezpečný. Existují konkrétní případy, kdy díky špatnému nastavení prvků jednoho AS došlo k výpadku internetu uvnitř jiných AS. To se stalo v Turecku v roce 2004, kdy jeden provozovatel internetu inzeroval do internetu své trasy tak, že je ostatní směrovače vyhodnocovaly jako nejlepší cíl pro své pakety. Došlo k tak masivnímu výpadku, že na mnoho místech na světě nebylo možné přistupovat do internetu. Obdobný případ se stal i v Pákistánu v roce 2008. Tehdy se pokusil místní ISP pomocí BGP protokolu zablokovat jeho uživatelům přístup na YouTube. Stalo se však to, že se trasa inzerovala i sousedním sítím, díky čemuž byla nedostupná adresa YouTube několik hodin i pro nepákistánské uživatele. [23]

Dalším, tentokrát českým případem zranitelnosti BGP je událost z roku 2009, kdy český ISP ovlivnil chod internetu celého světa. Konkrétně se jedná o poskytovatele internetu Supronet z Uherského Brodu. Za problémem stály 4 příčiny:

1. nová chyba ve směrovačích Cisco
2. chyba směrovače MikroTik
3. chybějící filtry tranzitních operátorů
4. chyba v konfiguraci směrovače Supronetu.

Chyba ve směrovači Cisco se týkala cyklického rozpadávání a opětovné navazování BGP spojení na směrovačích generující BGP UPDATE zprávu. Pokud délka cesty mezi AS překročila 255, je vygenerována nevalidní BGP UPDATE zpráva, která vede příjemce k ohlášení chyby a k ukončení spojení. Směrovače se pak snaží spojení obnovit, což způsobí generování velkého množství zpráv, které jsou odmítány. Lze to ošetřit nastavením maximální délky cesty. [94]

Příčinou byla chybná konfigurace ve směrovači MikroTik. Administrátor Supronetu zadal neplatné číslo pro prodloužení délky cesty. Software MikroTiku neprovedl žádnou kontrolu nad zadanou konfigurací. Problému šlo předejít, kdyby měli tranzitní operátoři nastavené filtry na blokování používání dlouhých cest. Pokud by filtry existovaly, nemuselo by dojít k propagaci dlouhých tras do internetu a nedošlo by ke kolapsu. [94]

3 OSPF

OSPF neboli Open Short Path First je Link-State směrovací protokol používaný uvnitř uzavřeného autonomního systému. Je pravděpodobně nejvíce používaným směrovacím protokolem. Je robustní, má integrované bezpečnostní funkce a je implementován v široké škále síťových zařízení. Existují tři verze: OSPFv1 (nikdy neopustil experimentální fázi vývoje), OSPFv2 (celosvětově nasazená funkční verze protokolu pro sítě s IPv4) a OSPFv3 (podpora IPv6 sítí). [24] [25]

Protokol OSPF je relativně komplexní. Lze jej popsat třemi hlavními pojmy. Prvním pojem jsou sousedé. Každý směrovač naváže vztah se sousedními směrovači, tj. těmi, kteří jsou ve stejné podsíti nebo sdílejí některou z dalších vlastností (typ oblasti, …). Dalším pojmem je *„Hello, advertisement and update"* – přeloženo do češtiny „Pozdrav, reklama a aktualizace". Jedná se o různé zprávy odesílané směrovačem za účelem sdílení informací o směrování. *„Fight-back mechanism"* neboli mechanismus boje je dalším pojmem protokolu OSPF. Jakmile směrovač obdrží falešnou reklamu či aktualizaci obsahující informace, které on sám odeslal na adresu vícesměrového vysílání OSPF (224.0.0.5), odešle novou informaci, která tu falešnou přepíše. [24]

3.1 Princip

Každý směrovač inzeruje LSA (Link-State advertisement) obsahující odkazy na sousední sítě. Každé LSA je rozšířeno po celé síti. Směrovače si tak z nich sestavují kompletní pohled na topologii autonomního systému. Poté jsou směrovače schopny dopočítat si z dostupné topologie svoji směrovací tabulku. Každé LSA je ve výchozím nastavení inzerován pravidelně každých 30 minut. Každé LSA obsahuje LSA pole obsahující informace o uplynulém čase od vypuštění do sítě. Jakmile uplynulý čas dosáhne jedné hodiny, je záznam odstraněn z databáze LSA. Autonomní systém se dvěma či více směrovači se nazývá tranzitní síť. Směrovač připojený k tranzitní síti inzeruje odkaz nejen na sousední směrovač, ale i na celou síť.[25]

Směrovač dynamicky zjišťuje své sousedy pomocí tzv. Hello zpráv. Směrovač pravidelně rozesílá tyto zprávy do sítě. Zpráva obsahuje identity všech směrovačů, od kterých byla přijata (tzn. zpráva putující sítí zaznamenává, kterým směrovačem byla přijata a putuje dále). Po vzájemném objevení mohou dva směrovače navázat speciální vztah nazývaný sousedství (adjacency). [25]

V autonomním systému, kde běží OSPF můžeme zvolit jeden směrovač jako Designated router – DR (určený směrovač) a jeden jako Backup Designated router – BDR (záložní směrovač). Určené směrovače jsou voleny proto, aby byl minimalizován počet vytvořených sousedství a byl vytvořen centrální bod pro výměnu informací o směrování OSPF. Na linkách typu bod-bod nejsou typy směrovačů definovány. Jsou pouze propojeny dva směrovače. Každý směrovač, který není DR ani BDR si bude vyměňovat informace o směrování pouze se směrovačem označeným jako DR nebo BDR, místo komunikace se všemi směrovači v síti. DR poté distribuuje získané informace o topologii sítě do všech ostatních směrovačů ve stejné oblasti. BDR slouží jako aktivní pohotovostní režim pro DR. Přijímá všechny informace o směrování od sousedních směrovačů OSPF, avšak tyto informace nebude šířit dále. K odesílání informací o směrování na DR nebo BDR je vyhrazena adresa 224.0.0.6. DR odesílá na adresu multicastu 224.0.0.5. Pokud DR selže, jeho roli převezme BDR. [26] Používání DR a BDR vede ke snížení nároků na paměť a zatížení sítě. [25]

3.2 Bezpečnost OSPF

Bezpečnost OSPF se opírá o pět základních pilířů. Prvním je ověřování paketů na každém spojení. Každý paket OSPF odeslaný na specifickou linku může být ověřován. [25] K ověřování veškerého provozu v síti se používá sdílený tajný klíč. Klíč není nikdy odeslán po síti v nezašifrované podobě – paket, jenž je odeslán do sítě, má k sobě připojenu část, která je jeho zhuštěnou a zašifrovanou variantou. V paketu je dále zahrnuto pořadové neopakující se číslo k ochraně před opakovacími útoky, které se mohou snažit do sítě posílat již odeslané pakety. Tím mohou zahltit síť a narušit tak její chod. Když je paket jednou přijat a ověřen, je nastaveno jeho ověřovací pořadové číslo na číslo, které je jeho pořadovým. Pokud dojde k opakovanému doručení takového paketu, bude již mimo pořadí a bude ignorován. [27]

Druhým bezpečnostním pilířem jsou tzv. záplavy – *flooding*. Způsobují, že každé LSA je rozšířeno po celém autonomním systému. Tudíž nelze zabránit tomu, aby se nedostala na škodlivý směrovač do té doby, než původce LSA nezmění trasu k cíli, která již nepovede přes škodlivý směrovač. [25]

Třetí pilíř, který zvyšuje bezpečnost OSPF, je výše zmíněný mechanismus *Fight – back*. Za čtvrtý pilíř je považován obsah LSA. LSA totiž obsahuje pouze malou část topologie sítě – pouze odkazy na bezprostřední sousedy. To proto, aby se útočníkovi ztížilo získat přehled

o topologii sítě. Za těchto podmínek bude muset útočník odposlechnout celou řadu LSA zpráv z mnoha směrovačů z autonomního systému, aby nabyl dostatečného přehledu o topologii sítě. Posledním pilířem jsou obousměrné odkazy. Informace o lince je přijata pouze tehdy, když obsahuje oba konce linky. Teprve tehdy je tato linka zohledněna při výpočtu směrovací tabulky směrovače. Pokud útočník inzeruje neexistující odkaz na jiný směrovač, nebude mít jeho informace vliv na směrovací tabulku směrovače, protože jiný směrovač nebude nikdy propagovat linku zpět na útočníka. [25]

4 AAA PROTOKOL

Pojmem AAA protokol označuje v oblasti počítačových sítí zabezpečení přístupu jen pro legitimní, oprávněné uživatele. Zkratka AAA má v angličtině význam *Authentication, Authorization and Accounting* – přeloženo do českého jazyka autentizace, autorizace a účtování. [28] Autentizace je bezpečnostní opatření, které zajišťuje proces ověřování totožnosti osoby či zařízení. Příkladem může být zadávání uživatelského jména a hesla při přihlašování na web. Po zadání správných přihlašovacích údajů je potvrzeno, o jakou osobu se jedná. [29] Autorizace je určení úrovně přístupu nebo oprávnění daného uživatele k jednotlivým funkcím nebo zdrojům daného systému: k souborům, programům, modulům a funkcím aplikace, přístupu k síti, a to na základě identity uživatele. [30] Posledním pojmem je účtování. Tento proces sleduje aktivitu uživatele při připojení do systému. Například čas, po který je uživatel do systému přihlášen nebo množství přenesených dat. Sledují se také například aktivity, které uživatel v systému vykonává. Tato data poté slouží pro různé trendy, výzkumy a šetření. Sledování pohybu uživatele může přispět při forenzní analýze a vyšetřování kybernetické bezpečnosti. [28]

Pro implementaci AAA v sítích poskytovatelů internetu (ISP) v současné době máme tři nejvíce používané technologie: PPPoE, IEEE 802.1x a Captive web portal. [31]

4.1 PPPoE

Point-to-Point over Ethernet je síťový protokol zapouzdřující rámce PPP do rámců ethernetových. [32] PPP neboli Point-to-Point protokol je používán vrstvami datových spojů, ve kterých je vyžadován pro zapouzdření protokolů vyšších síťových vrstev pro jednoduchý průchod přes synchronní a asynchronní komunikační linky. PPP rámce zapouzdřují informace a data, která obsahují konfigurační informace nebo data. [33]

PPPoE umožňuje zahájit dialog dvou bodů. Obecně se jedná o klienta a přístupový bod. Nastavení dialogu PPPoE vyžaduje dvě fáze: *Discovery* a *Session.* Fáze Discovery ethernetovou MAC adresu klienta. Poté se určí číslo relace (SESSION_ID), které slouží k identifikaci spojení. Během vyhledávací fáze může klient nalézt dva přístupové body, díky kterým má možnost se připojit. Spojení PPPoE je vždy pouze mezi dvěma stanicemi, tudíž si klient musí zvolit, ke kterému přístupovému bodu se připojí. Po vyhledání a zvolení vhodného přístupového bodu dochází k vytvoření a k následnému udržování spojení PPP. [31] [32]

K výhodám PPPoE patří, že lze použít pro technologie vytáčeného přístupu veřejné telefonní síti (PSTN – síť skládající se z telefonních linek, optických kabelů, mikrovlnných spojů, komunikačních satelitů apod.). Další výhodou je snadné přijmutí koncového uživatele. Do nevýhod přístupu PPPoE lze zařadit nízkou účinnost zapouzdření rámců, jelikož je nutné zapouzdřit rámec PPP do ethernetového rámce. PPPoE generuje velké množství přenosů během fáze zjišťování, což může výrazně ovlivnit výkon sítě. Služby vícesměrového (multicastového) vysílání je obtížné implementovat (většina video služeb je založena na vícesměrovém vysílání – IPTV). [31]

4.2 802.1X

Standard IEEE 802.1X je další metodou pro ověřování autentizace uživatelů pro přístup k LAN nebo WLAN síti. Standard definuje řízení přístupu k síti založené na logických portech, které jsou použity pro zajištění přístupu k sítím internet. [34]

Identita uživatele se ověřuje na základě jeho přihlašovacích údajů či certifikátu, který je potvrzen serverem RADIUS. Server RADIUS (Remote Authentication Dial-in User Service) funguje jako bezpečnostní prvek sítě. Při připojení uživatele do sítě server RADIUS začne ověřovat jeho identitu a autorizuje jej pro použití v síti. Server vyzve uživatele k zadání přihlašovacích údajů, které ověří, nebo ověřuje uživatelův certifikát. Tato situace se opakuje při každém novém připojení uživatele do sítě. Pokud nastane situace, že se nepodaří uživatele ověřit, je mu odepřen přístup k internetu. Servery RADIUS se využívají i k ověření uživatelů jiných organizací, než je organizace spravující daný RADIUS server. Příkladem takového řešení je Eduroam. Servery jsou v tomto řešení autentizace využívány jako RADIUS proxy servery. Jedná se o řešení pro univerzity, kdy student navštíví sousední univerzitu a pokusí se zde připojit k internetu. Jeho požadavek je proxy serverem odeslán na RADIUS server jeho domovské univerzity.[36]

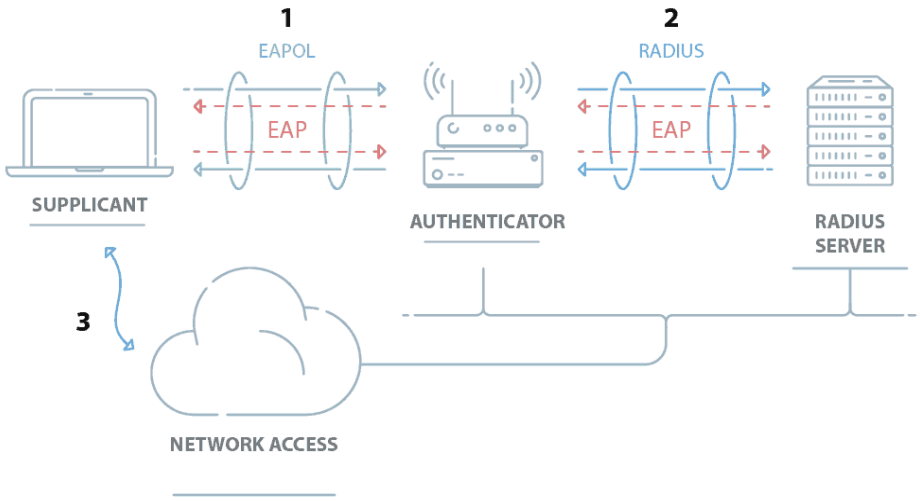
Za standardní ověřovací protokol je považován EAP – Extensible Authentication Protocol. Poskytuje bezpečnou metodu pro odesílání identifikačních informací pro ověřování v síti. Zabraňuje vnějším uživatelům odposlechu důvěrných informací skrz vytvořený šifrovaný tunel. [36]

4.2.1 Komponenty pro realizaci 802.1x

Bez ohledu na to, jestli bude realizace sestavena z profesionálních komponent a softwarů, nebo bude vytvořena pomocí opensource nástrojů, je kvalita a jednoduchost zcela designovým prvkem. Znamená to, že na výslednou funkci toto rozhodnutí nebude mít vliv.

Pokud správce sítě chce začít používat v síti standard 802.1X pro povolení připojení uživatelů k Ethernet portům organizace, je zapotřebí nainstalovat a nakonfigurovat do sítě různé komponenty. V první řadě je potřeba přepínač podporující standard 802.1X. Podpora 802.1X na straně přepínačů je v dnešní době velice rozsáhlá.

Zařízení uživatelů, připojovaná do sítě musí obsahovat klienty RADIUS. Musí mít nainstalovaný software zvaný Supplicant. Většina zařízení, u nichž se přepokládá připojení k internetu, jsou tímto softwarem vybavena (na mysli jsou herní konzole, wifi routery, počítače, smartphony atd.). Supplicant se bude účastnit počátečního vyjednávání EAP s přepínačem a má za úkol zašifrovat důvěrné ověřovací informace žadatele o připojení k internetu. Pokud klient nemá suppliciant, budou jeho pokusy o navázání komunikace



Obrázek 7: Komponenty 802.1X[36]

s RADIUS serverem ignorovány a nebude se moci ověřit. [34][36]

Přepínač iniciuje výměnu ověřovacích informací zasláním paketu EAPOL-Start, když se klient připojí k síti. Odpovědi klienta jsou při splnění výše zmíněných podmínek předávány na RADIUS server. Po dokončení ověřování se přepínač rozhodne, zda zařízení autorizuje pro přístup k internetu na základě atributů obsažených v paketu Access_Accept odeslaném

ze serveru RADIUS. Tento paket také může obsahovat informace, jak klienta připojit k síti (například jaký použít VLAN – VLAN pro hosty, VLAN pro zaměstnance apod.). [36]

Pro uložení přihlašovacích jmen a hesel, vůči kterým RADIUS server ověřuje získaná přihlašovací jména a hesla od klientů během fáze ověřování se využívá služba AD (Active Directory) nebo server LDAP (Lightweight Directory Access Protocol). Služba AD implementuje adresářové služby poskytující různé druhy funkcí jako jsou ověřování, správa uživatelských skupin a uživatelů samotných, správa zásad apod. LDAP je opensource multiplatformní protokol používaný pro ověřovací funkce. Jeho adresářové funkce ukládají přihlašovací údaje uživatelů, účty počítačů a sdílejí tyto informace s dalšími zařízeními v síti. [36][37]

Pro kompletní zavedení standardu je dále zapotřebí mít v síti umístěn server NPS. Network Policy Server umožňuje vytvářet zásady pro přístup do sítě pro danou organizaci a vyřizuje požadavky na autentizaci požadavků na připojení, autorizaci a účtování. Tyto funkce poskytuje ve třech variantách implementace. [34] [35]

4.2.2 NPS jako server RADIUS

NPS provádí centralizovanou autentizaci, autorizaci a účtování bezdrátových sítí. Dále realizuje autentizační přepínač a spojení pomocí VPN. Pokud je NPS server používán jako server RADIUS, jsou prvky pro přístup k sítí, (bezdrátové přístupové body, VPN servery atp.) konfigurovány jako klienti RADIUS. Je potřeba nakonfigurovat zásady pro autorizaci požadavků na připojení. NPS také poskytuje možnost zapisovat informace o jednotlivých požadavcích o připojení do protokolu uloženého na disku či zapisovat informace do databáze. [34]

4.2.3 NPS jako RADIUS proxy

V situaci, kdy je NPS server používán jako RADIUS proxy, jsou nakonfigurovány zásady na přijetí požadavků o připojení, které jsou pak předávány dalším RADIUS serverům. Opět je poskytováno protokolování informací jedním nebo více servery ve skupině RADIUS serverů. [34]

4.3 Web + Portal

Klient získá z DHCP serveru adresu (může použít i statickou IP adresu). Avšak stále nemá dostupný internet. Má pouze přístup na jednu konkrétní adresu, kde je dostupný web pro

přihlášení. Tento web je realizován serverem Portal. Uživatel zde zadá uživatelské jméno a heslo a pokud jsou data správná získá přístup do internetu. Pro ověření dat se může použít server RADIUS, jež je popsán na přechozích řádcích. [31]

5 DHCP

V začátcích vývoje protokolů TPC/IP nebyla velká motivace k tomu, aby existovala automatizace konfigurace zařízení, která protokoly TPC/IP používají. Počítačů bylo málo a nebyla možnost je jednoduše přenášet v rámci místnosti či budovy. A ještě důležitějším aspektem bylo, že každý počítač měl určeného správce. V dnešní době je tomu jinak. Existují sítě se stovkami až tisíci různých zařízení, které jsou připojeny k síti internetu. Navíc tato zařízení většinou ovládají uživatelé, kteří nemají znalosti v oblasti TCP/IP (není ani v jejich zájmu tyto znalosti mít). Zde vzniká potřeba jakési automatizace. Proto přichází protokol DHCP vyvinut společností IETF. DHCP je poskytovatelem automatizované konfigurace počítačů a ostatních zařízení, která používají protokoly TCP/IP. Díky DHCP může správce sítě přiřadit síťovou adresu, masku podsítě a směrovač, který má být pro zařízení výchozí. DHCP je typu klient-server, tzn. že klienti (počítače a jiná různá zařízení) se dotazují centrálního konfiguračního serveru na parametry. Správce sítě dodává tomuto serveru popis infrastruktury sítě společně s pravidly, podle kterých bude server přiřazovat adresy a ostatní konfigurační parametry, jež bude předávat klientům. [1]

DHCP server má v moci přidělovat klientům adresy staticky či dynamicky. Staticky přiřazená adresa znamená, že po každém připojení daného klienta do sítě dostane klient stejnou předem zvolenou adresu. Tato adresa je s klientem svázána pomocí jeho fyzické adresy. Dynamicky přidělované adresy jsou serverem náhodně přidělovány ze stanoveného rozsahu adres, který správce sítě zvolil. V takovémto případě může počítač dostat při opětovném připojení počítače do sítě jinou adresu. [1]

5.1 Benefity DHCP

Práce spojená s ručním přiřazováním IP adres zařízením umístěných v síti je velice časově náročná, zdlouhavá a vede k zavádění chyb. Správce již nemusí ručně konfigurovat každé zařízení zvlášť. DHCP umožňuje používat přenosná zařízení jako jsou notebooky, mobily, tablety a jiná zařízení v různých sítích bez jakéhokoliv složitějšího nastavování síťových parametrů. S využitím rozšířených možností DHCP můžou správci sítí volit kontrolu přiřazování adres a stále je zde možnost využít statického přidělení IP adresy pro zařízení. Též mají v moci ovlivnit, zda musí být zařízení před přidělením adresy registrováno. [1]

Za to, že jsou zařízení od výrobce nastavena jako DHCP klient, patří zásluhy společnosti Microsoft. Tato společnost začala své produkty konfigurovat jako DHCP klienty již od operačního systému Windows verze 95. Tímto inspirovala spoustu dalších firem ke

konfiguraci svých zařízení jako DHCP klienty, jako například Apple, který takto začal konfigurovat svůj operační systém Macintosh. Též i většina bezplatných operačních systémů typu Unix jednoduše přechází na DHCP klienty. Podpora přišla od Internet Software Consortium (ISC), která poskytla open source licenci pro DHCP, jenž zahrnuje sever, klienta a agenta přenosu (relay). Implementace DHCP od ISC je zcela běžně rozšířená na spoustě komerčních verzích Unixu, podobně jako na bezplatných operačních systémech typu Unix. [1]

Používání DHCP ve velkých sítích přináší obrovské výhody. Zde se odráží ona automatizace konfigurací, kdy je velké množství zařízení konfigurováno pomocí jednoho skriptu, což šetří spoustu času i potíží. I v malých sítích může být výhodné používat server DHCP. V malých sítích neřešíme časovou náročnost nastavování každého zařízení zvlášť. Může se tedy zdát, že konfigurace DHCP serveru se stane celkově časově náročnější než ruční konfigurace.

