FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Správa IP adres ve středně velké síti
Student:	Vít Pekárek
Vedoucí:	Ing. Jan Kubr, Ph.D.
Studijní program:	Informatika
Studijní obor:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	Do konce letního semestru 2019/20

Pokyny pro vypracování

1) Analyzujte aktuální nabídku open-source software implementující funkce DHCP, DHCPv6 a DNS serveru, zejména s ohledem na způsob ukládání
konfiguračních dat, monitorování stavu a konfigurace prostřednictvím API.

2) Analyzujte aktuální nabídku open-source software umožňující správu a dohled využívání IP a IPv6 adres v sítích LAN. Zaměřte se na funkce
umožňující propojení nástroje správy se servery uvedenými v bodě 1) prostřednictvím API a řízení jejich konfigurace pomocí tohoto software.

3) Vhodné kandidáty z bodů 1) a 2) testujte ve virtualizovaném prostředí a navrhněte architekturu systému, který bude umožňovat správu IPv4 a IPv6 adres,
DHCP a DHCPv6, a DNS záznamů středně velké sítě LAN (okolo 50 VLAN). Navržený systém realizujte ve virtualizovaném prostředí.

4) V případě nutnosti navrhněte, implementujte a otestujte software (nebo jeho část/doplněk) usnadňující správu IP adres a DNS jmen
pomocí výše zvolených nástrojů.

Seznam odborné literatury

Dodá vedoucí práce.

prof. Ing. Pavel Tvrdík, CSc.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 15. února 2019

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

Správa IP adres ve středně velké síti

Vít Pekárek

Katedra počítačových systémů
Vedoucí práce: Ing. Jan Kubr, Ph.D.

19. května 2019

Poděkování

Děkuji svému vedoucímu práce Ing. Janu Kubrovi za podporu, kterou mi během tvorby této práce věnoval. Dále bych chtěl poděkovat Ing. Elišce Šestákové za hodnotná doporučení při práci s LaTeXem a Jaroslavu Zdeňkovi, který vždy přišel s nějakou cenou radou. V neposlední řadě bych rád poděkoval své rodině a přátelům za podporu během mého studia.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo"), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 19. května 2019 .....

Odkaz na tuto práci

Pekárek, Vít. *Správa IP adres ve středně velké síti*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2019.

Abstrakt

Síť bez DHCP a DNS serverů nemůže v podstatě fungovat. Jedná se o klíčové nástroje výrazně usnadňující konfiguraci a používání sítě. Tato práce analyzuje nabídku těchto softwarů, vyírá z nich vhodné kandidáty a ukazuje jejich instalaci, konfiguraci a testování.

Klíčová slova DHCP, DNS, IPAM, IP adresa, správa sítě

Abstract

The internet network without DHCP and DNS servers cannot basically work. These software are key tools that significantly simplify network configuration and usage. This thesis analyses the offer of these software, selects suitable candidates and shows their instalation, configuration and testing.

Keywords DHCP, DNS, IPAM, IP address, network management

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů kódů

Úvod

V budově Fakulty elektrotechnické Českého vysokého učení technického v Praze (dále jen FEL ČVUT) na Karlově náměstí sídlí čtyři katedry. Každá z nich má vlastní DHCP server, který spravuje člověk z dané katedry. DNS server je společný, ale má pouze jednoho správce. Toto řešení je nevyhovující hlavně proto, že využívá zastaralé technologie. Dále není uživatelsky zrovna přívětivé. Problémy nastávají zejména u DNS, kdy katederní správce musí žádat administrátora DNS serveru o změnu a vznikají tak zbytečné prodlevy.

Toto téma jsem si vybral, protože má velký potenciál praktického využití. Softwarový backend sítě je třeba modernizovat nejenom na FEL ČVUT, ale také například v klubu Silicon Hill. V něm pomáhám se správou sítě a poznatky z této práce mohou být použity při výběru a nasazení nového řešení.

Hlavním přínosem této práce bude zlepšení fungování sítě na FEL ČVUT na Karlově náměstí, ulehčení práce správců jednotlivých služeb a zpřehlednění využití daných adresních rozsahů.

Struktura práce

Kapitola 1 ve stručnosti shrnuje cíle práce. V kapitole 2 dojde k seznámení s použitými technologiemi. Kapitola 3 popisuje stávající řešení a důvody, proč je nevyhovující. Dále obsahuje analýzu nástrojů pro správu DHCP, DNS a IP adres. V kapitole 4 je popsán použitý hardware, průběh nasazení vybraných aplikací a výsledky jejich testování. Závěr sumarizuje výsledky této práce a nabízí případné možnosti, jak na tuto práci navázat.

Kapitola 1

Cíle práce

Hlavním cílem této práce je vybrat a otestovat software pro správu IP adres a servery DHCP a DNS. Dále navrhnout architekturu kompletního systému a tu následně otestovat jako celek.

Dílčím úkolem je zjistit nabídku open-source softwaru implementující funkce DHCP, DHCPv6 a DNS serverů. U těchto nástrojů se zaměřit převážně na způsob ukládání konfiguračních dat, monitorování jejich stavu a možnosti konfigurace prostřednictvím API[1].

Dalším částečným cílem je prozkoumat nabídku open-source softwaru pro správu IP a IPv6 adres v sítích LAN[2]. Zde se zaměřit zejména na funkce umožňující propojení výše zmíněných serverů s těmito aplikacemi.

Pokud nalezené řešení nebude dostačující, součástí práce bude také návrh a implementace doplňku do stávajícího funkčního software, či návrh zcela nového systému.

[1] Application Programming Interface
[2] Local Area Network

Kapitola 2

Teorie

Pro seznámení s použitými technologiemi následuje jejich krátký popis a principy fungování.

2.1 DHCP

Jak uvádí RFC 1541 [1], *Dynamic Host Configuration Protocol* (DHCP) patří do rodiny TCP/IP[3] protokolů a vznikl z protokolu BOOTP[4] přidáním dynamického přidělování adres a dodatečných možností nastavení. Poskytuje framework pro předávání konfiguračních informací (např. IP adresy, výchozí brány, adresy DNS serveru nebo doménového jména) počítačům.

Princip fungování znázorňuje obrázek 2.1. Klient do sítě posílá požadavek `DHCPDISCOVER`, server odpovídá s nabídkou IP adresy `DHCPOFFER`. Pokud si ji klient zvolí, žádá o ni `DHCPREQUEST` a server posílá odpověď `DHCPACK`. Jakmile klient obdrží toto potvrzení, může danou adresu po dobu její platnosti využívat. Po vypršení platnosti musí znovu žádat o přidělení.

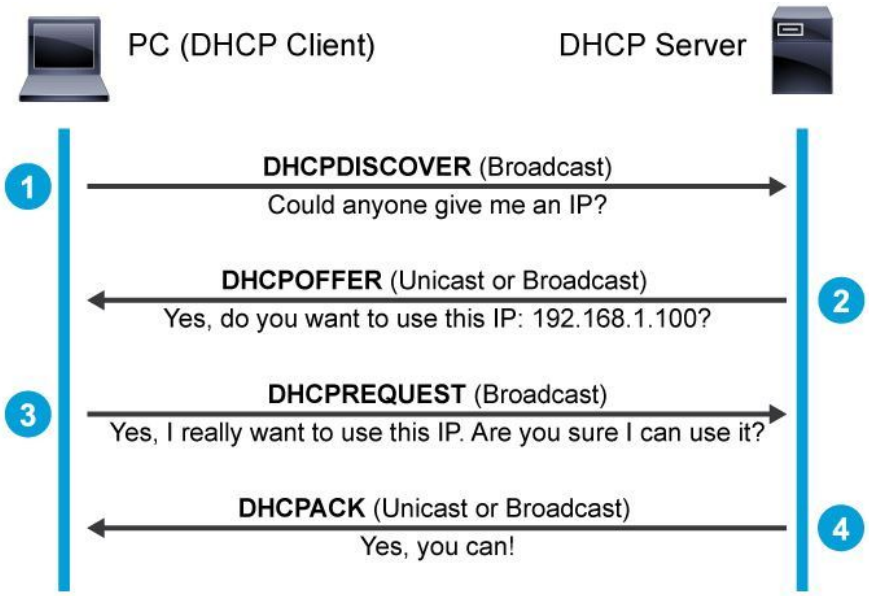
2.2 DNS

Dle RFC 1034 [3] slouží *Domain Name System* (DNS) k překladu jména zařízení na IP adresy (dříve řešeno pomocí souboru hosts[.txt]) a obráceně. To zajišťují DNS servery, komunikující pomocí stejnojmenného protokolu. DNS by se dalo přirovnat k velkému telefonnímu seznamu pro internet. Existují dva základní typy DNS serverů. Autoritativní mají záznamy své domény (zóny) trvale uložené. Oproti tomu vyrovnávací[5] DNS servery tyto záznamy získávají a pro urychlení překladu ukládají do své mezipaměti. Zde jsou záznamy ponechány pouze po dobu jejich platnosti, poté musí být znovu načteny.

