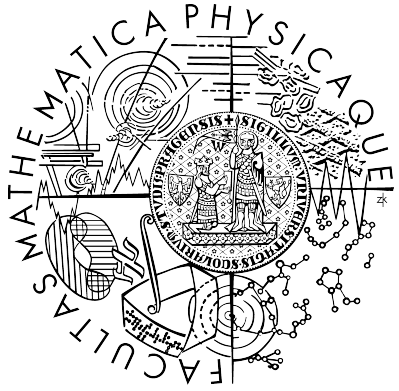
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Petr Šťastný

Analýza stavu DNS serverů domén druhé úrovně

Katedra softwarového inženýrství

Vedoucí bakalářské práce: RNDr. Ing. Jiří Peterka

Studijní program: Informatika
Studijní obor: správa počítačových systémů

Poděkování

Děkuji RNDr. Ing. Jiřímu Peterkovi za vedení této práce a za připomínky a rady.

Dále děkuji sdružení CZ.NIC, zejména výkonnému řediteli Mgr. Ondřeji Filipovi za nápad tento systém pro analýzu domén vytvořit a dále technickému řediteli Ondřeji Surému za konzultace a další nápady.

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce.

V Praze dne 20.5.2007. Petr Šťastný

Obsah

Název práce: Analýza stavu DNS serverů domén druhé úrovně
Autor: Petr Šťastný
Katedra (ústav): Katedra softwarového inženýrství
Vedoucí bakalářské práce: RNDr. Ing. Jiří Peterka
e-mail vedoucího: Jiri.Peterka@mff.cuni.cz
Abstrakt: Práce obsahuje úvod do systému doménových jmen na Internetu (DNS), seznámení s protokolem DNS a se způsobem jeho fungování. Hlavní částí je metodika pro systematické zkoumání konkrétní domény a jejích DNS serverů, obsahující kritéria pro kontrolu správnosti nastavení DNS záznamů a funkčnosti a dostupnosti DNS serverů. Tato metodika je následně implementována v podobě webové aplikace, která umožňuje provádět on-line analýzu domény a vyhodnocení zjištěných chyb a nesrovnalostí. Druhou částí implementace je nástroj pro hromadnou analýzu velkého množství domén, který byl následně využit k analýze všech domén CZ, jejíž stručné výsledky jsou uvedeny v příloze práce.
Klíčová slova: DNS, domény, doménová jména

Title: Analysis of SLD DNS servers state
Author: Petr Šťastný
Department: Department of Software Engineering
Supervisor: RNDr. Ing. Jiří Peterka
Supervisor's e-mail address: Jiri.Peterka@mff.cuni.cz
Abstract: The publication contains a brief introduction into the system of domain names on the Internet (DNS) and into DNS protocol and its functioning. The main part is a methodology for systematic examination of a domain name and its name servers, offering criteria for checking validity of DNS records and functionality and availability of DNS servers. This methodology is then implemented as a web application that allows us to perform an on-line analysis of a domain name and the evaluation of discovered errors and other problems. The second part of the implementation is a tool for bulk analysis of large number of domain names, which was subsequently used for analysis of all domain names under TLD CZ; its short results are mentioned in the end of the work.
Keywords: DNS, domain names

Kapitola 1 – Úvod

1.1 Cíl práce

Tato bakalářská práce má za cíl nejprve provést krátké seznámení se systémem doménových jmen (Domain Name System, DNS), shrnou standardy a doporučení, kterými je třeba se při správě doménových názvů a DNS serverů řídit, dále navrhnout metodiku pro provádění kontrol správnosti nastavení DNS záznamů na DNS serverech a následně tuto metodiku implementovat v podobě internetové aplikace, která umožní provádět jednorázové testy konkrétního doménového názvu druhé úrovně a také dávkové testy pro velké množství domén. Výsledkem dávkového zpracování budou statistické výstupy o stavu testovaného vzorku. Závěrečným cílem práce je provedení analýzy stavu všech domén druhého řádu (SLD) v doméně prvního řádu (TLD) .cz.

1.2 Jak číst tuto práci

Kapitoly 2, 3 a 4 poskytují teoretické i praktické informace o doménových názvech a činnosti protokolu DNS. Vysvětlují všechny pojmy a mechanismy, které je potřeba znát pro sestavení metodiky analýzy funkčnosti DNS serverů a správnosti jejich nastavení a pro následnou implementaci. Pokud některou část mechanismů a možností DNS pro účely této práce nepotřebujeme znát, nejsou v tomto textu zmíněny, popř. je uvedeno, ze kterého zdroje lze čerpat další informace. Tato práce si tedy nebere za cíl říci o DNS vše, ale pouze to nejdůležitější. Především zde není diskutována otázka bezpečnosti a autorizace vůči DNS serverům a příliš se nepracuje s IPv6 adresami, jelikož jejich rozšíření a používání je v současné době zanedbatelné.

1.3 Motivace

Cíl této bakalářské práce vychází z dlouholetého zájmu jejího autora o problematiku doménových jmen a DNS serverů v síti Internet. Na Internetu existuje množství různých nástrojů pro získávání informací o jednotlivých doménách a nastavení jejích DNS serverů, mnohé z nich jsou však již poměrně zastaralé a nerespektují současné trendy v DNS. Zde je taktéž cílem věnovat se dávkovému zpracování a sestavování statistických

výsledků pro velké množství domén, například pro všechny domény druhého řádu, spadající pod konkrétní doménu řádu prvního.

1.4 Podobné projekty

Na Internetu existuje několik aplikací, nabízející podobné služby:

- http://www.dnsreport.com/ - asi nejpokročilejší WWW služba pro analýzu stavu domény. U každého testu vysvětluje souvislosti. Pokročileji testuje MX záznamy, zkouší doručení e-mailu.
- http://www.ripe.net/cgi-bin/delcheck/delcheck2.cgi – Zone Delegation Checker na stránkách organizace RIPE NCC, provádí kontrolu zóny domény a SOA a NS záznamů.
- http://sourceforge.net/projects/dnswalk/ - DNSWalk – Perl skript pro příkazový řádek analyzující obsah zóny domény. Není udržovaný, poslední verze z roku 1997.
- http://www.zonecheck.fr/ - pokročilý nástroj, umí zjistit autonomní systémy a podsítě. Testuje mnoho dalších věcí – ICMP odpověď, MX záznamy, doručení e-mailu. Umí s DNS servery komunikovat po IPv6.
- http://atrey.karlin.mff.cuni.cz/~mj/sleuth/ - méně pokročilý nástroj, nereflektuje poslední trendy v nastavení DNS serverů
- http://www.ip-plus.net/tools/dns_check_set.en.html
- http://www.checkdns.net/ - pokročilý nástroj, navíc zkouška WWW a e-mailů

Za zmínku stojí také analýza COM, NET a ORG domén z června 2005 a podobná analýza ze srpna 2006, obě provedené organizací The Measurement Factory. Výsledky jsou k vidění na http://dns.measurement-factory.com/surveys/index.html.

Kapitola 2 – Doménové názvy a systém DNS

2.1 Pojmenování počítačů

Motivace pro vznik doménových názvů a systému DNS vyplývá z rozdílných způsobů identifikace zařízení v počítačové síti. Počítače se mezi sebou vzájemně identifikují pomocí číselných označení, což je pro ně nejjednodušší a nejpřirozenější způsob, používání označení jmény by pro ně bylo příliš komplikované a pomalé. Na druhé straně je člověk, který si nerad pamatuje identifikační čísla a různé kódy, ale raději všemu přiřazuje jednoduchá a snadno zapamatovatelná jména, která si dobře vybavuje jeho mozek. Vhodné pojmenovávání nabírá na významu v době, kdy mají nejrůznější organizace, uskupení, firmy a jednotlivci potřebu prezentovat se ostatním na Internetu a je pro ně nutností volit jasná a snadno zapamatovatelná označení místa, kde lze jejich prezentaci nalézt.

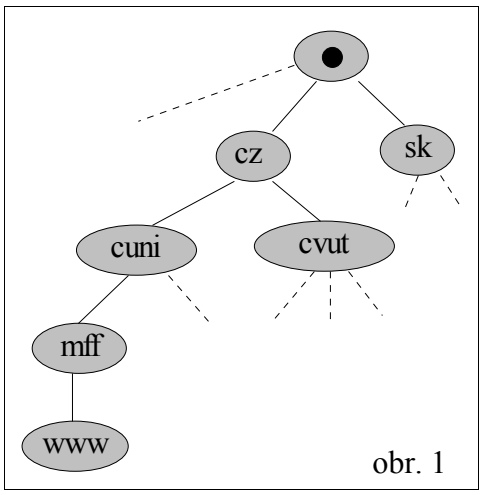
Jelikož tedy počítače si mezi sebou sdělují označení umístění v síti pomocí čísla a lidé názvem, musí existovat mechanismus, který umožní, aby se lidé s počítači dorozuměli. To je jeden z hlavních úkolů systému doménových jmen (DNS – Domain Name System), který se stará o převod mezi číselnými identifikátory (zde IPv4 adresami, dále jen IP adresy, pokud nebude explicitně řečeno, že je řeč o jiné verzi IP protokolu) a pojmenováním (zde doménová jména).

To ale není jediný rys DNS. Druhý zásadní problém vzniká v okamžiku existence velkého počtu doménových názvů, kdy je nutné dát systému pojmenovávání jasný řád a vyvarovat se situace, kdy by byl jeden název použit vícekrát. S tím souvisí i otázka, jak s ohromným množstvím názvů vůbec pracovat a jak z nich co nejrychleji odvozovat potřebnou číselnou identifikaci zařízení v síti. Je nemožné, aby jeden DNS server obsahoval seznam všech existujících názvů, navíc by byl problém zajistit synchronizaci všech DNS serverů, aby jejich úplné seznamy byly stále aktuální a správné. Proto je celý systém řešen hierarchickým způsobem, kdy si DNS servery mezi sebou převodní tabulky rozdělí a navíc mají informace o tom, který server obsahuje které informace.

2.2 Doménové názvy v síti Internet

V síti Internet je komunikace založena na rodině protokolů TCP/IP. Síťový protokol IP zavádí unikátní číselné označení každého zařízení (resp. rozhraní počítače), které je do sítě připojeno. Jedná se o tzv. IP adresu (připomínám, že zde mluvíme pouze o IPv4), což je 32-bitové číslo, které si lidé pro lepší čitelnost rozdělí na 4 části po 8 bitech a ty převedou do desítkové soustavy.

Na Internetu se názvy k IP adresám nepřiřazují napevno, ale jsou pojata jako obecné jmenné označení místa v síti, tedy nikoliv výlučně jako pojmenování konkrétního počítače. Těmto doménovým názvům se mohou dle potřeby příslušné IP adresy měnit, pokud se mění fyzické umístění informací, které jsou s tímto názvem spojeny. Skutečné umístění v síti tedy s názvem nesouvisí, na rozdíl od IP adres, pro které to částečně platí (ty jsou přidělovány především podle světadílů a poté už většinou nedochází k jejich geografickému přemisťování). Struktura doménového názvu bývá spíše dána informacemi, tedy např. webovými stránkami, které se pod tímto názvem schovávají (název firmy, označení zájmové oblasti apod.).



obr. 1

Prostor doménových názvů na Internetu je tvořen stromovou strukturou. Kořenem stromu je jedna speciální doména, které se říká doména nultého řádu, a označuje se tečkou. Názvy přímých potomků každého uzlu (tedy „bratrů“) musí být různé. Celý doménový název je pak tvořen cestou od kořene k nějakému uzlu ve stromě, kde skok mezi uzlem a jeho následovníkem na další úrovni je označen tečkou. Výsledné jméno se píše opačným směrem, kořen je zcela vpravo. Na příkladě na obrázku 1 je znázorněna část stromu, v níž je možno vidět doménový název WWW stránek Matematicko-fyzikální fakulty Univerzity Karlovy - www.mff.cuni.cz - ze zvyku se poslední tečka neuvádí (avšak nelze ji zapomenout v nastavení některých DNS serverů, jak bude zmíněno v dalších kapitolách). Doménám na druhé hladině pod kořenem se říká doména první úrovně či doména nejvyšší úrovně (TLD – Top Level Domain), např. doména cz. Doménám na další hladině se říká domény druhé úrovně

(SLD – Second Level Domain), tedy např. cuni.cz. Domény na druhé úrovni nás budou zajímat nejvíce.

Části názvu mezi tečkami (tedy pojmenování jednotlivých uzlů stromu) se mohou skládat pouze ze znaků anglické abecedy, číslic a znak pomlčky (ten však nesmí být na začátku a ani na konci). Na rozdílu ve velkých a malých znacích nezáleží. Tato část může být dlouhá maximálně 63 znaků, celé doménové jméno pak maximálně 255 znaků.

Zajímavý úvod do DNS, historii a jeho poslání lze nalézt v dokumentu RFC 3467[11].

2.3 Autoritativní DNS servery a delegace správy domén

Uvedený hierarchický systém domén v Internetu řeší hlavní problémy - umožňuje systematické přidělování jmen a delegaci správy celého systému. Každý uzel hierarchie doménových jmen je spravován konkrétním subjektem (organizace, sdružení apod., v nižších úrovních již konkrétní právnické a fyzické osoby), který má na starost administrativní i technické záležitosti, zajišťuje provoz tohoto uzlu a delegaci správy některých podstromů tohoto uzlu dalším subjektům.

Kořenovou doménu (doménu nultého řádu) má na základě dokumentu RFC 2870[9] na starost mezinárodní organizace ICANN (Internet Corporation for Assigned Names and Numbers), která nese odpovědnost za jmenný prostor DNS, distribuci velkých bloků IP adres, správu čísel autonomních systémů aj. Ta předává pravomoc pro správu jednotlivých TLD na další subjekty, které je rozkouskují na SLD a ty dále předávají dalším a dalším subjektům atd. Domény prvního řádu se dělí na ccTLD (country code TLD), které se vztahují k jednotlivým státům světa (např. cz pro Českou republiku, sk pro Slovensko, pl pro Polsko, de pro Německo, …), popř. uniím (např. us – United States, eu – European Union), a gTLD (generic TLD, generické domény), které nemají spojitost se státy, ale byly původně určeny k tématickému rozdělení (com – komerční stránky, org – stránky mezinárodních organizací, net – stránky týkající se sítí aj.). Určení domén není v dnešní době již tolik dodržováno, protože trh s doménami je víceméně volný. Musí být však pevně zachována delegace a musí být vždy zřejmé, kdo zodpovídá za provoz které domény.

Doménu cz, které je určena České republice, má na starost organizace CZ.NIC, což je zájmové sdružení právnických osob. Jeho úkolem je zajišťovat administrativní a technickou stránku provozu této domény. Stanovuje pravidla, podle kterých se domény druhé úrovně *.cz dávají dalším subjektům. To se v současné době činí prostřednictvím tzv. akreditovaných registrátorů, což jsou komerční subjekty, které jsou smluvními partnery CZ.NICu a které prodávají domény druhého řádu koncovým zákazníkům (právnickým či fyzickým osobám) a tímto prodejem v podstatě „delegují“ koupený název. Koupí-li si někdo tímto způsobem např. doménu seznam.cz, je celý příslušný podstrom v doménové hierarchii v jeho správě a může ho celý využívat a případně některé podstromy dále delegovat.

Podobný model jako u domény .cz se používá u většiny ostatních TLD. Je víceméně na příslušné organizaci, jaká stanoví pravidla, kdo a za jakých podmínek může doménové jméno pod danou TLD získat.

