VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF INFORMATICS

NÁVRH MODELU SLUŽEB SÍTE PRO FIRMU TECHNISERV IT S.R.O.

IMPROVEMENT PROPOSAL OF NETWORK SERVICES MODEL
FOR TECHNISERV IT S.R.O. COMPANY

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — JINDŘICH LAVICKÝ
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.
SUPERVISOR

BRNO 2010

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2009/10
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jindřich Lavický

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Návrh modelu služeb sítě pro firmu Techniserv IT s.r.o.

v anglickém jazyce:

Improvement Proposal of Network Services Model for Techniserv IT s.r.o. company

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

STANEK, W. R. Microsoft Windows Server 2008: Kapesní rádce administrátora. 1.vydání. Computer Press. 2008. 704 s. ISBN: 978-80-251-1936-5.
SAVILL, J. The Complete Guide to Windows Server 2008. 1.vydání. Addison-Wesley. 2008. 1752s.
ISBN: 0-321-50272-8.
ODOM, W. Počítačové sítě. 1.vydání. Computer press, 200ř. 384s. ISBN 80-251-0538-5.
BIGELOW, S. J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. 1.vydání. Praha : Computer Press, 2004. 990 s. ISBN 80-251-0178-9.

Vedoucí bakalářské práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2009/10.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ Fakulta podnikatelská

L.S.

Ing. Jiří Kříž, Ph.D.
Ředitel ústavu

doc. RNDr. Anna Putnová, Ph.D., MBA
Děkanka

V Brně, dne 26.3.2010

Abstrakt

Bakalářská práce popisuje návrh modelu služeb sítě pro firmu Techniserv IT s.r.o. Analyzuje současný stav IT infrastruktury v organizaci a navrhuje vhodné systémové a ekonomické řešení. Popisuje jednotlivé oblasti služeb sítě a jejich výhody. Detailně se zaměřuje na oblast nasazení služeb sítě, která je pro tuto práci klíčová. Na závěr navrhuje řešení a vyhodnocuje jejich přínos podniku.

Abstract

The bachelor thesis describes a proposal of network services model for Techniserv IT s.r.o. company. It analyses the present state of IT infrastructure in organization and suggests appropriate and economical solutions. It describes constituent areas of network services and their advantages. In detail, it focuses on the area of network services implementation, which is crucial for this type of work. At the end, it proposes solutions and evaluates their assets for a company.

Klíčová slova

Služby sítě, DNS, DHCP, NTP, Microsoft, Windows Server 2008

Keywords

Network services, DNS, DHPC, NTP, Microsoft, Windows Server 2008

Bibliografická citace mé práce:

LAVICKÝ, J. *Návrh modelu služeb sítě pro firmu Techniserv IT s.r.o.*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2010. 55 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně.

Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 31. května 2010

…….

Jindřich Lavický

Poděkování

Tímto bych chtěl poděkovat všem, kteří mi při vypracovávání bakalářské práce pomohli. Zejména vedoucímu bakalářské práce panu Ing. Viktoru Ondrákovi, Ph.D. Za jeho odbornou pomoc a ochotu.

OBSAH

ÚVOD

Bakalářskou práci jsem vypracoval pro firmu Techniserv IT s.r.o. v Brně, kde jsem pracoval jako správce informačních systémů. Téma práce vzniklo z požadavků organizace, přizpůsobit IT infrastrukturu rozvíjejícímu se prostředí firmy.

V dnešní době je každá firma závislá na správné funkci „core“ síťových služeb jako například DNS, DHCP, NTP. Bez jejich správné funkce aplikace nefungují, nefunguje ani autentizace pomocí Kerberos protokolu, a faktický dopad na infrastrukturu je téměř totožný s fyzickým výpadkem sítě.

Bakalářská práce je rozdělena do několika kapitol. V první kapitola je věnována vymezení problémů a cílů. V druhé kapitole je popsán současný stav IT infrastruktury organizace a jeho analýza. Ve třetí kapitole, která se zaměřuje na teoretickou část jsou představeny jednotlivé služby sítě. Čím se zabývají, jaké jsou její oblasti, jaké přináší výhody. Další kapitola je věnována návrhům řešení jednotlivých služeb a vybavení, na základě analýzy současného stavu a teoretických poznatků. V poslední kapitole je závěrečné zhodnocení.

1. VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem bakalářské práce je najít a navrhnout vhodné řešení služeb sítě a pro implementaci do stávající infrastruktury firmy Techniserv IT s.r.o. Zjistit, zda přechod na novou koncepci bude pro organizaci výhodný, jak po stránce finanční, tak i systémové. Investice při budovaní nové topologie by měli přinést úsporu v nákladech na pořizování nového hardware, ale i úspory v provozních nákladech a údržbě. V systémové oblasti očekávám výhody v maximalizaci využití výpočetních zdrojů, jednodušší správě, flexibilitě a vysoké dostupnosti celého prostředí.

2. ANALÝZA SOUČASNÉHO STAVU

2.1 Charakteristika organizace

Firma Techniserv IT s.r.o. je soukromou společností zabývající se činností v oblasti Informačních Systémů, Slaboproudých technologií a telekomunikací. Společnost TECHNISERV IT, spol. s r.o. je členem skupiny TECHNISERV, která zaměstnává více jak 200 zaměstnanců.

2.2 Struktura organizace

Společnost Techniserv IT s.r.o. je rozdělena z důvodu regionální působnosti do několika pracovišť. Hlavním sídlem jsou kanceláře v Brně s pobočkami v Praze a Ostravě.

2.3 IT infrastruktura

Celá IT infrastruktura firmy Techniserv IT s.r.o. je velmi různorodá. Tato práce si neklade za cíl provést detailní rozbor všech oblastí. Zmíněny budou pouze celky, které mají klíčový vliv na dále popisované řešení síťových služeb.

2.3.1 Serverové prostředí

Před dvěma lety bylo vyměněno serverové zařízení a přešlo se na model s operačním systémem Windows Server 2003 a hardwarem od jednoho výrobce. Tento stav platí i dnes. Nynější strategie je taková, že v rámci struktury existují dva nezávislé servery, který poskytují různorodou množinu služeb. Z toho na jednom ze serverů jsou kumulovány všechny služby sítě. Tudíž se jedná o typický scénář, kdy jsou služby sítě poskytovány centrálně i pobočkám bez jakékoli možnosti ochrany proti výpadkům. Lze tedy předpokládat, že toto prostředí bude vhodné k implementaci návrhu a nasazení služeb sítě v takovém rozsahu, aby bylo možno předejít možným výpadkům služeb.