[3] Transmission Control Protocol/Internet Protocol

[4] Bootsrap Protocol

[5] v praxi častěji nazývány *recursive* nebo *caching only*

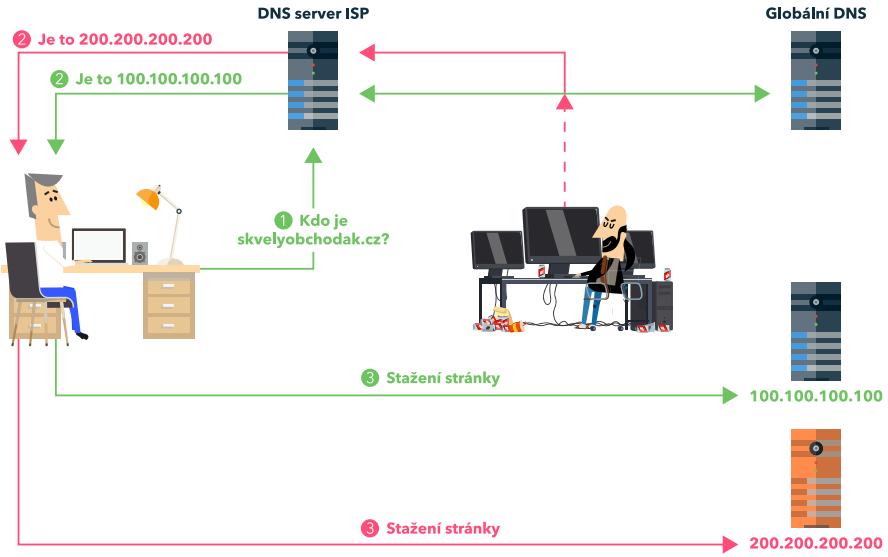


Obrázek 2.1: Vysvětlení principu DHCP (*Zdroj: [2]*)

Protože člověk si jednoduše nemůže pamatovat všechny IP adresy serverů, využívají se doménová jména, která jsou snáze zapamatovatelná. Pokud host nemá uloženou adresu lokálně, dojde při pokusu o přístup na server nejprve k dotazu do rekurzivního DNS serveru na danou IP. Pokud je adresa známa, je rovnou vrácena a požadavek může být zpracován. V opačném případě je směřován na autoritativní server, ten oznámí, kde se nachází server domény nejvyšší úrovně (.cz, .com nebo třeba .org). Odtud je požadavek poslán hierarchicky až k serveru domény nejnižší úrovně, který sdělí požadovanou IP adresu. Ta je zároveň uložena v rekurzivním serveru pro případné další použití.

2.2.1 DNSSEC

Zkratka pro Domain Name System Security Extensions. *„DNSSEC je rozšíření systému doménových jmen (DNS), které zvyšuje jeho bezpečnost. DNSSEC poskytuje uživatelům jistotu, že informace, které z DNS získal, byly poskytnuty správným zdrojem, jsou úplné a jejich integrita nebyla při přenosu narušena. DNSSEC zajistí důvěryhodnost údajů, získaných z DNS.“* [4] Pomocí tohoto rozšíření je možné bránit se například útoku DNS cache poisoning, při kterém útočník podvrhne DNS záznamy přímo na DNS serveru a přesměruje tak provoz na svoji podvodnou stránku. Schéma útoku můžeme vidět na obrázku 2.2.



Obrázek 2.2: Princip útoku typu DNS cache poisoning (*Zdroj: [5]*)

2.2.2 DNS over TLS

Dříve byla valná většina DNS dotazů posílána nešifrovaně, což je dělalo náchylné k odposlechnutí a případnému podvržení. V roce 2016 byl publikovaný standard DNS over TLS (DoT) [6], který definuje šifrování DNS dotazů pomocí TLS a zvyšuje tak bezpečí a soukromí uživatelů.

2.3 IPAM

IP adres management (IPAM) software slouží síťovým administrátorům k přehlednému zobrazení dostupných adresních rozsahů, jejich obsazenosti a stavu jednotlivých zařízení v nich. Aplikace samotná neposkytuje funkcionalitu DNS nebo DHCP serverů, často však dokáže s těmito systémy pracovat a zjednodušuje tak přiřazování adres nebo doménových jmen zařízením, čímž výrazně usnadňuje správu adresního prostoru.

Kapitola 3

Analýza

V této kapitole bude shrnuto dosavadní řešení a jeho nedostatky. Dále budou postupně charakterizovány vybrané nástroje pro DHCP server, DNS server a správu IP adres. U každého budou popsány jeho výhody a nevýhody oproti ostatním.

3.1 Stávající řešení

Stávající řešení nepodporuje ukládání konfigurace do databáze, proto musí být obě služby nastavovány přes terminál přímo v konfiguračních souborech. Ty vyžadují dodržení specifického formátování, například určitého typu odsazení, náchylnému k vytvoření syntaktické chyby. Dále je při vytvoření nebo změně záznamu zařízení potřeba restart služby pro aplikování konfigurace. To má za následek krátkodobé výpadky, které mohou vést třeba k nepřidělení IP adresy a tudíž nefunkčnímu připojení.

Pro DHCP server se aktuálně používá ISC DHCP. Ten byl poprvé vydaný již v roce 1999 a do roku 2007 nepodporoval DHCPv6. DNS server je postaven na softwaru BIND9. Ten, přestože byl z dřívějších verzí nově přepsán, obsahuje stále zranitelnosti [7].

3.2 Nástroje pro DHCP server

Drtivá většina softwarů poskytující funkcionalitu DHCP serveru je open-source. Analýza – shrnuto v tabulce 3.1 – byla provedena nad těmito:

ISC DHCP – aktuálně používaný software, napsaný v jazyce C. Nevýhody byly zmíněny výše – nelze ukládat data do databáze a podpora IPv6 není kompletní. Výhodou je stálý vývoj. Server je možné omezeně spravovat pomocí OMAPI [8] – nástroj příkazové řádky využívající vlastní syntaxi. Autoři ISC DHCP doporučují [9], aby správci zvážili použití

Kea a implementovali ISC DHCP pouze v případě, že Kea nesplňuje jejich potřeby.

Kea – nejmladší z porovnávaných nástrojů, nástupce ISC DHCP. Oproti němu plně podporuje IPv6 a ukládání leasů („zápůjčky“ adres) a rezervací IP adres do databáze. K tomu lze využít MySQL, PostreSQL nebo Cassandra databázi. Naopak nedisponuje funkcionalitou DHCP klienta a relay agenta. Kea je sice open-source, ale pokročilá funkcionalita [10] (např. správa rezervací IP adres pomocí API) je placená. Toto rozšíření v ceně 499 $ se po emailové komunikaci [11] povedlo získat pro akademické účely zdarma. Protože se však již nejedná o open-source software, není jeho implementace součástí této práce. REST[6] API umožňuje získávání statistik a práci s leasy a konfigurací. Do budoucna by měla přibýt podpora správy subnetů. Software je ve fázi aktivního vývoje a je k němu dostupná podrobná dokumentace. V následující verzi [12] – plánované vydání na konci května 2019 – má přibýt podpora ukládání subnetů a adresních poolů do databáze.