Každé doménové jméno (uzel hierarchie tohoto systému, resp. nějaký podstrom) má přiděleny tzv. autoritativní DNS servery. Je to množina serverů, které nesou informace potřebné k práci s danou doménou. Mohou obsahovat již konkrétní údaje (tj. IP adresy, názvy mailserverů atd.) a také především názvy dalších DNS serverů, které jsou autoritativní pro subdomény (tj. domény nižších řádů pod touto doménou). Slovo „autoritativní“ zde říká, že se jedná o servery, které nesou závazné informace o dané doméně a všechna zařízení v síti Internet by se jimi měla řídit, aby vždy skrz touto hierarchií došla ke správnému výsledku při překladu doménového názvu na IP adresu.

2.4 Postup překladu doménového názvu

Pro konkrétní představu si na ukázkovém příkladu znázorníme, jak z doménového názvu „www.mff.cuni.cz“ získáme příslušnou IP adresu. Překlad začíná v kořeni celé hierarchie a spočívá v tom, že se v každém uzlu zeptáme, kterým směrem máme jít při našem hledání dál. Začínáme tedy v u kořenové domény, jejímiž autoritativními DNS servery jsou:

- a.root-servers.net
- b.root-servers.net
- c.root-servers.net
- d.root-servers.net

- e.root-servers.net
- f.root-servers.net
- g.root-servers.net
- h.root-servers.net
- i.root-servers.net
- j.root-servers.net
- k.root-servers.net
- l.root-servers.net
- m.root-servers.net

Tyto kořenové DNS servery, jejich provoz, dostupnost a obsah má na starost již zmíněná organizace ICANN. Jejich názvy (a taktéž IP adresy) jsou všeobecně známé a pevně dané, jejich seznam musí mít k dispozici každé zařízení v síti Internet, které chce provádět překlad doménových názvů (musí z něčeho vycházet). Tyto kořenové DNS servery evidují seznam existujících subdomén (v tomto případě seznam existujících TLD) a k nim příslušné autoritativní DNS servery. Dotážeme-li se některého z nich na doménu www.mff.cuni.cz, sdělí nám, že celou tuto doménu nezná, ale že zná doménu cz a jejími autoritativními DNS servery jsou:

- ns.tld.cz
- nss.tld.cz
- ns-cz.ripe.net
- ns-ext.isc.org
- c.ns.nic.cz
- e.ns.nic.cz

Tím nám kořenový DNS server sdělil, kterou cestou se máme vydat dál k požadovanému výsledku. Ve stromě se tedy posouváme do uzlu cz, vybereme si jeden z jeho autoritativních DNS serverů (např. ns.tld.cz) a opět vzneseme dotaz na doménu www.mff.cuni.cz. Server nám na to odpoví, že celé toto jméno nezná, ale zná doménu cuni.cz a její autoritativní DNS servery jsou ns.ces.net a golias.ruk.cuni.cz. Pak se zeptáme třeba serveru ns.ces.net, ten nám sdělí autoritativní DNS servery pro doménu mff.cuni.cz a v dalším kroku budeme v cíli.

K uvedenému postupu je nutno podat několik vysvětlení. Především bylo řečeno, že se lze v kterémkoliv kroku zeptat libovolného z autoritativních DNS server dané domény, v jejímž uzlu stromu se právě nacházíme. Serverů pro každou doménu je více (většinou je minimální požadavek 2 servery). První důvod je redundance, tj. při poruše jednoho ze serverů nedochází k výpadku celé domény (a tedy i celého podstromu), ale ostatní

servery ho zastoupí (to je dáno mechanismem protokolu DNS, který bude vysvětlen v dalších kapitolách). Je proto zvykem (a někteří správci domén to dokonce vyžadují a v rámci možností kontrolují, např. DE.NIC), že servery pro stejnou doménu jsou rozmístěny v různých lokalitách a připojeny přes různé ISP. Mít všechny servery v jedné serverovně, připojené přes jeden přepínač a do jedné elektrické zásuvky je samozřejmě nesmysl a systém více serverů ztrácí efekt (nicméně v praxi to tak často bývá). Správci domén nulté a první úrovně si samozřejmě nic takového dovolit nemohou a např. 13 kořenových DNS serverů je rozmístěno různě po celém světě (a to celé je navíc podpořeno existencí tzv. anycastových zrcadel).

Druhý důvod pro více autoritativních DNS serverů pro jednu doménu je rozložení zátěže. Mechanismus protokolu DNS zajišťuje, že jedno zařízení se dané skupiny serverů dotazuje cyklicky, v globálním měřítku jsou pak servery přibližně rovnoměrně vytíženy.

Dalším důležitým poznatkem je to, že v každé úrovni některému ze serverů posíláme celý náš dotaz „www.mff.cuni.cz“, tedy nikoliv že bychom se serveru ns.tld.cz zeptali pouze na „cuni.cz“. Je to proto, že my jakožto dotazující se klient nikdy nemůžeme vědět, který ze serverů po cestě má celou požadovanou informaci. To, že kořenové DNS servery znají pouze domény první úrovně a autoritativní DNS servery na první úrovni znají jen domény na druhé úrovni, je jen zvyklost. Dokonce ani to přesně neplatí - například všechny kořenové DNS servery již znají přímo IP adresu pro název „ns.tld.cz“. To souvisí s tzv. glue IP adresami. Dotaz se tedy vždy posílá celý a DNS server se nám pokusí dodat co nejkonkrétnější informaci, kterou má. Od DNS serverů pro domény druhé úrovně to je již velmi variabilní.

2.5 Primární a sekundární DNS servery

Množina autoritativních DNS serverů pro konkrétní doménu se často dělí na jeden primární a na jeden nebo více sekundárních. Primární server je hlavním nositelem informace, je to tedy místo, kde je hlavní úložiště dat a kde jeho administrátor provádí úpravy DNS. Jakmile se na tomto serveru provedou změny v nastavení nějaké domény, sekundární servery si tyto změny synchronizují speciálními mechanismy protokolu

DNS (notifikace a AXFR přenos). Tyto mechanismy nejsou povinné – záleží na administrátorovi, jak zajistí, aby všechny servery měly aktuální údaje.

Je důležité si uvědomit, že rozdělení serverů na „primární“ a „sekundární“ jsou pro člověka, který není administrátorem těchto serverů, nedůležité. Všechny by měly obsahovat stejné informace a na jakýkoliv dotaz odpovídat shodným způsobem a mělo by být jedno, který z nich si vyberete. To je pravda samozřejmě jen za předpokladu, že jsou servery správně nastaveny a synchronizovány. Je chybné se domnívat, že překládání adres probíhá pomocí primárního DNS serveru a sekundární budou využity až v případě, že je primární mimo provoz.

Pro zajímavost – primárním DNS serverem pro kořenovou doménu je a.root-servers.net a pro doménu cz to je server ns.tld.cz. Ostatní servery ve skupinách si data z primárního zdroje kopírují.

2.6 Cachovací DNS servery

Mimo autoritativních DNS serverů, které jsou hlavními nositeli informací o doménách, existuje ještě další typ DNS serverů – tzv. cachovací. Jakýkoliv klient, který potřebuje pracovat s doménovými názvy, by v běžném případě musel pro překlad každého doménového názvu vždy obeslat množství DNS serverů s dotazy na záznamy pro každou část domény. To je však nešetrné a zbytečné, protože DNS záznamy se tak často nemění. Navíc čím více se ve stromě blížíme kořeni, tím je pravděpodobnost změny v záznamech nižší a nižší. Například je zřejmé, že seznam DNS serverů pro TLD se bude měnit jen jednou za velmi dlouhou dobu a je zbytečné se neustále dokola na to ptát kořenových DNS serverů a zatěžovat je i sebe.

Zde přichází na řadu cachovací DNS servery, které jednotlivým klientům (klienty jsou zde myšleni koncoví uživatelé Internetu – pracovní stanice, jednotlivé aplikační servery apod.) zprostředkovávají celý mechanismus překladů názvů a IP adres a průběžně získávaná data si ukládají do paměti. Průběžně zde znamená, že si neukládají nejenom výsledné údaje (např. IP adresy pro požadované doménové názvy), ale také veškeré mezivýsledky, tj. zjištěné autoritativní servery pro všechny uzly na cestě ve stromu od kořeni až k cíli.

Další motivací pro tyto DNS servery je představa, že mezi koncovým uživatelem Internetu a samotným Internetem je úzké hrdlo, např. v podobě vytáčené linky, kde je třeba se vyvarovat intenzivní komunikaci s DNS servery po celém světě. Proto každý poskytovatel připojení k Internetu svým zákazníkům poskytuje cachovací DNS server, který všechny záležitosti klientům obstará a ke klientovi již putuje jen finální odpověď.

Zde však vyvstává otázka, jak dlouho si mohou cachovací DNS servery držet nějakou informaci v paměti. Proto ke slovu přichází hodnota TTL (Time To Live), uvedená u každého záznamu v DNS, která udává dobu, po kterou si mohou DNS servery danou hodnotu cachovat. Po uplynutí tohoto času je nutné hodnotu v paměti zahodit a opět se zeptat příslušných autoritativních DNS serverů.

Pro zajímavost lze uvést, že NS záznamy kořenové domény mají TTL 6 dní, NS záznamy pro doménu cz mají TTL 5 hodin, NS pro cuni.cz 1 den, NS pro mff.cuni.cz 8 hodin. Ale například A záznam pro „www.seznam.cz“ má TTL pouhých 300 vteřin, tedy 5 minut.

Při rozhodování o nastavení TTL je nutné brát v úvahu dva protichůdné požadavky – zajistit, aby se musely dotazy provádět co nejméně, a na druhou stranu aby se v případě změny nové hodnoty záznamů co nejdříve rozšířily po světě. Je tedy nutné uvážit, jaká je pravděpodobnost, že se záznamy měnit budou.

2.7 Dokumenty RFC

RFC (Request for Comments – žádost o komentáře) je označení dokumentů, které popisují standardy, doporučení a informace o Internetových protokolech a službách. Nejedná se o dokumenty, které by něco někomu přikazovaly, ale jsou všeobecně uznávané a dodržované, díky čemuž v Internetu fungují standardizované technologie a protokoly a každý se může domluvit s každým. Dokumenty jsou číslovány podle pořadí jejich vydání. Již vydaný dokument se nikdy nemění, v případě změny v protokolu se vydá nový dokument, který označí ten předchozí za zastaralý (obsoleted).

Nejdůležitější a zajímavé RFC dokumenty, vztahující se k DNS:

- RFC 1034 – Domain Names - Concepts and Facilities[1]
- RFC 1035 – Domain Names - Implementation and Specification[2]
- RFC 1537 – Common DNS Data File Configuration Errors[3]
- RFC 1886 – DNS Extensions to support IP version 6[4]
- RFC 1912 – Common DNS Operational and Configuration Errors[5]
- RFC 1996 – A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)[6]
- RFC 2181 – Clarifications to the DNS Specification[7]
- RFC 2308 – Negative Caching of DNS Queries[8]
- RFC 2870 – Root Name Server Operational Requirements[9]
- RFC 3330 – Special-Use IPv4 Addresses[10]
- RFC 3467 – Role of the Domain Name System[11]

Z uvedených dokumentů bylo čerpáno při sestavování metodiky v této práci.

Kapitola 3 – DNS záznamy domény

Každá doména může mít u svých autoritativních DNS serverů vedeno mnoho nejrůznějších záznamů. Nejobvyklejším údajem je IP adresa pro toto jméno, která nás zajímá v případě, že se chceme spojit např. s webovým serverem a stáhnout si WWW stránku, která se na dané doméně nachází.

Záznamy vedené na autoritativním DNS serveru jsou rozděleny do tzv. zónových souborů. Každý takový soubor obsahuje záznamy o konkrétní doméně a dále může obsahovat záznamy svých subdomén (tedy domén nižších řádů), pokud nemají samy vlastní zónové soubory, či pro konkrétní subdomény specifikovat názvy autoritativních DNS serverů, které obsahují její zónu. Server může odkazovat i sám na sebe, to znamená, že subdoména má záznamy na stejném serveru, ale je pro ni vyhrazen vlastní zónový soubor.

V nejpoužívanější implementaci DNS serveru – BIND – jsou zónové soubory skutečně textové soubory v souborovém systému serveru, kde každý řádek odpovídá jednomu DNS záznamu. Zóna se edituje prostým editováním tohoto souboru libovolným textovým editorem, po dokončení změn administrátor voláním určitého příkazu sdělí DNS serveru, že byla provedena změna, a server si soubor znovu načte do paměti a začne propagovat aktualizované informace.

Každý záznam (řádek zónového souboru) obsahuje následující položky:

- název domény
- TTL záznamu (Time To Live) – délka platnosti záznamu v cache (sekundy)
- třída – rodina protokolů, k níž se záznam vztahuje, IN znamená Internet; jiné typy existují, ale nepoužívají se
- typ záznamu (A, MX, SOA, NS, CNAME, …)
- hodnota

Názvy domén lze v DNS záznamech uvádět dvěma způsoby. Pokud je název ukončen tečkou, znamená to, že se jedná o plně kvalifikovaný doménový název (FQDN – Fully Qualified Domain Name) – tečka na konci zde znázorňuje kořen systému DNS. Jestliže na konci tečka není, je název relativní a za jeho konec se doplní aktuální doména.

Máme-li tedy v zónovém souboru domény cuni.cz uveden záznam s názvem „mff“, celý název bude „mff.cuni.cz.“. Relativní názvy se mohou používat pro zjednodušený zápis záznamů.

3.1 Záznam typu SOA

SOA (Start Of Authority record) je speciální záznam, který se musí v každém zónovém souboru vyskytovat právě jednou. Jedná se o jakousi hlavičku, která obsahuje následující informace:

- MNAME – název primárního DNS serveru pro danou zónu
- RNAME – kontakt na správce zónového souboru - uvádí se e-mailová adresa, ve které je zavináč nahrazen za tečku (protože znak zavináče má v DNS speciální význam)
- SERIAL – sériové číslo zóny – jedná se o číselný údaj, který udává verzi zónového souboru; při změně v záznamech se číslo navýší a sekundární DNS servery si při porovnání s číslem, které mají uložené u sebe, zjistí, že došlo ke změně a že je třeba data aktualizovat
- REFRESH - počet sekund, po jejichž uplynutí od poslední kontroly či načtení zóny z primárního DNS provede sekundární server kontrolu sériového čísla
- RETRY - po zahájení zjišťování sériového čísla z předchozího bodu opakuje požadavek na primární DNS server po uplynutí RETRY sekund, pokud se předchozí požadavek nezdařil (pokud server neodpověděl)
- EXPIRE - pokud se nedaří stáhnout sériové číslo z primárního DNS a od posledního úspěšného pokusu uplynulo EXPIRE vteřin, je zóna považována za neplatnou a sekundární DNS server by ji měl vyřadit ze svých záznamů (zapomenout ji)
- MINIMUM – položka s historicky mnoha různými významy:
  - minimální TTL hodnota pro všechny záznamy v zóně (původní význam)
  - výchozí TTL pro záznamy, u kterých není tato hodnota specifikována (druhý význam)
  - TTL pro negativní cachování – tj. doba, po kterou si cachovací DNS servery pamatují, že nějaký záznam neexistuje (současný význam)

3.2 Záznam typu A

Záznam tohoto typu obsahuje IP adresu protokolu IPv4. Tyto adresy jsou udržovány v lidsky čitelné formě (avšak v protokolu DNS jsou předávány jako 32-bitové číslo).