Pokud se jedná o zkušeného správce sítě, konfigurace by neměla zabrat více času než ruční konfigurace. Stane-li se, že DHCP server bude konfigurovat méně zkušený správce, bude díky tomu konfigurace DHCP serveru časově náročnější. Ale v návaznosti na to, že se sítě rozrůstají, bude tato nově vzniklá malá síť lépe škálovatelná. [1]

5.2 Problémy DHCP

Jelikož žádný systém není dokonalý, i v případě DHCP jsou vnímány určité problémy, kvůli kterým někteří správci sítí odmítají do své sítě DHCP nasadit. Ti se domnívají, že díky DHCP je v síti generováno větší množství všesměrového provozu (broadcast). DHCP sice broadcast využívá, avšak zcela jistě ne ve velkém množství. Jedná se o první dvě zprávy, které musí být klientu DHCP doručeny a na tyto zprávy se očekává odpověď. Ve výsledku jsou to čtyři pakety, které jsou broadcastem přenášeny. To se navíc děje jen v ojedinělých případech. Typičtěji dochází k tomu, že pouze při spuštění klienta, kdy si klient nakonfiguruje své síťové připojení, je odeslán jeden paket unicastem směrem k DHCP serveru. Taková konfigurace vydrží až do vypršení platnosti výpůjčky či odpojení klienta od sítě, ať už vypnutím či restartováním. [1]

Dále se správci mylně domnívají, že je provoz DHCP šířen po celé síti. Ve skutečnosti se provoz DHCP šíří jen v segmentech sítě, kde je klient připojen. Navíc provoz, který se šíří sítí je unicastový, což znamená, že je směřovaný buď přímo klientu či serveru. Pro srovnání lze použít příklad s ARP (Address Resolution Protocol), který používají všechny IP sítě. Pokud zařízení potřebuje komunikovat s jiným zařízením a zná pouze svého souseda, rozešle

ARP broadcast, aby získal IP adresu cílového zařízení (uvažujeme, že na počátku zná jeho fyzickou adresu). Jakmile ji zjistí, ověřuje si tuto informaci odesíláním dalších ARP broadcastů. Některé implementace ARP tento úkon provádějí každé dvě minuty. [1]

Dalším problémem může být ztráta komunikace mezi DHCP serverem a klientem. To se může stát v okamžiku, kdy server byl delší dobu nedostupný, dobu delší, než byla výpůjčka adresy klientovi. V té chvíli musí klient přestat používat síť. V praxi je to vyřešeno tím, že klient požádá o prodloužení své adresy ještě před vypršením platnosti. Pokud nedostane od DHCP serveru žádnou odpověď, ponechá si stávající adresu. [1]

5.3 Spolehlivost DHCP

Při nasazování DHCP serveru je vhodné uvažovat o jeho záloze. Je vhodné mít spolehlivé redundantní síťové řešení. Pokud toto není možné uskutečnit, doporučuje se použít centrální řešení, místo provozování vlastního DHCP serveru. Pokud server rozdává statické adresy, (například svázané s MAC adresou zařízení) lze nastavit sekundární DHCP server kompletně redundantně.

Skupina DHCWG (Dynamic Host Configuration Working Group) spadající pod komisi pro technickou stránku internetu (IETF – Internet Engineering Task Force) vyvinula nový protokol DHCP failover, který umožňuje DHCP serverům pracujícím v režimu primární/sekundární server rozdávat IP adresy ze stejného rozsahu. Protokol dává možnost rozložit provozní zatížení na primární a sekundární sever rovnoměrně a umožňuje sekundárnímu serveru při výpadku primárního serveru pracovat jako plnohodnotná jeho náhrada. [1]

5.4 Přiřazování adres

Při přidělování IP adres je DHCP v roli agenta. Musí mít jasnou a jednoznačnou znalost rozložení sítě, stejně jako když přiděluje IP adresy správce sítě. Jelikož musí DHCP fungovat automaticky a nemůže posuzovat, co stalo se starými zařízeními, nepřiděluje adresy klientům do konce ukončení jejich činnosti. DHCP server přiděluje IP adresy na určitý čas. Je na klientovi, aby si před vypršením časového limitu, na který mu byla adresa přidělena, požádal o obnovení času výpůjčky. Většina DHCP klientů žádá o obnovení výpůjčky mnohokrát za sebou. Tím, že si klient po vypršení času IP adresu neobnoví, DHCP server ji získá zpět do své databáze. Nedochází tak k tomu, že jsou v síti nepoužívané adresy, jelikož

takto zpět získané adresy může přidělit jinému klientovi. Pokud zařízení ztratí adresu, je mu přidělena nová, pravděpodobně jiná, IP adresa. [1]

Díky systému výpůjček je také snadné přečíslování. To znamená, že pokud každé zařízení v síti používá DHCP server, může dostat jinou IP adresu, aniž by uživatel musel udělat nějaký zásah do nastavení svého zařízení. [1]

5.4.1 Statické přiřazování

Při statickém přidělování IP adres dostane DHCP server seznam identifikačních údajů klientu DHCP. Identifikační údaj jednoznačně a konkrétně určuje klienta. Když nastane okamžik, v němž DHCP klient požádá o přidělení adresy, DHCP server vyhledá klienta v obdrženém seznamu klientů a podle daného pravidla přiřadí klientovi IP adresu. Každému identifikátoru je totiž přiřazena konkrétní IP adresa správcem sítě. Pokud se jedná o klienta mobilního, správce mu může v každém segmentu sítě přiřadit adresu, ke které má být klient připojen. Pokud se však klient dostane do segmentu sítě, kde správce nechce, aby se připojil, adresu mu nepřidělí. [1]

5.4.2 Dynamické přiřazování

S dynamickým přidělováním adres přijímá DHCP server rozsahy IP adres pro každý segment sítě, ve kterých očekává konfigurace DHCP klientů. Jakmile DHCP klient požádá o přidělení adresy, DHCP server vyhledá volnou IP adresu v rozsahu odpovídajícímu segmentu DHCP klienta a takovou adresu klientovi přiřadí. [1]

5.4.3 Hybridní přiřazování

Hybridní přiřazování adres představuje pomyslný kompromis mezi výše zmíněnými dvěma způsoby přiřazování adres. Správce sítě serveru DHCP nadefinuje soubor identifikačních údajů klientů, kteří můžou obdržet IP adresu. Nedefinuje však již jakou adresu má přidělit. DHCP server dostane pouze rozsah adres, ze kterých bude DHCP klientům adresy přiřazovat. Ve chvíli, kdy DHCP klient požádá o přidělení adresy, DHCP server ověří, zda se klient nachází v seznamu obdržený od správce sítě a poté klientovi buď přiřadí nebo nepřiřadí adresu. Tento postup lze využít pro ošetření toho, že můžou být v síti pouze registrovaní klienti. [1]

Dalším způsob využití hybridního přiřazování adres spočívá v tom, že se registrovaným klientům přiřazuje adresa na pevno a neregistrovaným klientům se přiřadí adresa dynamicky

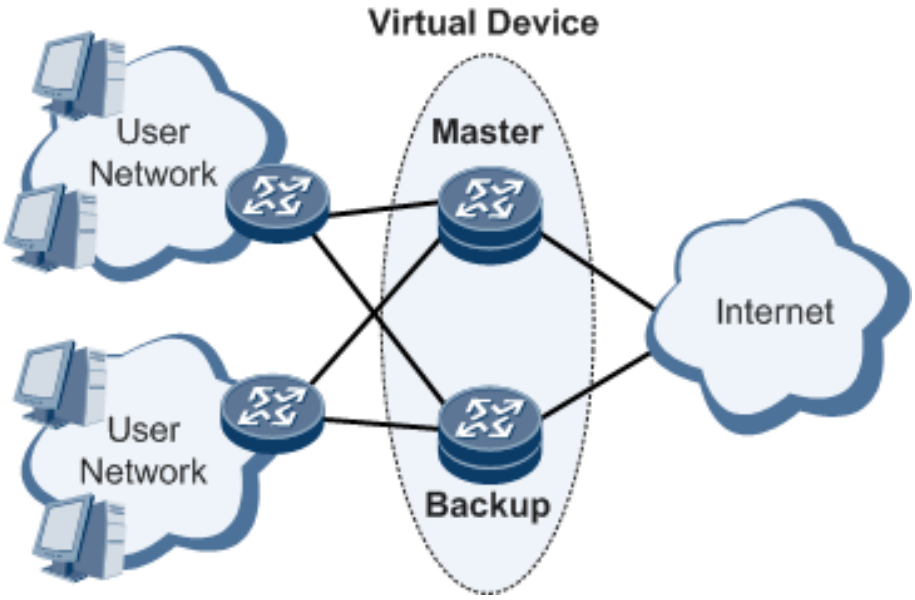
z daného rozsahu. Uživateli to umožní získat konkrétní adresu, avšak správce nemusí sledovat každé zařízení, které se k síti připojí. [1]

5.5 Autoritativní DHCP server

Pokud je DHCP server spravován správcem či skupinou správců, kteří provozují síť obsluhovanou tímto serverem, je nazývám autoritativním DHCP serverem. Server je neautoritativní, pokud je spravován někým jiným. Většina DHCP serverů, které jsou provozovány, jsou autoritativní. Každý oficiální DHCP server je potřeba konfigurovat jako autoritativní. Pokud tomu tak není, server neinformuje klienty o případných změnách v síti, tudíž pokud některý klient změní síť, nedostane novou IP adresu. [1]

6 VRRP

Virtual Router Redundancy Protocol (VRRP) je protokol, který je zodpovědný za dynamické přiřazování odpovědnosti za směrovací funkce mezi reálnými stroji. VRRP implementuje zálohování výstupní brány a zajišťuje kontinuitu a spolehlivost komunikace. Ve své podstatě seskupuje několik fyzických směrovačů do jednoho virtuálního směrovače. Hlavním úkolem VRRP je přepínat mezi fyzickými zařízeními v době výpadku jednoho z nich tak, aby došlo k co nejmenšímu výpadku služeb daného zařízení. Obrázek č. 8 zobrazuje schéma sítě s nasazeným VRRP. V oblasti Virtual Device se nachází dva fyzické stroje. Jeden je označen jako master (hlavní) a druhý jako backup (záložní). Typicky se virtuální směrovač skládá z jednoho hlavního a více záložních strojů – směrovačů. [61]



Obrázek 8: Schéma ukázkové sítě s VRRP [61]

V tomto případě dva směrovače tvoří jeden virtuální směrovač, kterému je přiřazena virtuální MAC adresa a virtuální IP adresa. Fyzické směrovače komunikují s ostatními zařízeními v jiných segmentech sítě prostřednictvím virtuálního směrovače. Pakety však předává pouze směrovač, který je v danou chvíli označen jako hlavní (záložní směrovač je označen jako hlavní ve chvíli, kdy je skutečný hlavní směrovač mimo provoz). [61]

Používání VRRP v síti přináší výhody. V první řadě se jedná o spolehlivost přenosu dat. Logická brána VRRP v lokální síti zajišťuje spolehlivý přenos přes klíčové prvky sítě. Zabraňuje přerušení služeb při výpadku jednoho ze zařízení. Dále lze jako o výhodě hovořit také o nízkých režijních nákladech na síť. Výhodou je též jednoduchá konfigurace pro klienty. Stačí pouze správně nastavit adresu brány a protokol VRRP se o zbytek postará.

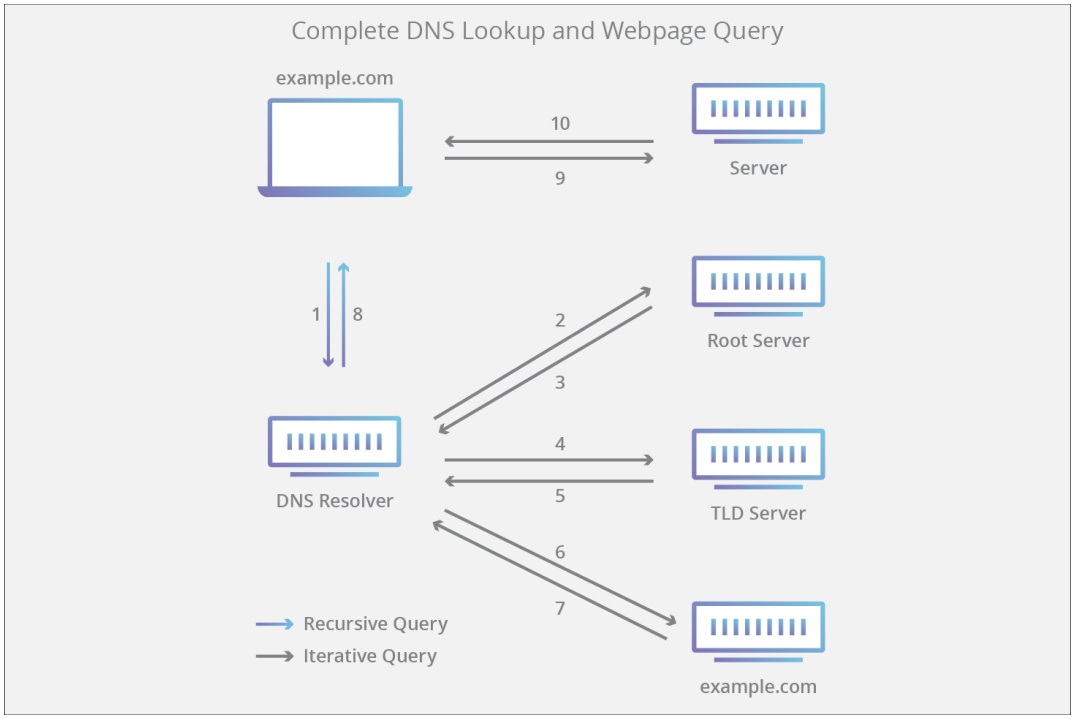
S použitím VRRP odpadá problém single point of failure – kritické místo poruchy. Další výhodou je flexibilita aplikace. Záhlaví VRRP je zapouzdřeno do hlavičky paketu. Znamená to, že je umožněno přidružení k různým protokolům vyšších vrstev. [61]

Zařízení s VRRP dynamicky volí primární a sekundární zařízení. Lze to realizovat pomocí typů, jak je zmíněno výše, nebo pomocí priorit. Priorita je číslo, které může nabývat hodnot od 1 do 255, přičemž hodnota 255 je brána jako nejvyšší (zařízení s hodnotou 255 bude vybráno jako primární). Volba zařízení podle nastavené priority bude probíhat pouze v případě, že jsou zařízení stejného stavu – typ je nadřazen prioritě. V provozu VRRP odesílá primární směrovač v pravidelných intervalech (výchozí hodnota je 0) informační pakety, které slouží k tomu, aby sekundární směrovač věděl, že je primární směrovač v provozu. Jakmile je primární směrovač bez odezvy, přebere úlohu primárního směrovače sekundární směrovač. [61]

7 DNS

Domain Name System (DNS) je jedním ze základů internetu. V nejjednodušší definici je to adresář jmen, které odpovídají číslům – IP adresám. Jedná se v podstatě o analogii telefonního seznamu. Každému jménu odpovídá určitá IP adresa, kam se odkazuje. Když internet začínal, bylo jednoduché si vzhledem k velikosti zapamatovat všechny, nebo alespoň většinu IP adres serverů. Když se však internet začal rozrůstat, nebyl tento proces už tak snadný. Čísla se člověku obecně pamatují hůře než slova, protože slova dávají určitý smysl. Úplně prvním, s nadsázkou řešeno, DNS serverem byla Elizabeth Feinler, která ručně zapisovala seznam přiřazených jmen k adresám do textového souboru *hosts.txt.* Vzhledem k růstu internetu byla tato metoda neudržitelná také z toho hlediska, že Elizabeth pracovala pouze do 18:00 a přes Vánoce si brala volno. K tomuto docházelo v 70. letech a počátkem 80. let minulého století. Tok 1983 byl pro DNS zlomový. Paul Mockapetris dostal úkol vytvořit kompromis mezi několika návrhy řešení problému. Všechny však ignoroval a vytvořil řešení, které se v základní úrovni používá dodnes. [54]

Proces vyřízení DNS zahrnuje převod názvu hostitele například www.google.com na IP adresu. Do adresního řádku prohlížeče je stále možné zadat čistě IP adresu. Do převodu jsou typicky zapojeny čtyři typy serverů: Rekurzivní DNS, Root nameserver, Jmenný server TLD, Autoritativní DNS. [54]



Obrázek 9: Typy DNS serverů a princip dotazování [57]

V následujících podkapitolách jsou rozebrány jednotlivé typy DNS serverů a princip dotazování zobrazený i na obrázku č. 9. Princip DNS dotazování lze shrnout do osmi kroků. Procesu dotazování se též nazývá DNS Lookup.

1. Uživatel zadá do vyhledávače například kiwi.com. Dotaz přejde do internetu a je přijat rekurzivním DNS.
2. Rekurzivní DNS se dotazuje kořenového serveru (root nameserver).
3. Kořenový server odpoví rekurzivnímu DNS adresu jmenného serveru TLD.
4. Rekurzivní DNS odešle dotaz na jmenný server TLD.
5. Jmenný server TLD odpoví rekurzivnímu DNS adresu autoritativního DNS pro danou doménu.
6. Rekurzivní DNS odešle požadavek na adresu autoritativního serveru domény.
7. Autoritativní DNS odpoví rekurzivnímu DNS adresu domény. Může také odpovědět subdoménu a tím se bude proces opakovat pro vyhledání adresy subdomény na jiném autoritativním server.
8. Rekurzivní DNS vrátí získanou adresu domény prohlížeči. Ten pak může získat data ze serveru pomocí http požadavku a vykreslí webovou stránku uživateli.[57]

7.1 Rekurzivní DNS

Rekurzivní DNS (též označován jako překladač DNS) je server, který přijímá dotaz od klienta DNS. Poté spolupracuje s jinými servery DNS a hledá správnou IP adresu. Ve chvíli, kdy rekurzivní server obdrží od klienta požadavek na překlad, chová se k ostatním DNS serverům též jako klient, který žádá o překlad. Jedná se takzvaně o rekurzivní dotaz. Když server nezná odpověď na dotaz uživatele, spustí algoritmus. Ten začne získávat odpovědi u kořenových DNS serverů (Root nameserver) a postupuje do nižších úrovní. [54] [55]

7.2 Root nameserver

Root nameserver neboli kořenový jmenný server je prvním krokem při překladu doménového jména na IP adresu. Sám o sobě slouží jako rozcestník. Ukazuje, kterým směrem jde odpověď na přijatý dotaz. Kořenové servery obsahují informace, které tvoří kořenovou zónu (root zone). Je to globální seznam domén nejvyšší úrovně (například .com, .net a .org), seznam domén nejvyšší úrovně s kódem země (například .cz, .sk apod.) a seznam

internacionalizovaných domén nejvyšší úrovně (domény napsané v místních znakových sadách). Kořenový server pouze ukazuje směr na jmenný server TLD. Na světě existuje 13 takových serverů, které jsou označeny písmeny A až M. Fyzicky jich není 13, existují desítky jejich záložních kopií a jsou rozmístěny po celém světě. Dohlíží na ně nezávislá společnost ICANN (Internet Corporation for Assigned Names and Numbers), která rovněž spravuje všechny názvy domén na internetu. [54][56]

7.3 Jmenný server TLD

TLD – Top Level Domain server je server domény nejvyšší úrovně. Tento jmenný server udržuje informace o názvech všech domén, které mají společnou příponu domény. Kupříkladu jmenný seznam TLD domény .com bude znát informace o všech doménách, které mají příponu .com. [56] Českou doménu .cz spravuje organizace CZ.NIC.

7.4 Autoritativní server

Autoritativní server poskytuje originální a definitivní odpovědi na dotazy DNS. Neposkytuje informace z mezipaměti získané z jiného jmenného serveru, pouze informace, které má uložené ve své konfiguraci. Odpovídá pouze na dotazy ohledně domény, případně domén, které spravuje. Autoritativní server je poslední zastávkou v dotazu na jmenný server. Odpovědí autoritativního serveru je IP adresa na konkrétní server, který je spojen s daným doménovým jménem.[54][56]

7.5 Typy dotazů

Při typickém vyhledávání DNS se vyskytují tři typy dotazů. Použitím kombinace těchto dotazů může optimalizovaný proces získat odpověď za kratší dobu. Prvním typem dotazu je rekurzivní dotaz. V rekurzivním dotazu vyžaduje klient DNS, aby server DNS odpověděl klientovi požadovaným záznamem nebo chybovou hláškou, pokud nemůže záznam nalézt. Rekurzivní DNS zahájí proces rekurzivního dotazu od kořenového serveru a pokračuje až do nalezení odpovědi, kterou je IP adresa pro zadanou doménu. Dalším typem je iterativní dotaz. V této situaci umožní klient DNS serveru DNS vrátit nejlepší možnou odpověď. Pokud dotazovaný server DNS nemá přesnou shodu pro zadanou doménu, vrátí se odkaz na autoritativní DNS pro nižší úroveň domén. Klient DNS poté provede dotaz na doporučenou adresu. Tento proces pokračuje dalšími DNS servery v řetězci dotazů, dokud nenastane chyba nebo nevyprší časový limit. Posledním typem DNS dotazu je nerekurzivní dotaz. DNS server obvykle ukládá záznamy do mezipaměti. Děje se to proto, aby bylo možné záznamy

znovupoužít a zabránilo se zbytečnému využívání a zatěžování serverů a linek. Pokud se klient DNS dotáže na záznam, který má rekurzivní DNS v mezipaměti. Ukládáním do mezipaměti se nejen šetří počet dotazů na DNS servery, ale také čas, po který trvá proces získání záznamu od autoritativního DNS.