Jagornet DHCP – jediný z porovnávaných serverů napsaný v Javě, v základu tedy podporuje Apache Derby databázi. Dále může být dle [13] nakonfigurován k použití H2, SQLite, Mongo nebo databáze přístupné přes JDBC[7]. Software nemá možnost ovládání přes API. Současná verze byla uvedena v červenci 2016.

dhcpy6d – již z názvu lze vyčíst základní informace. Jde o server psaný v Pythonu s podporou pouze DHCPv6. Podle [14] podporuje ukládání leasů a informací o zařízeních do MySQL, PostgreSQL a SQLite databází, nedisponuje žádným API. Poslední verze byla vydána v říjnu 2018 a vývoj stále pokračuje.

dnsmasq – jméno napovídá, že se jedná primárně o DNS server. Tento software [15] však poskytuje i možnosti DHCP serveru, router advertisementu nebo bootování ze sítě. Byl navržen pro malé sítě, přenosné hotspoty nebo například sdílení připojení přes chytré telefony. Podporuje IPv4 i IPv6, ale nemá možnost ukládání dat do databáze. První verze byla vydaná v roce 2001, poslední pak v říjnu 2018. Autor pro dnsmasq nevytvořil žádné API. REST API vzniklo jako samostatný projekt [16] v roce 2013 a od dubna 2014 nedošlo k žádným úpravám. Umožňuje pouze prohlížení leasů.

Jako DHCP server byl vybrán software Kea. Ten oproti ostatním kandidátům vyniká zejména v použitelnosti jak pro DHCPv4, tak DHCPv6. Dále je dobře zdokumentovaný a podporuje různé druhy databází na backendu.

[6] Representational State Transfer

[7] Java Database Connectivity – Java API pro přístup k relačním databázím

Tabulka 3.1: Srovnání softwarů DHCP serverů

Software	DHCP	DHCPv6	API	Datum vydání poslední verze	Programovací jazyk
ISC DHCP	✓	✓	OMAPI	únor 2018	C
Kea	✓	✓	REST	prosinec 2018	C++
Jagornet DHCP	✓	✓	✗	červenec 2016	Java
dhcpy6d	✗	✓	✗	říjen 2018	Python
dnsmasq	✓	✓	REST	říjen 2018	C

3.3 Nástroje pro DNS server

Pro správu DNS existuje celá řada jak volných, tak komerčních systémů, lišících se svoji funkcionalitou. Pro porovnání – zjednodušeno v tabulce 3.2 – byly vybrány tyto open-source softwary:

BIND – nejstarší a nejčastěji nasazované řešení [17]. Poskytuje funkcionalitu jak autoritativního, tak rekurzivního DNS serveru. Podporuje DNSSEC a DNS over TLS. BIND umožňuje ukládat zónová data do databáze pomocí dvou rozšíření [18]. První možností je DLZ[8], které data předává v textové podobě a je nutno je před odesláním překonvertovat, což způsobuje zpomalení. DLZ API navíc brání správnému předávání DNSSEC podepsaných dat. Druhým řešením je DynDB, které data vrací ve správném formátu pro vytvoření odpovědi klientovi. DynDB API obsahuje doplňkové nastavení, umožňující například předběžně se dotazovat na záznamy a uložit je do mezipaměti, což zlepšuje výkon při spouštění serveru nebo po vytvoření nové zóny.

PowerDNS – software skládající se ze tří hlavních částí, které lze provozovat i samostatně – autoritativního DNS serveru, rekurzoru a dnsdist. PowerDNS autoritativní server je dle [19] jediným řešením, které nativně podporuje všechny hlavní databáze. Měnit nastavení lze nejen pomocí terminálu, ale existuje řada nástrojů [20], které toto umožňují pomocí API nebo přímého přístupu do databáze. Plně podporuje DNSSEC a pomocí dnsdist i DNS over TLS. Dnsdist [21] funguje jako DNS loadbalancer provozu, pro funkčnost DNS serveru není nutná jeho instalace.

dnsmasq – jak již bylo zmíněno u DHCP nástrojů, tento software byl vytvořený pro podporu malých lokálních sítí. Nejedná se o rekurzor, v základu pouze odpovídá na požadavky pomocí vlastní mezipaměti, eventuálně je přeposílá na rekurzivní servery a následně ukládá. Může být nakonfigurován i jako autoritativní [22]. Podporuje DNSSEC a pomocí API je možné zobrazit a mazat dostupné zóny, zobrazit, přidat nebo ode-

[8] Dynamically Loadable Zones

brat záznam existující zóny, případně zálohovat a obnovit zóny. Vždy je ale nutné server restartovat.

Knot DNS – software od české společnosti CZ.NIC. Je neustále vyvíjen tak, aby poskytoval vysoký výkon, byl stabilní a bezpečný. Podporuje DNSSEC a DNS over TLS. Konfigurace může být dle [23] uložena do binární databáze, software však nemá žádné API. Jedná se pouze o autoritativní server, jako rekurzivní server může být využit Knot Resolver [24].

Unbound – další aktivně vyvíjený nástroj poskytující rekurzivní DNS server s možností [25] použití jako autoritativní v malé lokální síti. Pro plně funkční autoritativní DNS server je možné využít NSD [26] od stejného vývojáře. Unbound podporuje DNSSEC a DNS over TLS. Chybí možnost ukládání dat do databáze a ovládání přes API.

Tabulka 3.2: Srovnání softwarů DNS serverů

Software	DNSSEC	DoT	API	Datum vydání poslední verze	Programovací jazyk
BIND	✓	✓	pro databázové doplňky	duben 2019	C
PowerDNS	✓	✓	REST	březen 2019	C++
dnsmasq	✓	✗	REST	říjen 2018	C
Knot DNS	✓	✓	✗	duben 2019	C
Unbound	✓	✓	✗	březen 2019	C

Pro správu DNS byl zvolen PowerDNS, protože umožňuje spouštět autoritativní a rekurzivní DNS server nezávisle na sobě, podporuje IPv6 a DNSSEC. Díky možnosti ukládání dat do databáze, je možné integrovat ovládání do IPAMu.

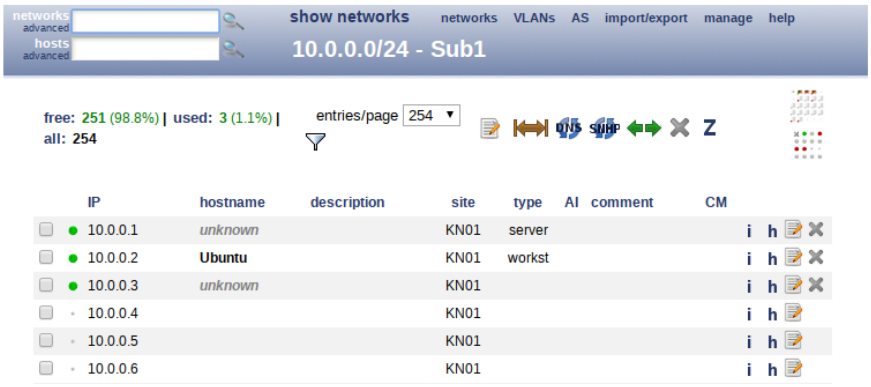
3.4 Nástroje pro správu IP

IPAM softwary jsou oproti předchozím mnohem více komerční záležitostí a neexistuje příliš mnoho open-source řešení. Srovnány byly následující:

GestióIP – software podporující IPv4 i IPv6, MySQL databázi a zobrazení dat z PowerDNS databáze. Protože je nástroj napsaný v perlu a první verze byla vydána již v roce 2009, není webové rozhraní úplně moderní (obrázek 3.1). Práva jsou zde řešena pomocí uživatelských skupin, které je možno vytvářet a editovat. Hledat nová zařízení jde prostřednictvím ping, DNS nebo SNMP[9], pomocí kterého lze objevovat i sítě a VLANy[10].

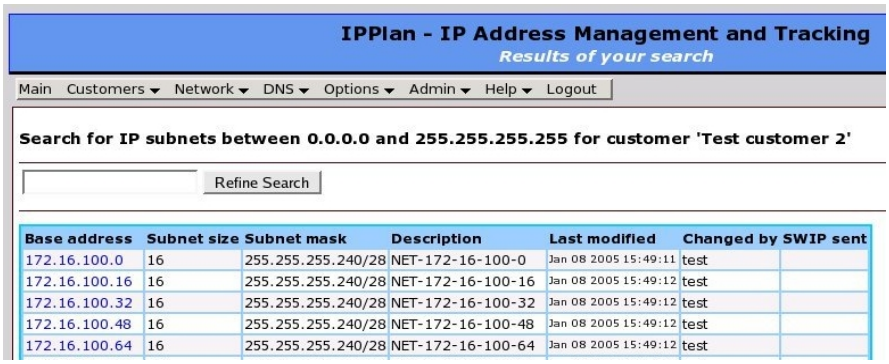
[9] Simple Network Management Protocol
[10] Virtual Local Area Network

Od poslední verze [27] je možná integrace serverů Microsoft DNS a BIND. GestióIP nabízí API jako placené rozšíření.