3.3 Záznam typu AAAA

Jedná se o IP adresu protokolu IPv6.

3.4 Záznam typu NS

Tento typ záznamu slouží ke sdělení seznamu autoritativních DNS serverů pro danou doménu. Uváděny jsou názvy serverů (tedy jejich doménová jména), nikoliv IP adresy. Chce-li se zařízení spojit s autoritativním DNS serverem nějaké domény, nejprve si na DNS server vyšší úrovně zjistí všechny záznamy typu NS pro hledanou doménu, vybere si jeden z nich a zjistí si k němu IP adresu, teprve pak může dojít ke komunikačnímu spojení přes protokol DNS.

Stejné záznamy jsou také uloženy již přímo v záznamech dané domény. Pro ilustraci, toto je výsledek dotazu na doménu „cuni.cz“, pokud se zeptáme serveru „ns.tld.cz“.

```
cuni.cz.      18000   IN    NS    ns.ces.net.
cuni.cz.      18000   IN    NS    golias.ruk.cuni.cz.
```

Vidíme, že jsme jako odpověď obdrželi 2 záznamy typu NS, které nám dávají požadovaný výsledek. Stejnou odpověď dostaneme i např. na dotaz „mff.cuni.cz“, protože celou odpověď server nezná, ale odkáže nás na jiné DNS servery, které by ji znát měly. Důležité je to, že opět stejný výsledek dostaneme, pokud se na doménu „cuni.cz“ zeptáme přímo některého z jejích autoritativních DNS serverů. To znamená, že každá doména má ve svých záznamech uloženy NS záznamy na sebe sama.

3.5 Záznam typu MX

Záznam uvádí doménový název mailserveru, na který se má doručovat pošta pro tuto doménu. Před názvem serveru se uvádí priorita, která má význam v případě, že MX záznamů pro jeden název je více. V takovém případě se zkouší servery podle vzrůstajícího čísla priority (tj. největší prioritu má server s nejnižším číslem). Pokud nám server neodpoví, zkoušíme další. Druhý a další servery, pokud jsou přítomny, tak slouží jako záložní mailservery.

Chceme-li např. zaslat e-mailovou zprávu na adresu jan.novak@mff.cuni.cz, zeptáme se na MX záznamy pro doménu „mff.cuni.cz“ a dozvíme se následující:

```
mff.cuni.cz.    28800   IN    MX    20 smtp1.ms.mff.cuni.cz.
mff.cuni.cz.    28800   IN    MX    20 smtp2.ms.mff.cuni.cz.
mff.cuni.cz.    28800   IN    MX    40 smtp1.kolej.mff.cuni.cz.
```

Zde si můžeme všimnout situace, kdy 2 servery mají stejnou prioritu, což znamená, že je jedno, kterému z nich se pokusíme zprávu doručit. Pokud nám ani jeden z nich neodpoví, pokusíme se zprávu doručit na třetí server. Samozřejmě před jakoukoliv komunikací s nimi si musíme nejprve zajistit překlad názvů mailserverů na IP adresy.

3.6 Záznam typu CNAME

CNAME záznam oznamuje, že daná doména je aliasem domény jiné. Pokud pro nějakou doménu existuje tento záznam, nesmí pro ni existovat žádný další. Příklad:

```
www1.domena.cz.  1800  IN  CNAME  domena.cz.
www2.domena.cz.  1800  IN  CNAME  domena.cz.
www3.domena.cz.  1800  IN  CNAME  domena.cz.
domena.cz.       1800  IN  A      1.2.3.4
domena.cz.       1800  IN  MX     10 mail.domena.cz
```

Zde jsou subdomény www1, www2 a www3 aliasem pro domena.cz a všechny mají IP adresu 1.2.3.4 a také shodný MX záznam. Smysl záznamu typu CNAME je zřejmý – mít skutečnou IP adresu a případně další záznamy pouze na jednom místě a při jejich změně je nemuset přepisovat u všech domén zvlášť.

3.7 Reverzní záznamy (PTR)

Systém DNS neposkytuje pouze mechanismus překladu doménových názvů na IP adresy, ale také naopak překlad IP adres na doménová jména. Toho se dnes využívá zejména při doručování elektronické pošty, kdy si mailserver, který přijímá od klienta zprávu, nejprve přeloží IP adresu klienta na název (čímž se může přibližně dozvědět, o koho se jedná) a poté si získaný název zpětně přeloží na IP adresu. Pokud mu skutečná a získaná IP adresa nesouhlasí, může považovat zdroj zprávy za nedůvěryhodný a odmítnout ho.

Reverzní záznamy mohou sloužit pro kohokoliv jako vodítko při pátrání po původu IP adresy. Mějme situaci, kdy jsme zjistili, že se na náš počítač pokoušel připojit nějaký útočník z IP adresy 88.100.88.36. Zeptáme-li se na reverzní záznam k této IP adrese, dozvíme se název „36.88.broadband5.iol.cz“ a z toho si ihned vyvodíme, že je útočník připojen nejspíše přes ADSL od poskytovatele IOL.cz. Reverzní záznamy je však třeba brát s rezervou, nemusí odpovídat skutečnosti.

Jak se však převede IP adresa na reverzní záznam? IP adresy jsou organizovány od nejobecnějšího ke konkrétnějšímu zleva doprava, tedy naopak než u doménových názvů. Řešení je snadné – IP adresu napíšeme obráceně a na konec přidáme speciální doménu in-addr.arpa. Vznikne nám platné doménové jméno, které lze opět rozložit na jednotlivé úrovně ve stromové struktuře: 36.88.100.88.in-addr.arpa. Autoritativními DNS servery domény „in-addr.arpa“ jsou stejné jako kořenové DNS servery.

U delegace názvů v doméně „in-addr.arpa“ je podstatný rozdíl, protože je třeba respektovat způsob přidělování IP adres. Celý rozsah IP je rozdělován několika mezinárodním organizacím (podle kontinentů), ty je přidělují ISP a ti je přidělí svým zákazníkům. Ukažme si to např. na IP adrese 195.113.20.9. Následují výpis postupného dotazování DNS serverů (pro zjednodušení byly vypuštěny některé nezajímavé řádky a sloupce výpisů):

```
195.in-addr.arpa.             NS  ns3.nic.fr.
195.in-addr.arpa.             NS  sec1.apnic.net.
195.in-addr.arpa.             NS  sec3.apnic.net.
195.in-addr.arpa.             NS  sunic.sunet.se.
195.in-addr.arpa.             NS  ns-ext.isc.org.
195.in-addr.arpa.             NS  ns-pri.ripe.net.
195.in-addr.arpa.             NS  tinnie.arin.net.
;; Received from 128.63.2.53#53(H.ROOT-SERVERS.NET)

113.195.in-addr.arpa.         NS  ns.ces.net.
113.195.in-addr.arpa.         NS  ns.ripe.net.
113.195.in-addr.arpa.         NS  ns.cesnet.cz.
;; Received from 192.134.0.49#53(ns3.nic.fr)

20.113.195.in-addr.arpa.      NS  ns.ms.mff.cuni.cz.
20.113.195.in-addr.arpa.      NS  sns.ms.mff.cuni.cz.
;; Received from 195.113.144.233#53(ns.ces.net)

9.20.113.195.in-addr.arpa.    PTR barbora.ms.mff.cuni.cz.
;; Received 1from 195.113.20.71#53(ns.ms.mff.cuni.cz)
```

Zde vidíme, že rozsah IP adres 195.113 je celý delegován CESNETu, rozsah IP adres 195.113.20 je celý delegován MFF UK na Malé Straně a nakonec nám DNS server ns.ms.mff.cuni.cz sdělí, že reverzní záznam pro tuto IP adresu je barbora.ms.mff.cuni.cz. Z uvedeného výpisu lze zjistit spoustu užitečných informací o zkoumané IP adrese.

3.8 Další typy záznamů

Ve zkratce několik dalších typů DNS záznamů:

- TXT – textový řetězec, který může sloužit k libovolnému popisu či k uložení informací ve formátu klíč=hodnota s nejrůznějším významem (viz. RFC 1464)
- SRV – specifikace umístění konkrétní služby (podle čísla portu) na dané doméně (viz. RFC 2782)
- SPF (Sender Policy Framework) – uvedení oprávněných hostitelů v síti Internet, kteří mohou odesílat elektronickou poštu s uvedením odesílatele v této doméně (slouží k boji se SPAMem s podvrženou adresou odesílatele), zatím experimentální RFC 4408

3.9 Záznamy stejného typu

Podobně jako by doména měla mít více záznamů NS (tedy více autoritativních DNS serverů), mohou se i další záznamy vyskytovat vícekrát, tedy více položek stejného typu

pro stejnou doménu, avšak s jinou hodnotou. Pokud se na takový záznam dotazujeme, vybereme si jednu ze získaných hodnot a při příštím dotazu se použije hodnota další (a cyklicky pokračujeme, tzv. round-robin). U příkladu MX záznamů pro doménu mff.cuni.cz jsme viděli 2 záznamy se stejnou prioritou. Záleží v podstatě na náhodě, který záznam bude skutečně použit. Stejně tak to lze použít např. u A záznamů, kdy můžeme pomocí DNS systému rozložit webové stránky pro jednu doménu na více IP adres (více serverů).

Pokud mají záznamy stejný název domény a typ, musí mít také stejné hodnoty TTL.

3.10 Glue záznamy

Jako glue záznamy se označují A záznamy, které jsou netradičně uloženy na autoritativním DNS serveru o úroveň výše, než je obvyklé. Dříve bylo zmíněno, že již kořenové DNS servery obsahují IP adresu pro doménový název „ns.tld.cz“. Je tomu proto, že autoritativní DNS servery jsou všude uváděny především svým názvem, ale abychom se s nimi mohli spojit, potřebujeme odpovídající IP adresu. Pro zjištění IP adresy k názvu „ns.tld.cz“ musíme nejprve přes doménu cz zjistit autoritativní DNS servery k doméně „tld.cz“, ale k tomu se nejdřív potřebujeme spojit s DNS servery domény „cz“, tím je však (mimo jiné) „ns.tld.cz“, takže jsme se zacyklili a běžným způsobem bychom se nemuseli nic dozvědět.

V těchto případech, kdy DNS server obsahuje ve svém názvu doménu, u které je autoritativní, musí být na DNS serveru o úroveň výše uvedena i jeho IP adresa. Tomu se říká glue záznam. Je tedy zřejmé, že A záznam pro „ns.tld.cz“ musí znát přímo všechny kořenové DNS servery, a opravdu při přímém dotazu na „ns.tld.cz“ nám root server A vrací „217.31.196.10“.

Glue záznam může být přítomen i pro NS záznamy, které to nevyžadují. Urychluje to práci s DNS systémem (v opačném případě je nutno udělat několik dalších kroků pro získání IP adresy DNS serveru). Na druhou stranu glue záznamy způsobují jistou duplicitní informaci (protože mimo glue existuje stejný A záznam přímo v zóně příslušné domény), a tak lze snadno udělat chybu tím, že při změně IP adresy DNS serveru ji změníme jen na jednom místě a na druhé zapomeneme. Proto se dnes glue záznamy tam, kde to není nutné, nepoužívají.

3.11 Dodatečná a autoritativní sekce v DNS odpovědi

DNS servery myslí i na další souvislosti mezi názvy a IP adresami. Pokud se ptáme nějakého DNS serveru např. na NS či MX záznam (které obsahují název) a daný server má také u sebe autoritativní informaci o IP adresách k získaným názvům, vrátí nám v tzv. additional section v paketu (paketech) DNS odpovědi rovnou i tyto IP adresy.

V další sekci, tzv. authority section nám vrací také NS záznamy pro doménu, na kterou se ptáme (a v additional section najdeme případně také IP adresy k těmto NS záznamům). Účel těchto dvou sekcí je zřejmý, ušetří nám to mnoho dalších případných dotazů na IP adresy ke všem získaným záznamům.

Zeptejme se DNS serveru ns.ms.mff.cuni.cz na MX záznamy pro doménu ms.mff.cuni.cz s podrobným výpisem výsledku (pro zjednodušení byly vypuštěny některé nezajímavé řádky a sloupce výpisů):

```
;; QUESTION SECTION:
;ms.mff.cuni.cz.          MX

;; ANSWER SECTION:
ms.mff.cuni.cz.          MX    20 smtp2.ms.mff.cuni.cz.
ms.mff.cuni.cz.          MX    40 smtp1.kolej.mff.cuni.cz.
ms.mff.cuni.cz.          MX    20 smtp1.ms.mff.cuni.cz.

;; AUTHORITY SECTION:
ms.mff.cuni.cz.          NS    golias.ruk.cuni.cz.
ms.mff.cuni.cz.          NS    ns.ms.mff.cuni.cz.
ms.mff.cuni.cz.          NS    ns.kolej.mff.cuni.cz.
ms.mff.cuni.cz.          NS    sns.ms.mff.cuni.cz.

;; ADDITIONAL SECTION:
smtp1.ms.mff.cuni.cz.    A     195.113.20.4
smtp2.ms.mff.cuni.cz.    A     195.113.20.5
smtp1.kolej.mff.cuni.cz. A     195.113.24.4
smtp1.kolej.mff.cuni.cz. AAAA  2001:718:1e03:a01::4
ns.ms.mff.cuni.cz.       A     195.113.20.71
ns.kolej.mff.cuni.cz.    A     195.113.24.1
sns.ms.mff.cuni.cz.      A     195.113.20.77
golias.ruk.cuni.cz.      A     195.113.0.2

;; SERVER: 195.113.20.71#53(195.113.20.71)
```

Vidíme, že nám server opravdu rovnou sdělil všechny jemu známé IP adresy ke všem názvům v odpovědích a ušetřil nám i sobě spoustu další práce s dalšími dotazy.

Kapitola 4 – Protokol DNS

4.1 Komunikace přes UDP a TCP

DNS servery komunikují s dalšími DNS servery a klienty (tzv. resolvery) nad protokoly TCP i UDP, v obou případech na portu 53. Při běžných dotazech se požadavek posílá jedním paketem UDP a odpověď se vrací opět v paketu UDP. Tento protokol byl zvolen pro svou jednoduchost a minimální režii, kdy se nemusí kvůli malým datům složitě navazovat spojení přes protokol TCP.

Jestliže se stane, že celá odpověď (která může obsahovat buď velkou samotnou odpověď nebo další data v dodatečných sekcích) se do jednoho UDP paketu nevejde (velikost odpovědi DNS je dle standardu omezena na 512 bytů, nepočítají se hlavičky UDP a IP protokolu), odešle se tazateli odpověď částečná (maximum co se do paketu vejde) a v hlavičce se nastaví příznak pro oznámení této skutečnosti. Tazatel se nyní může rozhodnout, zda mu přijatá data stačí. Pokud ne, odešle znovu ten samý dotaz, avšak tentokrát již s použitím protokolu TCP, přes který si může stáhnout celou odpověď v potřebném množství paketů.

Protokol UDP však neřeší ztráty paketů na cestě, proto se dotazy po několika sekundách opakují, po určitém počtu neúspěšných pokusů se DNS server považuje za nedosažitelný. To vše záleží na nastavení resolverů.