Název serveru	Provozované služby	Operační systém
TSNT1	DC, DNS,DHCP,NTP, MS Exchange	Windows Server 2003
TSNT2	SQL, FTP	Windows Server 2003

Tabulka 1: Přehled serverů a poskytovaných služeb

Serverová zařízení a síťové prvky jsou umístěny v jedné společné místnosti. Vstup do této místnosti je řízen přístupovým systémem, jehož účelem je omezení možnosti přístupu neprivilegovaných osob a zajištění evidence přístupů. Místnost je vybavena čidlem protipožárního systému EPS. Přístupový systém a protipožární systém je integrován se zabezpečovacím systémem EZS. V místnosti je instalována klimatizační jednotka, které udržuje teplotu v místnosti na 18°C.

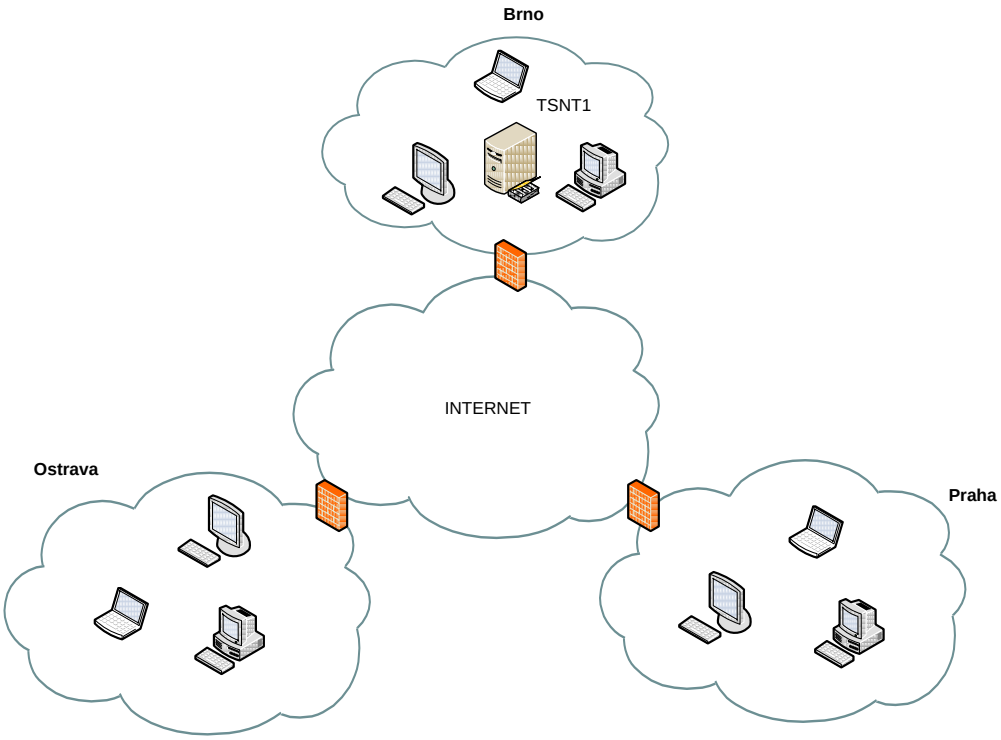
Na serveru jak bylo zmíněno jsou provozovány souběžně všechny služby. To je velkou nevýhodou, pokud dojde k havárii na serveru, jsou nedostupné všechny služby, které na něm běží. Server je denně zálohován pomocí nástrojů v operačním systému.

Všechna zařízení jsou připojena do domény Microsoft Windows s doménovým názvem tsit.cz, kterou zajišťuje doménový řadiče TSNT1. Server TSNT1 je autoritativním jmenný server pro doménu *tsit.cz*, určenou výhradně pro interní síťové prostředí společnosti. Zároveň TSNT1 server slouží jako antivirový uzel celé sítě, odkud se distribuují aktuální virové definice na koncové stanice a ostatní servery připojené do datové sítě.

Na serveru TSNT1 běží poštovní server Microsoft Exchange. Veškeré síťové aplikace, které využívají všichni zaměstnanci, např. právní systém ASPI jsou instalovány na TSNT2 serveru. Ten je zároveň i tiskovým serverem. Jako souborový server slouží TSNT2, kde jsou uložena společná a domovské složky uživatelů. Web server na serveru TSNT1 zajišťuje INTRANET a jsou na něm umístěny intranetové stránky firmy.

2.3.2 Síťové prostředí

Síť se skládá z několika podsítí, připojených pomocí vpn prvků. Aktivní síťové prvky jsou programovatelné a opět dodané jedním výrobcem. Rozvody sítě jsou realizovány formou strukturované kabeláže kategorie 5E umožňující vzájemnou komunikaci jednotlivých zařízení maximální rychlostí 1000Mbps, vlastní uspořádání jednotlivých komponent sítě vykazuje hvězdicovou topologii.



Obrázek 1: Současný stav

Aktivní prvky jsou nastaveny tak, aby zajišťovaly požadovanou bezpečnost a zamezovaly přístup do vnitřní sítě organizace. V síti se používá automatické přidělování IP adres.

2.3.3 Pracovní stanice

Všichni zaměstnanci mají k dispozici stolní počítač nebo notebook. Na začátku letošního roku došlo k výměně všech desktopů a tím opět k sjednocení celé struktury stolních počítačů. U notebooků situace není tak jasná. Snahou je postupem času zajistit jednotnost i v této oblasti.

Všechny pracovní stanice jsou zařazeny do domény tsit.cz. Přístup uživatelů je ověřován vůči této doméně. Pro větší bezpečnost se hlásí pomocí čipové karty a jsou povinni ji používat. Bezpečnost na stanicích zajišťuje antivirový program a centrální doménová politika.

2.4 Hodnocení současného stavu

Z výsledků vyplývá, že v současném prostředí firmy by bylo vhodné nasadit zařízení, které by poskytovali služby pobočkám nezávisle.

Ceny hardware neustále klesají, respektive za stejnou pořizovací cenu získáme daleko vyšší výkon. Náklady na opravu starších zařízení nesou i jiné problémy než vynaložení finančních prostředků. Jedním z klíčových problémů může být nedostupnost náhradních dílů nebo minimálně jejich delší dodací lhůty. Tím se doba opravy nepříjemně prodlužuje a havárie tak může ovlivnit plynulý provoz celé organizace.

Důležité rozhodnutí tedy bude volba vhodné koncepce. Zásadní vliv budou mít jistě dostupné finanční prostředky. V kapitole Návrh řešení se mimo jiné zaměřím na ekonomické zhodnocení, jehož výsledek může být opěrným bodem při rozhodování.