Obrázek 3.1: Správa subnetu v aplikaci GestióIP

IPplan – zastaralý systém s podporou IPv6 pouze v beta verzi [28]. K ukládání dat jde použít MySQL, PostgreSQL, Oracle nebo Microsoft SQL databázi. Software je napsaný v PHP a využívá XML[11] šablon, pomocí kterých je možné přidávat/odebírat jednotlivé funkce. Zjišťovat stav zařízení lze dle [29] velmi rychle a to i ve velkých sítích, protože příslušné skripty využívají nástroj *nmap*. IPplan umožňuje vytvářet DNS zóny v XML formátu, který je nutno pro potřeby DNS serverů převést do textové podoby. Existuje zde omezené dělené práv pomocí 3 skupin. Příklad stránky uživatelského rozhraní zobrazuje obrázek 3.2.

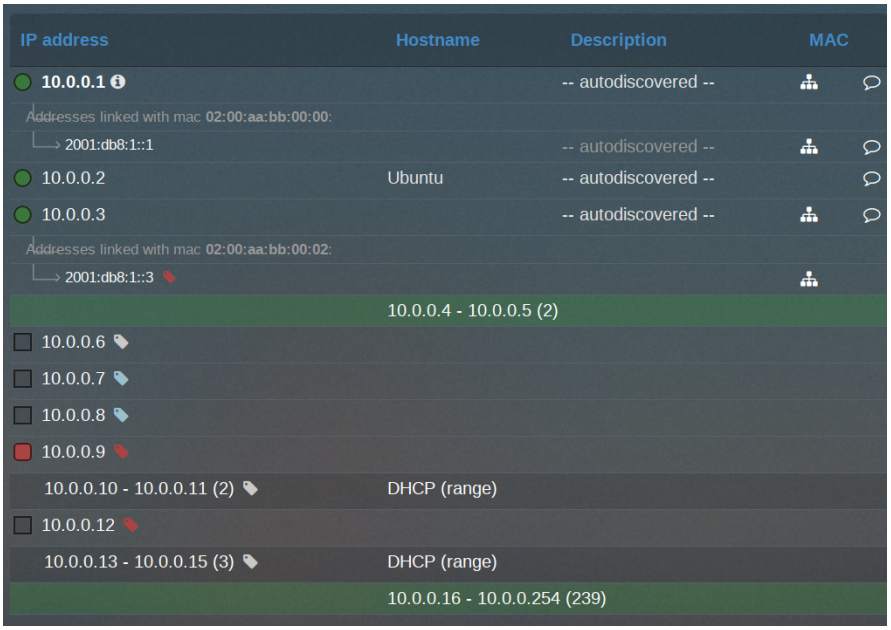


Obrázek 3.2: Webové rozhraní nástroje IPplan (*Zdroj: [30]*)

phpIPAM – nástroj psaný v PHP podporující širokou škálu funkcí [31] od REST API, přes práva jednotlivých uživatelů či skupin, až po přehledné

[11] eXtensible Markup Language

zobrazení využití IPv4 i IPv6 adres (obrázek 3.3). Kromě ukládání dat v MySQL databázi umožňuje napojení na databázi PowerDNS. Díky tomu lze spravovat doménová jména jednotlivých zařízení přímo z web GUI[12] phpIPAMu. Dříve byla zabudovaná podpora i pro DHCP Kea, ale kvůli chybám byla pro aktuální verzi odebrána z uživatelského rozhraní. Stále se však dá přes úpravu nastavení v databázi zapnout a poskytuje tak omezené možnosti náhledu IPv4 i IPv6 subnetů a rezervovaných adres a aktuálních IPv4 leasů. V následující verzi se dle [32] počítá s funkční podporou DHCP nejen pro software Kea. Přidávat nová a zjišťovat stav známých zařízení je možné nejen pomocí utility ping, ale také přes SNMP, pokud je nakonfigurován. Dále je možné hledat nové subnety nebo VLANy. PhpIPAM je trochu kanónem na vrabce, ale jednotlivé moduly se dají vypnout/zapnout v nastavení.



Obrázek 3.3: Přehled využití IP adres v síti v aplikaci phpIPAM

Volba v této kategorii padla na phpIPAM. Ten poskytuje širokou nabídku užitečných funkcí. Z těch je využita zejména možnost uživatelských účtů a omezení práv pro jednotlivé sekce a subnety. Dále propojení s databází PowerDNS, díky čemuž je možné spravovat domény a DNS záznamy zařízení, a zobrazení dat z Key.

[12] Graphical User Interface

Kapitola 4

Realizace

Na začátku této kapitoly je zmíněn hardware, na kterém probíhá testování a jeho konfigurace. Dále je popsáno, jak proběhla instalace a konfigurace jednotlivých softwarů, metody testování a jejich výsledky.

4.1 Hardware

Testování probíhá na virtuálních zařízeních. Vybraný software běží na stroji se systémem Debian 9, 20 GB diskem, 4 GB RAM a dvěma jádry z virtualizace nad procesorem Intel Xeon E5-2620 @ 2.00GHz. Dále jsou k dispozici dvě uživatelské stanice pro ověřování funkčnosti. Na jedné běží Ubuntu 18.04, na druhé pak Windows 10 Education. Všechny stroje mají dvě síťová rozhraní – jedno s veřejnou adresou pro dostupnost přes SSH[13], resp. RDP[14], druhé pro testování vybraných nástrojů v lokální síti. Pro dostupnost serverů stále na stejné adrese bylo toto rozhraní nakonfigurováno staticky – viz výpis kódu 4.1. Dvě adresy jsou přidány z důvodu spuštění autoritativního DNS serveru a rekurzoru na stejném zařízení (popsáno v sekci 4.2.2). Konfigurace záměrně neobsahuje, standardně nastavovanou, výchozí bránu, protože testování probíhá pouze v lokální síti.

Výpis kódu 4.1: Statická konfigurace druhého síťového rozhraní

```
iface ens7 inet static
        address 10.0.0.1/8
        dns-nameserver 10.0.0.1

iface ens7 inet6 static
        address 2001:db8:1::1
        netmask 64
        dns-nameserver 2001:db8:1::1
```

[13] Secure Shell
[14] Remote Desktop Protocol

```
iface ens7 inet static
        address 10.0.0.100/8

iface ens7 inet6 static
        address 2001:db8:1::100
        netmask 64
```

4.2 Instalace a konfigurace

4.2.1 Kea

Instalace proběhla podle instrukcí [33] a [34], jediná komplikace byla chybějící, nikde nezmíněná, knihovna *libmariadbclient-dev*. Kvůli té nešlo během instalace nastavit použití s MySQL. Po doinstalování knihovny již nebyl žádný problém.

Dále bylo, také podle dokumentace, nastaveno DHCPv4 a DHCPv6. Důležité části konfiguračních souborů můžeme vidět ve výpisu kódu 4.3, resp. 4.4.

Aby v síti fungovalo dynamické přiřazování IPv6 bylo potřeba zprovoznit Router Advertisement. Protože v síti není žádné zařízení, které by tyto pakety vysílalo, byl nakonfigurován router advertisement daemon *radvd*[35] a nastavena stateful konfigurace – zařízení si negenerují adresy (pseudo)náhodně, ale dostávají je přidělené z adresního rozsahu. Spouštěn byl příkazem `radvd -C /etc/radvd.conf -m logfile -l /usr/local/var/log/radvd.log`, který zajistí použití příslušných souborů pro načtení konfigurace a logování. Konfigurační soubor je zobrazen ve výpisu kódu 4.2.