4.2 Rekurzivní a nerekurzivní dotazy

Při posílání dotazu DNS serveru lze v hlavičce uvést, zda si tazatel přeje provést tzv. rekurzivní dotaz. To znamená, že pokud DNS server sám odpověď nezná (není autoritativní pro doménu, na kterou se ptáme), spustí standardní algoritmus pro vyhledání odpovědi (tj. začne u kořenových DNS serverů a postupuje do nižších úrovní až k cíli) a tazateli pošle konečný výsledek. Záleží však na serveru, zda skutečně rekurzivní dotaz provede. Může ho odmítnout a klientovi poslat pouze takovou odpověď, kterou zná sám. Pokud nezná ani část odpovědi, často pošle zpět seznam kořenových DNS serverů (čímž nám říká, kde máme začít hledat).

Pravidlem by mělo být, že autoritativní DNS servery rekurzivní dotazy neprovádí a starají se jen o svůj hlavní úkol, poskytovat autoritativní údaje o svém pevně daném seznamu domén a jejich záznamech. Naopak cachovací DNS servery musí ze své podstaty provádět rekurzivní dotazy.

Kombinace autoritativního a cachovacího DNS serveru na jednom stroji je špatný nápad, protože z toho mohou plynout problémy. Představme si doménu „xyz.cz“, která má autoritativní server „ns.abc.cz“ a my tento server současně používáme jako cachovací, tudíž nám zprostředkovává přístup k celému DNS systému v Internetu. Pokud se stane, že doména „xyz.cz“ změní své autoritativní DNS servery, tedy je DNS servery domény „cz“ delegována jinam než na „ns.abc.cz“, a administrátor serveru „ns.abc.cz“ zapomene tuto zónu na serveru smazat (případně se o změně situace vůbec nedozví) a my se na doménu „xyz.cz“ zeptáme, dostaneme odpověď od „ns.abc.cz“, která nejenom že nemusí být pravdivá, ale navíc se tváří jako autoritativní. Je to proto, že server „ns.abc.cz“ je stále nakonfigurován jako autoritativní pro tuto doménu a platnost delegace této domény na sebe si nijak neověřuje. Při striktním oddělování autoritativních a cachovacích DNS serverů k tomuto problému nedojde.

4.3 AXFR – zónové transfery

Tzv. zónový transfer je určen k přenosu celého obsahu zóny domény, tj. všech jejích DNS záznamů, z jednoho DNS serveru na druhý. Tento mechanismus používají sekundární servery pro stahování dat ze serverů primárních, pokud dojde v obsahu zóny domény ke změně. AXFR probíhá vždy po protokolu TCP.

AXFR má nevýhodu – vždy přenáší celý obsah zóny, přestože se změnil třeba jen jeden záznam. To řeší mechanismu IXFR (Incremental Zone Transfer, RFC 1995), který přenáší pouze změněné záznamy.

AXFR by nemělo být veřejně přístupné, mělo by být povoleno pouze mezi skupinou autoritativních DNS serverů. Pokud totiž bude mít kdokoliv možnost stáhnout si takto snadno všechny záznamy domény, mohou být kompromitovány některé neveřejné záznamy, na které by se jinak dalo dostat jen přímým dotazem – např. seznam počítačů v doméně, název subdomény pro přístup k interní administraci apod.

4.4 Autoritativní a neautoritativní odpověď

V souvislosti s cachováním DNS záznamů na serverech je nutné klienty informovat, zda odpověď, která je jim zasílána, pochází od cachovacího serveru anebo zda odpověď přichází přímo od autoritativního DNS serveru. K tomu slouží příznak v hlavičce zprávy protokolu DNS. Jako neautoritativní je označena i ta odpověď, kterou právě v tento okamžik cachovací DNS server, který nám dotaz zprostředkovává, přijal z příslušného autoritativního serveru. Jako autoritativní je tedy označena pouze ta, kterou jsme získali přímo bez jakéhokoliv prostředníka.

Na tomto místě je třeba znovu zdůraznit, že příznak autoritativní odpovědi ještě neznamená, že daná doména je skutečně delegována na tento DNS server. Rozhodující je, že administrátor tuto doménu na serveru přidal a vytvořil pro ni zónu. Servery si nijak neověřují, zda je jim doména opravdu delegována. Může zde vzniknout problém, který je popsán v oddílu „Rekurzivní a nerekurzivní dotazy“.

4.5 Formát DNS zpráv

Zpráva přenášená protokolem DNS se skládá z následujících částí:

- hlavička (header) – obsahuje základní informace o přenášených datech, jejich typu, obsahu a několik příznaků
- dotaz (question) – část nesoucí dotaz klienta, server dotaz ve zprávě s odpovědí zopakuje
- odpověď (answer section) – DNS záznamy, které dávají odpověď na vznesený dotaz
- informace o autoritě (authority section) – seznam autoritativních DNS serverů zóny, ze které byly záznamy z předchozí části získány (tedy NS záznamy domény této zóny), anebo odkaz na DNS servery, kterých se máme ptát dál (záleží na tom, zda dotazovaný server je autoritativní pro hledanou informaci či nikoliv)
- dodatečná sekce (additional section) – A a AAAA záznamy k názvům, které se vyskytují v hodnotách záznamů v odpovědi či autoritativní sekci a které DNS server zná (je pro ně autoritativní)

Hlavička obsahuje následující informace:

- ID – 16-bitový číselný identifikátor, který přidělí tazatel zprávě s dotazem, server ve zprávě s odpovědí zašle stejné ID, podle toho tazatel pozná, k čemu tato odpověď patří (je nutné, protože transportní protokol UDP je bezestavový)
- QR – příznak, zda se jedná o zprávu s dotazem či odpovědí
- OPCODE – označení typu dotazu
- AA (Authoritative Answer) – pokud je tento příznak nastaven, znamená to, že server, který nám odpověď poslal, je autoritativní pro název, na který se ptáme. Jinak řečeno to znamená, že data v části answer nepochází z cache a ani z rekurzivního dotazu, ale jedná se o aktuální data přímo ze zónového souboru a odpověď nebyla zprostředkována žádným cachovacím DNS serverem.
- TC (Truncation) – příznak signalizující zkrácení odpovědi, která je delší než 512 bytů a nemohla být celá poslána v jednom UDP paketu
- RD (Recursion Desired) – tento příznak nastaví tazatel v případě, že si od serveru přeje podle potřeby provést rekurzivní zpracování dotazu. Server může rekurzivní dotaz odmítnout, ale v odpovědi posílá stejné nastavení tohoto příznaku.
- RA (Recursion Available) – tento příznak nastaví server v případě, že tazateli nabízí rekurzivní dotazy. Pokud server tuto službu tazateli umožňuje, posílá příznak RA ve všech odpovědí jako oznámení o dostupných možnostech, nejedná se pouze o reakci na příznak RD v dotazu.
- RCODE (Response code) – kód označující výsledek dotazu
  - 0 – bez chyby
  - 1 – chyba ve formátu dotazu
  - 2 – chyba na straně serveru (porucha)
  - 3 – autoritativní server tím oznamuje, že požadovaný záznam neexistuje
  - 4 – nepodporovaný typ dotazu
  - 5 – odmítnuto
- QDCOUNT – počet záznamů v sekci s dotazem
- ANCOUNT – počet záznamů v sekci s odpovědí
- NSCOUNT – počet záznamu v autoritativní sekci
- ARCOUNT – počet záznamů v dodatečné sekci

Kapitola 5 – Analýza a návrh metodiky

Cílem tohoto projektu je na základě standardů, doporučení (dokumenty RFC, doporučení RIPE, viz. seznam literatury) a zkušeností s provozem DNS systému sestavit seznam pravidel, která musí nebo by měly testované DNS servery splňovat. Pravidla lze rozdělit do 3 skupin podle závažnosti situace, která nastane, pokud není pravidlo splněno:

- Chyba – nesplnění tohoto pravidla způsobuje úplnou nebo částečnou nefunkčnost či omezení provozu DNS systému, který tak neplní správně svůj účel. Systém nefunguje buď vůbec, což znamená, že domény, pro které je tento DNS systém autoritativní, nefungují (a pro Internet vypadají jako že neexistují), nebo funguje pouze část systému.
- Varování – nesplnění pravidla nezpůsobuje bezprostřední nefunkčnost systému, avšak jedná se o jeho nesprávný stav, který může v nefunkčnost či jiný problém vyústit, a tak je nutno tomuto varování věnovat pozornost
- Upozornění – sledovaný parametr je po funkční stránce v pořádku, avšak není nastaven tak, jak je všeobecně doporučené. Může se jednat o chybu v nastavení (překlep administrátora, neznalost problematiky) anebo to může být také speciální účelové nastavení.

Analýza domény a stavu jejích autoritativních DNS serverů spočívá v pokládání dotazů odpovídajícím DNS serverům a zkoumání vrácených výsledků. Vzhledem k povaze UDP protokolu musíme počítat s tím, že se nám občas nějaký paket v síti ztratí na cestě od nás k serveru či od serveru zpět k nám. Z tohoto důvodu je třeba vhodně zvolit časový limit pro čekání na odpověď a vhodný počet opakování dotazů.

U každého testu je uvedena tabulka možných výsledků tak, jak je produkuje implementace uvedená dále v této práci. Možných negativních výsledků je u většiny testů více, především proto, že některé z nich jsou závažnější než jiné, a také proto, aby mohla být chyba podrobněji vysvětlena ve výstupu implementované aplikace.

5.1 Obecná kontrola DNS serverů

5.1.1 Odpověď serverů

Před prováděním tohoto testu je potřeba nejprve k doméně zjistit její autoritativní DNS servery. To lze provést postupným dotazováním se na doménu od kořenových DNS serverů. Pokud se nepodaří k doméně zjistit žádný DNS server, může to znamenat, že doména své vlastní DNS servery nemá a její záznamy jsou součástí zóny domény vyšší úrovně, anebo doména vůbec neexistuje. Dalším důvodem neúspěchu může být problém v komunikaci. Každopádně nemá v takovém případě smysl jakékoliv testy provádět, protože nemůžeme o doméně získat žádné informace.

Když už získáme názvy DNS serverů domény, potřebujeme jejich názvy přeložit na IP adresu. Může se stát, že se nám to nepodaří (z jakéhokoliv důvodu). Pokud jsou některé názvy nepřeložitelné, budeme dané servery ignorovat a nebudeme s nimi nadále pracovat. Pokud nelze na IP adresu přeložit žádná, v testech nepokračujeme.

Od nyní předpokládejme, že máme k dispozici seznam názvů DNS serverů domény a že alespoň jeden se nám podařilo přeložit na IP adresu. V tomto testu se zkouší, zda všechny autoritativní servery reagují na DNS dotazy, tedy naslouchají na UDP portu 53, jsou dosažitelné a na základě DNS dotazu zašlou v daném časovém limitu korektní DNS odpověď. Pokud je odpověď na UDP paket příliš dlouhá (tj. v hlavičce odpovědi je uveden příznak TC), je potřeba dotaz zopakovat přes TCP protokol na portu 53. Při tomto testu se také sleduje rychlost reakce serverů, tedy délka prodlevy mezi odesláním dotazu a přijetím odpovědi. Z naměřeného času nelze usuzovat nic o rychlostech a schopnostech serveru, jelikož se do tohoto času započítává také prodleva při transportu paketů v síti Internet tam a zpět, navíc tyto časy mohou být z různých částí světa výrazně odlišné. Bereme to tedy pouze jako údaj orientační.

Jestliže je některý server nedosažitelný, dochází k prodlevám při komunikaci s DNS systémem. Klient, vznášející dotaz na nedosažitelný DNS server, čeká určitou dobu na odpověď serveru. Teprve po vypršení určitého času (timeoutu) (a popř. vyčerpání zvoleného počtu pokusů) tento server přeskočí a zkouší kontaktovat další ze stejné skupiny. Způsob chování záleží na implementaci klienta (resolveru).

Pokud žádný DNS server neodpověděl, opět nemá smysl v dalších testech pokračovat.

Správný výsledek		Všechny DNS servery odpovídají
E001	chyba	Nepodařilo se zjistit žádné autoritativní DNS servery k doméně
E002	chyba	Žádný z názvů autoritativních DNS serverů domény není přeložitelný na IP adresu
E003	chyba	Některý z názvů autoritativních DNS serverů domény není přeložitelný na IP adresu
E011	chyba	Nepodařilo se spojit s žádným z DNS serverů
E012	chyba	Nepodařilo se spojit s některými DNS servery

5.1.2 Sériová čísla zóny

Ze všech autoritativních DNS serverů, které jsou dosažitelné, se stahuje SOA záznam testované domény, ze kterého je nejzajímavější údaj serial (sériové číslo). Jestliže servery vrací čísla různá, může to znamenat:

- Trefili jsme se do okamžiku, kdy v obsahu zóny došlo ke změně a sekundární DNS servery si s určitou prodlevou data aktualizují ze serveru primárního – jedná se tedy o dočasný problém, který by měl během krátké doby zmizet a nemá vliv na funkčnost, pouze se provedená změna zcela projeví o něco později.
- Jedná se o trvalý problém, kdy nastala porucha v synchronizaci mezi servery (chyba v jejich nastavení, porucha software, porucha spojení mezi servery), což může způsobovat nefunkčnost domény. V případě, že se na primárním DNS serveru změní záznamy, nové údaje se na jednom nebo více serverech neprojeví a ty pak do světa stále šíří staré informace (např. IP adresu WWW stránek, která již neplatí a je nefunkční). Tato chyba se projevuje tím, že část lidí zcela náhodně vidí správný obsah stránek a druhá část lidí získává z DNS systému chybné údaje, což je dáno tím, že klienti ze seznamu autoritativních serverů volí v podstatě náhodně.

Pro lepší zjištění, zda se jedná pravděpodobně o první nebo druhý případ, je vhodné si zjistit, kolik různých sériových čísel skupina DNS serverů vrací. Pokud zjistíme dvě různá, jedná se nejspíš o první případ. Pokud jich je ale víc, může to signalizovat problém.

Pro potřeby další části tohoto testu je potřeba určit, který z DNS serverů je primární. To se zjišťuje z položky MNAME v SOA záznamu. To má však dvě úskalí. Zaprvé se může stát, že název, uvedený v položce MNAME, se nevyskytuje v NS záznamech domény (v tomto případě nás zajímají NS záznamy na nadřazeném serveru) anebo může být tento záznam chybný (tj. je uveden jiný server než který je skutečně primární). V první situaci se nepodaří určit, který server je primární a v tomto testu nepokračujeme. V druhém případě se jedná o chybu v nastavení SOA záznamu, avšak jiný způsob k rozlišení primární/sekundární server neexistuje, a tak primární server rozpoznáme chybně.

Situace, která nás v tomto testu ještě zajímá, spočívá v možnosti, že jeden či více sekundárních DNS serverů vrací vyšší sériové číslo než server primární. Pokud by tomu tak opravdu bylo (tj. server, uvedený v SOA MNAME, je skutečně ten pravý primární DNS server), jedná se o velmi závažnou chybu – sekundární DNS server si myslí, že má čerstvější informace, a tak změníme-li cokoliv na serveru primárním (a nové sériové číslo je stále nižší než na sekundárním), změna se na sekundárním serveru neprojeví (ten periodicky porovnává sériové číslo u sebe a číslo získané z primáru). Toto platí i v případě, že mezi servery funguje notifikace o změnách (i v takové situaci se začíná porovnáním sériových čísel).