7.6 Selhání DNS

Server DNS může selhat z několika důvodů. Jsou jimi výpadky elektřiny, kybernetické útoky nebo poruchy zařízení. Naštěstí je v dnešní době provozováno velké množství redundantních DNS serverů, což minimalizuje dobu výpadku serveru DNS. Existují záložní servery kořenové, jmenné servery TLD, a i poskytovatelé internetu většinou provozují záložní rekurzivní DNS. Jednotliví uživatelé mají možnost využít i veřejné překladače například od Google na adrese 8.8.8.8 nebo 8.8.4.4. V případě velkého výpadku serveru DNS mohou uživatelé zaznamenat prodlevu ve vyřízení požadavku od záložního serveru, vzhledem k množství požadavků, které záložní server bude muset vyřídit.

7.7 DNSSEC

Domain Name System Security Extensions (DNSSEC) je bezpečnostní rozšíření DNS. DNS bylo vynalezeno v době, kdy byl internet ještě malý a většina jeho uživatelů se mezi sebou dobře znala. Nebyla nejmenší potřeba ověřovat pravost získaných informací, proto v základu DNS žádná taková služba není implementována. Lze pouze ověřit, zda informace pochází ze zdroje, na který byl odeslán původní požadavek. To však není silný ověřovací prvek, jelikož se útočník může snadno vydávat za autoritativní server. Znamená to, že útočník může uživatele přesměrovat na škodlivé stránky, aniž by o tom uživatel věděl. Stránky můžou vypadat totožně jako internetové bankovnictví uživatele, kde uživatel v nevědomosti zadá své přihlašovací údaje a problém je na světě. To byl podklad k tomu vytvořit zabezpečující rozšíření pro DNS. Již výše je zmíněno, že rekurzivní překladače ukládají záznamy mezipaměti, aby urychlili získávání odpovědí na dotazy DNS klientů. Jenže to je dalším cílem útočníků. Útočník pošle falešnou DNS odpověď, která je rekurzivním DNS přijata. Uloží si ji do mezipaměti, čímž si otráví. Rekurzivní DNS je pak rozesílá všem, kteří se na ně dotazují. [62]

DNSSEC posiluje ověřování v DNS pomocí digitálních podpisů založených na kryptografii veřejných klíčů. Nejsou podepisovány dotazy a odpovědi, ale data DNS jsou podepsána vlastníkem dat. Každá zóna DNS má vlastní pár veřejného a soukromého klíče. Vlastník

zóny podepíše data svým soukromým klíčem. Veřejný klíč uvolní a ten slouží rekurzivním DNS k ověření původu dat, které přijímají. Pokud ověří platnost dat a je potvrzen původ dat, jsou poté předána uživateli. DNSSEC přidává do DNS dvě důležité funkce. Ověřuje se nejen původ dat, to že pochází ze správné DNS zóny, ale také se ověřuje integrita dat, jestli nebyla data během přenosu změněna. K zajištění toho, aby rekurzívní server používal pravý veřejný klíč se používá opět kryptografie. Veřejný klíč dané zóny je podepsán soukromým klíčem nadřazené zóny. Nadřazená zóna je tak zodpovědná za autentičnost svých podřízených DNS zón. Kořenový server však nadřazenou zónu nemá. Proto je důležitým výchozím bodem pro ověření údajů DNS. Pokud překladač důvěřuje veřejnému klíči kořenové zóny, může pak důvěřovat klíčům ostatních zón. Taková sekvence se nazývá řetězec důvěry.

7.8 DNS záznamy

DNS záznamy jsou pokyny, které jsou umístěny na autoritativních serverech. Poskytují informace o doméně, jenž autoritativní server spravuje. Například jaká IP adresa je k doméně přidružena a jak se mají požadavky na tuto doménu zpracovávat. Záznam se skládá řady textových souborů napsaných v DNS syntaxi. Syntaxe DNS je řetězec znaků používané jako příkazy říkající serveru DNS, co má dělat. Všechny DNS záznamy mají TTL (Time-to-Live) označující interval, jak často se má daný záznam obnovovat. [63]

7.8.1 Nejpoužívanější DNS záznamy

- A – záznam obsahující IPv4 adresu domény
- AAAA – záznam obsahující IPv6 adresu domény
- CNAME – tento záznam přeposílá jednu doménu nebo subdoménu do jiné domény (neposkytuje IP adresu)
- MX – směřuje poštu na emailový server
- TXT – umožňuje správci do záznamu textové poznámky
- NS – ukládá jmenný server pro položku DNS
- SOA – nese informace o správci domény
- SRV – určuje port konkrétní služby

- PTR – poskytuje název domény při zpětném vyhledávání[63]

```
filip@DESKTOP-ASJF70I:/mnt/c/Users/filam$ dig google.com

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43609
;; flags: qr rd ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             0       IN      A       172.217.23.238
ns2.google.com.         0       IN      A       216.239.34.10
ns1.google.com.         0       IN      A       216.239.32.10
ns3.google.com.         0       IN      A       216.239.36.10
ns4.google.com.         0       IN      A       216.239.38.10

;; Query time: 24 msec
;; SERVER: 172.19.224.1#53(172.19.224.1)
;; WHEN: Tue Apr 27 18:45:17 CEST 2021
;; MSG SIZE  rcvd: 174
```

Obrázek 10: Ukázka získání DNS záznamu zadané domény

V prostředí Linux lze získat informace o doméně pomocí příkazu dig a názvu vyhledávané domény, jak je vidět na obrázku č. 10. Zde je znázorněno vyhledání DNS záznamů pro doménu google.com. V části ANSWER SECTION jsou vidět DNS záznamy typu A. První se týká přímo domény google.com, které je přiřazena IP adresa 172.217.23.238. Další záznamy odkazují na další DNS servery dané domény. Klíčové slovo IN označuje třídu záznamu. V drtivé většině případů se používá třída IN – Internet. Existují také třídy CS (CSNET Class), CH (CHAOS Class) a HS (Hesiod). [69]

8 PRŮZKUM TECHNOLOGIÍ

Cílem moderních a nově vznikajících protokolů je přinést do sítě více škálovatelnosti. Některým protokolům se to daří více, jiným méně.

8.1 STP – Spanning tree protokol

STP je protokol druhé vrstvy vyhýbající se smyčkám v síti, když jsou v síti přepínače propojeny více cestami. Algoritmus protokolu má za úkol vytvářet síť bez smyček. Je to realizováno výměnou zpráv BPDU s jinými přepínači. Pokud je při detekci zjištěna smyčka, je rozhraní zablokováno. Algoritmus zaručuje, že mezi dvěma síťovými zařízeními bude pouze jedna aktivní cesta. [40] [41]

Nejběžnějším důvodem vzniku smyček v síti je snaha o redundantní – záložní – připojení některého z bodů sítě. Pokud v sítí existuje smyčka, existuje též pravděpodobnost rozesílání duplicitních zpráv. A pokud k tomu dochází, může to ovlivnit chod celé sítě. STP aktivně sleduje linky v síti. K vyhledávání redundantních linek používá algoritmus STA – Spanning Tree Algorithm. Algoritmus nejprve vytvoří topologii, poté odstraňuje (zakazuje) nadbytečné linky. Jakmile jsou redundantní linky zakázány, zůstanou aktivní pouze linky vybraní STP. Pokaždé když je přidána nová linka nebo je některá ze stávajících linek odstraněna, dojde k přepočtu topologie STA a úpravě linek tak, aby byly zakázány redundantní smyčky. [44]

BPDU (Bridge Protocol Data Unit) jsou rámce multicastového vysílání, které přepínačům slouží ke sdílní informací o sob a jejich připojeních. Díky informacím o propojeních jednotlivých přepínačů, je možnost sestavit topologii sítě. Topologie se vytváří ve formě stromu. Kořenový prvek vzniklého stromu se nazývá Root Bridge. K volbě kořenového přepínače se používají dva parametry. Prvním je hodnota priority (prvek s nižší hodnotou priority dostává přednost), druhým parametrem je MAC adresa prvku. Pokud je hodnota priorit u všech prvků v síti stejná, přistoupí se k porovnání MAC adres prvků – prvek s nejnižší hodnotou vyhrává. Proces výběru kořenového přepínače se provádí také při každé změně v síti (změna linek, přidání nového prvku apod.). V základním nastavení se čeká na odpověď prvku 20 sekund, poté je považován za neaktivní a dojde ke změně sítě. Pokud selže kořenový prvek, ostatní prvky zahájí volbu nového kořenového prvku. [44]

Pro výběr nejvhodnější cesty, tudíž pro výběr linky, která bude zachována a která bude zakázána, se používá cena portu. Na přepínači je možnost nastavit pro každý port jinou cenu.

Pokud je mezi dvěma přepínači více možných cest, vybere se ta, která má menší hodnotu ceny. Kořenový port je port, který se přímo připojuje ke kořenovému prvku nebo má k němu nejlevnější cestu. Nejlevnější cesta je ta, která má nejlevnější hodnotu nákladů při průchodu přes jednotlivé porty prvků. Je potřeba však mít pořád na mysli, že nejlevnější cesta nemusí být nejkratší, ale měla by být nejrychlejší. [44]

Dále se porty v technologii STP označují jako Designated a Non-Designated porty (určené a neurčené porty). Pokud je port označen přívlastkem Designated, znamená to, že má ve srovnání s ostatními porty v daném segmentu sítě nejnižší hodnotu nákladů a je určen jako předávací port pro předávání rámců. Port označen jako Non-Designated je blokovaný a blokované porty slouží pro zakazování redundantních linek. [44]

Všechny porty běžící na přepínačích STP prochází čtyřmi stavy. Prostřednictvím těchto stavů přepínač nejen porozumí topologii sítě, ale také vypočítá ceny cest a na základě toho poté volí nejlevnější trasy. Prvním stavem je stav blokování STP. Do tohoto stavu jsou uvedeny všechny porty přepínače po spuštění. V tomto stavu přepínač pouze naslouchá a zpracovává BPDU zprávy od okolních přepínačů. Z příchozích zpráv se naučí topologii sítě, určí si porty, které budou kořenové, určené a neurčené (blokované). Po dokončení všech procesů se kořenové a určené porty přesunou do stavu naslouchání. Nyní porty stále jen naslouchají zprávám BPDU (ostatní provoz je ignorován). Přepínač kontroluje vytvořenou topologii sítě, aby nedošlo ke smyčkám v síti. Dalším stavem, do nějž přejdou opět jen porty kořenové a určené je stav učení. Stále se naslouchá zprávám BPDU, avšak začíná se zpracovávat i běžný provoz. Uživatelské rámce jsou zpracovávány, avšak nejsou předány na cílový port. Rámce jsou přepínačem analyzovány a ze získaných informací i přepínač aktualizuje svoji tabulku CAM (tabulka portu, MAC adresy a VLAN ID [45]). Nyní může následovat stav předávání. Nyní již dochází k předávání uživatelských rámců na cílový port. Stále jsou zpracovávány zprávy BPDU pro aktualizaci CAM tabulky. [44][46]

8.2 TRILL vs. SPB

TRILL a SPB jsou velice podobné standardy se stejným cílem – nahradit STP. Protokol TRILL (Transparent Interconnection of Lots of Links) byl navržen v roce 2006 avšak nebyl zahrnut do skupiny protokolů IEEE 802.1. Byl přijat řídícím orgánem IETF. Společnosti jako Cisco, Brocade, Juniper také oznámili záměr tuto technologii podporovat. TRILL využívá protokol IS-IS pro získání topologie sítě. K výpočtu vzdáleností a cen cest používá Dijkstrův algoritmus. Upravuje strukturu paketu, přičemž změny jsou zejména v hlavičce,

kde jsou za standardní hlavičkou MAC umístěny informace o navázaných komunikacích mezi uzly TRILL. Bylo přidáno nové pole TTL (Time-to-Live). TRILL staví na myšlenkách technologie Spanning Tree. SPB (Short Path Bridging) používá podobně jako TRILL protokol IS-IS pro výpočet nejkratších cest mezi uzly. V rámci SPB existují dva druhy realizace přemostění: Shortest Path Bridging VLAN (SPBV) a Shortest Path Bridging Mac-in-Mac (SPVM). SPBV používá pro označení dostupnosti uzlu VLAN ID nejkratší cesty. SPBM používá ke stejnému účelu kombinaci páteřní Mac a páteřní VLAN ID.

[38][39][48]

Důvodem pro vznik nového protokolu TRILL, byla časová náročnost přepočtu algoritmu STA při používání STP v síti. Nedostupnost sítě při každé změně byla pro mnohé neúnosná a snažili se tuto situaci vyřešit.

8.3 FabricPath

FabricPath je další technologií snažící se nahradit datovým centrům nevyhovující STP pro jeho časovou náročnost přepínání. FabricPath je vylepšený TRILL od společnosti Cisco. Toto řešení je považováno za řešení, které se vyhýbá STP, a proto se považuje za náhradu STP. FabricPath kombinuje funkce vrstvy 2 a vrstvy 3, čímž spojuje jednoduchost vrstvy 2 a inteligenci vrstvy 3. Je postavena na principu IS-IS a základním protokolem je Ethernet, podobně jako má STP. FabricPath je flexibilní, odolný, jednoduchý a škálovatelný protokol. Je též známý jako směrovací či předávací MAC-in-MAC tunel, protože rámec je zapouzdřen prostřednictvím MAC-in-MAC techniky. FabricPath přináší následující výhody. Má jednoduchou konfiguraci, maximalizuje dostupnost šířky pásma, poskytuje flexibilitu, redundanci a odolnost proti chybám. Dále disponuje tím, že každý přepínač bude mít topologii sítě vypočítanou pomocí Dijkstrův algoritmu a nejkratší trasa mezi počátečním a cílovým směrovačem je vypočtena technikami protokolu IS-IS. Mezi výhody lze zařadit kompatibilita. FabricPath je totiž možné používat pouze na strojích společnosti Cisco. [74]

8.4 VxLAN

Virtual Extensible LAN (VxLAN) je protokol zapouzdření poskytující připojení datového centra pomocí tunelování. V datových centrech je VxLAN nejčastěji používaným protokolem k vytváření překryvných sítí umístěny na vrcholu fyzické sítě a umožňující použití virtuálních sítí. VxLAN řeší virtualizaci sítí datových center a zároveň potřeby segmentaci sítě ve velkém měřítku. Tunelování VxLAN zapouzdřuje rámce Ethernetu vrstvy

2 v paketech UDP vrstvy 3 a tím vytváří virtualizované podsítě (segmenty sítě) vrstvy, které překlenují fyzické sítě vrstvy 3. Každá podsíť je jednoznačně identifikována VNI identifikátorem. Entita provádějící zapouzdření paketů se nazývá VxLAN tunnel endpoint (VTEP), česky koncový bod tunelu VxLAN. Existují hardwarové a softwarové VTEP. Hardwarové VTEP jsou používané v zařízeních typu Bare metal (zařízení pronajímané jedinému nájemci) [75]. V zařízeních typu hypervisor (nájemci sdílí výpočetní výkon zařízení) je použitý softwarový VTEP. [76]

Lze teoreticky vytvořit až 16 milionů VxLAN sítí na rozdíl od VLAN, kterých lze vytvořit maximálně 4094. Tím je umožněno segmentovat síť na velkou množinu podsítí, což podporuje možnost uspokojit velmi vysoký počet nájemců v rámci datových center. Funkce VxLAN umožňují dynamicky přidělovat prostředky uvnitř nebo mezi datovými centry a také migraci virtuální strojů mezi servery.[76]

II. PRAKTICKÁ ČÁST

9 ŘEŠENÍ SÍTĚ

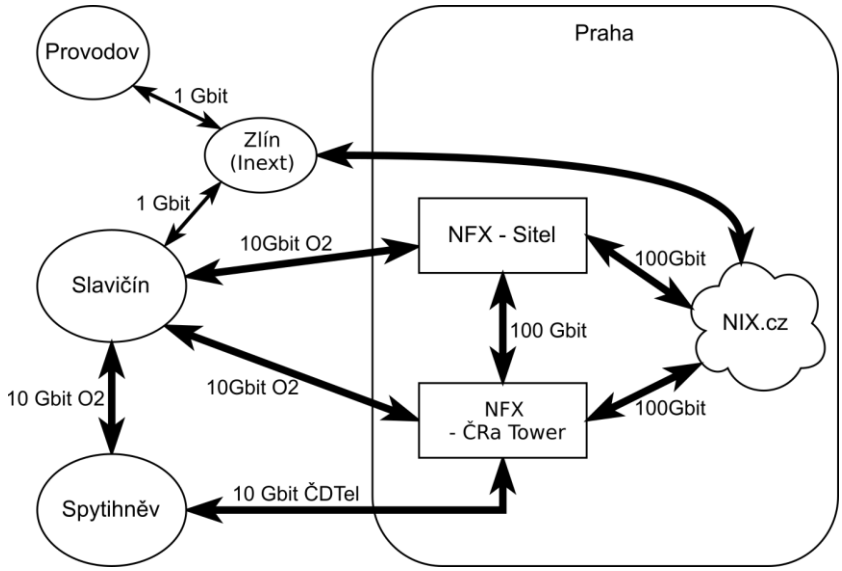
Síť sdružení UnArt Slavičín, která je předmětem této diplomové práce, je připojena do sítě sdružení NFX (Neutral CZFREE eXchange), jehož cílem je vzájemné propojení členských komunitních sítí a jejich společné připojení do sítě Internet. NFX zajišťuje připojení na peeringové centrum NIX.cz. V současné době tvoří NFX 10 spolků či ISP firem. Ve špičkách dosahuje denní provoz tekoucí z NFX 150Gbit/s. [86]

NIX.cz je největší neutrální IXP – Internet eXchange Point v České republice. [87] Do sítě NIX.cz je možno se připojit ze sedmi lokalit (peeringových center) v Praze.

Z naší sítě do NFX jsou vedeny 3 linky o kapacitě 10 Gbit/s, které jsou připojeny do přepínačům s funkcemi směrovačů na geograficky odlišných místech. Přepínače zastávají služby BGP, OSPF a podobně. Ke dvěma přepínačům jsou připojeny dvě brány, realizované jako linuxové stroje s operačním systémem Debian ve verzi 10.9 Buster, které kromě směrování provozují také služby DHCP, NAT a firewall.[86]

9.1 Hardware

Přepínače, které jsou připojeny ke dvěma Linuxovým branám, jsou typu HP 5920. Tato zařízení jsou zvolena kvůli jejich spolehlivosti a kvůli podpoře protokolů, jež mají být v síti implementovány. Podporují přepínací protokoly na vrstvě 2 (ARP, STP, VLAN) a směrovací protokoly na vrstvě 3 (VRRP, RIP, BGP, OSPF, IS-IS). Disponují porty s kapacitou 10 Gbit/s a dokáží směrovat a přepínat až 480 Gbit/s provozu, 367 milionů paketů za vteřinu s latencí menší než 1,7 µs (64 bytové pakety). [89]



Obrázek 11: Schéma připojení do sítě NFX a NIX

Problémem je, že HP 5920 se v dnešní době již neprodává. Dostupné jsou pouze renovované kusy na různých elektrotechnických bazarech. Nástupcem těchto strojů je HP 5510, který může být osazen až 40 gigabitovými porty. Jinak má podobnou specifikaci jako HP5920.

Hlavní brány s OS Linux jsou tvořeny 1U serverovými konfiguracemi s procesorem Intel Xeon Silver 4216 o taktu 2,1 GHz a 16 jádry. Základní deska je osazena 96 GB DDR4 RAM pamětí s frekvencí 2933 MHz. Dále jsou vybaveny SSD disky o kapacitě 480 GB. Základní deska je dále vybavena síťovou kartou s dvěma 10Gb porty SFP+.

Výše uvedené stroje (HP5920, 1U servery s Linuxem) byly pro realizaci této diplomové práce zakoupeny před jejím započetím a pro dané použití plně vyhovují.

Pro vnitřní oblasti sítě jsou ale potřeba ještě jiné typy strojů – s menšími rozměry a menší spotřebou, neboť typické místo pro nasazení jsou rozvaděče na stožárech nebo střechách domů. Na těchto místech, tj. uvnitř sítě, nejsou zatím potřeba drahé prvky s kapacitou >10Gbit/s, většinou stačí prvky s propustností min. 1 Gbit/s. Těchto strojů je ale potřeba násobně větší počet, proto by měly být také levnější než stroje pro hlavní brány sítě.