3. TEORETICKÁ VÝCHODISKA ŘEŠENÍ

3.1 Základní služby IP sítě

Infrastrukturními službami IP sítí rozumíme několik dílčích distribuovaných služeb, využívajících ke své činnosti protokol TCP/IP, které poskytují informace kritické pro funkci ostatních aplikací v prostředí sítě TCP/IP.

Jsou to (v pořadí dle klesajícího významu) služby:

- DNS – adresářové služby pro prostředí TCP/IP,
- DHCP – přidělování konfiguračních parametrů IP uzlům,
- NTP – synchronizace systémového času,

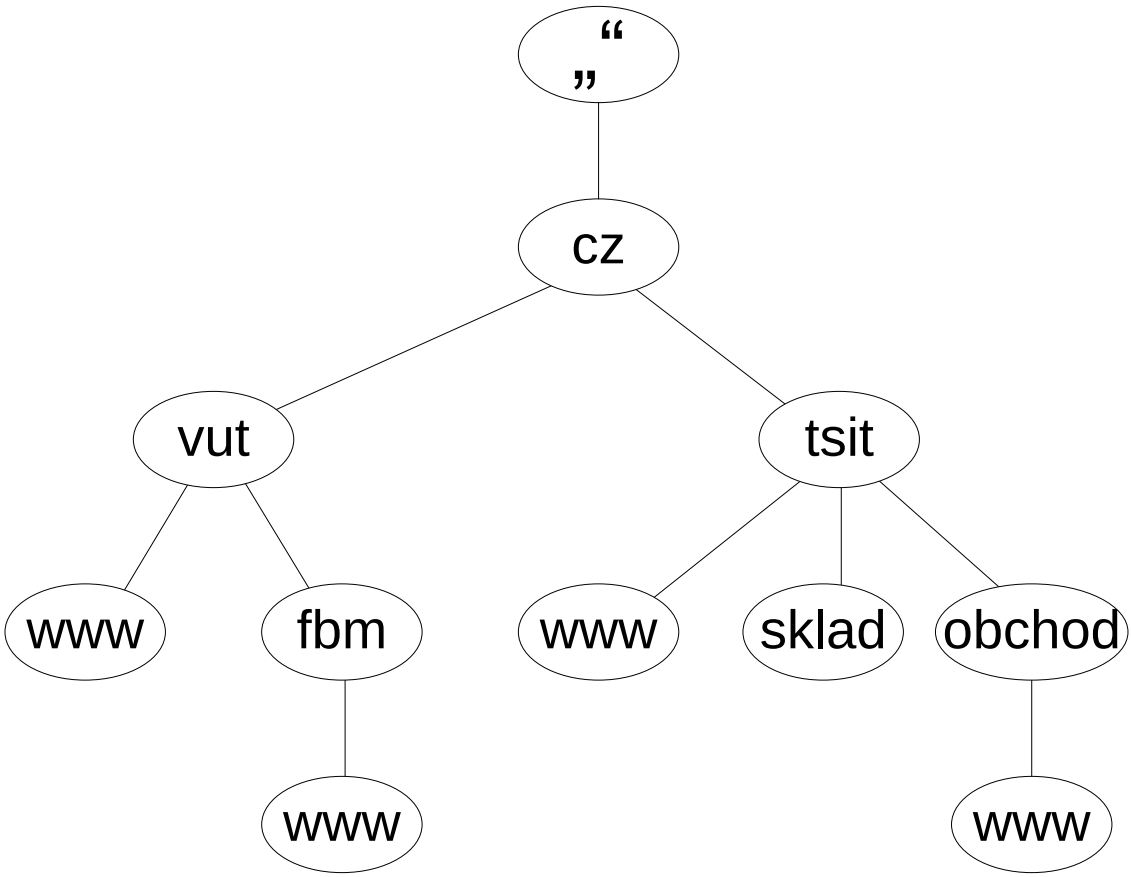
Tyto služby v rozsáhlé IP síti vždy tvoří jediný provázaný celek. V předkládaném návrhu je hlavní důraz kladen na efektivitu systému jejich poskytování, správy a využívání.

3.2 DNS

DNS (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného názvu, kterým si vyměňují informace. Jeho hlavním úkolem a důvodem vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a slouží dnes jako distribuovaná databáze síťových informací.

Protokol používá porty TCP/53 i UDP/53, je definován v RFC1035. Servery DNS jsou organizovány hierarchicky, stejně jako jsou hierarchicky tvořeny názvy domén. Jména domén umožňují lidem lepší orientaci, adresy pro stroje jsou však vyjádřeny pomocí adres 32 bitových (IPv4) A záznam nebo 128 bitových (IPv6) - AAAA záznam. Systém DNS umožňuje velmi efektivně udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy. Stejně tak zajišťuje zpětný překlad IP adresy na doménové jméno - PTR záznam.

Prostor doménových jmen tvoří stromovou strukturu. Každý uzel tohoto stromu obsahuje informace o části jména (doméně), které je mu přiděleno a odkazy na své podřízené domény. Kořenem stromu je tzv. kořenová doména, která se zapisuje jako samotná tečka. Pod ní se v hierarchii nacházejí tzv. domény nejvyšší úrovně (Top-Level Domain, TLD). Ty jsou buď tematické (*com* pro komerci, *edu* pro vzdělávací instituce atd.) nebo státní (*cz* pro Českou republiku, *sk* pro Slovensko.).



Obrázek 2: Stromová struktura DNS

Strom lze administrativně rozdělit do jednotlivých zón, které spravují jednotliví správci (organizace nebo i soukromé osoby), přičemž taková zóna obsahuje autoritativní informace o spravovaných doménách. Tyto informace jsou poskytovány autoritativním DNS serverem.

Výhoda tohoto uspořádání spočívá v možnosti zónu rozdělit a správu její části svěřit někomu dalšímu. Nově vzniklá zóna se tak stane autoritativní pro přidělený jmenný prostor. Právě možnost delegování pravomocí a distribuovaná správa tvoří klíčové vlastnosti DNS a jsou velmi podstatné pro jeho úspěch. Ve vyšších patrech doménové hierarchie platí, že zóna typicky obsahuje jednu doménu. Koncové zóny přidělené organizacím připojeným k Internetu pak někdy obsahují několik domén – například doména *tsit.cz* a její poddomény *vyroba.tsit.cz, marketing.tsit.cz a obchod.tsit.cz* mohou být obsaženy v jedné zóně a obhospodařovány stejným serverem.