Správný výsledek		Všechny DNS servery vrací stejné sériové číslo zóny
E021	varování	Servery vrací různá sériová čísla (obecný příznak, zahrnující všechny následující)
E022	varování	... vrací 2 různá
E023	varování	... vrací 3 různá
E024	chyba	... vrací 4 různá
E025	chyba	... vrací 5 a více různých
E026	chyba	Na jednom nebo více sekundárních DNS serverech je sériové číslo vyšší než na primárním (určen dle SOA MNAME)

5.1.3 Autoritativita serverů pro doménu

Při získávání SOA záznamu ze všech autoritativních DNS serverů domény je potřeba sledovat příznak „AA“ v hlavičce odpovědi, který říká, zda odpověď (obsah sekce answer v DNS odpovědi) je autoritativní. Jestliže je tento příznak nastaven, je server

skutečně autoritativní a data pochází ze zónového souboru, který má server u sebe uložen.

Chybou je, pokud příznak „AA“ nastaven není a server SOA záznam vrátí, tedy byl získán rekurzivním způsobem, nebo server záznam SOA nevrátí, protože ho nezná. To znamená, že je tento server buď chybně uveden v NS záznamu v zóně o úroveň výš (tomu se říká „lame delegation“) anebo by měl být autoritativní, ale lidskou nebo technickou chybou nemá server propagaci zóny domény nastavenu.

Správný výsledek		Všechny DNS servery jsou autoritativní pro doménu
E031	chyba	Žádný z DNS serverů není autoritativní pro tuto doménu
E032	chyba	Některé DNS servery nejsou autoritativní pro tuto doménu (ale nikoliv všechny)

5.1.4 Nastavení potřebných glue záznamů

Pokud název domény je součástí názvu jejího autoritativního DNS serveru, musí být u NS záznamu o úroveň výše také uveden A záznam s IP adresou pro daný název serveru. Jestliže tomu tak není, je tento server v určitých situacích nedosažitelný (pokud si klient pro pokračování v dotazech na danou doménu vybere tento server s chybějícím glue), protože neexistuje způsob, jak jeho IP adresu zjistit a tedy jak ho kontaktovat. Při každém dotazování na autoritativní DNS servery je třeba zjistit případný A záznam. Pokud neexistuje a je vyžadován, je to vážná chyba.

Správný výsledek		Jsou nastaveny všechny potřebné glue záznamy pro DNS servery
E041	chyba	Některým z DNS serverů chybí glue na nadřazeném serveru

- Reference: RFC 1912[5] (2.3)

5.1.5 Shoda glue záznamů a A záznamů v zóně domény

Glue záznamy způsobují duplicitu uložení IP adresy pro název DNS serveru, protože ta je uložena jak v samotném glue záznamu (tedy v zóně domény o jednu úroveň výše), tak v zóně samotné domény jako A záznam v klasickém významu. Je samozřejmě chyba, pokud tyto záznamy neobsahují stejnou IP adresu. Pro každý DNS server je tedy

třeba si zjistit IP adresu běžným způsobem v zóně domény a porovnat ji s IP adresou z glue záznamu. Jestliže DNS server glue nemá, tento test nemá smysl a může být přeskočen.

Správný výsledek		Glue záznamy souhlasí s A záznamem v zóně domény
E051	chyba	Některým z DNS serverů nesouhlasí glue na nadřazeném serveru a A záznam v zóně

5.1.6 Přítomnost NS záznamů v zóně domény

Zóna domény musí obsahovat v NS záznamech pro tuto doménu názvy autoritativních DNS serverů. Pokud NS záznamy chybí, doména je sice funkční, protože jsou k dispozici NS záznamy z nadřazeného DNS serveru, avšak formálně se jedná o vážnou chybu. V rámci tohoto testu je také potřeba zkontrolovat, zda NS záznamy náhodou neobsahují IP adresu, protože správně musí vždy obsahovat doménový název DNS serveru.

Správný výsledek		Zóna domény obsahuje NS záznamy
E061	chyba	Zóna domény neobsahuje žádný NS záznam
E062	chyba	Jeden nebo více NS záznamů obsahuje místo názvu IP adresu

- Reference: RFC 1912[5], kap. 2.8

5.1.7 Shoda NS záznamů se seznamem autoritativních serverů

Tento test souvisí s předchozím. NS záznamy domény v samotné zóně domény musí souhlasit s NS záznamy na nadřazeném serveru. Pokud jsou různé, nejsou data konzistentní a může se jednat o nevědomou chybu v konfiguraci.

Správný výsledek		NS záznamy souhlasí se seznamem autoritativních serverů
E071	varování	Zóna obsahuje více NS záznamů než nadřazený server
E072	varování	Zóna obsahuje méně NS záznamů než nadřazený server
E073	varování	Zóna obsahuje stejný počet NS záznamů, ale jsou jiné

- Reference: RFC 1912[5], kap. 2.8

5.1.8 Rekurzivní dotazy

Jak již bylo uvedeno v teorii v předchozích kapitolách, není vhodné kombinovat autoritativní a cachovací DNS server na jednom stroji, a tedy míchat autoritativní a cachované informace. V tomto testu se zkoumá, zda server ve svých odpovědích vrací příznak „RA“, tedy zda nám dává najevo, že nám může poskytnout rekurzivní služby.

Správný výsledek		Žádný ze serverů nenabízí zpracování rekurzivních dotazů
E081	varování	Všechny DNS servery nabízí rekurzivní služby
E082	varování	Některé DNS servery nabízí rekurzivní služby (nikoliv všechny)

5.1.9 Veřejné AXFR

Každému serveru ze skupiny se pošle AXFR požadavek na danou doménu, tedy žádost o zaslání úplného obsahu zóny. Pokud server vyhoví a data zašle, je to vyhodnoceno jako varování, protože celá zóna je veřejně přístupná a kdokoliv si může prohlédnout seznam všech subdomén, aliasů, případně počítačů v doméně aj. AXFR přenosy je vhodné povolit pouze mezi primárním a sekundárními DNS servery domény.

Správný výsledek		Žádný ze serverů neposkytuje obsah celé zóny této domény prostřednictvím AXFR
E091	varování	Všechny DNS servery nabízí AXFR zóny
E092	varování	Některé DNS servery nabízí AXFR zóny (nikoliv všechny)

5.1.10 DNS servery na veřejných IP adresách

Dokument RFC 3330[10] uvádí seznam IP adres, které nejsou určeny k veřejnému použití a slouží např. pro lokální sítě, testovací účely aj. Pokud použijeme takovou IP adresu pro DNS server, je celý Internet nedostupný, možná s výjimkou lokální sítě jejich provozovatele.

Podle zmíněného dokumentu pro použití v lokálních síti, pro loopback a podobné speciální účely vyhrazeny následující podsítě IPv4:

- 10.0.0.0/8

- 127.0.0.0/8 (loopback)
- 169.254.0.0/16 (link local, určeno dvoubodové spoje)
- 172.16.0.0/12
- 192.0.2.0/24 – rezervováno pro uvádění v příkladech (TEST-NET)
- 192.168.0.0/16

IP adresy z uvedených rozsahů by se na veřejném Internetu neměly objevit.

Správný výsledek		Všechny DNS servery jsou na veřejných IP adresách
E101	chyba	Všechny DNS servery jsou na neveřejné IP adrese
E102	chyba	Některé DNS servery jsou na neveřejné IP adrese (nikoliv všechny)

5.1.11 Doporučený počet DNS serverů

Minimální požadovaný počet DNS serverů jsou 2, což je zřejmé proto, že funkčnost domény nesmí být závislá na serveru jednom (tomu se říká single point of failure). Maximální doporučený počet je 7 serverů, což vyplývá z toho, že při vyšším počtu je pravděpodobné, že údaje o autoritě dané zóny (její NS záznamy) se nevejdou do limitu 512 bytů a tedy nebudou moci být přeneseny v jednom UDP paketu a komunikace bude muset být zopakována přes protokol TCP.

Správný výsledek		Doména má doporučený počet 2-7 DNS serverů
E111	chyba	Doména má pouze jeden autoritativní DNS server na nadřazeném serveru
E112	varování	Doména má více než 7 autoritativních DNS serverů na nadřazeném serveru

- Reference: RFC 1912[5] (2.8), RFC 1537[3] (6)

5.1.12 TTL hodnoty u NS záznamů na nadřazeném DNS serveru

Standard RFC stanovuje, že obecně jakékoliv záznamy, které se shodují názvem domény a typem, musí mít stejné hodnoty TTL. V opačném případě by měly být tyto záznamy považovány za neplatné. Tudíž je třeba zkontrolovat TTL hodnoty v NS záznamech, které jsme získali z nadřazeného DNS serveru.

Problém při různých TTL nastává u cachovacích DNS serverů, které by mohly vrátit pouze částečnou odpověď, protože část záznamů vypršela, ale zbytek je ještě platný. Vrácené záznamy pak neodpovídají skutečnosti, odpověď je zkrácena, přesto není nastaven v hlavičce odpovědi příznak TC (truncated). Proto RFC 2181 tuto možnost zakázalo.

Správný výsledek		TTL hodnoty u NS záznamů na nadřazeném DNS serveru se shodují
E131	chyba	Neshoda TTL u NS záznamů na nadřazeném DNS serveru

- Reference: RFC 2181[7] (5.2)

5.1.13 TTL hodnoty u NS záznamů v zóně

Podobný test jako předchozí, je potřeba zkontrolovat TTL hodnoty v NS záznamech ze zóny domény.

Správný výsledek		TTL hodnoty u NS záznamů v zóně se shodují
E141	chyba	Neshoda TTL u NS záznamů v zóně

5.1.14 Reverzní záznamy DNS serverů

Pro všechny A záznamy u domény by měl existovat odpovídající PTR záznam, který mapuje zpětně IP adresu na jeden nebo více doménových názvů, a ty by měly opět směřovat na původní IP. Obecně to však dodržováno není s výjimkou MX a NS záznamů. V obou případech to slouží ke zjišťování důvěryhodnosti daného doménového názvu a jeho IP adresy a vypovídá to o tom, zda má v názvech a IP adresách příslušný správce DNS serverů pořádek.

Kontrolovat doménové názvy v reverzních záznamech by bylo příliš striktní. Pokud na jednu IP adresu směřuje více doménových názvů, měl by správně existovat odpovídající počet PTR záznamů, ale v praxi se uvádí PTR záznam jen jeden, většinou se jedná o název počítače. Je to dáno především chybným povědomím, že PTR záznam může být jen jeden. O tom hovoří dokument RFC 2181[7] v kapitole 10.2. Test by tedy měl

provést o krok více – získaný název z reverzního záznamu dále přeložit na IP adresu a tu porovnat s původní IP adresou DNS serveru.

Správný výsledek		Reverzní záznamy DNS serverů se shodují s jejich IP adresami
E151	varování	Reverzní záznamy se neshodují u všech DNS serverů
E152	varování	Reverzní záznamy se neshodují u některých DNS serverů (nikoliv u všech)
E153	varování	Reverzní záznamy u některých DNS serverů neexistují

- Reference: RFC 1912[5] (2.1)

5.2 Kontrola umístění serverů v síti Internet

5.2.1 Různé autonomní systémy (AS) DNS serverů

Síť Internet byla již od počátku budována tak, aby byla decentralizovaná a aby v případě poruchy některé její části zbytek sítě nadále fungoval. To by se mělo odrazit i v systému DNS. Je chyba mít všechny DNS servery domény schované za jednou přípojkou do Internetu a spoléhat na to, že k poruše na této přípojce nedojde. Při nedostupnosti všech DNS serverů přestává doména pro celý Internet „existovat“.

Autonomním systémem (AS) se nazývá nezávislá samostatně fungující část Internetu, nejčastěji to bývá síť jedné firmy, jejíž vnitřní struktura je zvenku neviditelná či nepodstatná, funguje samostatně jako celek a na své periferii je propojena s dalšími autonomními systémy. Každý autonomní systém v Internetu má přiděleno unikátní číslo ASN - Autonomous System Number. Autoritou pro přidělování ASN je organizace IANA (Internet Assigned Numbers Authority), která přiděluje rozsahy čísel lokálním registrům, např. pro evropský kontinent je jím organizace RIPE NCC.

V tomto testu je pro každý DNS server (resp. jeho IP adresu) třeba zjistit číslo autonomního systém, ve kterém se nachází. Jestliže jsou všechny DNS servery v jednom autonomním systému, znamená to závislost funkčnosti domény na funkčnosti jediné sítě. Ke zjišťování ASN slouží WHOIS servery jednotlivých lokálních registrů dle přiřazených rozsahů IP adres.

Existuje situace, kterou nedokáže tento test odhalit, a sice to, že v Internetu existuje daný DNS server ve více kopiích (tzv. anycastová zrcadla), kdy je více fyzických serverů umístěno v různých lokalitách a používající stejnou IP adresu. Mechanismus routování v síti Internet zajistí, že klienta to nasměruje na „bližší“ server („bližší“ ve významu routovacích protokolů, tedy lépe dostupný). Běžné je to u autoritativních DNS serverů pro doménu 0. úrovně a pro domény 1. úrovně, pro SLD to obvyklé není. Servery jsou pak sice fyzicky rozmístěny po světě a jsou v podstatě napojeny do různých autonomních systémů, ale není způsob, jak něco takového zjistit. Autonomní systém se zjišťuje podle originálního původu IP adresy serveru. Tento systém pro testování domén je však zaměřen zejména na domény 2. úrovně, a tak to nečiní problémy.

Správný výsledek		DNS servery jsou v alespoň dvou různých autonomních systémech (AS)
E161	varování	Všechny DNS servery jsou v jednom autonomním systému

- Reference: RFC 1912[5] (2.8)

5.2.2 Různé podsítě DNS serverů

Tento požadavek se velmi podobá předchozímu, ale je daleko striktnější. Autonomní systémy se dělí dále na tzv. podsítě, ty mohou být velikostně a prostorově velmi rozmanité (v rámci místnosti, budovy, ale i větší). Mít všechny DNS servery v jedné podsíti je mnohem závažnější problém, protože ta může být závislá např. na funkčnosti jediného routeru, jedné elektrické přípojky, správci sítě atd., a tedy jeden problém či jedna chyba může způsobit ihned nedostupnost všech DNS serverů.

Ke každé IP adrese je třeba v rámci možností zjistit co nejkonkrétnější určení podsítě. Ne však všichni ISP zveřejňují podrobné informace o struktuře jejich sítě. Sítě lze opět zjišťovat pomocí vhodných WHOIS serverů. Pro tento test taktéž platí poznámka o anycastových zrcadlech DNS serverů.

Správný výsledek		DNS servery jsou v alespoň dvou různých podsítích
E171	chyba	Všechny DNS servery jsou v jedné podsíti

5.2.3 Různé IP adresy DNS serverů

Tento bod navazuje na předchozí dva a zkoumá ještě horší prohřešek, kdy správce domény obejde požadavek na minimální počet 2 DNS serverů u domény tím, že jednomu fyzickému serveru přidělí 2 pojmenování a ty uvede jako autoritativní DNS servery domény. Funkčnost domény je pak závislá na jednom jediném stroji.

Může také nastat situace, kdy jeden fyzický DNS server má více IP adres, které se použijí pro DNS služby. Takovou situaci však nelze rozlišit.