Výpis kódu 4.2: Konfigurace radvd

```
interface ens7 {
        #povoleni RA na interface
        AdvSendAdvert on;
        MinRtrAdvInterval 30;
        MaxRtrAdvInterval 100;
        #stateful protokol pro IP adresy
        AdvManagedFlag on;
        #stateful protokol pro ostatni
        AdvOtherConfigFlag on;
        prefix 2001:db8:1::/64
        {
                #vypnuti autonomni konfigutrace
                AdvAutonomous off;
        };
};
```

Výpis kódu 4.3: Konfigurace DHCPv4

```
{
  "Dhcp4": {
    "valid-lifetime": 4000,
    "renew-timer": 1000,
    "rebind-timer": 2000,

    "interfaces-config": {
      "interfaces": [ "ens7" ]
    },

    "lease-database": {
      "type": "mysql",
      "name": "kea",
      "user": "kea",
      "password": "kea"
    },

    "hosts-database": {
      "type": "mysql",
      "name": "kea",
      "user": "kea",
      "password": "kea"
    },
    "match-client-id": false,
    "host-reservation-identifiers": [ "hw-address" ],
    "subnet4": [
      {
        "subnet": "10.0.0.0/23",
        "id": 1,
        "pools": [
            { "pool": "10.0.0.0/24" }
        ]
      }
    ],
    "option-data": [
        {
            "name": "domain-name-servers",
            "data": "10.0.0.1"
        }
    ]
  }
}
```

Výpis kódu 4.4: Konfigurace DHCPv6

```
{
  "Dhcp6": {
    ...
    "preferred-lifetime": 3000,

    ...
    "mac-sources": [ "any" ],
    "host-reservation-identifiers": ["hw-address"],

    "subnet6": [
      {
        "subnet": "2001:db8:1::/64",
        "id": 1,
        "pools": [
            { "pool": "2001:db8:1::2/104" }
        ],
        "interface": "ens7"
      }
    ],
    "option-data": [
        {
            "name": "domain-name-servers",
            "data": "2001:db8:1::1"
        }
    ]
  }
}
```

Dále byl nakonfigurován – viz výpis kódu 4.5 – Kea Control Agent, který zpřístupňuje RESTový interface pro ovládání serveru a některých jeho částí. Umožňuje tak řízení přes API. Pro práci s DHCPv4 nebo v6 je potřeba přidat do jejich nastavení příslušné sockety a knihovny. Doplnění konfigurace je vidět ve výpisu kódu 4.6.

Výpis kódu 4.5: Konfigurace Kea Control Agenta

```
{
  "Control-agent": {
    "http-host": "10.0.0.1",

    "control-sockets": {
        "dhcp4": {
        "socket-type": "unix",
        "socket-name": "/tmp/kea-dhcp4-ctrl.sock"
      },
        "dhcp6": {
        "socket-type": "unix",
        "socket-name": "/tmp/kea-dhcp6-ctrl.sock"
      }
    }
  }
}
```

Výpis kódu 4.6: Doplnění souborů s konfigurací DHCPv4/v6 pro fungování s Control Agentem (X označuje verzi protokolu)

```
{
  "DhcpX": {
  ...
    "control-socket": {
        "socket-type": "unix",
        "socket-name": "/tmp/kea-dhcpX-ctrl.sock"
    },

    "hooks-libraries": [
        {
            "library": "/usr/local/lib/hooks/
               libdhcp_stat_cmds.so",
            "parameters": { }
        },
        {
            "library": "/usr/local/lib/hooks/
               libdhcp_lease_cmds.so",
            "parameters": { }
        }
    ],
  }
}
```

4.2.2 PowerDNS

Nejprve byl software nainstalován z debian balíčků ve verzi 4.0 (poslední dostupná stable verze). Novější jsou dostupné [36] jenom jako sid(unstable) a experimental. Samostatně fungoval autoritativní server bez problémů, to se změnilo při zprovozňování rekurzoru. Protože obě aplikace používají port 53, bylo nejprve potřeba vyřešit spuštění obou zároveň na stejném stroji. Toho bylo dosaženo pomocí dvou rozdílných IP adres, protože každá aplikace pracovala s konkrétní IP a nedocházelo tak ke kolizi na portu.

Další problém nastal s rekurzí samotnou. Při povolení rekurze z adresy localhostu byl rekurzor dostupný z celého internetu a vznikal tak tzv. open resolver [15]. Naopak při nepřidání této adresy do povolených nefungoval rekurzor vůbec.

Protože se chybu nepodařilo i přes různá nastavení odstranit, byl PowerDNS odinstalován a pomocí návodu [37] nainstalována verze 4.1. Konfigurace proběhla podobně jako u předchozí verze podle manuálu [38] a [39]. Úpravy v nastavení autoritativního serveru jsou vidět ve výpisu kódu 4.7. Změněnou konfiguraci rekurzoru zobrazuje výpis kódu 4.8.

Výpis kódu 4.7: Konfigurace PowerDNS autoritativního serveru

```
# Allow DNS updates from these IPs
allow-dnsupdate-from=127.0.0.0/8, ::1
allow-dnsupdate-from+=10.0.0.1, 2001:db8:1::1
allow-dnsupdate-from+=10.0.0.100, 2001:db8:1::100

# Enable/Disable DNS update (RFC2136) support
dnsupdate=yes

# Configuration of the backends
launch=gmysql
gmysql-dbname=pdns
gmysql-user=pdns
gmysql-password=pdns@123
gmysql-dnssec=yes

# Local IP addresses to which we bind
local-address=127.0.0.1,10.0.0.100

# Local IP address to which we bind
local-ipv6=::1,2001:db8:1::100
```

[15] Termín open resolver označuje rekurzivní DNS server, který odpovídá na dotazy z celého internetu. Toho lze zneužít pro DDoS (Distributed Denial of Service) útok typu DNS amplification, kdy útočník podvrhne, odkud byl dotaz poslán. Odpověď je pak směřována právě na toto zařízení. Protože je odpověď větší než velikost dotazu, dá se i s nízkokapacitním připojením vyvolat velký útok

Výpis kódu 4.8: Konfigurace PowerDNS rekurzoru

```
# Only allow these netmasks to recurse
allow-from=127.0.0.0/8, 10.0.0.0/8
allow-from+=::1/128, fe80::/10, 2001:db8:1::/64

# Zones for which we forward queries
forward-zones=felkn.cvut.cz=127.0.0.1:53;[::1]:53
forward-zones+=0.0.10.in-addr.arpa
   =127.0.0.1:53;[::1]:53
forward-zones+=1.0.10.in-addr.arpa
   =127.0.0.1:53;[::1]:53
forward-zones+=0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.
   b.d.0.1.0.0.2.ip6.arpa=127.0.0.1:53;[::1]:53


# IP addresses to listen on
local-address=10.0.0.1, 2001:db8:1::1
```

4.2.3 phpIPAM

Po kompletaci potřebných závislostí byl software bez obtíží nainstalován dle návodu [40]. Následně byl zprovozněn apache mód *mod_rewrite*, který umožňuje v nastavení zapnout možnost Prettify links. Ta mění složité URL[16](`?page=administration&link2=settings`) na lehce čitelné (`/administration/settings/`) a je potřeba pro funkčnost API. To bylo v nastavení aplikace zapnuto a byl pro ně vytvořen klíč. Dále byly v nastavení vypnuty/zapnuty (ne)potřebné moduly. Pro potřeby této práce jsou využívány moduly pro API, PowerDNS, překládání DNS jmen a záznam změn. Následně byly zadány údaje pro přístup do PowerDNS databáze, uživatelské skupiny a jednotliví uživatelé.

Co nejde ve webovém rozhraní zapnout je modul pro DHCP, který byl zprovozněn úpravou v databázi. V tabulce *settings* byla změněna položka *enableDHCP* na hodnotu 1 u položky *DHCP* byla upravena cesta ke konfiguračnímu souboru DHCP serveru. Vzhledem k tomu, že Kea má nastavení DHCPv4 a v6 rozdělené do dvou souborů, byly tyto dva spojeny do jednoho a naformátovány tak, aby splňovaly JSON[17] standard.

[16] Uniform Resource Locator
[17] JavaScript Object Notation

4.3 Testování

Kromě „uživatelského“ testování, během kterého byly stroje různě připojovány, odpojovány a měněny jejich záznamy – obecně úkony, které bude se zařízeními dělat uživatel nebo správce, byla ověřena funkčnost dostupného API a provedeno zátěžové testování DHCP a DNS.