3.2.1 Složení doménového jména

Celé jméno se skládá z několika částí oddělených tečkami. Na jeho konci se nacházejí domény nejobecnější, směrem doleva se postupně konkretizuje.

- část nejvíce vpravo je doména nejvyšší úrovně, např. tsit.cz má TLD cz.
- jednotlivé části (subdomény) mohou mít až 63 znaků a skládat se mohou až do celkové délky doménového jména 255 znaků. Doména může mít až 127 úrovní. Bohužel některé implementace jsou omezeny více.

3.2.2 DNS servery (name servery)

DNS server může hrát vůči doméně (přesněji zóně, ale ve většině případů jsou tyto pojmy zaměnitelné) jednu ze tří rolí:

- **Autoritativní**

  Primární server je ten, na němž data vznikají. Pokud je třeba provést v doméně změnu, musí se editovat data na jejím primárním serveru. Každá doména má právě jeden primární server.
  Sekundární server je automatickou kopií primárního. Průběžně si aktualizuje data a slouží jednak jako záloha pro případ výpadku primárního serveru, jednak pro rozkládání zátěže u frekventovaných domén. Každá doména musí mít alespoň jeden sekundární server.

- **Pomocný** (caching only) server slouží jako vyrovnávací paměť pro snížení zátěže celého systému. Uchovává si odpovědi a poskytuje je při opakování dotazů, dokud nevyprší jejich životnost.

- **Rekurzivní** (forward only) server rekurzivně vyřizuje příchozí dotazy.

Odpověď pocházející přímo od primárního či sekundárního serveru je autoritativní, čili je brána za správnou. Z hlediska věrohodnosti odpovědí není mezi primárním a sekundárním serverem rozdíl, oba jsou autoritativní. Naproti tomu odpověď poskytnutá z vyrovnávací paměti není autoritativní. Klient může požádat o autoritativní odpověď, v běžných případech ale stačí jakákoli.

3.2.3 Root servery

Kořenové jmenné servery (root name servers) představují zásadní část technické infrastruktury Internetu, na které závisí spolehlivost, správnost a bezpečnost operací na internetu.

Tyto servery poskytují kořenový zónový soubor (root zone file) ostatním DNS serverům. Jsou součástí DNS, celosvětově distribuované databáze, která slouží k překladu unikátních doménových jmen na ostatní identifikátory.

Kořenový zónový soubor popisuje, kde se nacházejí autoritativní servery pro domény nejvyšší úrovně. Tento kořenový zónový soubor je relativně velmi malý a často se nemění – operátoři root serverů ho pouze zpřístupňují, samotný soubor je vytvářen a měněn organizací IANA.

Pojem root server je všeobecně používán pro 13 kořenových jmenných serverů. Technické prostředky na kterých jsou provozovány jednotlivé root servery se nacházejí ve 34 zemích světa, na více než 80 místech. Root servery jsou spravovány organizacemi, které vybírá IANA.

Následující tabulka zobrazuje těchto 13 root serverů:

Název root serveru	Operátor
A	VeriSign Global Registry Services
B	University of S. California - Information Sciences Institute
C	Cogent Communications
D	University of Maryland
E	NASA Ames Research Center
F	Internet Systems Consortium, Inc.
G	U.S. DOD Network Information Center
H	U.S. Army Research Lab
I	Autonomica/NORDUnet
J	VeriSign Global Registry Services
K	RIPE NCC
L	ICANN
M	WIDE Project

Tabulka 2: Seznam root serverů

3.2.4 Software DNS serverů

Porovnání nejpoužívanějšího software (implementací DNS serverů) z hlediska podporovaných funkcionalit je uveden v následující tabulce:

Název	Pomocný	Rekurzivní	Autoritativní
Microsoft	Ano	Ano	Ano
BIND	Ano	Ano	Ano
PowerDNS	Ano	Ano	Ano
djbdns	Ano	Ano	Ano
MyDNS	Ano	Ne	Ano
NSD	Ne	Ne	Ano

Tabulka 3: Typy Dns serverů.

3.2.5 Řešení dotazu

Každý koncový počítač má ve své konfiguraci síťových parametrů obsaženu i adresu DNS serveru, na nějž se má obracet s dotazy. V operačních systémech odvozených od Unixu je obsažena v souboru */etc/resolv.conf*, v MS Windows lze nalézt ve vlastnostech protokolu TCP/IP (případně lze vypsat nastavenou hodnotu z příkazového řádku zadáním textového příkazu *ipconfig/all*. Adresu DNS serveru počítač typicky obdrží prostřednictvím DHCP.

Pokud počítač hledá určitou informaci v DNS (např. IP adresu k danému jménu), obrátí se s dotazem na tento lokální server. Pokud dotazovaný DNS server nedokáže poskytnout přímou odpověď (např. sever není autoritativní pro daný dotaz, záznam není v paměti) na daný dotaz spustí se níže popsaný proces získávaní informací v rámci hierarchie DNS.

Každý DNS server má ve své konfiguraci uvedeny IP adresy kořenových serverů (autoritativních serverů pro kořenovou doménu). Obrátí se tedy s dotazem na některý z nich.

Kořenové servery mají autoritativní informace o kořenové doméně. Konkrétně znají všechny existující domény nejvyšší úrovně a jejich autoritativní servery. Dotaz je tedy následně směrován na některý z autoritativních serverů domény nejvyšší úrovně, v níž se nachází cílové jméno. Ten je opět schopen poskytnout informace o své doméně a posunout řešení o jedno patro dolů v doménovém stromě. Tímto způsobem řešení postupuje po jednotlivých patrech doménové hierarchie směrem k cíli, až se dostane k serveru autoritativnímu pro hledané jméno, který pošle definitivní odpověď.

Získávání informací z takového systému probíhá rekurzí. Resolver (program zajišťující překlad) postupuje od kořene postupně stromem směrem dolů dokud nenalezne autoritativní záznam o hledané doméně.

Jednotlivé DNS servery jej postupně odkazují na autoritativní DNS pro jednotlivé části jména.

- Uživatel zadal do svého WWW klienta doménové jméno *www.techniservit.cz*. Resolver v počítači se obrátil na lokální DNS server s dotazem na IP adresu pro *www.techniservit.cz*.

- Lokální DNS server tuto informaci nezná. Má však k dispozici adresy kořenových serverů. Na jeden z nich se obrátí a dotaz mu přepošle.

- Kořenový server také nezná odpověď. Ví však, že existuje doména nejvyšší úrovně *cz*, a jaké jsou její autoritativní servery, jejichž adresy tazateli poskytne.

- Lokální server jeden z nich vybere a pošle mu dotaz na IP adresu ke jménu *www.techniservit.cz*.