Správný výsledek		DNS servery mají různé IP adresy
E181	chyba	Některé DNS servery mají stejnou IP adresu

5.3 Kontrola údajů v SOA záznamu domény

5.3.1 Server ze SOA MNAME jako NS záznam

Položka MNAME v SOA záznamu uvádí název primárního DNS serveru pro danou doménu, stejný server by měl mít také svůj NS záznam v zóně domény. Pokud tam chybí, nemá to sice na nic vliv, protože položka MNAME má pouze informativní charakter, ale mohlo by to znamenat nedostatek v nastavení či správě domény. Častou chybou je uvedení názvu samotné domény. Je sice možné, že DNS server se skutečně jmenuje jako doména (tedy směřuje na něj A záznam), ale je to velmi nepravděpodobné.

Správný výsledek		DNS server z položky SOA MNAME je uveden v zóně jako NS záznam
E511	varování	Název serveru v SOA MNAME je shodný s názvem domény, pravděpodobně se jedná o chybu
E512	upozornění	Primární DNS server (ze SOA MNAME) není uveden v NS záznamech v zóně

- Reference: RFC 2181[7] (7.3)

5.3.2 Kontrola položky MNAME

Známou chybou v položce MNAME při použití systému BIND je zapomenutí tečky na konci názvu, systém tedy na konec připojí název aktuální domény. U domény example.com by mohl záznam MNAME vypadat „ns.example.com.“. Pokud na konci není uvedena tečka, vznikne z toho název „ns.example.com.example.com“. V tomto testu se tedy zjišťuje, zda se aktuální doména konci řetězce dvakrát neopakuje. Navíc se zkouší přeložit název v MNAME na IP adresu.

Správný výsledek		Položka MNAME v SOA záznamu je syntakticky v pořádku
E521	varování	Vypadá to, že MNAME neobsahuje v zónovém souboru tečku na konci (je ve formátu xx.domena.domena)
E522	chyba	MNAME nelze přeložit na IP adresu

5.3.3 Stejné MNAME v SOA od všech serverů

Při stahování SOA záznamů z DNS serverů je třeba zkontrolovat, zda se ve všech získaných SOA záznamech shoduje název primárního DNS serveru (položka MNAME). Pokud se neshodují, je to vážnější prohřešek než rozdílná sériová čísla, protože to již skutečně znamená chybu v konfiguraci, poruchu synchronizace či chybné uvedení některého DNS serveru jako autoritativního.

Správný výsledek		Všechny servery vrací stejné MNAME v SOA záznamu
E531	chyba	DNS servery vrací různou hodnotu MNAME, nejspíš chyba v konfiguraci a synchronizaci

5.3.4 Kontrola položky RNAME

Podobně jako u kontroly položky MNAME, i zde často dochází k opomenutí uvedení tečky za koncem názvu (v tomto případě kontakt na správce zóny domény). Výsledkem může být hodnota „hostmaster.example.com.example.com“.

Standard DNS navíc zakazuje použití zavináče v této položce, znak zavináče musí být nahrazen tečkou (RFC 1912[5], 2.2).

Správný výsledek		Položka RNAME v SOA záznamu je syntakticky v pořádku
E541	chyba	V údaji RNAME se nachází znak zavináč
E542	varování	Vypadá to, že RNAME neobsahuje v zónovém souboru tečku na konci (je ve formátu xx.domena.domena)

5.3.5 Doporučený tvar sériového čísla YYYYMMDDnn

Doporučeným formátem sériových čísel je YYYYMMDDnn (YYYY = rok, MM = měsíc, DD = den, nn = číslo revize dne). Při použití tohoto formátu se snadno pozná datum poslední změny u domény. Jedná se však jen o doporučení, obecně jde jen o jakékoliv navýšení čísla při změně obsahu zóny, aby sekundární DNS servery při porovnání čísel zjistily, že ke změně došlo. Když už se tento formát dodržuje, velmi často se jako první revize ze dne uvádí číslo „00“, dokument RIPE-203[12] však říká, že první revize dne by měla mít číslo „01“.

Správný výsledek		Sériové číslo má doporučený tvar YYYYMMDDnn
E551	upozornění	Zóna má sériové číslo ve tvaru YYYYMMDDnn, avšak chybně interpretuje první změnu dne (číslo revize) jako nn=00
E552	upozornění	Zóna nemá sériové číslo ve tvaru YYYYMMDDnn

- Reference: RIPE-203[12], RFC 1912[5] (2.2)

5.3.6 Kontrola hodnoty REFRESH

Dokument RFC 1912[5] (kap. 2.2) doporučuje používat hodnotu v rozsahu 20 minut až 12 hodin. V případě, že primární server zasílá sekundárním serverům při změně obsahu zóny notifikace (RFC 1996[6]), není třeba používat takto krátké intervaly. Test je tedy prováděn tak, že pokud je hodnota nižší než 20 minut, je oznámeno varování o příliš nízké hodnotě a zbytečně častém ověřování aktuálnosti zóny ze strany sekundárních DNS serverů, což znamená buď chybu v nastavení SOA záznamu anebo pokud je opravdu potřeba provádět tak časté změny, je vhodnější implementovat mechanismus notifikací.

Pokud je hodnota vyšší než 12 hodin, je oznámeno upozornění o této skutečnosti, avšak s vysvětlením, že vysoký údaj může být uveden úmyslně, protože je používán jiný mechanismus aktualizace zónových dat. Ovšem je třeba brát v úvahu, že notifikace dle

standardu RFC 1996 probíhají po UDP protokolu bez kontroly zpětné vazby, tudíž se může taková informace ztratit. Je tedy přesto nutné pravidelně změny kontrolovat, i když je možno zvolit delší intervaly.

Správný výsledek		Hodnota REFRESH je v doporučeném intervalu 20m-12h
E561	upozornění	Hodnota REFRESH je příliš nízká
E562	varování	Hodnota REFRESH je příliš vysoká

5.3.7 Kontrola hodnoty RETRY

Jestliže při dotazu sekundárního serveru na primární ohledně aktuálnosti zóny dojde k chybě (porucha v síti, porucha primárního serveru aj.), opakuje sekundární server svůj dotaz po uplynutí doby RETRY (sekundy). Smysl mají pouze hodnoty, které jsou nižší než REFRESH, protože v případě poruchy je třeba pokusit se opakovat dotaz v kratších intervalech, aby se zabránilo zbytečnému „stáří“ zóny, pokud chyba vznikla kvůli krátké poruše v konektivitě apod.

V dokumentu RIPE-203[12] je jakou doporučená hodnota uvedeno 2 hodiny. Nejnižší doporučená hodnota se v žádném dokumentu nenachází. Není vhodné se o komunikaci znovu pokoušet příliš často (v několikaminutových intervalech), protože je pravděpodobné, že porucha na trase či na serveru nebude tak rychle opravena. Při zkoumání množství nejrůznějších domén první a druhé úrovně bylo zjištěno, že se nejčastěji používají hodnoty 15 minut, 30 minut, 1 hodina a 2 hodiny. Oněch 15 minut se zdá jako rozumná dolní mez pro tyto účely, protože doporučené minimum pro hodnotu REFRESH je 20 minut.

Správný výsledek		Hodnota RETRY je nižší než REFRESH a nejméně 15m
E571	varování	Hodnota RETRY je vyšší než REFRESH
E572	upozornění	Hodnota RETRY se zdá příliš nízká

5.3.8 Kontrola hodnoty EXPIRE

Jestliže se nepodaří sekundárnímu DNS serveru aktualizovat zónu po dobu delší než EXPIRE, stává se zóna neplatnou a server by ji měl zapomenout. Vážnou chybou je hodnota, která je nižší než součet hodnot REFRESH+RETRY či dokonce nižší než

samotné REFRESH. Ve druhém případě zóna expiruje dříve, než mají sekundární DNS servery šanci provést aktualizaci, což vůbec nedává smysl. V prvním případě se nedává šanci zóně, u které dojde při prvním pokusu k chybě a už nedojde k opakování po uplynutí doby RETRY.

Mimo tyto 2 závažné stavy je doporučeným rozmezím hodnoty EXPIRE 2-4 týdny (dle RFC 1912[5], kap. 2.2), což je však často interpretováno jako 14-30 dní a mnohými pokusy s nejrůznějšími doménami bylo zjištěno, že se často jako měsíc bere 31 dní. Pro potřeby tohoto testu budeme tedy brát jako rozumné hodnoty 14-31 dní, jelikož jde především o to, abychom za problémový označili údaj, který se výrazně liší od běžných zvyklostí, a pár dnů navíc zde nehraje roli.

Správný výsledek		Hodnota EXPIRE je v doporučeném intervalu 14d-31d a větší než REFRESH+RETRY
E581	chyba	Hodnota EXPIRE je menší než REFRESH
E582	chyba	Hodnota EXPIRE je menší než součet hodnot REFRESH + RETRY
E583	varování	Hodnota EXPIRE je nižší než doporučené minimum 14 dní
E584	upozornění	Hodnota EXPIRE je vyšší než doporučené maximum 31 dní

5.3.9 Kontrola hodnoty MINIMUM

Dokument RFC 2308[8] v části 2.2.1 uvádí „Hodnoty od 1 do 3 hodin byly shledány jako správně fungující a měly by být rozumné pro standardní použití. Hodnoty přesahující 1 den byly shledány jako problematické.“

Je třeba dát pozor na správnou interpretaci této hodnoty, která původně udávala minimální TTL záznamů v zóně domény, poté implicitní hodnotu TTL pro záznamy, které ji nemají uvedenu, a nejnověji tato hodnota značí TTL pro cachování negativních odpovědí (jak dlouho si má cachovací DNS server pamatovat, že záznam neexistuje).

Správný výsledek		Hodnota MINIMUM je v doporučeném intervalu 1-3h
E591	upozornění	Hodnota MINIMUM je nižší než doporučené minimum 1 hodina
E592	upozornění	Hodnota MINIMUM je větší než doporučené maximum 3 hodiny

Kapitola 6 – Implementace

6.1 Způsob implementace

Jak bylo zmíněno v úvodu této práce, jejím cílem je především vytvoření webové aplikace, která bude interaktivně provádět testy jednotlivých domén. Z tohoto důvodu byly pro implementaci zvoleny webové technologie. V úvahu přicházely nejpoužívanější technologie ASP.NET na serveru Windows spolu s databází MS SQL a dále technologie PHP na serveru Linux s databází MySQL. Nakonec byla zvolena kombinace PHP+MySQL z několika důvodů – zkušenosti s vývojem webových aplikací těmito prostředky autorem této práce a jejich snadná dostupnost (vše je zdarma a open-source). Díky tomu lze také tuto aplikaci provozovat na libovolném webhostingu, který podporuje PHP a nabízí databázi MySQL, což je dnes standardní výbava.

Protože druhým cílem je, aby aplikace uměla provádět dávkové zpracování domén, byla rozdělena do několika nezávislých modulů. Základem je výkonné testovací jádro, které pro každou doménu provede sadu testů a vyhodnotí výsledky. Testy jsou iniciovány buď z webové aplikace, která výsledky přijaté od jádra zobrazí v podobě webové stránky, anebo pomocí modulu pro dávkové zpracování, který volá testování pro každou doménu ze svého seznamu a výsledky ukládá do databáze (k jejich pozdějšímu vyhodnocení a interpretaci).

Aplikace na testování domén běží nad PHP frameworkem vlastní výroby, který se stará o komunikaci s databázovým serverem, zpracováním chyb v aplikaci, generování stránek v HTML jazyce, kontrolu syntaxe a formátování řetězců, logování aktivity aj.

obr. 2 – schéma modulů aplikace

6.2 Komunikace s DNS servery

Jádro je mimo databáze, kterou používá pro cachování některých výsledků, napojeno také na DNS resolver, tedy modul, který provádí samotnou komunikaci s DNS servery přes DNS protokol. Pro tento modul byl zvolen volně dostupný balíček Net_DNS z knihovny PEAR (knihovna volně dostupných open-source zdrojových kódů v PHP), který je k dispozici na adrese http://pear.php.net/package/Net_DNS. Jeho použití je velmi jednoduché – vstupem je dotazovaný název, typ záznamu a cílový DNS server, výsledkem je PHP objekt, reprezentující veškerá získaná data včetně hlaviček DNS protokolu a dodatečných sekcí. Navíc lze ovlivnit používaný transportní protokol (vynucení TCP), timeouty pro čekání na odpověď, počet pokusů při neúspěchu aj. Balíček umí provádět taktéž AXFR přenosy.

Pro potřeby této aplikace byly jako rozumné hodnoty zvoleny timeout 3 sekundy pro čekání na přijetí odpovědi od DNS serveru a každý pokus je zopakován maximálně třikrát. Pokud ani po těchto 3 pokusech není žádná odpověď přijata, je server považován za nedostupný. 3 vteřiny je rozumný čas pro dopravu paketu s dotazem od zdroje k cíli, vyřízení požadavku DNS serverem a dopravení paketu s odpovědí zpět ke zdroji. 3 pokusy se zdají být rozumné, počítá se tedy se 2 ztrátami UDP paketů. Pro tolerantnější výsledky by mohly být zvoleny vyšší hodnoty, avšak na úkor celkové rychlosti testů (návštěvník webové aplikace by musel příliš dlouho čekat, dávkové testování by mohlo

trvat příliš dlouho). Pokud nastavené limity DNS serveru nestačí, zjevně je s ním nebo s trasou od zdroje k cíli něco v nepořádku a stejně tak to cítí uživatelé domén, které server obsluhuje.

Kořenové DNS servery, tedy autoritativní DNS servery pro doménu nulté úrovně, se mění jen zcela výjimečně (některá jejich IP adresa se změní jednou za několik let), a tak pro účely tohoto testu je seznam jejich názvů a IP adres uveden v aplikaci staticky ve zdrojovém kódu jádra.

Jako první v seznamu kořenových serverů je F.ROOT-SERVERS.NET. Je to proto, že společnost CZ.NIC provozuje tzv. anycastové zrcadlo tohoto kořenového serveru, které je přímo propojeno v peeringovém uzlu NIXu v Praze. To znamená, že je velmi dobře dostupné z většiny sítí v České republice se zanedbatelným přenosovým zpožděním. Dostupnost tohoto zrcadla závisí na tom, zda síť, ze které pochází DNS dotaz, má v NIXu aktivován peering s tímto projektem F-ROOT. Získávání informaci z kořenové zóny je pak velmi rychlé a spolehlivé. Teprve v případě nedostupnosti tohoto serveru se zkouší další. Rychlost komunikace s kořenovými DNS servery však není kritická, protože je prováděna jen velice výjimečně, jelikož jejich NS záznamy pro TLD domény mají vysoký údaj TTL, často několik dní.

Pro analýzu domény je základem zjištění seznamu jejích autoritativních DNS serverů. Aplikace to činí tak, že rozdělí doménový název na jednotlivé části, začíná od domény nulté úrovně a ke každé úrovni si zjišťuje autoritativní DNS servery. Zjištěných DNS serverů se zeptá na doménu další úrovně atd. až dorazí k původní doméně. Řešení je univerzální, a tak aplikace umí pracovat s doménou libovolné úrovně, která má svoji vlastní zónu (a jako jiné testy, dostupné na Internetu, se tedy neomezuje jen na 2. úroveň). Samozřejmě je možné, že pokus o zjištění autoritativních DNS serverů skončí neúspěchem, protože doména svou vlastní zónu nemá (a její záznamy jsou uvedeny v zóně nějaké domény úrovně vyšší).