Pro realizaci této diplomové práce jsme zkoumali možnost použití několika různých zařízení, které takovéto specifikaci vyhovují, zároveň podporují OSPF a také technologii VxLAN. Všechny tato kritéria omezují výběr na několik málo dostupných typů, např.:

- Aruba série 2930 F,
- Cisco řady Catalyst 9300,
- Router Ubiquiti EdgeRouter ER-12P,
- Mikrotik RB4011iGS-RM,
- Mikrotik CCR10XX a CCR2004-1G-12S+2XS,
- PC Engines APU.4D4,
- Mikrotik CRS328-24P-4S+RM

Název zařízení	Cena s DPH	Porty	Spotřeba [W]	Výkon L2/L3	OS	Pozn.
Aruba 2930F 24G 4SPF+	38 407 Kč	24x1Gbps (RJ-45) 4x10Gbps (SFP+)	29.3	182Gbps />45Gbps[4]	ArubaOS	[95] [97]
Cisco C9300-24T	61 341 Kč[2]	24x1Gbps (RJ-45) 8x10Gbps (SFP+)	128	208Gbps /73Gbps[4]	IOS XE	[98] [99] [3]
Ubiquiti EdgeRouter ER-12P	7 191 Kč	11x1Gbps (RJ-45) 2x1Gbps (SFP)	40	33.9Gbps /6,8Gbps[4]	EdgeOS	[100] [101] [3]
MikroTik RB4011iGS+RM	4 391 Kč	8x1Gbps (RJ-45) 1x1Gbps (SFP)	33	2,8Gbps /2,6Gbps[4]	RouterOS	[102] [103] [3]
MikroTik CCR2004-1G-12S+2XS	12 321 Kč	12x10Gbps (SFP+) 2x25Gbps (SFP28)	49	5,9Gbps /5,2Gbps[4]	RouterOS	[104] [108] [3]
PC Engines APU.4D4	3 279 Kč	4x1Gbps (RJ-45)	6-10[5]	>1Gbps[6]	Linux FreeBSD	[105]
MikroTik CRS328-24P-4S+RM	8 535 Kč	24x1Gbps (RJ-45) 4x10Gbps (SFP+)	44	128Gbps /175Mbps[4]	RouterOS	[106] [107][3]

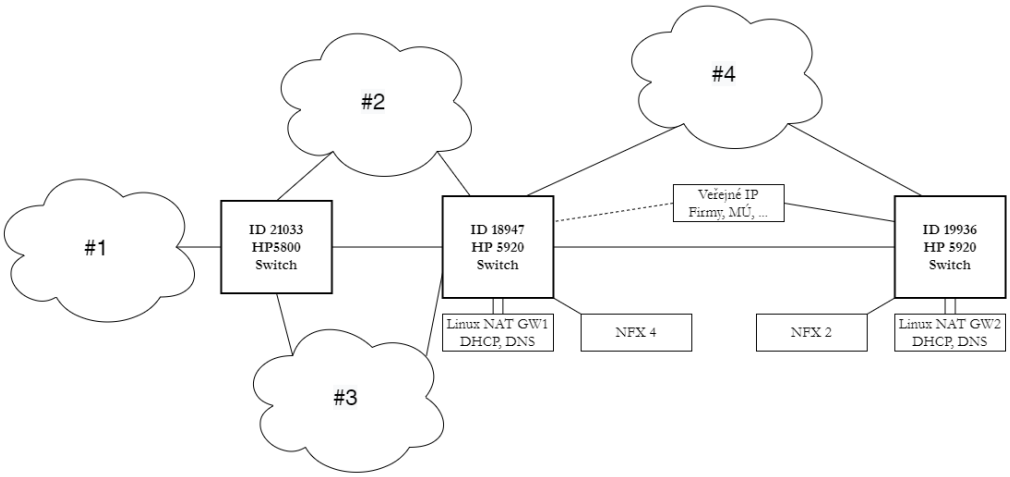
Tabulka 2: Přehled specifikací možných alternativních zařízení

Při realizaci této diplomové práce jsem kromě fyzických strojů pro hlavní brány sítě používal pro experimentální ověření různých protokolů a služeb sítě buď virtuální síť v prostředí VirtualBox s virtuálními routery Linux a MikroTik, nebo fyzické stroje Mikrotik CRS328, které jsem měl při práci volně k dispozici k libovolným experimentům. Jedná se o L3 přepínač, který má 24 gigabitových ethernetových portů s podporou POE+ a Passive POE (26 nebo 53 V) a 4 SFP+ porty. Kapacita přepínání činí 128 Gbit/s, pro směrování bohužel pouze 175-200 Mbps.

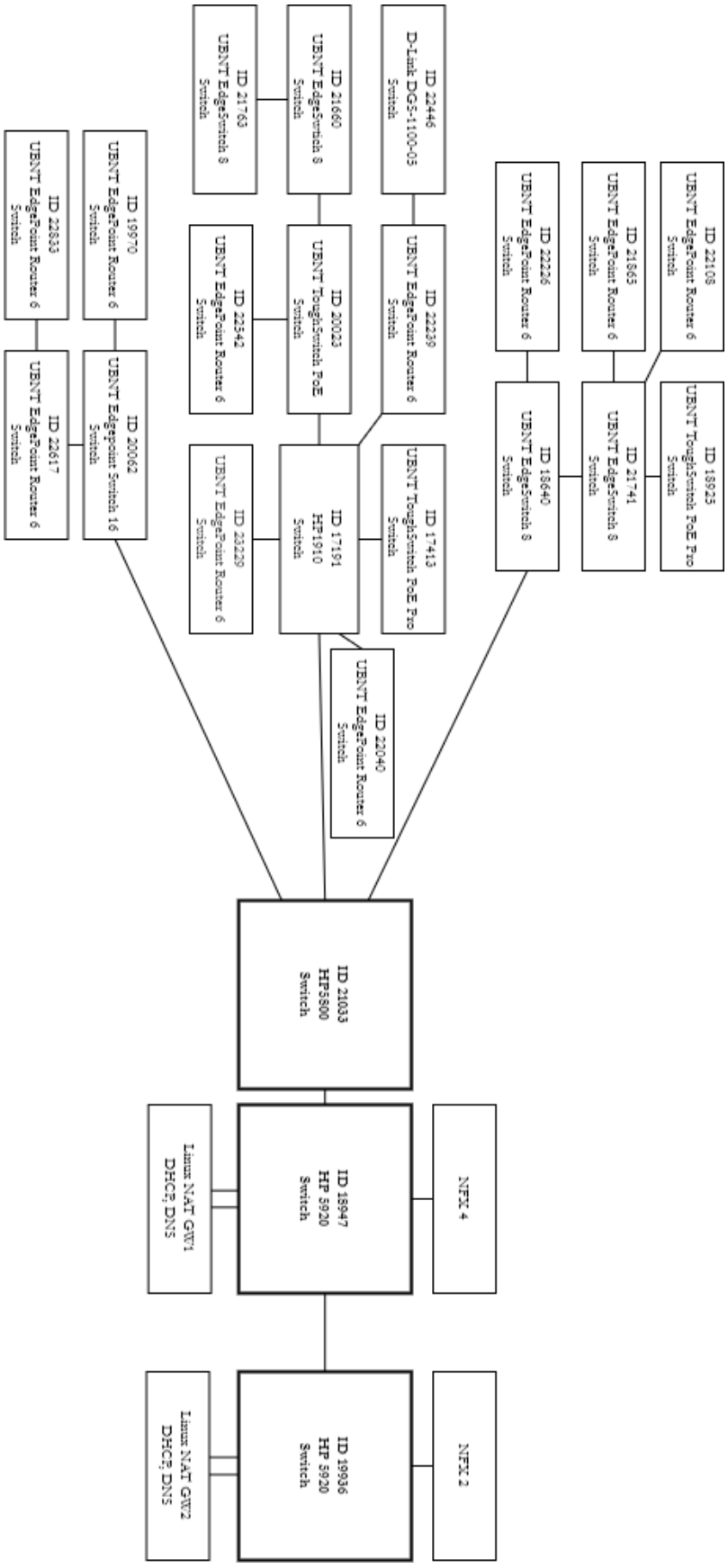
[2] Cena nezahrnuje licence. Cena licence „Network Advantage“ s podporou VxLAN je $1774 na 3 roky.
[3] Disponuje vlastností OSPF Route summarization, která šetří kapacitu routovacích tabulek
[4] Při velikosti paketu 64 bajtů
[5] Dle zatížení CPU
[6] Výrobce přesnější hodnotu neuvádí. Testy rychlostí uživatelů na internetu jsou jen strohé, viz [96]

9.2 Struktura sítě

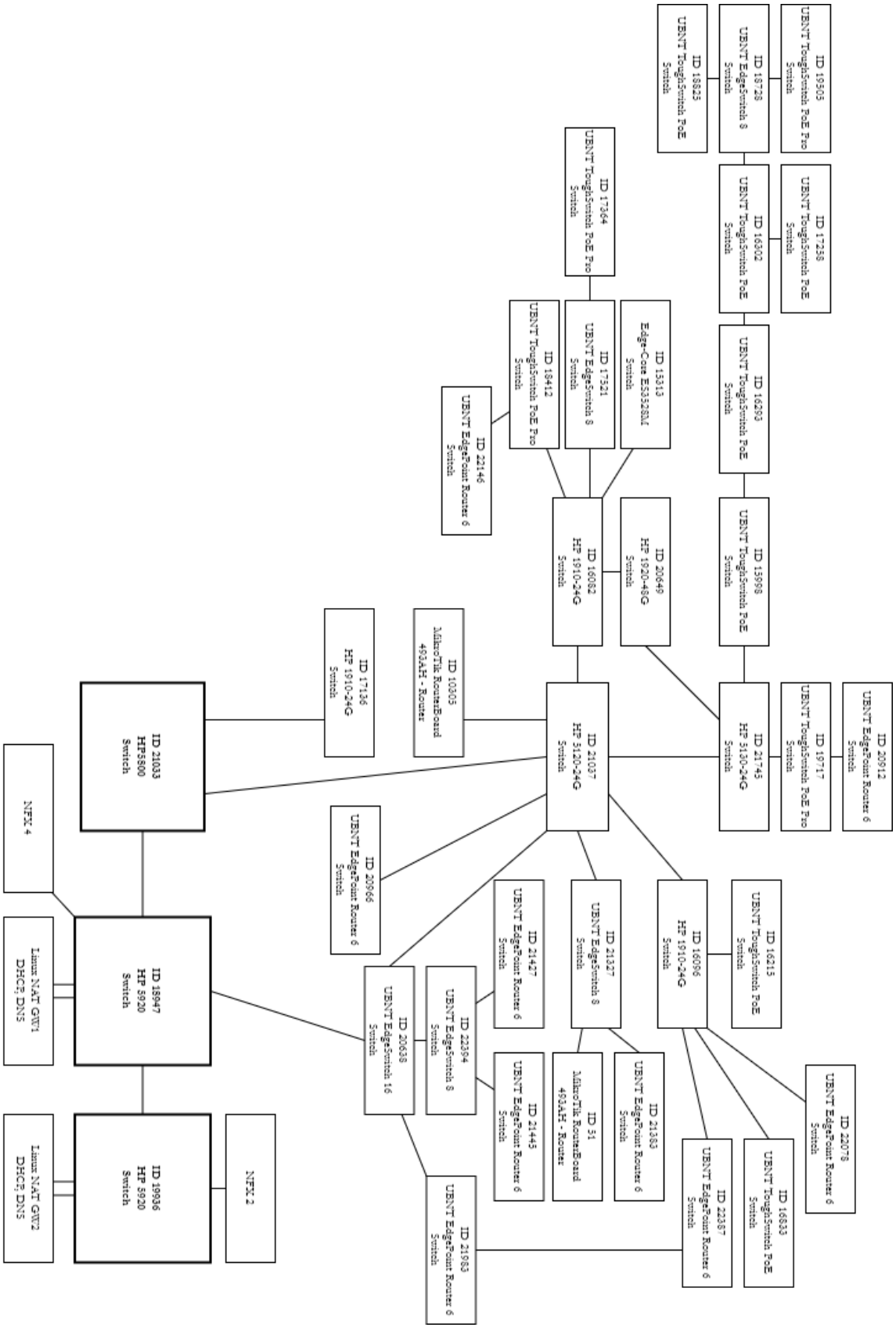
V následujících obrázcích je zobrazeno schéma sítě, která je předmětem této diplomové práce. Pro přehlednost je schéma rozděleno do oblastí #1 (Obrázek 13) – #4 (Obrázek 16) Obrázek 12 zobrazuje páteřní síť propojující jednotlivé oblasti. Bloky NFX 2 a NFX 4 jsou uzly sdružení NFX v Praze.



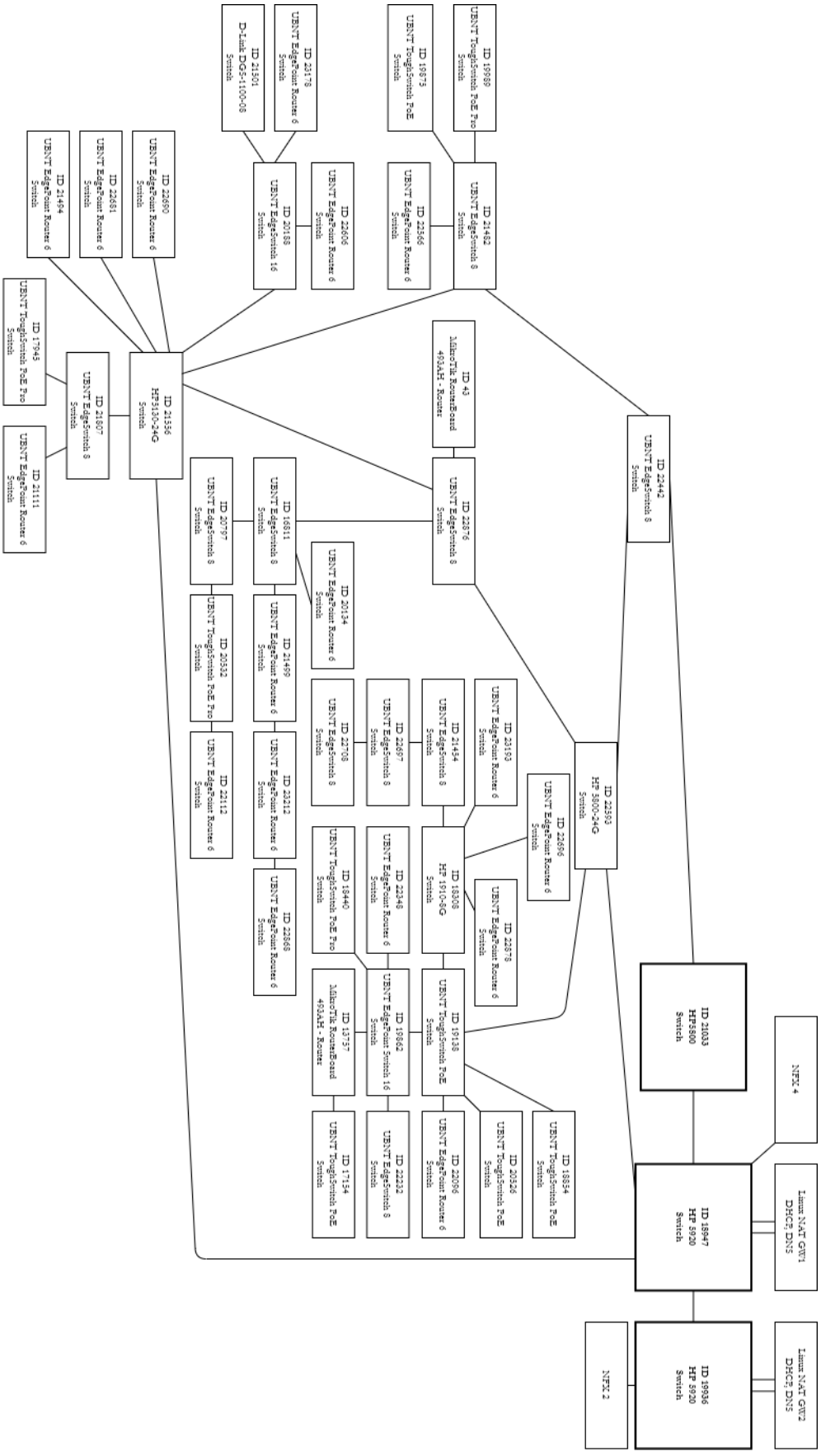
Obrázek 12: Páteř sítě



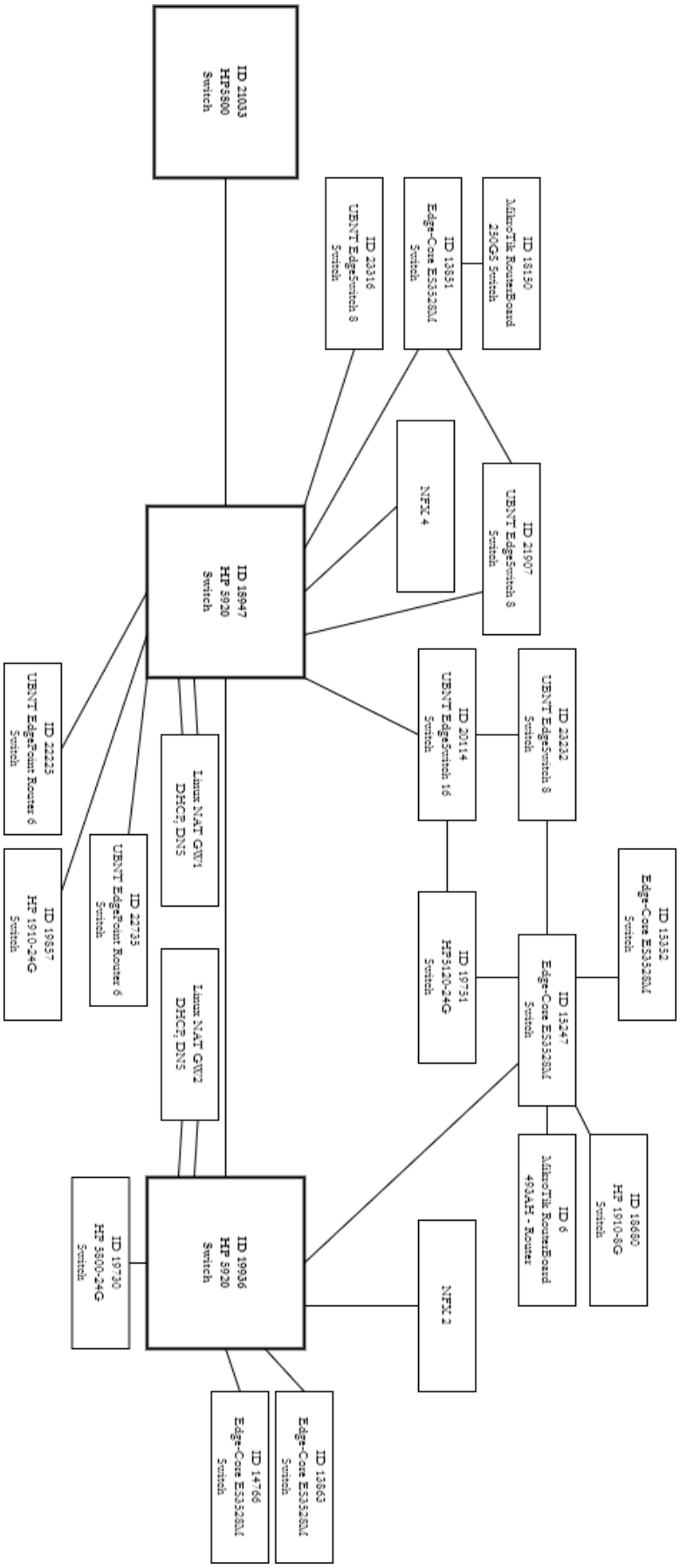
Obrázek 13: Oblast sítě #1



Obrázek 14: Oblast sítě #2



Obrázek 15: Oblast sítě #3



Obrázek 16: Oblast sítě #4

9.3 Firewall

Pro řešení firewallu na linuxových branách je zvoleno řešení založené na subsystému nftables. Jde o subsystém jádra Linuxu, jehož úkolem je filtrovat provoz sítě. Poprvé byl představen v roce 2008 a v roce 2014 byl oficiálně zahrnut do Linux kernelu. Nftables je následovníkem systému iptables, jenž měl stejný úkol. Důvodem k vytvoření nového systému implementující firewall bylo vytvoření jednoduššího a univerzálnějšího řešení, jenž potřebuje v jádře méně kódu a usnadní tak správcům sítě práci díky jednomu univerzálnímu nástroji, který obslouží více typů úkolů. [80]

V následující ukázce je zobrazen výstup po zadání příkazu `nft list ruleset`, který zobrazuje aktuální konfiguraci. Konfigurace nftables sestává z objektů. Nejobecnějším objektem je `table` neboli tabulka. Každá tabulka má definovanou rodinu adres, pro které se její pravidla uplatňují. Rodina adres je definována parametrem napsaným za klíčovým slovem table v definici tabulky. Může nabývat hodnot `ip`, `ipv6`, `inet`, `arp` a `bridge`. Výhodné je použít rodinu `inet`, protože dokáže obsluhovat IP adresy IPv4 i IPv6 a díky tomu není nutné definovat dvě tabulky, pokud je záměrem mít stejná pravidla pro obě skupiny. Za parametrem výběru rodiny IP adres je zapsán název tabulky (v tomto konkrétním případě filter). [81]

Uvnitř tabulky jsou řetězce neboli `chain`, které obsahují jednotlivá pravidla, které správce sítě nastaví. Řetězce jsou dvou typů: `base` a `regular`. Řetězce typu `base` fungují jako vstupní body. Skrze ně vtéká provoz do dané skupiny řetězců a pravidel. `Regular` řetězce nejsou přímo napojeny na rozsah adres a slouží pro přesměrování provozu z jiných řetězců, přičemž musí být na některý `base` řetězec napojen. Každý řetězec `base` musí mít definovaný další typ. Může být typu `filter`, `route` nebo `nat`. Typ `route` slouží k vyhledání cesty pro vyřízení paketu. Typ `nat` definuje pravidla pro překlad adres s využitím subsystému „connection tracking“. Dále musí mít řetězec definován `hook` neboli bod, ze kterého bude do řetězce odkláněn datový tok. Parametr nabývá hodnot `prerouting`, `input`, `forward`, `output` nebo `postrouting`. Poslední vlastností definovanou řetězci je `priority` (priorita). Priorita určuje postup zpracování paketu přes jednotlivá pravidla v daném řetězci.[81]

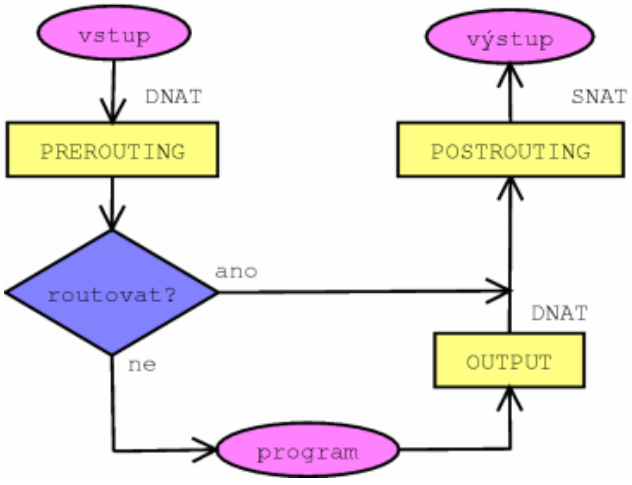
Jednotlivá pravidla definovaná v řetězcích pak jádru slouží pro porovnání každého paketu. Pokud paket odpovídá definovaným pravidlům, je postoupen dále, pokud ne je zahozen. [81]

```
1. table inet filter
2. {
3.     # omezení příchozího provozu NA bránu

1.     chain input
2.     {
3.         type filter hook input priority 0

4.         ct state established,related counter accept
5.         icmp type echo-request counter accept comment "Povolení IPv4
   pingu na bránu"
6.         tcp dport { ssh, bgp } counter accept comment "Povolení SSH a BGP
   na bráně"
7.         iifname $wan counter drop comment "Zakázání přístupu na bránu z
   internetu a CZF"
8.         counter comment "Povolení přístupu na bránu z lokální sítě"
9.         policy accept
10.    }
11.    # omezení provozu PŘES bránu

4.     chain forward

12.    {
13.        type filter hook forward priority 0
14.        ct state established,related counter accept
15.        iifname lo counter accept
16.        oifname $net counter accept comment "Povoleni vše do internetu"
17.        counter comment "Ostatní provoz blokovat"
18.        policy drop
19.    }
20.}
21.
```