- Oslovený server informaci opět nezná, ale poskytne IP adresy autoritativních serverů pro doménu *tsit.cz.*

- Lokální server opět jeden z nich vybere a pošle mu dotaz na IP adresu ke jménu *www.techniservit.cz.*

- Jelikož toto jméno se již nachází v doméně *tsit.cz*, dostane od jejího serveru nepochybně autoritativní odpověď.

- Lokální DNS server tuto odpověď předá uživatelskému počítači, který se na ni ptal.

Výše popsaný postup popisuje kompletní řešení daného dotazu. Může se ale stát, že některý z oslovených serverů má hledanou informaci ve své vyrovnávací paměti, protože odpovídající dotaz nedávno řešil. V takovém případě poskytne neautoritativní odpověď z vyrovnávací paměti a další dotazování odpadá.

Ve vyrovnávací paměti mohou být i mezivýsledky - například lokální DNS server v ní skoro jistě bude mít informaci o autoritativních serverech pro doménu *cz*, protože v ní pravděpodobně hledá každou chvíli. V takovém případě by vypadly kroky 2 a 3 a lokální server by se s dotazem rovnou obrátil na některý z autoritativních serverů domény *cz.*

Všimněte si, že oslovené servery v popsaném příkladu vykazují dva odlišné druhy chování. Při rekurzivním řešení dotazu se server chopí vyřízení dotazu, najde odpověď a pošle ji tazateli.

Rekurzivní přístup server zatěžuje (musí sledovat postup řešení, ukládat si mezivýsledky apod.), ale projde jím odpověď a tu si může uložit do vyrovnávací paměti. Typicky se tak chovají lokální servery, aby si plnily vyrovnávací paměti a mohly dalším tazatelům poskytovat odpovědi rovnou.

Při nerekurzivním řešení dotazu server dotaz neřeší, pouze poskytne tazateli adresy dalších serverů, jichž se má ptát dál. Takto se chovají servery ve vyšších patrech doménové hierarchie (kořenové a autoritativní servery TLD), které by rekurzivní chování kapacitně nezvládaly.

V příkladu výše se rekurzivně choval lokální server, zatímco autoritativní servery pro kořenovou doménu a doménu *cz* se chovaly nerekurzivně (což odpovídá realitě).

3.2.6 Reverzní dotazy

Nejběžnějším úkolem DNS je poskytnout informace (nejčastěji IP adresu) pro zadané doménové jméno. Dovede ale i opak – sdělit jméno, pod kterým je daná IP adresa zaregistrována.

Při vkládání dat pro zpětné dotazy, bylo třeba vyřešit problém s opačným uspořádáním IP adresy a doménového jména. Zatímco IP adresa má na začátku obecné informace (adresu sítě), které se směrem doprava zpřesňují až k adrese počítače, doménové jméno má pořadí přesně opačné. Instituce připojená k Internetu typicky má přidělen začátek svých IP adres a konec svých doménových jmen.

Tento nesoulad řeší DNS tak, že při reverzních dotazech obrací pořadí bajtů v DNS adrese. K obrácené adrese pak připojí doménu *in-addr.arpa* a výsledné *„jméno“* pak vyhledává standardním postupem.

Hledá-li například jméno k IP adrese *146.97.39.155*, vytvoří dotaz na *155.39.97.146.in-addr.arpa*. Obrácení IP adresy umožňuje delegovat správu reverzních domén odpovídajících sítím a podsítím správcům dotyčných sítí a podsítí.

V příkladu použitou síť *146.97.0.0/16* spravuje autoritativní správce a ten má také ve správě jí odpovídající doménu *97.146.in-addr.arpa*. Kdykoli zavede do sítě nový počítač, může zároveň upravit data v reverzní doméně, aby odpovídala skutečné situaci.Je dobré mít na paměti, že na data z reverzních domén nelze zcela spoléhat. Do reverzní domény se v principu dají zapsat téměř libovolná jména. Nikdo například nemůže zabránit autoritativnímu správci, aby o počítači *146.97.1.1* prohlásil v reverzní zóně, že se jedná třeba o *www.techniservit.cz.* Pokud na tom záleží, je záhodno si poskytnutou informaci ověřit dopředným dotazem (zde nalézt IP adresu k *www.techniservit.cz* a porovnat ji s *146.97.1.1).* Jestliže odpovědí na něj bude původní IP adresa, jsou data důvěryhodná – správce klasické i reverzní domény tvrdí totéž. Pokud se liší, znamená to, že data v reverzní doméně jsou nekorektní.

3.2.7 DNS cache

Téměř každý DNS server funguje zároveň jako DNS cache. Při opakovaných dotazech pak nedochází k rekurzivnímu prohledávání stromu, ale odpověď je získána lokálně. V DNS záznamech je totiž uložena i informace o době platnosti záznamu (TTL). Po vypršení platnosti je záznam z DNS cache odstraněn.

3.2.8 Doba uložení záznamu

Problém s uložením záznamů v cache nastává v případě změny záznamu. Pokud administrátor nastaví TTL na 6 hodin, a poté provede změnu záznamu, nastane situace, že někteří uživatelé sítě dostanou informaci již novou a někteří ještě starou. Tato situace bude trvat právě oněch 6 hodin, v závislosti na nastavení ostatních serverů a také v závislosti na době která uplynula od jejich posledního dotazu.

Je proto nutné zvolit správný poměr mezi rychlostí šíření změn a ušetřeným výkonem a přenosovým pásmem DNS serveru. Pokud se změny provádí často, je vhodné zvolit kratší TTL v řádu jednotek hodin, pokud se změny téměř neprovádějí, může být TTL ve dnech.

3.2.9 Zónové soubory

Obsah zóny (domény či několika domén) je uložen v tzv. zónovém souboru. Skládá se z jednotlivých záznamů (přesný název zní zdrojové záznamy, resource records (RR) obsahujících dílčí informace.

Jejich názvy a nesené informace jsou přesně definovány v příslušných dokumentech, většina v RFC 1035. Formát textového zápisu zónového souboru se liší v závislosti na použitém serveru.

Záznamy v něm mají tvar:

jméno životnost třída typ parametry

- *jméno* je doménové jméno, pro něž záznam vytváříte. Zpravidla patří do aktuálně definované domény, pak se píše jen samotné jméno bez tečky na konci a bude k němu doplněna aktuální doména. Pokud jméno ukončíte tečkou, nic se k němu nedoplňuje a bere se jako kompletní. Nemusí být uvedeno, pak se přebírá z předchozího záznamu.