6.3 Zjišťování čísel ASN a podsítí

Možná nejkomplikovanějším úkolem bylo vymyslet a implementovat způsob, jak co nejspolehlivěji zjišťovat podle IP adresy příslušné číslo autonomního systému a co nejpřesněji určit podsíť, do které IP adresa spadá.

Jako nejjednodušší se ukázaly autonomní systémy. Používá se k tomu WHOIS server whois.radb.net, který má informace o všech autonomních systémech a jejich IP adresách. Položí se mu přes WHOIS protokol jednoduchý dotaz obsahující IP adresu a výsledek je hned k dispozici. RADB je označení pro „Merit Network Routing Assets Database“, což je veřejná komerční databáze routovacích informací o sítích Internetu a současně mirror mnoha dalších zdrojů (říká se jim Internet Routing Registry – IRR). Drtivá většina informací je zde k dispozici, neznámé sítě jsou velmi vzácnou výjimkou.

Největší oříšek jsou podsítě. Celý blok IPv4 adres má pod svojí správou organizace Internet Assigned Numbers Authority (IANA), která velké bloky přiděluje dalším několika organizacím dle jejich působnosti. Těmto organizacím se říká „Regional Internet registries“ (RIR):

- AfriNIC (African Network Information Centre) – Afrika
- APNIC (Asia Pacific Network Information Centre) – Asie a Pacifická oblast
- ARIN (American Registry for Internet Numbers) – Severní Amerika
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latinská Amerika a některé Karibské ostrovy
- RIPE NCC (Réseaux IP Européens) – Evropa, Střední Východ a Střední Asie

Tyto dále přidělují jimi spravované bloky tzv. „Local Internet registries“ (LIR), což jsou již konkretní ISP společnosti (poskytovatelé připojení). Každá RIR má WHOIS server, na kterém lze zjišťovat informace o přidělených blocích IP adres, LIR jsou pak povinni tato data aktualizovat. Pravidla u jednotlivých RIR se však velmi liší, nejlépe na tom je asi RIPE NCC, v jehož WHOIS serveru lze nalézt skutečně podrobné informace, protože každý LIR je povinen vkládat do databáze informace o každé podsíti svého bloku, který obdržel od RIPE NCC. Je to především proto, aby bylo v případě bezpečnostního incidentu či spamování jednoduché zjistit co nejkonkrétnější informace

o původu zdroje. Oproti tomu některé další RIR poskytují velmi chabé či žádné informace o některých sítích, které pod ně spadají.

Základem je určit, pod kterou RIR IP adresa spadá. K tomu slouží především stránka http://www.iana.org/assignments/ipv4-address-space, kde je uvedeno přiřazení bloků velikosti třídy A. Informace jsou však málo konkrétní, proto byly doplněny informacemi z konfiguračního souboru programu jwhois, což je oblíbený open-source WHOIS klient, dalšími informacemi ze stránek jednotlivých RIR a nakonec zkoušením několika IP adres a sítí. Navíc některé informace o sítích obsahuje i již zmíněný WHOIS server whois.radb.net (překvapivě většinou podrobnější než údaje na WHOIS serveru příslušného RIR mimo Evropu). Je to tedy vyřešeno tak, že se aplikace zeptá WHOIS serveru příslušného RIR, poté serveru whois.radb.net a vezme se nejkonkrétnější informace.

Z výše uvedeného vyplývá, že takto získané informace je skutečně nutné brát hodně s rezervou. V případě evropských sítí je většina údajů podrobných a spolehlivých, mimo Evropu je to mnohem horší.

6.4 Cachování získávaných dat

Zjišťovaná data, která se příliš často nemění, je vhodné cachovat, tedy ukládat si je do databáze a příště se na ně nedotazovat DNS serverů, čímž se výrazně zrychlí především dávkové zpracování. Po úvaze bylo rozhodnuto, že cachovat se budou seznamy autoritativních DNS serverů pro domény, a to na všech úrovních, přitom se respektují TTL hodnoty u příslušných NS záznamů, tedy po uplynutí daného času se příslušné záznamy v databázi zneplatní a znovu se získají dotazem na DNS servery.

Naopak bylo rozhodnuto, že se nebudou cachovat žádná další data, tedy údaje a výsledky o konkrétních testovaných doménách (tedy záznamy z jejich zóny). Bylo tak zvoleno proto, že se předpokládá, že webovou aplikaci budou využívat osoby, které se o dané domény na DNS serverech starají a zjištěné chyby budou opravovat a budou hned chtít vidět výsledek po provedených úpravách. Pro dávkové zpracování toto není relevantní, protože se v něm každá doména testuje právě jednou, a tak cachování by nemělo vůbec smysl.

Cachování se provádí také v případě čísel autonomních systémů a podsítí, jelikož to jsou údaje, které se mění velmi zřídka anebo vůbec. Druhý důvod je ten, že komunikace s WHOIS servery je poměrně drahá z toho pohledu, že některé z nich omezují počet dotazů za nějaký časový úsek, přitom je naprosto zbytečné se jich na jednu IP adresu ptát vícekrát během krátkého času. Čas uchovávání výsledků od WHOIS serverů byl stanoven na 1 měsíc. Klíčem pro záznamy v cache je IP adresa DNS serveru.

Protože unikátních DNS serverů je mnohem méně než domén (některé DNS servery obsluhují stovky, tisíce či desetitisíce domén), je cachování čísel autonomních systémů a podsítí velmi účinné, zejména při dávkovém zpracování, kdy se analyzují v jistém smyslu „příbuzné“ domény.

6.5 Databázové struktury

Tabulka **ns_cache** pro cachování seznamu autoritativních DNS serverů

položka	typ	popis
ID	int	unikátní ID záznamu
domain	varchar(255)	název domény
server	varchar(255)	název DNS serveru
server_ip	varchar(15)	IP adresa DNS serveru
from_server	varchar(255)	název DNS serveru, ze kterého byl tento záznam získán
glue	varchar(15)	glue záznam
ttl	int	hodnota TTL záznamu
query_date	datetime	datum a čas získání záznamu
expires_date	datetime	datum a čas vypršení platnosti záznamu

Tabulka **ip_net** pro cachování čísel autonomních systémů a podsítí k IP adresám

položka	typ	popis
ipbin	int	IP adresa v číselné reprezentaci
ip	varchar(15)	IP adresa v tečkované notaci
net_ip	varchar(15)	IP adresa podsítě v tečkované notaci
prefix	tinyint	prefix podsítě
asn	int	číslo autonomního systému
created_date	datetime	datum a čas získání informací
expires_date	date	den vypršení platnosti

Pro dávkové zpracování existuje několik dalších tabulek:

- **batch_dom** – informace o jednotlivých doménách, údaje ze SOA záznamu, výsledky jednotlivých testů, počty NS záznamů na nadřazeném DNS serveru a počty A a MX záznamů v zóně domény
- **batch_ns** – tabulka unikátních DNS serverů (dle IP adresy serveru), obsahuje IP adresu (verze 4 i verze 6), informace o autonomním systému a podsíti a příznak podpory rekurzivních dotazů
- **batch_dom_ns** – provázání mezi doménami a jejich DNS servery, pro každou doménu obsahuje seznam DNS serverů (názvy) a jejich IP adresy
- **batch_as** – do této tabulky se pro každou doménu ukládají autonomní systémy jejích DNS serverů; ty by šlo sice zjistit složením dat z tabulek předchozích, avšak jednalo by se o poměrně komplikovaný a na první pohled nejasný dotaz
- **batch_net** – zde si ukládáme ke každé doméně podsítě DNS serverů ze stejného důvodu jako v předchozím bodě
- **batch_ns_avail** – tabulka DNS serverů a jejich dostupnosti z různých lokalit
- **as_name** – tabulka pro cachování výsledků převodu čísel autonomních systémů na název

Z těchto tabulek lze vhodnými SQL dotazy získat nejrůznější statistické údaje o zkoumaném vzorku domén.

6.6 Webové rozhraní aplikace

Webové rozhraní, které je určeno veřejnosti ke zjišťování informací o jednotlivých doménách a stavu jejich DNS serverů, se skládá z jedné WWW stránky. Na ní je jednoduchý formulář, ve kterém se vyplní název domény a dále lze vybrat některé další možnosti analýzy:

- zjistit a zkontrolovat podsítě a autonomní systémy
- zjistit MX záznamy
- zjistit A záznamy
- zkontrolovat zónové transfery (AXFR)
- zkontrolovat reverzní záznamy DNS serverů

Analýza autonomních systémů, podsítí, AXFR a reverzních záznamů je volitelná a standardně není zvolena, protože se jedná o náročnější operace. Formulář je pro jistotu chráněn proti robotům a hromadnému používání této služby prostřednictvím tzv. captcha, tedy je nutné opsat text, který je umístěn v obrázku. Dalším ochranným prvkem je omezený počet dotazů za určitý časový interval z jedné IP adresy.

Výstupem testu jsou nejprve tabulky, obsahující veškeré zjištěné informace o dané doméně a jejích autoritativních DNS serverech:

- Seznam DNS serverů (dle zjištění ze zóny domény o úroveň výše) – TTL příslušného NS záznamu, IPv4 a IPv6 adresa serveru, IPv4 glue, vracené sériové číslo v SOA záznamu a rychlost reakce serveru (čas mezi odesláním dotazu a přijetí odpovědi, uvedeno v milisekundách)
- Seznam DNS serverů, tentokrát se zjištěnou podsítí a číslem autonomního systému
- Informace ze SOA záznamu se stručnými vysvětlivkami, co tyto informace říkají. Časové údaje jsou uvedeny jak v původních jednotkách (sekundách), tak ve větších jednotkách pro lepší představu jejich hodnoty (např. 604800 = 7d). Data pochází ze SOA záznamu primárního DNS serveru (který je určen podle údaje MNAME) anebo z prvního zjištěného serveru (pokud nelze primární určit).
- Výpis MX záznamů domény
- Výpis A záznamů domény

Jako poslední je uvedena tabulka s výsledkem jednotlivých testů. U každého testu je uveden jeho krátký název, výrazně barevně je uveden výsledek (OK, VAROVÁNÍ, UPOZORNĚNÍ) a nakonec podrobnější textové vyjádření buď toho, že zkoumaný údaj je v pořádku, či informace o zjištěné chybě a její stručná charakteristika (v čem problém spočívá, jaká je jeho závažnost a co může způsobit za problémy).

Výslednou aplikaci lze nalézt na stránkách http://www.pweb.cz/cs/dns-test/.

6.7 Požadavky na provoz aplikace

Webová aplikace potřebuje ke svému provozu:

- PHP ve verzi >= 4.4.2 s povolenou podporou soketů, knihovnou GD a podporou freetype (pro generování captcha obrázků)
- balíček Net_DNS z http://pear.php.net/
- databázi MySQL ve verzi => 4.1
- webový server Apache s povoleným mod_rewrite (pokud je třeba provozovat aplikace ve více jazycích)

Aplikace byla otestována na operačním systému Linux s webovým serverem Apache 2, PHP verze 4.4.2 a 5.2.1 a MySQL verze 5.0.37. Zda aplikace v pořádku běží na operačním systému Windows nebylo vyzkoušeno. Webové rozhraní by mělo bez problémů fungovat i na běžných webhostingových serverech.

Kapitola 7 – Analýza stavu DNS serverů všech domén 2. úrovně v doméně CZ

7.1 Způsob provedení analýzy

Analýza stavu všech domén CZ byla prováděna ve spolupráci se sdružením CZ.NIC, správcem domény CZ. Především s ním bylo konzultováno, jaké výstupy by měla analýza poskytovat a jaké informace budou nejzajímavější.

Celá analýza probíhala v těchto fázích:

1. Nejprve byl proveden hromadný test na zkušebním vzorku 10 tisíc domén, především proto, aby se na nich odladilo chování celé aplikace a zjistily případné chyby či nesrovnalosti. U každého testu byla vzata alespoň jedna doména, která tímto testem neprošla, a ručně zkontrolována, zda tomu tak skutečně je.
2. Skutečný test začal stažením aktuálního zónového souboru zóny CZ z primárního DNS serveru této domény prostřednictvím AXFR. Tento soubor byl parserem analyzován a byl z něj získán seznam domén, které byly v tu dobu v zóně, a také autoritativní DNS servery pro jednotlivé domény 2. úrovně. Tyto DNS servery byly vloženy do tabulky, která funguje jako cache autoritativních DNS serverů (ns_cache) s umělým TTL 1 týden, aby se během samotné analýzy ušetřil čas (nebude se provádět dotazování na DNS servery CZ.NICu pro každou doménu). Zóna samozřejmě obsahuje také A záznamy v roli glue, které se také zaznamenaly.
3. Pak probíhal samotný test. Již při analýze zkušebního vzorku se zjistilo, že je problém v tom, že analýza se občas zasekne na nějaké doméně, jejíž DNS servery neodpovídají (test jedné domény může trvat až několik desítek sekund, pokud se nevrací žádné odpovědi, dokud nevyprší všechny timeouty a pokusy). Proto analýza probíhala v několika instancích paralelně (nakonec bylo zvoleno 20 paralelních běhů). Systémem zámků bylo zajištěno, že každý proces si bez zásahu ostatních „vyzvednul“ další doménu z fronty a nemohlo se stát, že by v jeden okamžik jednu doménu analyzovalo více procesů.

4. Pak přišly na řadu 2 dodatečné testy. Úkolem bylo zjistit pro každý DNS server, zda a jak je dostupný z několika dalších lokalit po světě a jaký DNS software je na jednotlivých DNS serverech nainstalován. O způsobu provedení pojednávají další kapitoly.
5. Po dokončení analýzy se provedlo získání souhrnných výsledků pomocí již předem připravené sady SQL dotazů, které dle různých kritérií získávaly nejrůznější přehledy. Jednalo se především o počty domén u jednotlivých chybových stavů. Na základě zjištěných výsledků se postupně vymyslely další a další výstupy.

7.2 Zjištění dostupnosti DNS serverů z více lokalit

Pro tento test bylo důležité, aby byl co nejsnadnějším způsobem proveditelný na libovolném Unixovém serveru, aniž by bylo nutné cokoliv instalovat či konfigurovat. Výsledkem je jednoduchý bash skript, který čte seznam DNS serverů z textového souboru, pro každý server (jeho IP adresu) volá utilitu dig a zaznamenává její výstup. Ke každému DNS serveru je na vstupu uvedena některá z domén, pro kterou je autoritativní, aby byly zasílané dotazy smysluplné. V odpovědích se nezkoumal výsledek, sledoval se pouze údaj o době odpovědi, popř. zda server neodpověděl vůbec. Získaná data jsou poté uložena do výstupního souboru, ten je přenesen do aplikace, která výstup parsuje a zanáší výsledky do databáze. Z toho je nakonec vygenerován výstup v podobě tabulky, obsahující rozdělení počtu DNS serverů podle rychlosti jejich reakce z dané lokality.

Pro měření z nové lokality tedy stačí komukoliv, kdo má na příslušný server přístup, zaslat skript a vstupní textový soubor, skript na serveru spustit a zaslat zpět výsledek k dalšímu zpracování.

V příloze této práce je k dispozici výsledek měření ze sítě MFF UK. Měření z dalších lokalit bylo prováděno pracovníky sdružení CZ.NIC.