Pomocí služby nftables je také realizován NAT (Network Address Translation) neboli překlad adres. Pro přístup k internetu je potřeba mít veřejnou IP adresu. Myšlenkou NAT je umožnit více zařízením s neveřejnou IP adresou přístup k internetu prostřednictvím jedné veřejné IP adresy. Dosahuje se toho překladem neveřejné IP adresy na veřejnou. SNAT ("source NAT") je proces, při kterém se překládá více neveřejných adres na jednu či více veřejných adres zpět: když paket putuje z vnitřní sítě do Internetu, je jeho IP adresa přeložena na veřejnou a pokud putuje do vnitřní sítě, je jeho veřejná IP adresa přeložena na neveřejnou adresu. SNAT může měnit také čísla zdrojových portů. Může se totiž stát, že budou v síti dva hostitelé požadující stejný cíl a stejné číslo cílového portu. Pokud by SNAT provedl pouze překlad IP adresy na veřejnou adresu, kterou by měly oba požadavky stejnou, nebude pak jasné, komu patří odpověď, která dorazí zpět na NAT. Proto jsou čísla zdrojových portů přenastavena na unikátní hodnoty a přidávána do tabulky „connection tracking" pro zpětné rozpoznávání zdrojů požadavků. [83]

Následující ukázka zobrazuje konfiguraci NAT pomocí nftables. NAT se nejčastěji používá ve spojení s IPv4 adresami. Proto je také tabulce v následující ukázce přiřazena rodina IPv4 adres skrz klíčové slovo `nat`. V tabulce je definována mapa s názvem `snat_map`. Tato mapa slouží jako asociativní pole, kde jsou uloženy páry IP adres ve vztahu klíč-hodnota (typ klíče a hodnoty je definován parametrem `type`). V této mapě je definován rozsah adres v parametru `elements`. Pravidla pro překlad adres jsou definována v řetězci typu postrouting, tzn. že je značkování paketů provedeno až po akci směrování viz Obrázek 17. [82][84]

```
1. table ip nat
2. {
3.     # mapování NATu ve formátu vnitřní IP : veřejná IP
4.     map snat_map
5.     {
6.         type ipv4_addr : ipv4_addr
7.         flags interval
8.         elements =
9.         {
10.            "Rozsah IP adres"
11.        }
12.    }
13.    # SNAT
14.    chain postrouting
15.    {
16.        type nat hook postrouting priority 0
17.        oifname $net counter snat ip saddr map @snat_map comment "Vnitřní
   IPv4 adresy z mapy snat_map sNATujeme za jim přiřazené veřejné IPv4
   adresy"
18.        oifname $net counter masquerade comment "Ostatní vnitřní IPv4
   adresy zaNATujeme za veřejnou IP brány"
19.    }
20.}
21.
```



Obrázek 17: Prerouting vs. Postrouting [85]

10 IMPLEMENTACE DHCP

DHCP bylo historicky implementováno jako rozšíření Bootstrap protokolu (BOOTP), který byl používán síťovými klienty k získání IP adresy. Motivací pro rozšíření protokolu BOOTP byla nutnost manuálního zásahu do konfigurace pro přidání informací o připojení každého klienta. BOOTP také neposkytoval mechanismus pro znovuvyužití IP adres. První samostatný DHCP protokol pro IPv4 byl definován v roce 1997 v RFC 2131. Verze DHCPv6 není jen rozšíření DHCPv4 pro adresy IPv6. Jedná se o výrazně odlišný protokol. Například zařízení používající adresy IPv6 může požádat o přidělení více IP adres, což je v DHCPv6 vyřešeno mechanismem delegace předpon (prefix delegation). [42]

V současné době jsou udržovány společností ISC dvě hlavní softwarové řešení DHCP. ISC DHCP server byl původně napsán společností Ted Lemon a Vixie Enterprises pro ISC a sloužil jako referenční implementace nově vzniklého protokolu DHCP. Novější implementace KEA DHCP server je přepracovaná verze ISC DHCP a má postupně nahrazovat stárnoucí ISC DHCP. Obě řešení se řídí standardy IETF a obě jsou open source. [42]

10.1 Architektonická řešení

Pro implementaci DHCP existuje spousta řešení. Tato práce popíše tři možná řešení. Prvním řešením jsou plnohodnotné DHCP servery běžící na lokálních směrovačích v různých částech sítě. Konfigurace pro jednotlivé DHCP servery je generována a průběžně aktualizována informačním systémem pro správu sítě a uživatelů. Řešení je spolehlivé tím, že je DHCP decentralizováno. To znamená, že neexistuje centrální prvek zajišťující služby DHCP serveru, ale existuje více prvků obsluhující danou část sítě. Výhodou je minimalizace počtu dotčených uživatelů při výpadku zařízení poskytující služby DHCP serveru. Pokud lokálně dojde k výpadku zařízení, dotčeni budou uživatelé pouze v dané časti sítě. Nevýhoda je nutnost mít robustní informační systém s generátorem konfiguračních souborů pro jednotlivé DHCP servery. Údržba a/nebo implementace informačního systému, který toto zvládne, může být velmi pracná a komplikovaná, zvláště v heterogenních sítích s mnoha různými typy směrovačů nebo DHCP serverů. Obrázek 18 zobrazuje ukázkovou síť řešenou pomocí lokálních DHCP serverů a IS.

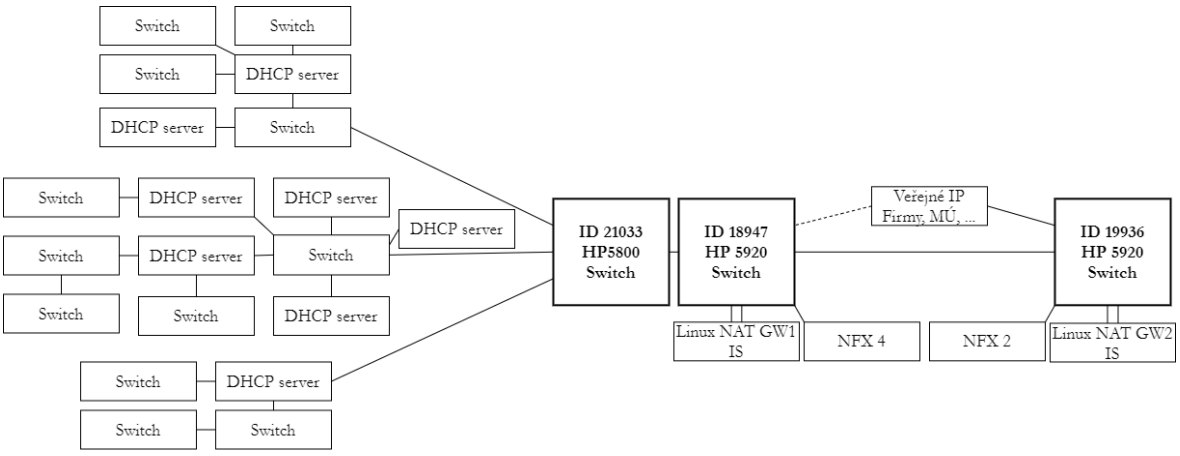
Druhým řešením jsou opět DHCP servery na lokálních směrovačích, avšak se statickými konfiguracemi, tzn. konfigurační soubory DHCP serveru nejsou generovány z IS. Místo toho DHCP servery čerpají data o přiřazení IP adres uživatelům z RADIUS serverů, které mohou

být opět instalovány přímo na lokálních směrovačích nebo na lokálních DHCP serverech. Toto řešení eliminuje nutnost implementovat generátor(y) konfiguračních souborů pro DHCP servery. Nevýhodou je ale různorodost (nebo zcela chybějící) implementace podpory RADIUS serveru v DHCP serverech, např.:

- KEA DHCP server má napojení na RADIUS server implementováno knihovnou „RADIUS Hooks“. Hlavní funkcí knihovny je přijetí paketu DHCP a následné odeslání požadavku na RADIUS server pro ověření autorizace uživatele odeslaného paketu. [78]
- MikroTik má RADIUS klienta jako součást RouterOS. Klient dokáže provádět ověřování připojení skrz HotSpot, PPP, PPPoE, L2TP a ISDN. [77]
- Ubiquiti pro produkt EdgeRouter umožňuje do svého operačního systému EdgeOS instalovat Debian balíčky. Díky tomu je možné do EdgeOS instalovat balíček FreeRADIUS, který kromě RADIUS klienta implementuje i DHCP server. [79]

Dalším řešením je využití mechanismu „DHCP Relay“, který je široce podporován všemi výrobci směrovačů pro použití v páteřních sítích. Všechny směrovače v síti tak mohou být nastaveny do režimu DHCP relay a zprostředkovávat komunikaci DHCP protokolu mezi klienty a jedním nebo více DHCP servery v síti. V této architektuře je nutné mít na zřeteli problém kritického místa poruchy („single point of failure“) centralizovaného DHCP serveru, které lze řešit nasazením více instancí DHCP serverů, nebo implementací vysoké dostupnosti centralizovaného DHCP serveru pomocí VRRP.

DHCP relay je prvek, který slouží jako prostředník mezi klientem a serverem – předává zprávy mezi oběma stranami. Proces, během kterého je klientu dynamicky přiřazena IP



Obrázek 18: Decentralizované řešení DHCP

adresa, se nazývá proces DORA. Během něj jsou odesílány požadavky a potvrzovací zprávy mezi klientem a DHCP serverem v rámci jedné sítě. Přes směrovač do jiné sítě žádná taková zpráva neprojde. Proto pokud není směrovač v síti v roli DHCP serveru ani síťového mostu, musí být nakonfigurován jako DHCP agent, aby předával zprávy procesu DORA do jiné sítě, kde se nachází DHCP server. [47]

10.2 ISC DHCP

První verze ISC DHCP byla vydána v červnu 1998. O rok později byla následována verzí 2.0 a v roce 2001 verzí 3.0. Na verzi 4.0 se čekalo až do roku 2007. V dnešní době jsou všechny verze starší než 4.0 označeny jako EOL (End Of Life). Poslední vydanou verzí je 4.4. O údržbu a vývoj ISC DHCP se staral Ted Lemon a Shawn Routhier. Dnes již není ISC DHCP aktivně vyvíjen. [42]

10.3 ISC KEA DHCP

Původně měla být nová implementace DHCP protokolu součástí aplikačního rámce BIND 10 společně s DNS. A ačkoliv v roce 2014 byla ukončena aktivní práce na části DNS, práce na DHCP části pokračovali dál. Původními vývojáři nové implementace nazvané KEADHCP byli Tomek Mrugalski a Marcin Siodelski, tým se však postupně rozrůstal Nejvýznamnějším rozdílem mezi Kea a ISC DHCP byl závazek vývojářů i implementace rozhraní REST API pro správu. Dále se liší od svého předchůdce novým grafickým panelem zvaným Stork pro správu více DHCP serverů. Jsou zde k nalezení DHCP výpůjčky, rezervace klientů apod. [42]

10.3.1 Implementace

Realizace DHCP je řešena na dvou linuxových hlavních branách, které jsou umístěny v síti. Konfigurační soubory KEA DHCP se po instalaci umístí v linuxovém souborovém systému do složky */etc/kea/*. Hlavním konfiguračním souborem je kea-dhcp4.conf. Obsah souboru zobrazuje následující úryvek kódu. Konfigurační soubor Kea DHCP serveru je ve formátu JSON. Všechny parametry DHCP serveru pro IPv4 adresy jsou umístěny pod značkou Dhcp4 ve složených závorkách. Na pořadí jednotlivých parametrů nezáleží, je však důležité zachovávat syntaxi JSON. To znamená, že je potřeba parametry oddělovat čárkami a za posledním parametrem čárka být nesmí. Dále je potřeba dát pozor na opakující se nastavení parametrů. Pokud je jeden parametr nastaven v souboru vícekrát, z hlediska syntaxe JSON

je to v pořádku. Použita však bude pouze poslední definovaná hodnota, ostatní předchozí budou ignorovány. [43]

První parametry v sekci Dhcp4 jsou globálními parametry. První tři parametry jsou časové v jednotkách sekund. Parametr `valid-lifetime` definuje čas, po který jsou adresy vypůjčeny klientům. Znamená to, že pokud nedojde ke změně, je klient oprávněn používat adresu po dobu 500 sekund. Parametry `renew-timer` a `rebind-timer` definují časy, kdy klient zahájí proceduru obnovení adresy. [43]

Sekce `interface-config` nese parametry týkající se síťových rozhraní, které budou sloužit pro komunikaci serveru s klienty. Parametr `interfaces` je seznam konkrétních síťových rozhraní, na kterých bude server naslouchat. Když je místo konkrétního rozhraní uvedena hvězdička, jakož tomu je v tomto případě, znamená to, že bude server naslouchat na všech dostupných síťových rozhraních. [43]

Kea umožňuje ukládat informace o rezervacích hostitelů do databáze. Pravidla pro ukládání těchto informací jsou definována v sekci `hosts-database`. Podporované typy databází jsou MySQL, PostgreSQL a Cassandra. Rezervace také můžou být uloženy v samostatném konfiguračním souboru, což je doporučený postup v případě malého počtu obsluhovaných klientů. Lze využít i kombinaci obou způsobů. Pokud jsou klienti definováni na obou místech, je prvně zkontrolován obsah konfiguračního souboru, poté obsah externího úložiště. Pro připojení k databázi je potřeba definovat typ databáze (parametr `type`), název databáze (parametr `name`), jméno a heslo uživatele (parametry `user` a `password`). V parametrech `host` a `port` definovat adresu a port databáze, a nakonec omezení na počet pokusů připojení a čas, po který se bude čekat na znovu připojení (parametry `max-reconnect-tries` a `reconnect-wait-time`). Tímto způsobem může být definováno více databází. Budou se procházet v pořadí, v jakém budou definovány v konfiguračním souboru.

Všechny vypůjčené adresy se ukládají do databáze výpůjček definované v sekci parametrů `lease-database`. Možnosti jsou totožné jako u definování databáze rezervací adres klientů. Opět je možné definovat soubor, ve kterém budou uloženy informace o výpůjčkách nebo definovat připojení na podporovanou databázi. [43]

Sekce parametrů `expired-leases-processing` definuje periodické zjišťování uvolněných adres a jejich zpětné získávání. Tímto procesem jsou položky v databázi výpůjček upraveny či smazány. Během toho procesu server přestane přijímat příchozí zprávy DHCP, aby nedocházelo ke kolizím současného přístupu i informacím v databázi. Tím dojde k výpadku

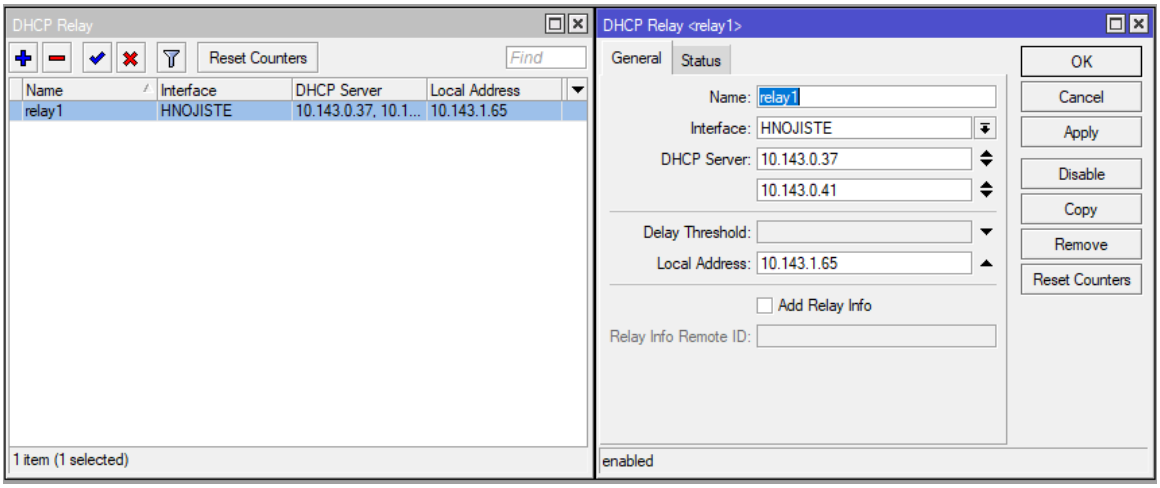
služby serveru, což není ideální řešení. Proto jsou definovány konfigurační parametry pro řízení frekvence cyklů rekultivace adres k minimalizaci přerušení služby serveru. Parametrem `reclaim-timer-wait-time` je definován čas, po který server čeká mezi jednotlivými rekultivačními cykly. Během této doby server zůstává aktivní pro odpovědi na DHCP dotazy. Parametr `hold-reclaim-time` nastavuje počet sekund po vypršení platnosti adresy pro její zdržení v databázi k opětovnému přiřazení stejnému klientovi. Pro pravidelné odebírání výpůjček, u nichž vypršel čas pro zdržení v databázi, slouží parametr `flush-reclaim-timer-wait-time`. Pokud je nastaven na 0 jakož je to tomu v tomto případě, jsou odstraněny hned, jakmile jim vyprší čas zdržení. [43] Parametr `max-reclaim-leases` slouží pro nastavení maximálního počtu najednou odbavovaných rekultivovaných výpůjček. `Max-reclaim-time` definuje maximální čas, který může rekultivace výpůjčky trvat. Může se stát, že server nebude díky nastavení schopen získat všechny výpůjčky dříve, než vyprší jejich čas zdržení v databázi a poté nebude mít co přiřadit novým klientům. Server na tento problém může správce sítě upozornit, pokud je nastaven parametr `unwarned-reclaim-cycles`. [43] V konfiguraci pro síť, jež popisuje kapitola 9, je databáze výpůjček a rezervací řešena prostřednictvím generovaného souboru z informačního systému společnosti a není realizováno napojení na databázi. Výše uvedený text má za úkol demonstrovat možnosti ISC KEA DHCP serveru.

Další sekcí parametrů je `subnet4`, v níž se definují parametry pro podsítě. Server tyto informace používá ke zpracování požadavků klientů. Definují se zde pravidla pro všechny podsítě, ze kterých se očekává, ze kterých bude server vyřizovat požadavky DHCP. Tato sekce je seznamem podsítí, které jsou samostatně uzavřeny ve složených závorkách, celý seznam je uzavřen v hranatých závorkách. Každá podsíť musí mít definován rozsah adres, ze kterých může přiřazovat adresy v parametru `pool`, a v parametru `subnet` definici konkrétní podsítě ve formátu adresa sítě/prefix. Parametrem `reservation-mode` je definován typ rezervace. Každý typ rezervace má různá omezení kontrol, které server provádí při přiřazování nebo obnovování výpůjčky pro klienta. V tomto konkrétním případě se jedná o typ `all` – povoluje všechny typy rezervací klientů (nejstabilnější a nejbezpečnější řešení). Dalšími možnostmi jsou `out-of-pool`, `global` a `disabled`. Ostatní nastavovací parametry podsítí jsou umístěny v podsekci `option-data`. Parametry zde umístěné jsou volitelné. [43]

```
root@gw1:~# cat /etc/kea/kea-dhcp4.conf
{
 "Dhcp4":
  {
    "valid-lifetime": 500,
    "renew-timer": 100,
    "rebind-timer": 250,
    "server-tag": "all",
    "interfaces-config":
          {
      "interfaces": ["*"]
    },
    "hosts-database": {
      "type": "mysql",
      "name": "",
      "user": "",
      "password": "",
      "host": "",
      "port": 3306,
      "readonly": true,
      "max-reconnect-tries": 10000,
      "reconnect-wait-time": 30000
    },
    "lease-database": {
      "type": "mysql",
      "name": "",
      "user": "",
      "password": "",
      "host": "",
      "port": 3306,
      "max-reconnect-tries": 10000,
      "reconnect-wait-time": 30000
    },
    "expired-leases-processing": {
      "reclaim-timer-wait-time": 3,
      "flush-reclaimed-timer-wait-time": 0,
      "hold-reclaimed-time": 3600,
      "max-reclaim-leases": 100,
      "max-reclaim-time": 50,
      "unwarned-reclaim-cycles": 10
    },
    "host-reservation-identifiers": [
      "hw-address",
      "duid"
    ],
    "control-socket": {
      "socket-type": "unix",
      "socket-name": "/tmp/kea4-ctrl-socket"
    },

    "hooks-libraries": [{
      "library": "/usr/lib/x86_64-linux-
   gnu/kea/hooks/libdhcp_lease_cmds.so"
    }],

    "subnet4": [{
      "subnet": "10.143.122.0/25",
      "reservation-mode": "all",
      "id": 167,
```

```
      "pools": [{
        "pool": "10.143.122.2 - 10.143.122.123"
      }],
      "option-data": [{
        "name": "routers",
        "data": "10.143.122.1"
      }, {
        "name": "domain-name-servers",
        "data": "10.143.122.1,10.143.128.1,10.143.128.2"
      }]
    }, {
      "subnet": "10.143.122.128/25",
      "reservation-mode": "all",
      "id": 425,
      "pools": [{
        "pool": "10.143.122.130 - 10.143.122.251"
      }],
      "option-data": [{
        "name": "routers",
        "data": "10.143.122.129"
      }, {
        "name": "domain-name-servers",
        "data": "10.143.122.129,10.143.128.1,10.143.128.2"
      }]
    }]
  }
}
```

10.4 Implementace DHCP relay



Obrázek 19: Konfigurace DHCP relay

Jelikož pro nasazení OSPF protokolu, které je popsáno v kapitole 13, je potřeba mít v síti směrovače a v řešení sítě se počítá se dvěma (nebo více) hlavními DHCP servery, je také potřeba na směrovačích implementující OSPF nakonfigurovat DHCP relay (DHCP agent). Úkol DHCP relay je popsán v kapitole 10.1. Implementace DHCP relay je v dalším textu demonstrována na prvcích MikroTik, na prvcích jiných typů bude nastavení podobné.