- *životnost* určuje dobu platnosti záznamu v sekundách. Většinou se neuvádí a záznamům se ponechává implicitní životnost. Umožňuje vám však udělat výjimku.

- *třída* určuje rodinu protokolů, k níž se záznam vztahuje. DNS lze teoreticky používat i pro jiné síťové architektury, v praxi však třída vždy bývá IN, což znamená Internet.

- *typ* určuje typ definovaného záznamu (viz níže).

- *parametry* se vztahují k typu záznamu, poskytují mu potřebná data. Obsahem parametrů často bývají doménová jména. Je třeba zdůraznit, že v parametrech se smí vyskytovat jen skutečná jména, nikoli přezdívky zavedené pomocí CNAME (viz níže).

Zónový soubor vždy musí začínat záznamem typu SOA.

3.2.10 Typy záznamů

Nejčastěji používané jsou následující typy zdrojových záznamů (v abecedním pořadí):

- **A** (address record) obsahuje IPv4 adresu přiřazenou danému jménu, například když jménu *priklad.tsit.cz* náleží IP adresa *1.2.3.4*, bude zónový soubor pro doménu *tsit.cz* obsahovat záznam

  priklad IN A 1.2.3.4

- **AAAA** (IPv6 address record) obsahuje IPv6 adresu. Zmíněnému stroji bychom IPv6 adresu *2001:718:1c01:1:02e0:7dff:fe96:daa8* přiřadili záznamem

  priklad IN AAAA 2001:718:1c01:1:02e0:7dff:fe96:daa8

- **CNAME** (canonical name record) je alias - jiné jméno pro jméno již zavedené. Typicky se používá pro servery známých služeb, jako je například WWW. Jeho definice pomocí přezdívky umožňuje jej později snadno přestěhovat na jiný počítač. Pokud náš priklad.tsit.cz má sloužit zároveň jako *www.techniservit.cz,* vložíme do zónového souboru

  www IN CNAME priklad

- **MX** (mail exchange record) oznamuje adresu a prioritu serveru pro příjem elektronické pošty pro danou doménu. Tentokrát jsou parametry dva - priorita (přirozené číslo, menší znamená vyšší prioritu) a doménové jméno serveru. Pokud poštu pro počítač *priklad.tsit.cz* přijímá nejlépe počítač *mail.tsit.cz* a případně jako záložní i *mail.tsnt.cz*, bude zónový soubor obsahovat záznamy (všimněte si použití jmen s tečkou a bez tečky)

  priklad IN MX 10 mail.
  IN MX 20 mail.tsnt.cz.

- **NS** (name server record) ohlašuje jméno autoritativního DNS serveru pro danou doménu. Bude-li mít doména *tsit.cz* poddoménu *obchod.tsit.cz*, jejímiž servery budou *ns.tsit.cz* (primární) a *ns.tsnt.cz* (sekundární), bude zónový soubor pro *tsit.cz* obsahovat

  obchod IN NS ns
  IN NS ns.tsnt.cz.

- **PTR** (pointer record) je speciální typ záznamu pro reverzní zóny. Obsahuje na pravé straně jméno počítače přidělené adrese na straně levé (adresa je transformována na doménu výše popsaným postupem). Držme se našeho příkladu pro záznam typu A - v souladu s ním by zónový soubor pro doménu *3.2.1.in-addr.arpa* měl obsahovat (zónový soubor definuje reverzní doménu, proto je třeba psát na pravé straně kompletní jméno s tečkou, jinak by za ně připojil reverzní doménu)

  4 IN PTR priklad.tsit.cz.

- **SOA** (start of authority record) je zahajující záznam zónového souboru. Obsahuje jméno primárního serveru, adresu elektronické pošty jejího správce (zavináč je v ní ale nahrazen tečkou) a následující údaje:

  Serial — sériové číslo, které je třeba zvětšit s každou změnou v záznamu. Podle něj sekundární server pozná, že v doméně došlo ke změně. Pokud jej zapomenete zvětšit, rozejde se obsah sekundárních serverů s primárním, což rozhodně není dobré. Pro přehlednost často ve formátu YYYYMMDDHH.
  Refresh — jak často se má sekundární server dotazovat na novou verzi zóny (v sekundách).
  Retry — v jakých intervalech má sekundární server opakovat své pokusy, pokud se mu nedaří spojit s primárním.
  Expire — čas po kterém označí sekundární servery své záznamy za neaktuální, pokud se jim nedaří kontaktovat primární server.
  TTL — implicitní doba platnosti záznamů.

Časové údaje jsou v sekundách. Novější implementace umožní pro vyšší pohodlí používat k číslům přípony 'M','H','D' a 'W' (minuta, hodina, den, týden) – například 8h znamená 8 hodin, čili totéž co hodnota 28800.

Podívejme se na příklad SOA záznamu:

```
@       IN   SOA   ns.tsit.cz.  administrator.tsit.cz. (
        201005050
         1h
        5m
        1w
        1d
         )
```

3.2.11 Příklad zónového souboru

Zkusme dát dohromady lehce upravené úseky popsané výše a vytvořit příklad zónového souboru pro doménu *tsit.cz*. O takovýto záznam se stará správce (majitel) domény a má možnost jej měnit.

```
$TTL 1w
@       IN   SOA   server.tsit.cz.  administrator.tsit.cz. (
                   201005050
                   1h
                   5m
                   1w
                   1d
                   )
                     IN   NS   server
                     IN   NS   ns.tsnt.cz.
                     IN   MX   10 server
                     IN   MX   20 mail.tsnt.cz.
priklad              IN   A    1.2.3.4
                     IN   AAAA 2001:718:1c01:1:02e0:7dff:fe96:daa8
server               IN   A    1.2.3.1
www                  IN   CNAME server
```

V příkladu je uvedena implicitní životnost jeden týden, dále SOA záznam popsaný výše, určující, že se záznam týká domény *tsit.cz*, jejíhož správce je možné kontaktovat na emailu *administrator@tsit.cz*.

V zónovém souboru je v emailové adrese znak „@" nahrazen znakem „.". Důvodem je speciální význam znaku „@" v rámci zónového souboru. Při prohledávání daného zónového souboru DNS serverem jsou všechny výskyty znaku „@" nahrazeny názvem dané domény.

V rámci dat doménového souboru platí konvence, že všechna doménová jména uvedená v doménovém souboru, která nejsou zakončena znakem „." představují relativní odkazy pro obdržení absolutního názvu je nutné k těmto doplnit název domény daného doménového souboru oddělený znakem „.".

Následují odkazy na dva DNS servery, které o doméně poskytují autoritativní informace – jeden místní a druhý externí. Dále MX záznamy, určující kam se bude doručovat elektronická pošta pro tuto doménu.