4.3.1 Kea

Uživatelské testování ověřilo funkčnost přidělování IPv4 i IPv6 adres z definovaných adresních rozsahů a to jak dynamicky, neznámým zařízením, tak staticky podle rezervací IP adres jednotlivých hostů.

Při testování API byla ověřena funkčnost dostupných příkazů [41]. Téměř všechny splňují očekávanou funkcionalitu. Mírně zavádějící je příkaz *leaseX-add*, který při zvolení již použité IP adresy se stejnou MAC[18] adresou, nepřidá nový záznam, ani stávající neaktualizuje, ale přesto vrací výsledek, že lease byl přidán. Příkaz *leaseX-wipe* není dostupný pro MySQL databázový backend. Ačkoli by dle [42] mělo jít komunikaci přes API zabezpečit pomocí reverzní proxy a ověřování na základě certifikátů, nepodařilo se toto zabezpečení vynutit a Control Agent reagoval i na neautentikované požadavky. Ovládat šel tedy v závislosti na nastavení, buďto pouze z lokální stanice nebo z celé sítě/internetu.

Během zátěžového testování byla porovnána rychlost ukládání DHCP leasů do CSV[19] souboru a do databáze. Ve statistikách nástroje perfdhcp – spouštěno s parametry *-4 -l ens7 -r 150 -R 16900000* – můžeme vidět (viz tabulka 4.1), že při 150 požadavcích za sekundu je výkonnost lepší při využití lokálního CSV souboru. V neprospěch databáze zde hraje slabý hardware nebo neoptimalizovaný MySQL server. Při frekvenci pouze 100 požadavků za sekundu byla výkonnost již srovnatelná. Průměrně se při ukládání do databáze poměr DHCP požadavků pohyboval okolo 115 za sekundu.

4.3.2 PowerDNS

U PowerDNS proběhlo uživatelské testování velmi jednoduše – pomocí nástroje *dig* bylo ověřeno, zdali vytvořené záznamy opravdu existují. Dotaz na adresy hosta `debian.dcgi.felkn.cvut.cz` a odpověď na něj můžeme vidět ve výpisu kódu 4.9.

Protože vytvářet a měnit záznamy lze přímo z phpIPAMu, nebyl pro API testován každý dostupný příkaz, ale pouze náhodný výběr. Všechny zkoušené dotazy fungovaly jak pro autoritativní server, tak pro rekurzor. Povolení funkčnosti API v nastavení zároveň spouští integrovaný webserver, který poskytuje statistiky dotazovaných domén.

[18] Media Access Control
[19] Comma-separated Values

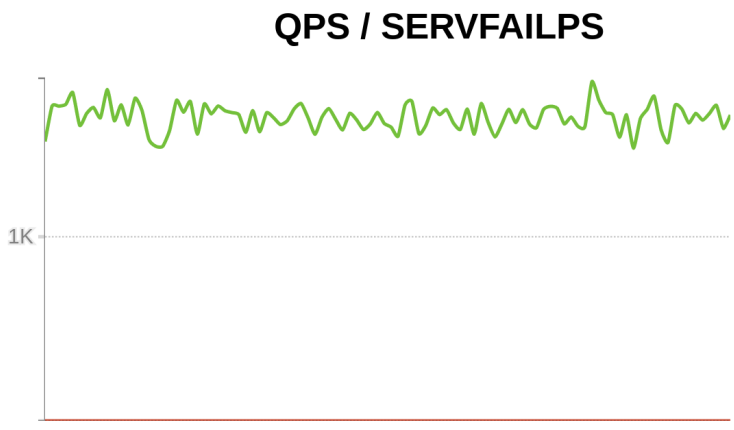
CSV	MySQL
Rate statistics	***Rate statistics***
Rate: 147.017 4-way exchanges/second	Rate: 113.707 4-way exchanges/second
Statistics for: DISCOVER-OFFER*	**Statistics for: DISCOVER-OFFER***
sent packets: 134036	sent packets: 134208
received packets: 134035	received packets: 104246
drops: 1	drops: 29962
min delay: 0.799 ms	min delay: 5.412 ms
avg delay: 1.466 ms	avg delay: 408.935 ms
max delay: 252.304 ms	max delay: 737.685 ms
std deviation: 4.240 ms	std deviation: 50.144 ms
collected packets: 0	collected packets: 28742
Statistics for: REQUEST-ACK*	**Statistics for: REQUEST-ACK***
sent packets: 134035	sent packets: 104246
received packets: 134035	received packets: 104144
drops: 0	drops: 102
min delay: 0.489 ms	min delay: 13.768 ms
avg delay: 0.998 ms	avg delay: 412.382 ms
max delay: 35.920 ms	max delay: 737.737 ms
std deviation: 0.748 ms	std deviation: 50.262 ms
collected packets: 0	collected packets: 0

Tabulka 4.1: Srovnání rychlosti metod ukládání DHCP4 leasů

Výpis kódu 4.9: Vyhledání přiřazených IP adres pomocí nástroje *dig* (výpis zkrácen)

```
@ubuntu:/$dig gw.felkn.cvut.cz @10.0.0.1 ANY

; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<
        >> gw.felkn.cvut.cz @10.0.0.1 ANY

;; flags: qr rd ra; QUERY: 1, ANSWER: 2,
                 AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;gw.felkn.cvut.cz.                IN      ANY

;; ANSWER SECTION:
gw.felkn.cvut.cz.    10800    IN    A       10.0.0.1
gw.felkn.cvut.cz.    3600     IN    AAAA    2001:db8:1::1

;; Query time: 48 msec
```

Pro zátěžové testování autoritativního DNS serveru existuje nástroj *dnsperf* [43], který posílá dotazy a hodnotí, kolik jich zvládl server odbavit. Pro tento test bylo v databázi vytvořeno přibližně 210000 náhodných A záznamů pro domény felkn.cvut.cz, dcgi.felkn.cvut.cz a dce.felkn.cvut.cz. Následně byl vygenerován soubor s 386672 dotazy na zařízení v těchto doménách. Výsledky testu jsou ve výpisu kódu 4.10. Můžeme vidět, že byla vrácena odpověď na všechny dotazy, z toho pro necelých 15% existoval na autoritativním serveru záznam, pro zbytek nikoli. Počet dotazů za sekundu v průběhu testu znázorňuje graf na obrázku 4.1.



Obrázek 4.1: Počet dotazů za sekundu směrovaných v průběhu testu *dnsperf* na autoritativní DNS server

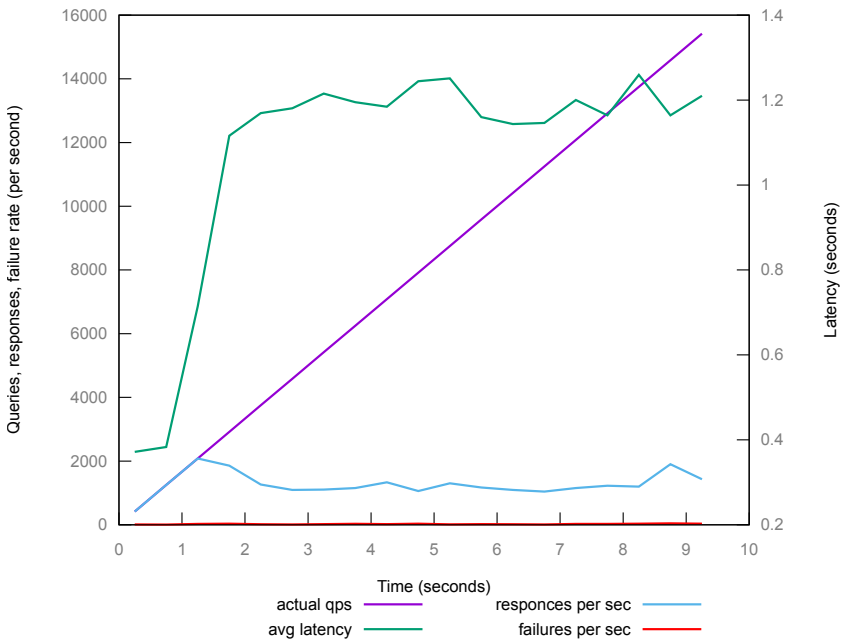
Výpis kódu 4.10: Výsledky testu autoritativního serveru pomocí *dnsperf*

```
DNS Performance Testing Tool
Nominum Version 2.0.0.0

[Status] Command line: dnsperf -s 10.0.0.1 -a
   10.0.0.2 -d q_cvut.cz -n 1 -l 600 -c 30
[Status] Stopping after 600.000000 seconds or 1 run
   through file

Statistics:
  Queries sent:         386672
  Queries completed:    386672 (100.00%)
  Queries lost:         0 (0.00%)

  Response codes:       NOERROR 57052 (14.75%),
     NXDOMAIN 329620 (85.25%)
  Average packet size:  request 36, response 86
  Run time (s):         239.930288
  Queries per second:   1611.601450

  Average Latency (s):  0.062019
        (min 0.023158, max 23.937393)
```