Konfigurační prostředí Mikrotik Winbox zobrazuje Obrázek 20. V sekci IP se nachází pole DHCP relay, kde se konfiguruje konkrétní nastavení. Je potřeba založit nový DHCP relay pomocí tlačítka + a poté přiřadit správné rozhraní a adresy DHCP serverů, na které se má relay odkazovat. V našem příkladě používáme 2 DHCP servery, může jich být samozřejmě přidáno i více. Prostředí konfigurace DHCP relay ukazuje Obrázek 19.

11 VRRP – KEEPALIVED

Pro implementaci protokolu VRRP bylo zvoleno SW řešení Keepalived. Keepalived je nástroj určený pro realizaci vyrovnávání zatížení (load balancing) a pro realizaci vysoké dostupnosti (high availability). V této implementaci je nástroj využit pro řešení vysoké dostupnosti s využitím protokolu VRRP. Hlavními poskytovanými úkoly jsou failover[7], instance synchronization[8] nice fallback, integrita paketu a systémové volání[9].[60]

Instalace balíčku v linuxovém prostředí je poměrně snadná: `apt-get install keepalived`. Pak už je potřeba pouze konfigurovat. Hlavní konfigurační soubor `keepalived.conf` je v linuxovém souborovém systému umístěn v `/etc/keepalived/.` Konfigurační soubor se v podstatě skládá ze sekcí, jenž každá představuje konfiguraci pro jednu VRRP instanci začínající klíčovým slovem `vrrp_instance` a názvem konkrétní instance. Konfigurace instance je uzavřena do složených závorek. Klíčovým slovem `state` je označen parametr pro definování typu instance. Může nabývat hodnoty `MASTER` (instance je zodpovědná za předávání paketů) a `BACKUP` (instance předává pakety tehdy, když je master instance nedostupná). Parametrem interface je definováno fyzické či logické rozhraní, na kterém má instance běžet. Parametr `virtual_router_id` definuje identifikátor VRRP směrovače, který náleží instanci. Pokud v jedné síti poběží dva VRRP směrovače typu master, jako primární bude nastaven ten, který bude mít vyšší číslo v parametru `priority`. [60]

[7] Záložní provozní režim, kdy sekundární zařízení převezme funkce [59].
[8] Monitorování stavu mezi dvěma instancemi VRRP – zaručení stejného stavu dvou instancí – vzájemně se sledují.
[9] Externí skript či programu během přechodu stavu VRRP.

```
root@gw1:~# cat /etc/keepalived/keepalived.conf
vrrp_instance vlan702 {
    state MASTER
    interface vlan702
    virtual_router_id 1
    priority 200

    use_vmac vrrp702
    vmac_xmit_base

    virtual_ipaddress {
        10.143.122.129
    }
}

vrrp_instance vlan3905 {
    state MASTER
    interface vlan3905
    virtual_router_id 1
    priority 200

    use_vmac vrrp3905
    vmac_xmit_base

    virtual_ipaddress {
        10.143.1.1
    }
}

vrrp_instance vlan3955 {
    state MASTER
    interface vlan3955
    virtual_router_id 1
    priority 100

    use_vmac vrrp3955
    vmac_xmit_base

    virtual_ipaddress {
        10.143.1.33
    }
}
```

12 IMPLEMENTACE DNS

Implementace DNS je realizována, podobně jako DHCP, na obou linuxových hlavních branách, které jsou v síti umístěny. Pro implementaci DNS bylo zvoleno open-source řešení BIND 9. Jedná se o nejčastěji nasazované řešení DNS serverů. Alternativami můžou být řešení KNOT nebo PowerDNS. Bind je řešení otevřené uživatelům, kteří chtějí přispívat novými funkcemi. Je to možné prostřednictvím otevřeného GitLabu. V rámci implementace je řešen pouze rekurzivní server. Hlavními konfiguračními soubory jsou `named.conf.local` a `named.conf.options` umístěné ve složce `/etc/bind/` linuxového souborového systému. [64]

12.1 Instalace

Před instalací balíčku Bindu 9 je potřeba pro využití nových funkcí povolit v Linuxu stahování z backportů (využití schválených částí balíčků, které se ještě nedostaly do oficiální produkce). Je to uskutečněno pomocí příkazu `deb http://deb.debian.org/debian buster-backports main` a poté `apt-get update`.

Instalace balíčků Bindu probíhá spuštěním příkazu `sudo apt install bind9/buster-backports bind9utils/buster-backports bind9-doc/buster-backports`. Poté je potřeba nastavit Bind pro IPv4, tím že se v souboru /etc/default/bind9 nastaví hodnota parametru `OPTIONS` na "`-u bind -4`". Následně je nutné službu Bind restartovat prostřednictvím příkazu `sudo systemctl restart bind9`. Pak je již možné přistoupit k samotné konfiguraci.

12.2 named.conf.local

Následující úryvek zobrazuje konfigurační soubor `named.conf.local`. Zde jsou konfigurovány lokální DNS zóny, konkrétně pro domény místní sítě *slavicin.unart.czf* a *slfree.czf*. Odkazuje se na autoritativní server umístěn v síti. Zóna je definována pomocí klíčového slova `zone` a názvu dané domény. Parametry zóny jsou uzavřeny do složených závorek. Zóna nese parametry `type`, `forward` a `forwarders`. Typ zóny může nabývat hodnot master, slave, stub, forward a hint. Zóna typu master má hlavní kopii dat a bude schopna poskytovat autoritativní odpovědi. Slave zóna je replikou hlavní zóny. V parametru `masters` má seznam IP adres master zón pro kontaktování, aby si mohla aktualizovat data podle hlavních zón. Stub zóna je podobná jako `slave` zóna, ale replikuje pouze NS záznamy hlavní zóny. Forward zóna se používá k přesměrování všech dotazů na jiné servery. Specifikace adres serverů je v parametru `forwarders`. Pokud je seznam prázdný, nebude provedeno

žádné přeposlání. Hint zóna slouží jako nápověda pro určení sady kořenových serverů. [64][65]

Parametr `forward` má smysl pouze tehdy, když se jedná o zónu typu `forward`. Hodnota `only` zapříčiní že vyhledávání selže, pokud není žádný ze serverů v seznamu `forwarders` dostupný. Parametr může též nabýt hodnoty `first`, což znamená že je umožněno i normální vyhledávání.[65]

```
root@gw1:~# cat /etc/bind/named.conf.local
// lokalni zony
// pouze je presmerovavame na nas autoritativni DNS server

// zona slavicin.unart.czf
zone "slavicin.unart.czf" {
    type forward;
    forward only;
    forwarders {
        10.143.126.9;
    };
};

// zona slfree.czf
zone "slfree.czf" {
    type forward;
    forward only;
    forwarders {
        10.143.126.9;
    };
};

// rekurzivni zona pro rozsah 10.143.0.0/16
zone "143.10.in-addr.arpa" {
    type forward;
    forward only;
    forwarders {
        10.143.126.9;
    };
};

// RPZ zona pro omezeni hazardnich her
zone "rpz.cesnet.cz" {
    type slave;
    masters {
        2001:718:1:101::144:228;
        195.113.144.228;
    };
    file "rpz.cesnet.cz";
};

```

12.3 RPZ zóna

V předchozím úryvku z konfiguračního souboru `named.conf.local` byla konfigurována zóna RPZ. Jedná se o zóny, které blokují přístup k nepovoleným hazardním webům. Tato blokace vychází ze zákona č. 186/2016 Sb. o hazardních hrách, který ISP (poskytovatelům internetu) nařizuje blokovat přístup k webům uvedených na seznamu nepovolených her vydaného 26. 7. 2017. Blokace pomocí DNS není náročná na prostředky a způsobené vedlejší škody jsou jen minimální. Běžným řešením pro blokaci určitých domén je technologie RPZ – Response Policy Zone. Je to speciální zónový soubor obsahující místo obyčejných DNS odpovědí instrukce k blokování (popřípadě změnění) odpovědí DNS serveru. Sdružení CESNET vytvořilo k těmto účelům veřejnou zónu rpz.cesnet.cz. Blokované domény jsou nahrazovány v DNS odpovědích adresou serveru *poker.cesnet.cz*. Web vrací stavový kód HTTP 451 – Nedostupné z právních důvodů. Tento typ HTTP stavového kódu byl standardizován kvůli těmto účelům. [66]

Při používání veřejné zóny sdružení CESNET je v konfiguraci Bindu zapotřebí vytvořit zónu typu `slave`. V parametru `masters` jsou IP adresy na master zónu. Dále je vhodné v parametru `file` specifikovat název souboru. Pokud je soubor zadán, replika se zapíše do tohoto souboru při každé změně zóny a při případném restartu serveru se načte z tohoto souboru. Ušetří se čas při startu serveru a eliminuje se přenos dat.[65] [66]

12.4 named.conf.options

Následuje úryvek z konfiguračního souboru `named.conf.options`. Klíčové slovo `options` obsahuje parametry pro nastavení globálních možností. Tato sekce se může v konfiguraci bindu objevit pouze jednou. Pokud je definována víckrát, je zahlášeno varování a v potaz se bude brát první definice. Naopak pokud tento blok parametrů chybí, jsou použity výchozí hodnoty. Prvním použitým parametrem je directory sloužící pro nastavení pracovní složky serveru. Hodnotou by měla být absolutní cesta adresáře určeného pro DNS server. Pokud adresář není zadán, použije se cesta, ze které byla služba spuštěna. Parametrem `allow-recursion` se určuje seznam IP adres, který říká, jací hostitelé mají povolenou provádět rekurzivní dotazy prostřednictvím tohoto serveru. Pokud není vyplněn, je to povoleno všem. Parametrem `validate-except` je určen seznam domén, pod kterými se nemá provádět ověření DNSSEC. Parametr `response-policy` definuje seznam povolených názvů RPZ. [67][68]

```
root@gw1:~# cat /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";
        dnssec-enable yes;
        dnssec-validation auto;
        dnssec-lookaside auto;
        listen-on-v6 { any; };

        allow-recursion {
                127.0.0.1;
                10.143.0.0/16;
                5.104.16.0/21;
                ::1;
                2a05:2100::/29;
        };

        validate-except {
                slavicin.unart.czf;
                slfree.czf;
        };

        response-policy {
                zone "rpz.slavicin.unart.cz";
                zone "rpz.cesnet.cz";
        };
};

```

13 IMPLEMENTACE OSPF

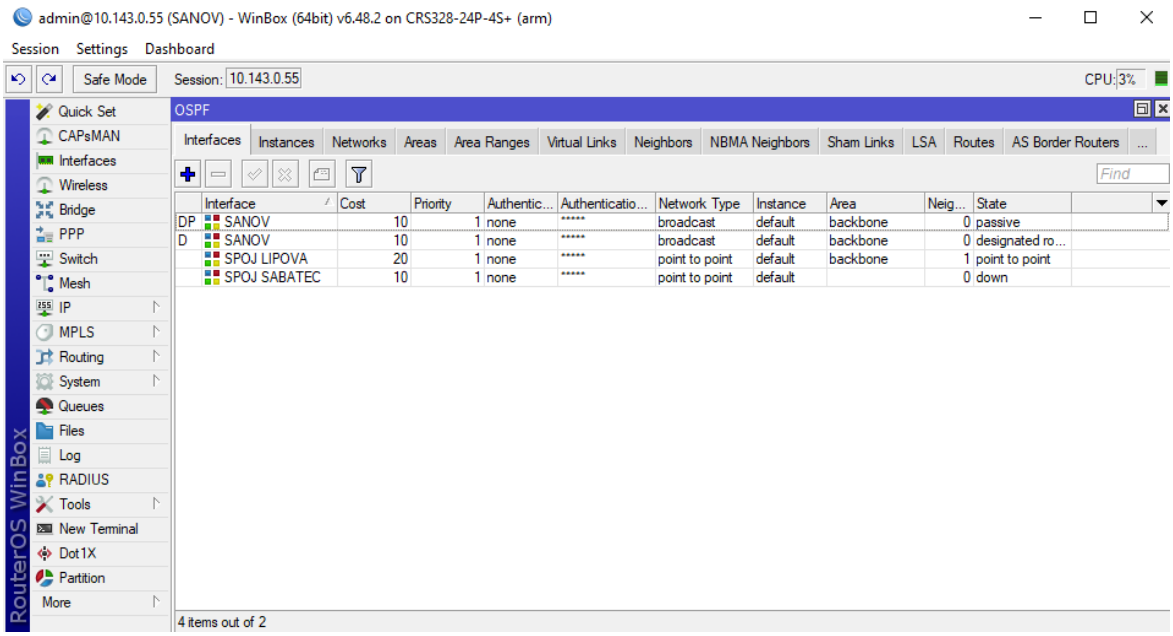
Nasazení dynamického směrování pomocí OSPF je vhodné v těch uzlech sítě, kde existuje více než jedna cesta směrem k hlavní bráně, takže v případě poruchy jedné trasy zajistí OSPF automatické směrování jinou funkční trasou. V takových uzlech může/musí být instalován směrovač s dostatečným výkonem a schopností OSPF směrování – viz kapitola 9.1.

V následujícím textu ukážu konfiguraci OSPF na přepínači/směrovači MikroTik CRS328, který v dnešní době dostačuje již jen pro okrajové, méně vytížené uzly sítě, protože při směrování poskytuje na dnešní poměry malou propustnost (mezi 200-300Mbit/s).

Konfigurace zařízení MikroTik je realizována prostřednictvím aplikace WinBox. Ukázku prostředí zobrazuje Obrázek 20.

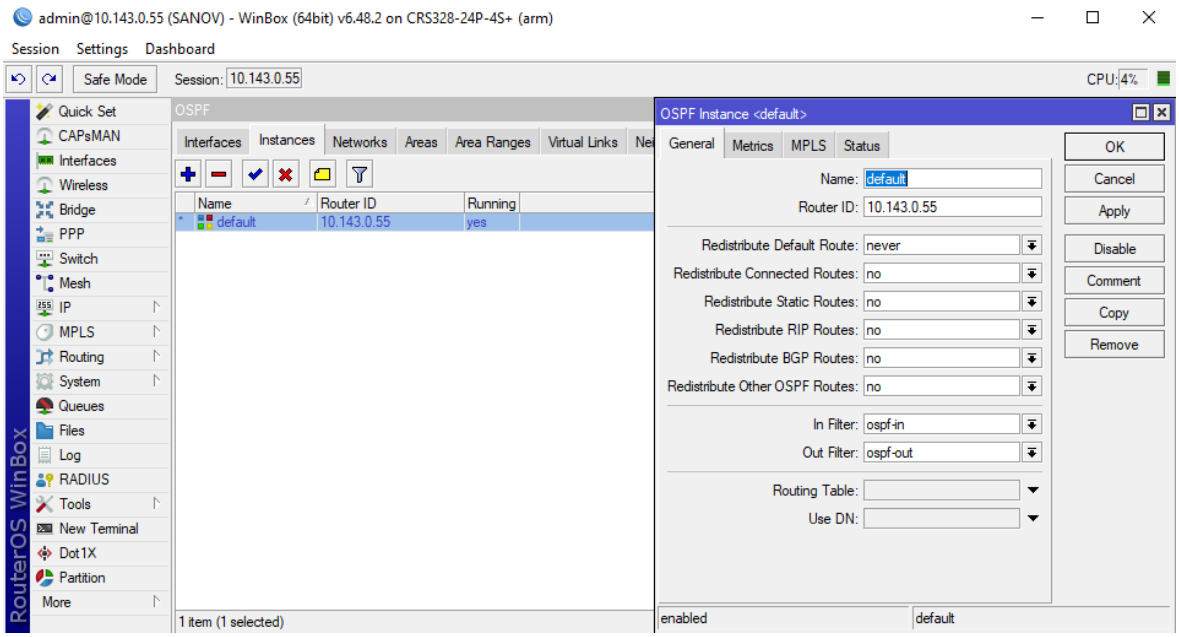
Obrázek 20: Ukázka prostředí konfigurace MikroTik

Konfigurace OSPF se nachází v sekci Routing, společně s BGP, RIP a dalšími směrovacími protokoly. V následujícím obrázku je zobrazeno okno konfigurace OSPF.



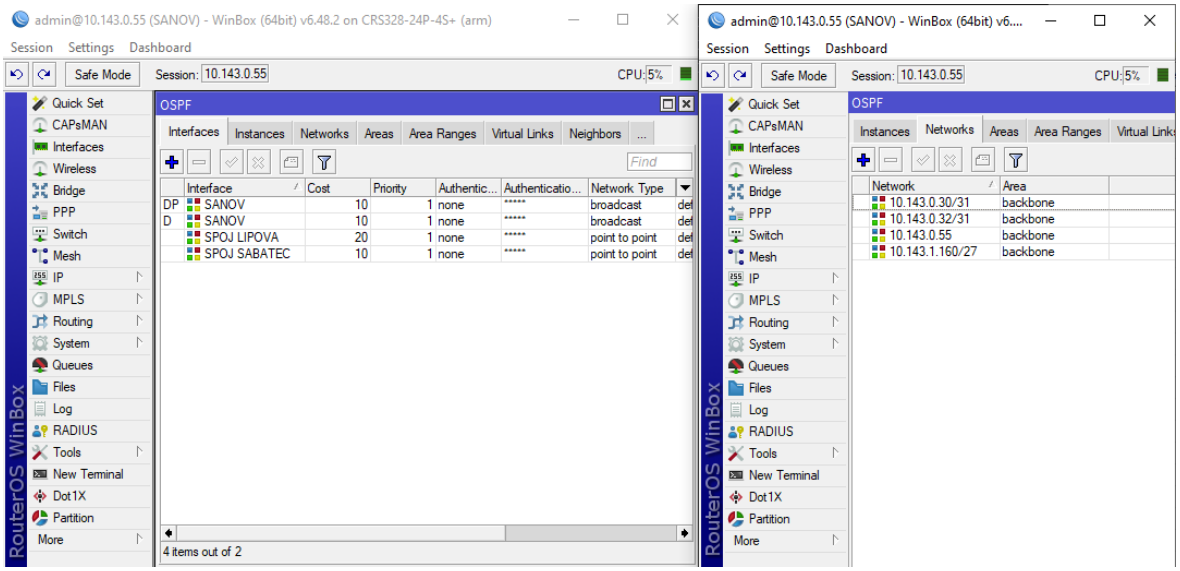
Obrázek 22: Konfigurace OSPF

V konfiguraci OSPF jsou zásadní záložky Interfaces, Instances, Networks a Areas. V první řadě je potřeba definovat instanci v záložce Instances. Zde je již v základní konfiguraci vytvořena jedna instance. Této instanci je potřeba nastavit RouterID. RouterID má tvar IP adresy a v tomto případě je i hodnota stejná jako IP adresa.



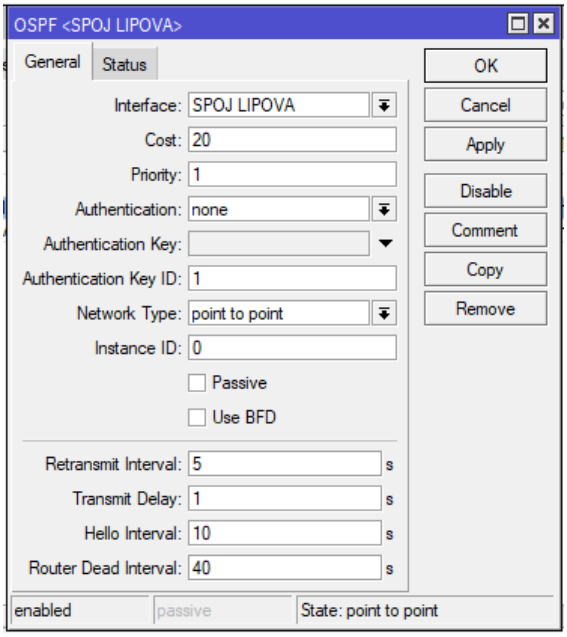
Obrázek 21: Konfigurace instance

Dále je potřeba mít definovanou Areu v sekci Area. V základní konfiguraci je již vytvořená, je pojmenována Backbone a není nutné ji pro základní potřeby měnit. V sekci Network se



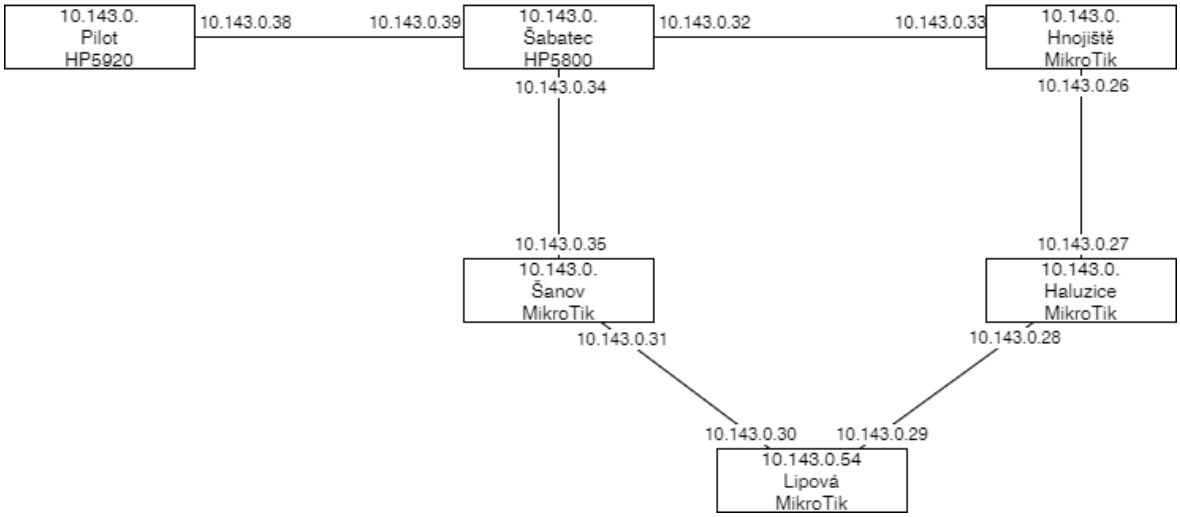
Obrázek 24: Konfigurace Networks a Interfaces

definují adresy sítí. Každá síť musí mít definovanou adresu sítě a areu, do které patří. V této konkrétní konfiguraci jsou definovány sítě 10.143.0.30/31 a 10.143.0.34/31 pro propojení



Obrázek 23: Konfigurace rozhraní

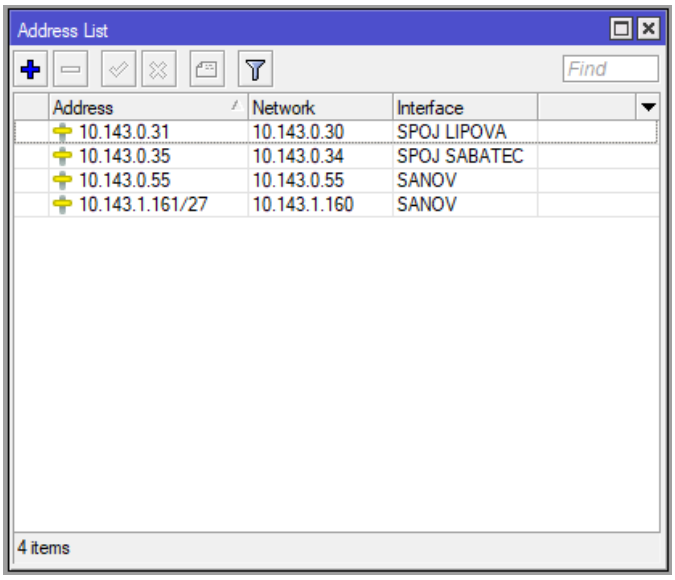
sousedních OSPF směrovačů a síť 10.143.1.160/27 pro adresy připojených klientů. Na základě definic adres sítí se vygenerují definice rozhraní v záložce Interfaces. Zde je však problém s tím, že se vygenerují rozhraní s typem sítě broadcast, což pro sítě s maskou 31 nelze použít, jelikož nemají broadcastovou adresu. Proto je potřeba rozhraní duplikovat, po



Obrázek 25: Schéma sítě – prvky OSPF

čemž v něm lze nastavit typ sítě (Network Type) na point to point. Dále se na rozhraní definuje cena (cost) za průchod provozu. Provoz bude upřednostňovat cesty přes rozhraní s nižší cenou. Naopak je to u priorit, kdy provoz upřednostní rozhraní s vyšší prioritou. Je také důležité mít nastaveny IP adresy z rozsahu sítí definovaných v OSPF. Konkrétně v tomto případě jsou nastaveny adresy 10.143.0.30 pro spoj s Haluzicemi a 10.143.0.34 pro spoj s Šanovem. Adresa 10.143.0.161 je z rozsahu pro klienty, pro které tato adresa slouží jako brána – gateway.