Další dva řádky obsahují A a AAAA záznamy určující adresy počítače *priklad.tsit.cz.* Za nimi je definována IPv4 adresa pro *server.tsit.cz* a konečně je mu přidělena přezdívka *www.techniservit.cz.*

3.3 DHCP

DHCP (anglicky Dynamic Host Configuration Protocol) je v informatice aplikační protokol z rodiny TCP/IP. Používá se pro automatické přidělování IP adres jednotlivým osobním počítačům v počítačových sítích, čímž zjednodušuje jejich správu.

DHCP protokol umožňuje prostřednictvím jediného DHCP serveru nastavit všem stanicím sadu parametrů nutných pro komunikaci v sítích používajících rodinu protokolů TCP/IP včetně parametrů doplňujících a uživatelsky definovaných. Významným způsobem tak zjednodušuje a centralizuje správu počítačové sítě (například při přidávání nových stanic, hromadné změně parametrů nebo pro skrytí technických detailů před uživateli).

DHCP servery mohou být sdruženy do skupin, aby bylo přidělování adres odolné vůči výpadkům. Pokud klient některým parametrům nerozumí, ignoruje je.

Parametry nastavitelné pomocí DHCP:

- IP adresa
- maska sítě
- brána (anglicky default gateway)
- DNS servery (seznam jedné nebo více IP adres DNS serverů)

a další údaje, např. servery pro NTP, WINS, …

3.3.1 Princip činnosti

Klienti žádají server o IP adresu, ten u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji klient smí používat (doba zapůjčení, anglicky lease time). Poté co vyprší, smí server adresu přidělovat jiným klientům. Klient komunikuje na UDP portu 68, server naslouchá na UDP portu 67.

Níže je výpis souhrnné tabulky konverzace mezi klientem a serverem, následovaný úrovní paketů a popis procesu:

Source MAC addr	*Dest MAC addr*	*Source IP addr*	*Dest IP addr*	*Packet Description*
Client	*Broadcast*	*0.0.0.0*	*255.255.255.255*	*DHCP Discover*
DHCPsrvr	*Broadcast*	*DHCPsrvr*	*255.255.255.255*	*DHCP Offer*
Client	*Broadcast*	*0.0.0.0*	*255.255.255.255*	*DHCP Request*
DHCPsrvr	*Broadcast*	*DHCPsrvr*	*255.255.255.255*	*DHCP ACK*

Princip přidělení IP adresy:

- Po připojení do sítě klient vyšle broadcastem DHCPDISCOVER paket.
- Na ten odpoví DHCP server paketem DHCPOFFER s nabídkou IP adresy.
- Klient si z (teoreticky několika) nabídek vybere jednu IP adresu a o tu požádá paketem DHCPREQUEST. Server mu ji vzápětí potvrdí odpovědí DHCPACK.
- Jakmile klient obdrží DHCPACK, může už IP adresu a zbylá nastavení používat.

Podrobná konverzaci mezi klientem DHCP a DHCP serverem je následující:

DCPDISCOVER

Klient odešle paket DHCPDISCOVER. Následuje výňatek ze sběru monitoru sítě zobrazující částí DHCPDISCOVER paketů IP a DHCP. V části IP lze vyčíst cílovou adresu *255.255.255.255* a zdrojovou adresu *0.0.0.0.* V části DHCP identifikuje paket jako discover paket a identifikuje klienta na dvou místech pomocí fyzické adresa síťové karty.

IP: ID = 0x0; Proto = UDP; Len: 328
IP: Version = 4 (0x4)
IP: Header Length = 20 (0x14)
IP: Service Type = 0 (0x0)
IP: Precedence = Routine
IP: ...0.... = Normal Delay
IP: ....0... = Normal Throughput
IP: .....0.. = Normal Reliability
IP: Total Length = 328 (0x148)
IP: Identification = 0 (0x0)
IP: Flags Summary = 0 (0x0)
IP: .....0 = Last fragment in datagram
IP: .....0. = May fragment datagram if necessary
IP: Fragment Offset = 0 (0x0) bytes
IP: Time to Live = 128 (0x80)
IP: Protocol = UDP - User Datagram
IP: Checksum = 0x39A6
IP: Source Address = 0.0.0.0
IP: Destination Address = 255.255.255.255
IP: Data: Number of data bytes remaining = 308 (0x0134)
DHCP: Discover (xid=21274A1D)
DHCP: Op Code (op) = 1 (0x1)
DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
DHCP: Hardware Address Length (hlen) = 6 (0x6)
DHCP: Hops (hops) = 0 (0x0)
DHCP: Transaction ID (xid) = 556223005 (0x21274A1D)
DHCP: Seconds (secs) = 0 (0x0)
DHCP: Flags (flags) = 0 (0x0)
DHCP: 0..... = No Broadcast
DHCP: Client IP Address (ciaddr) = 0.0.0.0
DHCP: Your IP Address (yiaddr) = 0.0.0.0
DHCP: Server IP Address (siaddr) = 0.0.0.0
DHCP: Relay IP Address (giaddr) = 0.0.0.0

DHCP: Client Ethernet Address (chaddr) = 08002B2ED85C
DHCP: Server Host Name (sname) = <Blank>
DHCP: Boot File Name (file) = <Blank>
DHCP: Magic Cookie = [OK]
DHCP: Option Field (options)
DHCP: DHCP Message Type = DHCP Discover
DHCP: Client-identifier = (Type: 1) 08 00 2b 2e d8 5c
DHCP: Host Name = JUMBO-WS
DHCP: Parameter Request List = (Length: 7) 01 0f 03 2c 2a 2f 06
DHCP: End of this option field

DHCPOFFER

DHCP server odpoví odesláním paketu DHCPOFFER. Ve zdrojové části IP adres je nyní adresa IP serveru DHCP a cílová adresa je adresa všesměrového vysílání (*255.255.255.255*). V části DHCP paket identifikuje jako nabídku. Lze zde nalézt také pole různých možnosti které jsou odesílány serverem spolu s adresou IP. V tomto případě server odesílá masku podsítě, výchozí bránu (směrovač), dobu zápůjčky, adresu WINS serveru.