Obdobný nástroj existuje také pro testování rekurzorů. Jedná se o *resperf* [44]. Aby při testech nedocházelo k úplnému zahlcení produkčního serveru, inkrementuje se počet posílaných dotazů lineárně. Pro tento test byl stažen vzorový soubor s 10 miliony dotazů. Průběh testu můžeme vidět na obrázku 4.2, výsledky pak ve výpisu kódu 4.11.

Výpis kódu 4.11: Výsledky testu rekurzivního serveru pomocí *resperf*

```
DNS Resolution Performance Testing Tool
Nominum Version 2.0.0.0

[Status] Command line: resperf -P 20190513-2005.
   gnuplot -s 10.0.0.1 -a 10.0.0.2 -d queryfile
[Status] Reached 65536 outstanding queries

Statistics:
  Queries sent:         75791
  Queries completed:    75791
  Queries lost:         0
  Run time (s):         100.000000
  Maximum throughput:   2082.000000 qps
  Lost at that point:   0.00%
```



Obrázek 4.2: Počet dotazů za sekundu směrovaných v průběhu testu *dnsperf* na rekurzivní DNS server

4.3.3 phpIPAM

Nad phpIPAMem proběhlo pouze uživatelské testování, které pomocí více uživatelských účtů s různými přístupovými právy ověřilo funkčnost vytváření subnetů, přidávání a odebírání zařízení, správu DNS domén a záznamů. Bylo vytvořeno několik adresních rozsahů a testovacích domén.

V IPv4 byla vytvořena testovací síť `10.0.0.0/23`(*felkn*) se dvěma podsítěmi `10.0.0.0/24`(*dcgi.felkn*) a `10.0.1.0/24`(*dce.felkn*). Původní plán byl, že síť *felkn* bude sloužit „superadminovi“ pro rychlý přehled nad všemi subnety, ale ukázalo se, že to způsobuje zmatek a nekonzistenci nastavení. Není tedy doporučeno vytvářet překrývající se sítě. Pro IPv6 byla vytvořena pouze jedna síť. PhpIPAM umožňuje svázání IPv4 a IPv6 adres na základě MAC adresy, názvu, IP adresy nebo vlastníka zařízení. Testováno bylo propojení pomocí MAC, které fungovalo bezchybně.

Správa domén a DNS záznamů je uživatelsky přívětivá, neumožňuje však, na rozdíl od správy sítí, omezení podle uživatelů. Každý uživatel tak může měnit záznamy všech zařízení nezávisle na tom, jestli spadají do oblasti/subnetu, kde má právo editovat či nikoli. Jediné, co lze omezit, je viditelnost celého PowerDNS modulu pro jednotlivé uživatele.

Uživatelské rozhraní je vesměs intuitivní, občas se najde například nějaké tlačítko, které by mohlo být uživateli bez potřebných práv skryto, namísto

zobrazení chybové zprávy nebo žádné reakce aplikace. Lehce zmatečné je nastavení práv dle uživatelské skupiny pro oblast a následně ještě pro každou síť v oblasti samostatně. Pro sítě a zařízení je k dispozici přehledný výpis změn provedených v jejich nastavení.

Protože se jedná o aplikaci, kterou uživatel ovládá přes webové rozhraní, není potřeba využívat API. I přesto bylo otestováno na několika příkladech, kde všechny splňovaly požadovanou funkcionalitu.

Závěr

Cílem této práce bylo prozkoumat nabídku open-source softwarů poskytujících funkcionalitu DHCP serveru a DNS serveru a softwaru pro správu IP adres. Z analyzovaných nástrojů následně vybrat vhodné kandidáty pro kompletní systém na správu sítě.

Práce nejprve ukázala technologie DHCP, DNS a IPAM a popsala nevýhody stávajícího řešení správy sítě na FEL ČVUT. Dále byla provedena analýza softwarů pro jednotlivé části systému a z ní vybrány nástroje pro nahrazení současného řešení. Následně byla popsána instalace a konfigurace každého nástroje a nakonec jejich testování.

Pro DHCP server byl vybrán software Kea, zejména pro jeho podrobnou dokumentaci a aktivní vývoj. Aktuální verze sice nepodporuje požadovanou funkcionalitu, ale vydání nové verze, které by mělo přinést potřebné změny (ukládání subnetů a adresních poolů do databáze a s tím spojené ovládání přes API), je plánováno na konec května 2019.

DNS server obsluhuje software PowerDNS, který umožňuje samostatný běh autoritativního a rekurzivního serveru. Další nespornou výhodou je přímé provázání s nástrojem pro správu IP adres.

Z porovnávaných nástrojů pro správu IP adres byl phpIPAM jedinou možnou volbou. Má moderní rozhraní a širokou nabídku funkcí. V následující verzi má přibýt podpora pro všechny DHCP servery.

Aktuální verze vybraných softwarů dohromady vytváří plně funkční systém pro správu sítě. Některá funkcionalita není dostupná, což ale nijak nebrání funkčnosti. Následující verze vybraných nástrojů by měli tuto funkcionalitu přinést a umožnit tak spravovat síť ještě efektivnější.

Bibliografie

1. DROMS, Ralph. *Dynamic Host Configuration Protocol* [online]. 1993 [cit. 2019-04-18]. Dostupné z: `https://www.rfc-editor.org/rfc/rfc1541.txt`. RFC. RFC Editor.
2. BAUL, Himadri Shekhaar. *Understanding Dynamic Host Configuration Protocol (DHCP) working principle* [online]. 2018 [cit. 2019-05-04]. Dostupné z: `http://whilenetworking.com/2018/04/19/understanding-dynamic-host-configuration-protocol-dhcp-working-principle/`.
3. MOCKAPETRIS, Paul. *Domain names – implementation and specification* [online]. 1987 [cit. 2019-04-20]. Dostupné z: `https://www.rfc-editor.org/rfc/rfc1034.txt`. RFC. RFC Editor.
4. CZ.NIC, z. s. p. o. *O DNSSEC* [online]. 2019 [cit. 2019-05-02]. Dostupné z: `https://www.nic.cz/page/513/about-dnssec/`.
5. CZ.NIC, z. s. p. o. *DNSSEC* [online]. 2018 [cit. 2019-04-30]. Dostupné z: `https://www.dnssec.cz/`.
6. HU, Zi et al. *Specification for DNS over Transport Layer Security (TLS)* [online]. 2016 [cit. 2019-05-04]. Dostupné z: `https://www.rfc-editor.org/rfc/rfc7858.txt`. RFC. RFC Editor.
7. GOLDLUST, Suzanne; CONRY, Brian. *BIND 9 Security Vulnerability Matrix* [online]. 2019 [cit. 2019-05-01]. Dostupné z: `https://kb.isc.org/docs/aa-00913`.
8. GOLDLUST, Suzanne. *ISC DHCP 4.4 Manual Pages – omapi* [online]. 2019 [cit. 2019-04-30]. Dostupné z: `https://kb.isc.org/docs/isc-dhcp-44-manual-pages-omapi`.
9. *ISC DHCP* [online]. 2018 [cit. 2019-04-30]. Dostupné z: `https://www.isc.org/downloads/dhcp/`.
10. *Kea Premium Hook Library – Kea 1.5 package* [online]. 2018 [cit. 2019-05-01]. Dostupné z: `https://www.isc.org/product/kea-premium-1-5/`.