Předchozí ukázky nastínily konfiguraci OSPF na jednom zařízení MikroTik. Konfiguraci je potřeba provést na každém zařízení smyčky OSPF. Obrázek 25 zobrazuje schéma prvků, na kterých je OSPF provozováno



Obrázek 26: IP adresy

14 BGP

BGP je realizováno na strojích HP 5920, které využíváme především pro připojení do pražských uzlů sítě sdružení NFX. Dva tyto stroje se starají o dva 10GbE okruhy do uzlů NFX2 (CE Colo, býv. Sitel) a NFX 4 (vysílač ČRa Tower – Žižkov). Třetí 10 GbE okruh je propojuje Slavičín a Spytihněv, odkud vede další 10GbE okruh do uzlu NFX2.

Následující ukázka konfigurace je zobrazena v OS HPE Comware pomocí příkazu `display current-configuration configuration bgp`. Nejprve je potřeba definovat seznam předpon adres pro filtrování odchozích tras. Je to provedeno příkazem `ip ip-prefix`, jak je zřetelné na začátku ukázky. V dalším odstavci je pomocí příkazu `route-policy` definována politika směrování. Je to základní nástroj BGP a lze jej využít ke konfiguraci zásad směrování BGP nebo k filtrování tras. V tomto konkrétním případě se definované politiky odkazují na IP předpony nad nimi nastavené. [90]

Poté je pomocí klíčového slova `bgp` a čísla AS definováno nové nastavení BGP spojení. Číslo AS je přiděleno od správcovské organizace, jak popisuje kapitola 2. Pro každé zařízení, které je do BGP konfigurováno, musí mít nastavené `router-id`, které musí být v rámci BGP jedinečné, proto se často využívá jeho veřejné IP adresy. Důležité je nastavit rozsah spravovaných IP adres v parametru `network`. Pro připojení do sítě NFX je vytvořena skupina `NFXPUB` pomocí parametru `group`. Skupiny je vhodné vytvořit tehdy, kdy je realizováno dva a více propojů do jiné sítě, což odpovídá tomuto případu. Příkazem `peer NFXPUB as-number` a číslo sousedního AS je definováno připojení k síti NFX.

```
1. ip ip-prefix DEFAULT index 10 permit 0.0.0.0 0
2. ip ip-prefix UNARTPUB index 5 permit 5.104.16.0 21 less-equal 32
3. ip ip-prefix UNARTPUB index 15 permit 185.69.70.0 23 less-equal 32
4.
5. route-policy NFXPUB-in permit node 10
6.     if-match ip-prefix DEFAULT
7. route-policy NFXPUB-in permit node 20
8.     if-match community NFXMEMBERS
9. route-policy NFXPUB-in deny node 90
10. route-policy NFXPUB-out permit node 50
11.     if-match ip-prefix UNARTPUB
12. route-policy NFXPUB-out deny node 90
13.
14. bgp 198977
15.     router-id 5.104.16.24
16.     compare-different-as-med
17.     bestroute compare-med
18.     default local-preference 200
19.     ignore-first-as
20.     preference 50 100 150
21.     network 5.104.16.0 255.255.248.0
```

```
22.     network 185.69.70.0 255.255.254.0
23.     undo synchronization
24.     timer keepalive 5 hold 20
25.     graceful-restart
26.     graceful-restart timer restart 20
27.     graceful-restart timer wait-for-rib 10
28.     group NFXPUB external
29.     peer NFXPUB as-number 8251
30.     peer NFXPUB description NFX L3 switche
31.     peer NFXPUB route-policy NFXPUB-in import
32.     peer NFXPUB route-policy NFXPUB-out export
33.     peer NFXPUB route-limit 2000 95 reconnect 1
34.     peer NFXPUB timer keepalive 10 hold 30
35.     peer NFXPUB advertise-community
36.     peer 78.108.106.12 group NFXPUB
37.     peer 78.108.106.12 description NFX4
38.     peer 78.108.106.38 group NFXPUB
39.     peer 78.108.106.38 description NFX2
40.     peer 78.108.106.38 preferred-value 50
41.
```

15 FREENETIS

FreeNetIS je informační systém pro počítačové sítě. Je vytvořen pro sítě provozované neziskovými organizacemi, jako jsou vnitřní sítě škol, internátů, kolejí apod. Spravuje uživatele, skupiny uživatelů, přístupová práva uživatelů v systému. Zajišťuje správu sítě jako je monitorování stavu zařízení, DHCP servery a statistiky provozu. Mezi další funkce patří správa plateb, podvojné účetnictví, výkazy práce aktivních uživatelů, tickety pro podporu uživatelů atd. FreeNetIS má licenci GNU/GPL, což je svobodná licence a jeho zdrojový kód je zveřejněn na GitHubu, tudíž je možné jej svobodně nasadit na jakoukoli síť. Je také možnost se zapojit do vývoje. FreeNetIS je napsán v PHP MVC frameworku Kohana a databáze je řešena skrz MySQL. Je k dispozici v českém a anglickém jazyce a v případě zájmu jej lze snadno přeložit do dalších světových jazyků. FreeNetIS je postupně vyvíjen také skrz kvalifikační práce studentů FAI UTB ve Zlíně a FEL ČVUT v Praze. [91]

15.1 FreeNetIS DHCP

Správu DHCP rezervací v síti řeším prostřednictvím DHCP modulu ve FreeNetISu, který komunikuje se skripty, spouštěnými na DHCP serverech. Libovolný DHCP server může požádat FreeNetIS o vygenerování konfiguračního souboru s DHCP výpůjčkami, které FreeNetIS eviduje ve vazbě na uživatele sítě, jejich zařízení, síťová rozhraní, jejich MAC adresy a IP adresy. Generování je možné provést pro ISC DHCP nebo pro ISC KEA DHCP. Skript načítající konfiguraci DHCP serveru ověří, o kterou konfiguraci se jedná, viz. následující ukázka skriptu.

```
1.  # DHCP server is old ISC DHCP
2.  if [[ "$SERVER" == "isc-dhcp" ]];
3.  then
4.    DHCP_CONF=${DHCP_CONF:="/etc/dhcp/dhcp.conf"}
5.    CUSTOM_DHCP_CONF=${CUSTOM_DHCP_CONF:="/etc/dhcp/dhcp.conf.custom"}
6.    FULL_PATH=$PATH_FN"/index.php/en/devices/export/"$DEVICE_ID"/debian-etc-dhcp-
    dhcpd/text"
7.  # DHCP server is newer ISC KEA
8.  elif [[ "$SERVER" == "isc-kea" ]];
9.  then
10.   DHCP_CONF=${DHCP_CONF:="/etc/kea/kea-dhcp4.conf"}
11.   # custom dhcp config is not possible for ISC KEA
12.   CUSTOM_DHCP_CONF=""
13.   FULL_PATH=$PATH_FN"/index.php/en/devices/export/"$DEVICE_ID"/debian-etc-kea-kea-
    dhcp4/text"
14. # another DHCP servers are not implemented yet
15. else
16.   echo "[ERROR] `date -R`   Wrong configuration (SERVER not set properly)"
17.   exit 1
18. fi
19.
```

V následující ukázce je zobrazen PHP skript pro generování konfiguračního souboru DHCP.

```
{
  "Dhcp4": {
    "valid-lifetime": 500,
    "renew-timer": 100,
    "rebind-timer": 250,
    "server-tag": "all",
    "interfaces-config": {
      "interfaces": ["*"]
    },
    "expired-leases-processing": {
      "reclaim-timer-wait-time": 3,
      "flush-reclaimed-timer-wait-time": 0,
      "hold-reclaimed-time": 3600,
      "max-reclaim-leases": 100,
      "max-reclaim-time": 50,
      "unwarned-reclaim-cycles": 10
    },
    "host-reservation-identifiers": [
      "hw-address",
      "duid"
    ],
    "control-socket": {
      "socket-type": "unix",
      "socket-name": "/tmp/kea4-ctrl-socket"
    },
    "subnet4": [
<?php foreach ($result->dhcp_servers as $server_id => $dhcp_server): ?>
        # <?php echo $dhcp_server->name ?>
        {
            "subnet": "<?php echo $dhcp_server->cidr ?>",
            "pools": [
<?php foreach ($dhcp_server->ranges as $range_id => $range): ?>
                {
                    "pool": "<?php echo $range->start ?> - <?php echo
$range->end ?>"
                }<?php echo $range_id < (count($dhcp_server->ranges) - 1)
? ',': '' ?>
<?php endforeach ?>
            ],
            "option-data": [{
                "name": "routers",
                "data": "<?php echo $dhcp_server->gateway ?>"
            }, {
                "name": "domain-name-servers",
                "data": "<?php echo implode(",", $dhcp_server-
>dns_servers) ?>"
            }],
            "reservations": [
<?php foreach ($dhcp_server->hosts as $host_id => $host): ?>
                # <?php echo
text::cs_utf2ascii(text::object_format($host, $host->comment)) ?>
                {
                    "hw-address": "<?php echo $host->mac ?>",
                    "ip-address": "<?php echo $host->ip_address ?>"
                }<?php echo $host_id < (count($dhcp_server->hosts) - 1) ?
',': '' ?>
```

```
52. <?php endforeach ?>
53.             ]
54.         }<?php echo $server_id < (count($result->dhcp_servers) - 1) ?
    ',': '' ?>
55. <?php endforeach ?>
56.     ]
57.   }
58. }
59.
```

Vygenerovaný skript je přijat bránou, která ověří HTTP stavový kód a kontrolní součet pro kontrolu, že skript není podvržený a že v pořádku dorazil. Pomocí příkazu `kea-dhcp4` s použitím parametru `-t` je provedena kontrola správnosti vygenerovaného skriptu, tj. kontrola toho, že server bude schopen po aplikování konfiguračního souboru přiřazovat adresy (pro ISC DHCP je to příkaz `dhcpd -t`).

```
1. test_config ()
2. {
3.   if [[ "$SERVER" == "isc-dhcp" ]];
4.   then
5.           dhcpd -4 -t -cf "$TMPFILE" &>/dev/null
6.   elif [[ "$SERVER" == "isc-kea" ]];
7.   then
8.           kea-dhcp4 -t "$TMPFILE" &>/dev/null
9.   fi
10. }
```

Pokud jsou všechny kontroly úspěšné, dojde k restartování DHCP serveru pomocí skriptu z následující ukázky.

```
1. restart_dhcp ()
2. {
3.   if [[ "$SERVER" == "isc-dhcp" ]];
4.   then
5.           killall -w dhcpd 2>/dev/null
6.           dhcpd -4 -q -cf "$DHCP_CONF"
7.
8.           pidof -q dhcpd
9.   elif [[ "$SERVER" == "isc-kea" ]];
10.  then
11.          if pidof -q kea-dhcp4;
12.          then
13.                  killall -w -s SIGHUP kea-dhcp4 2>/dev/null
14.          else
15.                  systemctl start isc-kea-dhcp4-server.service
16.          fi
17.
18.          pidof -q kea-dhcp4
19.  fi
20. }
```

Celý proces výměny konfiguračních souborů, kontrol a restartu pak vystihuje poslední ukázka.

```
1.  # check download
2.    if [ "$status" = "200" ]; then
3.              # attach custom conf if exists
4.              if [ -r "$CUSTOM_DHCP_CONF" ]; then
5.                        cat "$CUSTOM_DHCP_CONF" >> "$TMPFILE"
6.              fi
7.              # config has been change
8.              if [ `diff "$TMPFILE" "$DHCP_CONF" | wc -l` -gt 0 ]; then
9.                        echo "[INFO] `date -R`   Downloaded (code: $status)"
10.                       echo "[INFO] `date -R`   Testing new config..."
11.                       # new config is valid
12.                       if test_config;
13.                       then
14.                                 echo "[INFO] `date -R`   New config is valid"
15.                                 echo "[INFO] `date -R`   Backuping old config to
                                    $DHCP_CONF.save"
16.                                 mv -f "$DHCP_CONF" "$DHCP_CONF".save
17.                                 echo "[INFO] `date -R`   Loading new config to
                                    $DHCP_CONF.save..."
18.                                 # copy config
19.                                 mv -f "$TMPFILE" "$DHCP_CONF"
20.                                 # make readable for all
21.                                 chmod +r "$DHCP_CONF"
22.                                 # restart DHCP server with new configuration
23.                                 echo "[INFO] `date -R`   Restarting DHCP server"
24.                                 if ! restart_dhcp;
25.                                 then
26.                                           echo "[ERROR] `date -R`   DHCP server is not
                                              running -> keeping old configuration"
27.                                           mv -f "$DHCP_CONF".save "$DHCP_CONF"
28.                                           # restart DHCP server with old configuration
29.                                           echo "[INFO] `date -R`   Restarting DHCP
                                              server"
30.                                           if restart_dhcp;
31.                                           then
32.                                                     echo "[INFO] `date -R`   Restart
                                                        completed"
33.                                           else
34.                                                     echo "[ERROR] `date -R`   DHCP
                                                        server is not running"
35.                                           fi
36.                                 else
37.                                           echo "[INFO] `date -R`   Restart completed"
38.                                 fi
39.                       else
40.                                 echo "[ERROR] `date -R`   Invalid new config ->
                                    keeping old configuration"
41.                                 mv -f "$DHCP_CONF".save "$DHCP_CONF"
42.                       fi
43.             else
44.                       echo "[INFO] `date -R`   No change -> keeping old configuration"
45.             fi
46.   elif [[ "$status" =~ ^30[0-9] ]]; then
47.             echo "[INFO] `date -R`   DHCP configuration not changed"
48.   elif [ "$status" = "404" ]; then
49.             echo "[ERROR] `date -R`   Download failed (code: $status). Wrong path to
                FreenetIS or device $DEVICE_ID not exists."
50.   elif [ "$status" = "403" ]; then
51.             echo "[ERROR] `date -R`   Download failed (code: $status). Device
                $DEVICE_ID not configured properly."
52.   else
53.             echo "[ERROR] `date -R`   Download failed (code: $status)"
54.   fi
```

16 ZÁVĚR

Cílem práce bylo nastudovat možnosti a implementovat nová řešení pro zlepšení spolehlivosti a vysoké dostupnosti konkrétní počítačové sítě. V teoretické části jsem se snažil čtenáře seznámit se základními technologiemi sítě Internet. V jednotlivých kapitolách teoretické části jsem čtenáři nastínil princip funkce protokolů a služeb pro realizaci vysoké dostupnosti počítačových síti, které jsou implementovány v praktické části práce. Poslední 8. kapitola teoretické části se věnuje průzkumu nových protokolů a služeb.

V úvodu praktické části jsem se věnoval implementaci služby pro přidělování IP adres zařízením – DHCP. Součástí této kapitoly je popis architektonických řešení sítě. Jsou popsány výhody a úskalí centralizovaného a decentralizovaného řešení. Dále je zde popsána konkrétní síť, pro níž je implementace realizována. Ve schématech jsou zachycena zařízení nacházející se v síti. Schémata zobrazují centralizovanou architekturu sítě, která je výsledkem rozhodnutí mít v síti menší počet směrovacích prvků.

Dále se praktická část věnuje popisu konfiguračních souborů služeb VRRP pro redundanci klíčových prvků sítě, kterými jsou dvě hlavní brány. Také rekurzivního serveru DNS pro vyřizování požadavků na překlad doménových jmen. Pro dynamické směrování provozu sítě je nasazen a popsán protokol OSPF.

Budoucí pokračování této práce bude téměř jistě spočívat v nasazení technologie VxLAN, kterou popisuji v teoretické části práce. Řešení VxLAN je poměrně nové a zatím má jen velmi malé zastoupení na trhu směrovačů a přepínačů, vhodných i pro realizaci „poslední míle“. Jakmile se tato technologie stane standardem v oblasti malých směrovačů a L3 přepínačů, její nasazení přinese zjednodušení správy a zvýšení spolehlivosti sítí našeho typu.

Práce mi byla velkým přínosem při rozšiřování znalostí v oblasti počítačových sítí. Seznámil jsem se směrovacími protokoly, jejich použitím a praktickým nasazením a ponořil jsem se do problematiky návrhu a stavění počítačové sítě.

SEZNAM POUŽITÉ LITERATURY

[1] DORMS, PH.D., Ralph a Ted LEMON. Assigning IP Addresses Using DHCP. The DHCP Handbook. The DHCP Handbook, Second Edition. United States of America: SAMS, 201 West 103rd Street, Indianapolis, Indiana 46290 USA, 2003, ISBN 0-672-32327-3.

[2] GRYGAREK. Směrovací protokol OSPF. FEI, VŠB-TUO [online]. [cit. 2021-02-27]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html

[3] MOY, John. OSPF: Anatomy of an Internet Routing Protocol. 1st edition. vyd. Reading, Mass: Addison-Wesley Professional, 1998. ISBN 978-0-201-63472-3.