7.3 Zjištění software na DNS serverech

DNS servery nezveřejňují informace o tom, jaký software na nichž běží a o jakou se jedná verzi. Je to mimo jiné z bezpečnostních důvodů, protože ze znalosti konkrétní verze softwaru si lze zjistit existující zranitelnosti a opatřit si exploity. Z těchto důvodů strategické DNS servery (např. kořenové) úmyslně používají na jednotlivých uzlech různé DNS programy v různých verzích tak, aby v případě nalezené a zneužité bezpečnostní díry nebyl okamžitě ovlivněn celý systém.

Zjistit, jaký software na DNS serveru běží, se tedy zdá na první pohled nemožné. Naštěstí existuje program fpdns (Fingerprinting DNS servers), který rozpoznává DNS servery tak, že jim posílá zvlášť připravené dotazy, o kterých ví, že na ně různé programy v různých verzích reagují jinak, případně některý software nemá implementovány všechny součásti DNS protokolu apod. Dobře formulovanými dotazy tak lze s velkou pravděpodobností úspěchu určit jak název programu, tak jeho konkrétní či alespoň přibližnou verzi.

Test tedy probíhal tak, že se nástroj fpdns pustil na všechny DNS servery, které byly v průběhu analýzy CZ domén zjištěny (bylo jich celkem 9913). Nebylo třeba vynakládat žádné velké úsilí pro rychlé provedení testu, protože fpdns samo o sobě umí provádět hromadné zkoumání velkého množství serverů paralelně. Výstup programu byl pak zpracován a do databázové tabulky se seznamem DNS serverů byla ke každému serveru přiložena zjištěná informace. DNS software pak byl pro lepší orientaci rozdělen do několika nejpoužívanějších „rodin“ – BIND, TinyDNS, MS Windows DNS, PowerDNS a další. Z toho pak byly ve výstupu analýzy sestaveny tabulky.

7.4 Seznam výstupů analýzy

Výstupem každého reportu jsou počty domén, nikde nejsou uváděny jejich konkrétní názvy.

- počty úspěšně a neúspěšně analyzovaných domény
- tabulky s počty chybných domén pro jednotlivé testy
- tabulky s kombinacemi příbuzných testů
- nejpoužívanější údaje MNAME u domén

- nejpoužívanější údaje RNAME u domén
- počty DNS serverů u domény (dle nadřazeného DNS serveru)
- počty MX záznamů v zóně
- počty A záznamů v zóně s www a bez
- názvy DNS serverů s největším počtem domén, které obsluhují
- IP adresy DNS serverů s největším počtem domén
- autonomní systémy s největším počtem DNS serverů a odpovídající počty domén
- podsítě s největším počtem DNS serverů a odpovídající počty domén
- počty domén u jednotlivých autonomních systémů, které jsou na nich plně závislé (všechny DNS servery domény jsou pouze v tomto jednom AS)
- počty domén u jednotlivých podsítí, které jsou na nich plně závislé (všechny DNS servery domény jsou pouze v tomto jednom AS a pouze v jedné podsíti)
- DNS servery a odpovídající počty domén dosažitelné přes protokol IPv6
- počet názvů DNS serverů na IP adresu (tedy pokud má některý DNS server více názvů, započítá se vícekrát)

Nakonec je výstupem tabulka s mnoha dalšími zajímavými informacemi, shrnutí a závěr.

7.5 Výsledky analýzy

Následují stručné výsledky této analýzy. Jejich úplné znění lze nalézt na CD, které je přílohou této práce, a taktéž na stránkách:
http://www.pweb.cz/analyzy/cz/200704/index.html

Test byl proveden nad doménami a jejich DNS servery podle zónového souboru, obdrženého ze serverů CZ.NICu dne 14.4.2007 v 13:30. V úvahu tedy byly vzaty pouze domény, které byly v tento okamžik delegovány. Ze zónového souboru bylo získáno celkem 301921 domén. Poté byl v průběhu 2 dnů proveden test na každou doménu. Víkend byl zvolen záměrně, protože během něho se v nastavení domén provádí zanedbatelné množství změn. Samozřejmě mohlo k několika změnám dojít, např. v okamžiku analýzy domény zónový soubor obsahoval již neaktuální DNS servery domény, ale takových mohly být jednoty, maximálně desítky a v souhrnných výsledcích se viditelně neprojevily.

7.5.1 Souhrn a zajímavosti

položka	*počet*	*%*
Celkem domén k otestování	301921	
Celkem otestovaných domén	301359	99.81
Nebylo možno otestovat (nelze získat žádné údaje o doméně)	562	0.19
Počet unikátních DNS serverů dle názvu	13153	
Počet unikátních DNS serverů dle IP adresy	9913	
Průměrný počet domén na DNS serveru (dle IP adresy)	69.6655	
Počet DNS serverů s IPv6	27	0.27
Počet domén na DNS serverech dostupných přes IPv6	687	0.23
Počet DNS serverů (dle názvu), kterým nesouhlasí glue	209	1.59
Počet domén, které jsou aliasem	37	0.01
Počet autonomních systémů	1369	
Počet podsítí	5821	
Suma NS záznamů na nadřazeném serveru	693518	
Suma NS záznamů v zónách domén	716704	
Suma MX záznamů v zónách domén	441147	
Suma A záznamů bez WWW v zónách domén	236155	
Suma A záznamů s WWW v zónách domén	283550	
Počet všech chyb	72976	
Počet všech varování	537627	
Počet všech upozornění	434224	
Počet domén s chybami	63979	21.19
Počet domén s varováním (a bez chyb)	210693	69.78
Počet domén s upozorněním (a bez chyb a varování)	17108	5.67
Počet domén bez jakéhokoliv problému	9579	3.17

Software DNS serverů - rodiny				
poř.	***položka***	***počet***	***%***	
1	BIND	6974	70.35	
2	TinyDNS	413	4.17	
3	MS Windows DNS	412	4.16	
4	PowerDNS	365	3.68	
5	MyDNS	167	1.68	
6	NSD	20	0.20	
7	UltraDNS	18	0.18	
8	ANS	10	0.10	
9	Cisco CNR	9	0.09	
10	MaraDNS	2	0.02	
	ostatní	123	1.24	
	nezjištěno	1400	14.12	
	celkem	9913		

7.5.2 Dostupnost DNS serverů ze sítě MFF UK

Dostupnost z MFF UK (síť CESNET)				
čas	***podíl***		***celkem***	
<= 5 ms	1917	19.34 %	1917	19.34 %
<= 10 ms	1440	14.53 %	3357	33.86 %
<= 15 ms	813	8.20 %	4170	42.07 %
<= 20 ms	590	5.95 %	4760	48.02 %
<= 30 ms	1270	12.81 %	6030	60.83 %
<= 50 ms	1305	13.16 %	7335	73.99 %
<= 100 ms	538	5.43 %	7873	79.42 %
<= 150 ms	758	7.65 %	8631	87.07 %
<= 200 ms	349	3.52 %	8980	90.59 %
<= 300 ms	61	0.62 %	9041	91.20 %
<= 500 ms	87	0.88 %	9128	92.08 %
<= 1000 ms	28	0.28 %	9156	92.36 %
> 1000 ms	28	0.28 %	9184	92.65 %
nedostupný	729	7.35 %		
nezjištěno	0	0.00 %		

Měření bylo prováděno z počítače v počítačové laboratoři v budově MFF UK na Malostranském náměstí. Zkoumalo se celkem 9913 DNS serverů, které byly zjištěny při předchozích testech.

7.5.3 Nejzávažnější zjištěné problémy

Zřejmě nejzávažnějšími problémy u zkoumaných domén jsou uvedeny v následujícím seznamu, který je setříděn dle závažnosti problému s přihlédnutím k počtu ovlivněných domén.

1. **41793 (14%) domén** má všechny své DNS servery v jedné podsíti (single point of failure)
2. **123545 (41%) domén** má všechny své DNS servery v jednom autonomním systému
3. **209 (1,6%) DNS serverů** má chybně uvedené glue
4. **4746 (48%) DNS serverů** nabízí rekurzivní služby, jedná se tedy o kombinaci autoritativního a cachovacího serveru
5. U **2721 (0,9%) domén** se vyskytují DNS servery se stejnou IP adresou
6. U **1050 domén** nelze přeložit některý název DNS serveru na IP adresu
7. U **159 domén** se nelze spojit s žádným DNS serverem
8. Pro **1915 (0,6%) domén** není žádný DNS server (u ní uvedený) autoritativní
9. U **54362 (18%) domén** lze z alespoň jednoho serveru získat obsah celé zóny prostřednictvím AXFR
10. **1504 (15%) DNS serverů** má problém se svým reverzním záznamem (záznam nemá nebo nesouhlasí)

7.5.4 Závěr z analýzy

Přísnými kritérii prošlo pouze **9579** domén - u nich se nevyskytla žádná chyba, varování ani upozornění. Nutno však podotknout, že negativní výsledky označené jako upozornění nejsou závadou, jen se dané parametry vymykají z doporučovaných hodnot. Často to může být úmyslné speciální nastavení. Relevantnější tedy bude nejspíš číslo **17108**, které udává počet domén bez chyb a varování, a dále **237942 domén (79%)** nemá žádný negativní výsledek označený jako chyba. Avšak plných **63979 domén (21%)** u sebe nějakou chybu má!

Z uvedeného se zdá, že čeští správci DNS serverů se příliš nezajímají o to, aby byly jejich domény a domény jejich zákazníků dostupné i v kritických situacích (výpadky napájení, poruchy konektivity apod.), protože DNS servery domén soustředí do společných lokalit, sítí či autonomních systémů a většinou používají pouze 2 DNS servery. Tím sice nejspíš ušetří náklady na provoz dalších DNS serverů, jejich správu, umístění do jiných lokalit atd., ale předpokládám, že při prvním větším výpadku služeb budou vzniklé škody mnohem vyšší.

Stejně závažný se mi jeví fakt, že polovina DNS serverů slouží současně jako cachovací, což sice opět vede k ušetření několika málo peněz na provoz dalšího serveru, ale je to špatná volba. Míchání autoritativních a cachovaných dat na jednom stroji může zapříčit problémy.

Kapitola 8 – Závěr

8.1 Splnění cíle

V rámci této bakalářské práce byla na základě množství zdrojů sestavena metodika pro provádění analýzy nastavení DNS u domén. Následně byla s použitím technologií PHP a MySQL vytvořena webová aplikace, která umožňuje jakémukoliv zájemci provést on-line analýzu konkrétní domény a dozvědět se zjištěné nedostatky a problémy. Stránky této aplikace splňují normy XHTML 1.0 Transitional a CSS 2 a byly vyzkoušeny v množství internetových prohlížečů (Internet Explorer, Firefox, Opera aj.). Aplikace umožňuje provést test domény libovolné úrovně (s výjimkou nulté), pokud tato doména má svoji vlastní zónu (tedy není součásti zóny domény vyšší úrovně). Webové rozhraní bylo také přeloženo do angličtiny, čímž se stalo přístupné téměř všem uživatelům Internetu.

Na závěr byla provedena hromadná analýza všech domén CZ, jejímž výsledkem je množství statistických údajů, vyjadřující „zdraví“ českých domén. Výsledky poukazují na mnohé problémy a nesprávná nastavení a naznačují, čemu by se měli správci příslušných DNS serverů více věnovat a jaká rizika zjištěné problémy přináší.

Zdrojové kódy aplikace jsou podrobně komentovány, jednotlivé části (moduly, třídy, funkce, metody apod.) jsou komentovány stylem JavaDoc a lze např. nástrojem phpDocumentor vygenerovat programátorskou referenční dokumentaci. Ta je také přílohou této práce.

K bakalářské práci patří CD, které obsahuje:

- zdrojové kódy a dalších součásti, potřebné ke zprovoznění testovacího jádra a webové aplikace pro testování jednotlivých domén
- návod k instalaci webové aplikace
- dokumentace zdrojových kódů, vygenerovaná nástrojem phpDocumentor
- tato bakalářská práce ve formátu PDF
- úplné výsledky analýzy CZ domén ve formátu HTML

Funkční webová aplikace je k dispozici na stránkách:
http://www.pweb.cz/cs/dns-test/

Úplné výsledky analýzy CZ domén jsou také na stránkách:
http://www.pweb.cz/analyzy/cz/200704/index.html

8.2 Praktické zkušenosti s aplikací

Aplikace byla ve zkušebním provozu několik měsíců a mnoho lidí ji během té doby vyzkoušelo a použilo pro test nejrůznějších domén. Na základě ohlasů a kontroly výstupů byla prováděna nejrůznější vylepšení a aplikace se stala uživatelsky přívětivější. Během zkušebního provozu se nevyskytl žádný závažný problém.

Hromadnému testu všech CZ domén předcházelo zkoumání několika menších vzorků domén, na kterých byla aplikace odladěna a vylepšena.

8.3 Možnosti dalšího vývoje

Nabízí se mnoho dalších věcí, které by mohla aplikace analyzovat a provádět. Jedná se zejména o:

1. Provádění kontroly MX záznamů
2. Zkouška doručení pošty na mailservery, uvedené v MX záznamech
3. Zkouška spojení na WWW servery, uvedené v A a AAAA záznamech
4. Zkouška spojení s DNS servery přes protokol IPv6 – to však vyžaduje podporu webového serveru a sítě
5. Zkoumání přítomnosti dalších druhů záznamů, např. DNSSEC, SPF
6. Zjištění, zda jsou DNS servery domény v různých verzích DNS softwaru. To by znamenalo volat fpdns nástroj při každém testu. zřejmě by nebylo vhodné veřejně pro každý DNS server uvádět název a verzi software, který je na něm provozován.

Literatura

[1] Mockapetris P. (1987): *Domain Names - Concepts and Facilities*, STD 13, RFC 1034, WWW http://rfc.net/rfc1034.html

[2] Mockapetris P. (1987): *Domain Names - Implementation and Specification*, STD 13, RFC 1035, WWW http://rfc.net/rfc1035.html

[3] Beertema P. (1993): *Common DNS Data File Configuration Errors*, RFC 1537, WWW http://rfc.net/rfc1537.html

[4] Thomson S., Huitema C. (1995): *DNS Extensions to support IP version 6*, RFC 1886, WWW http://rfc.net/rfc1886.html

[5] Barr D. (1996): *Common DNS Operational and Configuration Errors*, RFC 1912, WWW http://rfc.net/rfc1912.html

[6] Vixie P. (1996): *A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)*, RFC 1996, WWW http://rfc.net/rfc1996.html

[7] Elz R., Bush R. (1997): *Clarifications to the DNS Specification*, RFC 2181, WWW http://rfc.net/rfc2181.html

[8] Andrews M. (1998): *Negative Caching of DNS Queries, RFC 2308*, WWW http://rfc.net/rfc2308.html

[9] Bush R., Karrenberg D., Kosters M. (2000): *Root Name Server Operational Requirements*, RFC 2870, WWW http://rfc.net/rfc2870.html

[10] IANA (2002): *Special-Use IPv4 Addresses*, RFC 3330, WWW http://rfc.net/rfc3330.html

[11] Klensin J. (2003): *Role of the Domain Name System*, RFC 3467, WWW http://rfc.net/rfc3467.html

[12] Koch P. (1999): *Recommendations for DNS SOA Values*, RIPE-203, WWW http://www.ripe.net/docs/ripe-203.html

[13] Peterka J. (2007): *Rodina protokolů TCP/IP, verze 2.4*, přednáška, WWW http://www.earchiv.cz/l217/index.php3

[14] Kabelová A., Dostálek L. (2002): *Velký průvodce protokoly TCP/IP a systémem DNS*, 3. aktualizované a rozšířené vydání, Computer Press