11. LASKY, Jason. *Re: [ISC] DHCP Form from CTU at Prague* [elektronická pošta]. 2019 [cit. 2019-05-01]. Příjemce zprávy: pekarvit@fit.cvut.cz 1. května 2019 2:31.

12. *Kea1.6 · Milestones · ISC Open Source Projects / Kea* [online]. 2019 [cit. 2019-05-16]. Dostupné z: `https://gitlab.isc.org/isc-projects/kea/milestones/3`.

13. RABIL, A. Gregory. *Jagornet DHCP Server* [online]. 2012 [cit. 2019-04-28]. Dostupné z: `http://www.jagornet.com/products/dhcp-server/docs`.

14. WAHL, Henri et al. *dhcpy6d* [online] [cit. 2019-04-28]. Dostupné z: `https://dhcpy6d.ifw-dresden.de/`.

15. KELLEY, Simon. *Dnsmasq* [online]. 2018 [cit. 2019-04-28]. Dostupné z: `http://www.thekelleys.org.uk/dnsmasq/doc.html`.

16. PAQUET, Bertrand. *dnsmasq-rest-api* [online]. 2014 [cit. 2019-04-28]. Dostupné z: `https://github.com/bpaquet/dnsmasq-rest-api`.

17. *BIND 9 Open Source DNS Server* [online]. 2018 [cit. 2019-05-01]. Dostupné z: `https://www.isc.org/downloads/bind/`.

18. GOLDLUST, Suzanne; CONRY, Brian. *What is dyndb and how is it better than DLZ?* [online]. 2018 [cit. 2019-05-01]. Dostupné z: `https://kb.isc.org/docs/aa-01420`.

19. *PowerDNS Authoritative Server* [online] [cit. 2019-05-02]. Dostupné z: `https://www.powerdns.com/auth.html`.

20. LMCRO. *WebFrontends* [online]. 2019 [cit. 2019-05-02]. Dostupné z: `https://github.com/PowerDNS/pdns/wiki/WebFrontends`.

21. POWERDNS.COM BV; CONTRIBUTORS, its. *dnsdist Overview* [online]. 2019 [cit. 2019-05-14]. Dostupné z: `https://dnsdist.org/`.

22. KELLEY, Simon. *DNSMASQ* [online]. 2018 [cit. 2019-05-01]. Dostupné z: `http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html`.

23. SALZMAN, Daniel. *Operation — Knot DNS 2.8.1 documentation* [online]. 2019 [cit. 2019-05-01]. Dostupné z: `https://www.knot-dns.cz/docs/2.8/html/operation.html`.

24. *Knot Resolver* [online]. 2019 [cit. 2019-05-01]. Dostupné z: `https://www.knot-resolver.cz/`.

25. *Unbound DNS Server Tutorial* [online]. 2019 [cit. 2019-05-01]. Dostupné z: `https://calomel.org/unbound_dns.html`.

26. *Unbound DNS Server Tutorial* [online]. 2019 [cit. 2019-05-01]. Dostupné z: `https://nlnetlabs.nl/projects/nsd/about/`.

27. UEBEL, Marc. *GestióIP Actualizations* [online]. 2018 [cit. 2019-05-07]. Dostupné z: `http://www.gestioip.net/actualizations_gestioip_en.html`.

28. *ipplan [IP address management and tracking]* [online]. 2010 [cit. 2019-05-14]. Dostupné z: `http://iptrack.sourceforge.net/`.

29. ELLERBROCK, Richard. *IPplan – IP address management and tracking* [online]. 2007 [cit. 2019-05-07]. Dostupné z: `http://iptrack.sourceforge.net/documentation/README.html`. Cesta: bod 18. External command line poller.

30. *Screenshots* [online]. 2010 [cit. 2019-05-08]. Dostupné z: `http://iptrack.sourceforge.net/doku.php?id=screenshots`. obrázek oříznut, původní soubor dostupný z: `http://iptrack.sourceforge.net/screenshots/displaysubnet.jpg`.

31. PETKOVSEK, Miha. *phpIPAM Feature list* [online] [cit. 2019-05-05]. Dostupné z: `https://phpipam.net/documents/features/`.

32. PETKOVSEK, Miha. *Kea DHCP management functional?* [online]. 2016 [cit. 2019-05-05]. Dostupné z: `https://github.com/phpipam/phpipam/issues/777`. Cesta: příspěvek od phpipam ze 7. října 2016 (issuecomment-252345677).

33. *Kea Administrator Reference Manual* [online]. 2018 [cit. 2019-04-21]. Dostupné z: `https://ftp.isc.org/isc/kea/1.5.0/doc/kea-guide.html`.

34. RISK, Vicky; CLEGG, Alan. *Kea build on Debian* [online]. 2019 [cit. 2019-04-21]. Dostupné z: `https://kb.isc.org/docs/kea-build-on-debian`.

35. *radvd.conf (5) – Linux Man Pages* [online] [cit. 2019-05-10]. Dostupné z: `https://www.systutorials.com/docs/linux/man/5-radvd.conf/`.

36. SPI, Inc. *Debian – Package Search Results – pdns-server* [online]. 2019 [cit. 2019-05-13]. Dostupné z: `https://packages.debian.org/search?suite=all&keywords=pdns-server`.

37. *PowerDNS repositories* [online] [cit. 2019-05-13]. Dostupné z: `https://repo.powerdns.com/`. Cesta: Debian; Debian 9; PowerDNS Authoritative Server, Recursor; version 4.1.X.

38. POWERDNS.COM BV. *Authoritative Server Settings* [online]. 2019 [cit. 2019-05-14]. Dostupné z: `https://doc.powerdns.com/authoritative/settings.html`.

39. POWERDNS.COM BV. *Basic setup: configuring database connectivity* [online]. 2019 [cit. 2019-05-14]. Dostupné z: `https://doc.powerdns.com/authoritative/guides/basic-database.html`.

40. PETKOVSEK, Miha. *phpipam installation guide* [online] [cit. 2019-05-14]. Dostupné z: `https://phpipam.net/documents/installation/`.

41. GOLDLUST, Suzanne. *commands · Wiki · ISC Open Source Projects / Kea* [online]. 2018 [cit. 2019-05-15]. Dostupné z: `https://gitlab.isc.org/isc-projects/kea/wikis/designs/commands`.

42. *Kea Administrator Reference Manual* [online]. 2018 [cit. 2019-05-15]. Dostupné z: `https://ftp.isc.org/isc/kea/1.5.0/doc/kea-guide.html`. Cesta: sekce 7.3.

43. *dnsperf (1) – Linux Man Pages* [online] [cit. 2019-05-16]. Dostupné z: `https://www.systutorials.com/docs/linux/man/1-dnsperf/`.

44. *resperf (1) - Linux Man Pages* [online] [cit. 2019-05-16]. Dostupné z: `https://www.systutorials.com/docs/linux/man/1-resperf/`.

Příloha **A**

Seznam použitých zkratek

API Application Programming Interface

BOOTP Bootsrap Protocol

CSV Comma-separated Values

DDoS Distributed Denial of Service

DHCP Dynamic Host Configuration Protocol

DLZ Dynamically Loadable Zones

DNS Domain Name System

DNSSEC Domain Name System Security Extensions

DoT DNS over TLS

ČVUT České vysoké učení technické

FEL Fakulta elektrotechnická

GUI Graphical User Interface

IPAM IP Address Management

JDBC Java Database Connectivity

JSON JavaScript Object Notation

LAN Local Area Network

MAC Media Access Control

RA Router Adrvertisement

RDP Remote Desktop Protocol

REST Representational State Transfer

SNMP Simple Network Management Protocol

SSH Secure Shell

TCP/IP Transmission Control Protocol/Internet Protocol

URL Uniform Resource Locator

VLAN Virtual Local Area Network

XML eXtensible Markup Language

Příloha B

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `conf` ..... konfigurační soubory
  - `access.txt` ..... přístupové údaje
  - `thesis.tex` ..... zdrojová forma práce ve formátu LaTeX
- `text`
  - `thesis.pdf` ..... text práce ve formátu PDF
- `attachment` ..... přílohy
  - `kea.pdf` ..... emailová komunikace se společností ISC