[4] What is a packet? | Network packet definition | Cloudflare. [cit. 02.03.2021]. Dostupné z: https://www.cloudflare.com/learning/network-layer/what-is-a-packet/

[5] EDITOR. Network Packet [online] [cit. 03.03.2021]. Dostupné z: https://networkencyclopedia.com/network-packet/

[6] Router: Definition, advantages & functions | NFON Knowledgebase. [cit. 03.03.2021]. Dostupné z: https://www.nfon.com/en/service/knowledge-base/knowledge-base-detail

[7] SAMPLE, Ian. What is the internet? 13 key questions answered. The Guardian [online]. 2018 [cit. 03.03.2021]. ISSN 0261-3077. Dostupné z: https://www.theguardian.com/technology/2018/oct/22/what-is-the-internet-13-key-questions-answered

[8] PETERKA, Jiri. Jiří Peterka: Báječný svět počítačových sítí, část III. - Síťové architektury. [cit. 03.03.2021]. Dostupné z: http://www.earchiv.cz/b05/b0500001.php3

[9] Srovnání RM ISO/OSI a TCP/IP. [cit. 03.03.2021]. Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=15&Itemid=121

[10] How to Turn a Linux Server into a Router to Handle Traffic Statically and Dynamically – Part 10. [cit. 05.03.2021]. Dostupné z: https://www.tecmint.com/setup-linux-as-router/

[11] Routing Protocols Types: Static, Dynamic, IP, CISCO. [cit. 05.03.2021]. Dostupné z: https://www.guru99.com/routing-protocol-types.html

[12] Practical routing attacks (2/3): OSPF [online]. 2018 [cit. 08.03.2021]. Dostupné z: https://microlab.red/2018/05/03/practical-routing-attacks-2-3-ospf/

[13] What is dynamic routing? Educative: Interactive Courses for Software Developers [online] [cit. 08.03.2021]. Dostupné z: https://www.educative.io/edpresso/what-is-dynamic-routing

[14] ANTONIOU STELIOS. Dynamic Routing Protocols: Distance Vector and Link State Protocols. Pluralsight [online]. 12. 12. 2007 [cit. 30.03.2021]. Dostupné z: https://www.pluralsight.com/blog/it-ops/dynamic-routing-protocol

[15] SAURABH SHARMA. Link State Advertisement (LSA) [online]. 2019 [cit. 30.03.2021]. Dostupné z: https://www.geeksforgeeks.org/link-state-advertisement-lsa/

[16] ANIKET SINGH. Unicast Routing – Link State Routing [online]. 2018 [cit. 30.03.2021]. Dostupné z: https://www.geeksforgeeks.org/unicast-routing-link-state-routing/

[17] ANKIT KUMAR SINGH. Difference between Distance vector routing and Link State routing [online]. 2018 [cit. 30.03.2021]. Dostupné z: https://www.geeksforgeeks.org/difference-between-distance-vector-routing-and-link-state-routing/

[18] NIKITHA SRI. Exterior Gateway Protocol (EGP) [online]. 2020 [cit. 01.04.2021]. Dostupné z: https://www.geeksforgeeks.org/exterior-gateway-protocol-egp/

[19] HUNT, Craig. TCP/IP Network Administration. 1-56592-322-7 [online]. 4. 2. 1999 [cit. 01.04.2021]. Dostupné z: http://web.deu.edu.tr/doc/oreily/networking/tcpip/ch07_05.htm

[20] MANEESH KUMAR SINGH. Difference between Static and Dynamic Routing [online]. 2019 [cit. 01.04.2021]. Dostupné z: https://www.geeksforgeeks.org/difference-between-static-and-dynamic-routing/

[21] SAURABH SHARMA. Types of Routing [online]. 2018 [cit. 01.04.2021]. Dostupné z: https://www.geeksforgeeks.org/types-of-routing/

[22] Distance Vector, Link State, and Path Vector | Introduction to the Border Gateway Patrol | InformIT. [cit. 01.04.2021]. Dostupné z: https://www.informit.com/articles/article.aspx?p=331613&seqNum=2

[23] What Is BGP? | BGP Routing Explained. Cloudflare [online] [cit. 01.04.2021]. Dostupné z: https://www.cloudflare.com/learning/security/glossary/what-is-bgp/

[24] Practical routing attacks (2/3): OSPF [online]. 2018 [cit. 06.04.2021]. Dostupné z: https://microlab.red/2018/05/03/practical-routing-attacks-2-3-ospf/

[25] NAKIBLY, Gabi et al. Persistent OSPF Attacks. [Stanford University], s. 12. Dostupné z: http://theory.stanford.edu/~dabo/papers/ospf.pdf

[26] UNIVERSITY, Geek. Designated router and backup designated router | CCNA [online] [cit. 06.04.2021]. Dostupné z: https://geek-university.com/ccna/designated-router-and-backup-designated-router/

[27] OSPF. [cit. 07.04.2021]. Dostupné z: https://help.fortinet.com/fadc/4-5-1/olh/Content/FortiADC/handbook/ospf.htm

[28] JOHN BUSSO. Authentication, Authorization, Accounting and Identity Management [online]. 2018 [cit. 09.04.2021]. Dostupné z: https://www.ccsinet.com/blog/aaa-identity-management/

[29] Authentication Definition. [cit. 09.04.2021]. Dostupné z: https://techterms.com/definition/authentication

[30] What is Authorization? Definition of Authorization, Authorization Meaning. The Economic Times [online] [cit. 09.04.2021]. Dostupné z: https://economictimes.indiatimes.com/definition/authorization

[31] Comparison between PPPoE,Web+Portal,and 802.1x Authentication Modes. Huawei Enterprise Support Community [online] [cit. 09.04.2021]. Dostupné z: https://forum.huawei.com/enterprise/en/comparison-between-pppoe-web-portal-and-802-1x-authentication-modes/thread/585058-869

[32] MICHAL KRUMNIKL. PPPoE. In:. 20. 1. 2006 [cit. 09.04.2021]. Dostupné z: http://www.cs.vsb.cz/grygarek/TPS/projekty/0506Z/Krumnikl/index.htm

[33] MADHURI HAMMAD. Point-to-Point Protocol (PPP) Frame Format [online]. 2020 [cit. 09.04.2021]. Dostupné z: https://www.geeksforgeeks.org/point-to-point-protocol-ppp-frame-format/

[34] ARCHIVEDDOCS. 802.1X Authenticated Wired Access Overview. [cit. 14.04.2021]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831831(v=ws.11)

[35] JASONGEREND. Network Policy Server (NPS). [cit. 14.04.2021]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top

[36] What is 802.1X? How Does it Work? [online] [cit. 14.04.2021]. Dostupné z: https://www.securew2.com/solutions/802-1x

[37] UPDATED: 3/29/2020, Rob Sobers. The Difference Between Active Directory and LDAP. Inside Out Security [online]. 13. 7. 2016 [cit. 14.04.2021]. Dostupné z: https://www.varonis.com/blog/the-difference-between-active-directory-and-ldap/

[38] Compare and Contrast SPB and TRILL., s. 10. Dostupné z: http://www.techdata.ca/business/avaya/DataCenterSolutions/files/A%20-%20Why%20Avaya/2%20-%20Learn%20More%20About%20VENA/SPB-TRILL_Compare_Contrast-DN4634.pdf

[39] TRILL vs. SPB s. 31. Dostupné z: https://www.trex.fi/2014/xtrm-trill-vs-spb.pdf

[40] Spanning Tree Protocol (STP): No Loop ! [cit. 14.04.2021]. Dostupné z: https://web.archive.org/web/20151227040910/http://www.networkel.com/2015/10/spanning-tree-protocol-stp-no-loop.html

[41] Spanning Tree Protocol. Cisco [online] [cit. 14.04.2021]. Dostupné z: https://www.cisco.com/c/en/us/tech/lan-switching/spanning-tree-protocol/index.html

[42] INC, Internet Systems Consortium. The History of DHCP. 29. 9. 2020 [cit. 20.04.2021]. Dostupné z: https://www.isc.org/dhcphistory/

[43] 8. The DHCPv4 Server — Kea 1.8.1-git documentation. [cit. 21.04.2021]. Dostupné z: https://kea.readthedocs.io/en/kea-1.8.1/arm/dhcp4-srv.html

[44] STP – Spanning Tree Protocol Explained With Examples. ComputerNetworkingNotes [online] [cit. 21.04.2021]. Dostupné z: https://www.computernetworkingnotes.com/ccna-study-guide/stp-spanning-tree-protocol-explained-with-examples.html

[45] Greycampus. [cit. 21.04.2021]. Dostupné z: https://www.greycampus.com/opencampus/ethical-hacking/arp-and-cam-cable

[46] Spanning Tree Port States, Blocking, Listening, Learning, Forwarding, Disabled. [cit. 22.04.2021]. Dostupné z: https://www.omnisecu.com/cisco-certified-network-associate-ccna/spanning-tree-port-states.php

[47] SAURABH SHARMA. DHCP Relay Agent in Computer Network [online]. 2018 [cit. 22.04.2021]. Dostupné z: https://www.geeksforgeeks.org/dhcp-relay-agent-in-computer-network/

[48] SHAMUS, McGillicuddy. TRILL versus Shortest Path Bridging: Hard feelings? - The Network Hub. [cit. 22.04.2021]. Dostupné z: https://searchnetworking.techtarget.com/blog/The-Network-Hub/TRILL-versus-Shortest-Path-Bridging-Hard-feelings

[49] What is VLAN? Types, Advantages, Example. [cit. 24.04.2021]. Dostupné z: https://www.guru99.com/vlan-definition-types-advantages.html

[50] What is VLAN? How VLAN Works and Common Examples. N-able [online]. 8. 7. 2019 [cit. 24.04.2021]. Dostupné z: https://www.n-able.com/blog/what-are-vlans

[51] Introduction to port-based VLAN. [cit. 24.04.2021]. Dostupné z: https://techhub.hpe.com/eginfolib/networking/docs/routers/msrv5/cg/5200-2316_l2-lan-cg/content/459302545.htm

[52] Configuring protocol-based VLANs. [cit. 24.04.2021]. Dostupné z: https://techhub.hpe.com/eginfolib/networking/docs/switches/5510hi/5200-0075b_l2-lan_cg/content/496798309.htm

[53] What is a MAC-based VLAN and how does it work with my managed switch? | Answer | NETGEAR Support. [cit. 24.04.2021]. Dostupné z: https://kb.netgear.com/21586/What-is-a-MAC-based-VLAN-and-how-does-it-work-with-my-managed-switch

[54] FRUHLINGER, Keith Shaw and Josh. What is DNS and how does it work? Network World [online]. 26. 8. 2020 [cit. 26.04.2021]. Dostupné z: https://www.networkworld.com/article/3268449/what-is-dns-and-how-does-it-work.html

[55] Protokol DNS – rekurzivní a nerekurzivní dotazy [online]. 2019 [cit. 26.04.2021]. Dostupné z: https://kb.wedos.com/cs/dns/protokol-dns-rekurzivni-a-nerekurzivni-dotazy/

[56] Dynu. Dynu Systems – Free dynamic DNS service [online] [cit. 26.04.2021]. Dostupné z: http://www.dynu.com

[57] What Is DNS? | How DNS Works. Cloudflare [online] [cit. 26.04.2021]. Dostupné z: https://www.cloudflare.com/learning/dns/what-is-dns/

[58] DNS Types: Types of DNS Records, Servers and Queries. NS1 [online] [cit. 27.04.2021]. Dostupné z: https://ns1.com/resources/dns-types-records-servers-and-queries

[59] VRRP failover-delay Overview | High Availability User Guide | Juniper Networks TechLibrary. [cit. 27.04.2021]. Dostupné z: https://www.juniper.net/documentation/us/en/software/junos/high-availability/topics/concept/vrrp-failover-delay-overview.html

[60] Software Design — Keepalived 1.2.15 documentation. [cit. 27.04.2021]. Dostupné z: https://keepalived.readthedocs.io/en/latest/software_design.html#failover-vrrp-framework

[61] Overview of VRRP – NE20E-S V800R010C10SPC500 Configuration Guide – Network Reliability 01 - Huawei. [cit. 27.04.2021]. Dostupné z: https://support.huawei.com/enterprise/en/doc/EDOC1100055104/a5b057b1/overview-of-vrrp

[62] DNSSEC – What Is It and Why Is It Important? - ICANN. [cit. 27.04.2021]. Dostupné z: https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

[63] DNS records. Cloudflare [online] [cit. 27.04.2021]. Dostupné z: https://www.cloudflare.com/learning/dns/dns-records/

[64] 3. Name Server Configuration — BIND 9 documentation. [cit. 28.04.2021]. Dostupné z: https://bind9.readthedocs.io/en/latest/configuration.html#a-caching-only-name-server

[65] BIND zone Statement. [cit. 28.04.2021]. Dostupné z: http://web.mit.edu/darwin/src/modules/bind/bind/doc/html/zone.html

[66] CALETKA, Ondřej. Jak blokujeme nepovolené hazardní weby. Root.cz [online] [cit. 28.04.2021]. ISSN 1212-8309. Dostupné z: https://www.root.cz/clanky/jak-blokujeme-nepovolene-hazardni-weby/

[67] BIND options Statement. [cit. 28.04.2021]. Dostupné z: http://web.mit.edu/darwin/src/modules/bind/bind/doc/html/options.html

[68] INC, Internet Systems Consortium. BIND 9.13.3. 13. 9. 2018 [cit. 28.04.2021]. Dostupné z: https://www.isc.org/blogs/bind-9-new-versions/

[69] MOCKAPETRIS, Paul. DOMAIN NAMES – IMPLEMENTATION AND SPECIFICATION. RFC 882, 883, 973 [online]. 11. 1987 [cit. 28.04.2021]. Dostupné z: https://www.rfc-editor.org/rfc/rfc1035.txt

[70] BEIJNUM, Iljitsch van. BGP: Building Reliable Networks with the Border Gateway Protocol. 1st edition. B.m.: O'Reilly Media, 2002.

[71] What is BGP | Border Gateway Protocol Explained [online]. 2015 [cit. 28.04.2021]. Dostupné z: https://www.imperva.com/blog/bgp-routing-explained/

[72] GRYGAREK. Směrovací protokol BGP. BGP [online] [cit. 28.04.2021]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html

[73] Dynamic Routing : A Complete Guide for Beginner and Expert [online]. 2019 [cit. 28.04.2021]. Dostupné z: https://www.gns3network.com/dynamic-routing-complete-guide-for-beginner-and-expert/

[74] What is Cisco FabricPath? - Our Technology Planet [online] [cit. 28.04.2021]. Dostupné z: https://ourtechplanet.com/what-is-cisco-fabricpath/

[75] What is a Bare Metal Server? | Rackspace Technology. [cit. 29.04.2021]. Dostupné z: https://www.rackspace.com/en-gb/library/what-is-a-bare-metal-server

[76] What is VXLAN? Juniper Networks [online] [cit. 29.04.2021]. Dostupné z: https://www.juniper.net/us/en/products-services/what-is/vxlan/

[77] Manual:RADIUS Client - MikroTik Wiki. [cit. 01.05.2021]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:RADIUS_Client

[78] 16. Hooks Libraries — Kea 1.9.7 documentation. [cit. 01.05.2021]. Dostupné z: https://kea.readthedocs.io/en/latest/arm/hooks.html#radius-radius-server-support

[79] EdgeRouter – Add Debian Packages to EdgeOS. Ubiquiti Support and Help Center [online] [cit. 01.05.2021]. Dostupné z: https://help.ui.com/hc/en-us/articles/205202560-EdgeRouter-Add-Debian-Packages-to-EdgeOS

[80] KRČMÁŘ, Petr. nftables: linuxový firewall s moderními vlastnostmi. Root.cz [online] [cit. 03.05.2021]. ISSN 1212-8309. Dostupné z: https://www.root.cz/clanky/nftables-linuxovy-firewall-s-modernimi-vlastnostmi/

[81] KRČMÁŘ, Petr. nftables: správa tabulek, řetězců a pravidel s utilitou nft. Root.cz [online] [cit. 03.05.2021]. ISSN 1212-8309. Dostupné z: https://www.root.cz/clanky/nftables-sprava-tabulek-retezcu-a-pravidel-s-utilitou-nft/

[82] KRČMÁŘ, Petr. nftables: akce prováděné nad pravidly včetně nastavení NAT. Root.cz [online] [cit. 03.05.2021]. ISSN 1212-8309. Dostupné z: https://www.root.cz/clanky/nftables-akce-provadene-nad-pravidly-vcetne-nastaveni-nat/

[83] SAURABH, Sharma. Network Address Translation (NAT) [online]. 2018 [cit. 03.05.2021]. Dostupné z: https://www.geeksforgeeks.org/network-address-translation-nat/

[84] Maps – nftables wiki. [cit. 03.05.2021]. Dostupné z: https://wiki.nftables.org/wiki-nftables/index.php/Maps

[85] PETŘÍČEK, Miroslav. Stavíme firewall (2). Root.cz [online] [cit. 03.05.2021]. ISSN 1212-8309. Dostupné z: https://www.root.cz/clanky/stavime-firewall-2/

[86] NFX – Neutral czFree eXchange. [cit. 03.05.2021]. Dostupné z: https://www.nfx.cz/

[87] NIX.CZ - Neutral Internet Exchange. [cit. 04.05.2021]. Dostupné z: https://www.nix.cz/cs

[88] NIX.CZ - Neutral Internet Exchange. [cit. 04.05.2021]. Dostupné z: https://www.nix.cz/cs

[89] HP 5920 Switch Series – Specifications. [cit. 04.05.2021]. Dostupné z: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=c03255324

[90] BGP Fundamentals 20 – Using Route-Policy in BGP. Huawei Enterprise Support Community [online] [cit. 05.05.2021]. Dostupné z: https://forum.huawei.com/enterprise/en/bgp-fundamentals-20-using-route-policy-in-bgp/thread/561991-861

[91] FreenetIS [online] [cit. 06.05.2021]. Dostupné z: https://www.freenetis.org/

[92] KEJDUŠ, Radomír. Technologie počítačové sítě: jak pracuje TCP/IP a ISO/OSI [online]. 2012 [cit. 07.05.2021]. Dostupné z: https://www.cnews.cz/technologie-pocitacove-site-jak-pracuje-tcpip-a-isoosi/

[93] Route Poisoning and Count to infinity problem in Routing [online]. 2017 [cit. 07.05.2021]. Dostupné z: https://www.geeksforgeeks.org/route-poisoning-and-count-to-infinity-problem-in-routing/

[94] SURÝ, Ondřej. Proč a zda Supronet shodil Internet. Lupa.cz [online] [cit. 07.05.2021]. ISSN 1213-0702. Dostupné z: https://www.lupa.cz/clanky/proc-a-zda-supronet-shodil-internet/

[95] A.S, Mironet cz. Aruba 2930F 24G. In: Mironet.cz [online] [cit. 14.05.2021]. Dostupné z: https://www.mironet.cz/aruba-2930f-24g-24x-gigabit-rj45-portu-4x-sfp-porty+dp454504/

[96] PC Engines APU2 1Gbit traffic not achievable. [cit. 14.05.2021]. Dostupné z: https://forum.opnsense.org/index.php?topic=9264.0

[97] ARUBA 2930F SWITCH SERIES: Datasheet [online]. Hewlett Packard Enterprise Development LP, 2020 [cit. 2021-5-14]. Dostupné z: https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf

[98] PROVANTAGE: Cisco Systems C9300-24T-1A C9300 24 Port Data Only Network Advantage 1-Year. [cit. 14.05.2021]. Dostupné z: https://www.provantage.com/cisco-systems-c9300-24t-1a~7CSCO5X6.htm

[99] Cisco Catalyst 9300 Series Switches Data Sheet. In: Cisco [online] [cit. 14.05.2021]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html

[100] Ubiquiti EdgeRouter ER-12P Elektronické předplatné časopisu Reflex a novin E15 na půl roku v hodnotě 1518 Kč + O2 TV Sport Pack na 3 měsíce (max. 1x na objednávku). In: [cit. 14.05.2021]. Dostupné z: https://www.czc.cz/ubiquiti-edgerouter-er-12p/262620/produkt

[101] Ubiquity EdgeRouter: Datasheet [online]. Ubiquiti, 2020 [cit. 2021-5-14]. Dostupné z: https://dl.ubnt.com/datasheets/edgemax/EdgeRouter_DS.pdf

[102] MikroTik RouterBoard RB4011iGS+RM | T.S.BOHEMIA. In: [cit. 14.05.2021]. Dostupné z: https://www.tsbohemia.cz/mikrotik-routerboard-rb4011igs-rm_d303351.html?utm_source=google&utm_medium=srovnavac&gclid=CjwKCAjwv_iEBhASEiwARoemvCt3fjZdW-dVcmezAq_wbabWpW0mmvuHodTosppaL2LlFeeRFMpqWBoCPAQQAvD_BwE#sticomment

[103] RB4011iGS+RM. MikroTik [online]. 2020 [cit. 2021-5-14]. Dostupné z: https://mikrotik.com/product/rb4011igs_rm#fndtn-testresults

[104] Mikrotik Cloud Core CCR2004-1G-12S+2XS Elektronické předplatné časopisu Reflex a novin E15 na půl roku v hodnotě 1518 Kč + O2 TV Sport Pack na 3 měsíce (max. 1x na objednávku). In: [cit. 14.05.2021]. Dostupné z: https://www.czc.cz/mikrotik-cloud-core-ccr2004-1g-12s-2xs/286673/produkt

[105] i4wifi.cz | PC Engines APU.4D4 APU4D4. In: [cit. 14.05.2021]. Dostupné z: https://www.i4wifi.cz/cs/239600-pc-engines-apu-4d4

[106] A.S, Mironet cz. MikroTik CRS328-24P-4S+RM. In: Mironet.cz [online] [cit. 14.05.2021]. Dostupné z: https://www.mironet.cz/mikrotik-crs32824p4srm-24x-1gbps-lan-4x-sfp-1x-rj45-seriovy-port-19quot+dp411547/

[107] CRS328-24P-4S+RM. MikroTik [online]. 2020 [cit. 2021-5-14]. Dostupné z: https://mikrotik.com/product/crs328_24p_4s_rm#fndtn-testresults

[108] CCR2004-1G-12S+2XS. MikroTik [online]. 2020 [cit. 2021-5-14]. Dostupné z: https://mikrotik.com/product/ccr2004_1g_12s_2xs#fndtn-testresults

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAA	Authentication, Authorization, Accounting
AD	Active Directory
API	Application Programming Interface
ARP	Address Resolution Protocol
AS	Autonomní systém
ASN	Autonomous System Number
BDR	Backup Designated Router
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CAM	Content Addressable Memory
CESNET	Czech Education and Scientific Network
EAP	Extensible Authentication Protocol
EOL	End Of Life
DHCP	Dynamic Host Configuration Protocol
DHCWG	Dynamic Host Configuration Working Group
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DR	Designated Router
č.	číslo
EAP	Extensible Authentication Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EGP	Exterior Gateway Protol
HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol

IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
IPTV	Internet Protocol Television
IS-IS	Intermediate System to Intermediate System
ISC	Internet Software Consortium
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISO/OSI	International Organization for Standadization / Open System Interconnection
JSON	JavaScript Object Notation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LSA	Link State Advertisement
MAC	Media Access Control
NAT	Network Address Translation
NFX	Neutral czFree eXchange
NIX	Neutral Internet Exchange
NPS	Network Policy Server
OS	Operační systém
OSPF	Open Short Path First
POE	Power Over Ethernet

PPP	Point-to-Point Protocol
PPPoE	Point-to-Point over Ethernet
PSTN	Public Switch Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial-in User Service
RIP	Routing Information Protocol
RIR	Regionální Internetový Register
RPZ	Response Policy Zone
SPB	Short Path Bridging
SPBM	Shortest Path Bridging Mac-in-Mac
SPBV	Shortest Path Bridging VLAN
STP	Spanning Tree Protocol
STA	Spanning Tree Algorithm
TCP/IP	Transmission Control Protocol/Internet Protocol
TLD	Top Level Domain
TRILL	Transparent Interconnection of Lots of Links
TTL	Time To Live
tzn.	To znamená
tzv.	takzvaný
UDP	User Data Protocol
VLAN	Virtual Local Area Network
VNI	VxLAN Network Identifier
VPN	Virtual Private Network
VRRP	Virtual Redundancy Protocol
VTEP	VxLAN Tunnel EndPoint
VxLAN	Virtual Extensible Local Area Network

WAN Wide Area Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: CD

Přiložené CD obsahuje:

- Text:
    - Implementace_vysoke_dostupnosti_sluzeb_pocitacove_site_Filip_Miskarik.docx – Diplomová práce ve formátu DOCX
    - Implementace_vysoke_dostupnosti_sluzeb_pocitacove_site_Filip_Miskarik.pdf – Diplomová práce ve formátu PDF