IP: ID = 0x3C30; Proto = UDP; Len: 328
IP: Version = 4 (0x4)
IP: Header Length = 20 (0x14)
IP: Service Type = 0 (0x0)
IP: Precedence = Routine
IP: ...0.... = Normal Delay
IP: ....0... = Normal Throughput
IP: .....0.. = Normal Reliability
IP: Total Length = 328 (0x148)
IP: Identification = 15408 (0x3C30)
IP: Flags Summary = 0 (0x0)
IP: .....0 = Last fragment in datagram
IP: ......0. = May fragment datagram if necessary
IP: Fragment Offset = 0 (0x0) bytes
IP: Time to Live = 128 (0x80)
IP: Protocol = UDP - User Datagram
IP: Checksum = 0x2FA8
IP: Source Address = 192.168.48.151
IP: Destination Address = 255.255.255.255
IP: Data: Number of data bytes remaining = 308 (0x0134)
DHCP: Offer (xid=21274A1D)

DHCP: Op Code (op) = 2 (0x2)
DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
DHCP: Hardware Address Length (hlen) = 6 (0x6)
DHCP: Hops (hops) = 0 (0x0)
DHCP: Transaction ID (xid) = 556223005 (0x21274A1D)
DHCP: Seconds (secs) = 0 (0x0)
DHCP: Flags (flags) = 0 (0x0)
DHCP: 0..... = No Broadcast
DHCP: Client IP Address (ciaddr) = 0.0.0.0
DHCP: Your IP Address (yiaddr) = 192.168.50.5
DHCP: Server IP Address (siaddr) = 0.0.0.0
DHCP: Relay IP Address (giaddr) = 0.0.0.0
DHCP: Client Ethernet Address (chaddr) = 08002B2ED85C
DHCP: Server Host Name (sname) = <Blank>
DHCP: Boot File Name (file) = <Blank>
DHCP: Magic Cookie = [OK]
DHCP: Option Field (options)
DHCP: DHCP Message Type = DHCP Offer
DHCP: Subnet Mask = 255.255.255.0
DHCP: Renewal Time Value (T1) = 8 Days, 0:00:00
DHCP: Rebinding Time Value (T2) = 14 Days, 0:00:00
DHCP: IP Address Lease Time = 16 Days, 0:00:00
DHCP: Server Identifier = 192.168.48.151
DHCP: Router = 192.168.48.1
DHCP: NetBIOS Name Service = 192.168.16.154
DHCP: NetBIOS Node Type = (Length: 1) 04
DHCP: End of this option field

DHCPREQUEST

Klient odpoví DHCPOFFER odesláním DHCPREQUEST. Zdrojová IP adresa klienta je stále *0.0.0.0* a cíle paketu je stále *255.255.255.255*. Klient zachová *0.0.0.0*, protože klient nebyl ověřen na serveru, který danou adresu nabídnul. Cíl stále naslouchá, protože může odpovědět víc než jeden server DHCP.

IP: ID = 0x100; Proto = UDP; Len: 328
IP: Version = 4 (0x4)
IP: Header Length = 20 (0x14)
IP: Service Type = 0 (0x0)
IP: Precedence = Routine
IP: ...0.... = Normal Delay
IP: ....0... = Normal Throughput
IP: .....0.. = Normal Reliability

IP: Total Length = 328 (0x148)
IP: Identification = 256 (0x100)
IP: Flags Summary = 0 (0x0)
IP: .....0 = Last fragment in datagram
IP: ......0. = May fragment datagram if necessary
IP: Fragment Offset = 0 (0x0) bytes
IP: Time to Live = 128 (0x80)
IP: Protocol = UDP - User Datagram
IP: Checksum = 0x38A6
IP: Source Address = 0.0.0.0
IP: Destination Address = 255.255.255.255
IP: Data: Number of data bytes remaining = 308 (0x0134)
DHCP: Request (xid=21274A1D)
DHCP: Op Code (op) = 1 (0x1)
DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
DHCP: Hardware Address Length (hlen) = 6 (0x6)
DHCP: Hops (hops) = 0 (0x0)
DHCP: Transaction ID (xid) = 556223005 (0x21274A1D)
DHCP: Seconds (secs) = 0 (0x0)
DHCP: Flags (flags) = 0 (0x0)
DHCP: 0..... = No Broadcast
DHCP: Client IP Address (ciaddr) = 0.0.0.0
DHCP: Your IP Address (yiaddr) = 0.0.0.0
DHCP: Server IP Address (siaddr) = 0.0.0.0
DHCP: Relay IP Address (giaddr) = 0.0.0.0
DHCP: Client Ethernet Address (chaddr) = 08002B2ED85C
DHCP: Server Host Name (sname) = <Blank>
DHCP: Boot File Name (file) = <Blank>
DHCP: Magic Cookie = [OK]
DHCP: Option Field (options)
DHCP: DHCP Message Type = DHCP Request
DHCP: Client-identifier = (Type: 1) 08 00 2b 2e d8 5c
DHCP: Requested Address = 192.168.50.5
DHCP: Server Identifier = 192.168.48.151
DHCP: Host Name = JUMBO-WS
DHCP:Parameter Request List =(Length: 7) 010f032c2a2f06
DHCP: End of this option field

DHCPACK

DHCP server odpoví DHCPREQUEST s DHCPACK tedy dokončí inicializaci cyklu. Zdrojová adresa je adresa IP serveru DHCP a cílová adresa je stále *255.255.255.255*.

IP: ID = 0x3D30; Proto = UDP; Len: 328
IP: Version = 4 (0x4)
IP: Header Length = 20 (0x14)
IP: Service Type = 0 (0x0)
IP: Precedence = Routine
IP: ...0.... = Normal Delay
IP: ....0... = Normal Throughput
IP: .....0.. = Normal Reliability
IP: Total Length = 328 (0x148)
IP: Identification = 15664 (0x3D30)
IP: Flags Summary = 0 (0x0)
IP: .....0 = Last fragment in datagram
IP: .....0. = May fragment datagram if necessary
IP: Fragment Offset = 0 (0x0) bytes
IP: Time to Live = 128 (0x80)
IP: Protocol = UDP - User Datagram
IP: Checksum = 0x2EA8
IP: Source Address = 192.168.48.151
IP: Destination Address = 255.255.255.255
IP: Data: Number of data bytes remaining = 308 (0x0134)
DHCP: ACK (xid=21274A1D)
DHCP: Op Code (op) = 2 (0x2)
DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
DHCP: Hardware Address Length (hlen) = 6 (0x6)
DHCP: Hops (hops) = 0 (0x0)
DHCP: Transaction ID (xid) = 556223005 (0x21274A1D)
DHCP: Seconds (secs) = 0 (0x0)
DHCP: Flags (flags) = 0 (0x0)
DHCP: 0..... = No Broadcast
DHCP: Client IP Address (ciaddr) = 0.0.0.0
DHCP: Your IP Address (yiaddr) = 192.168.50.5
DHCP: Server IP Address (siaddr) = 0.0.0.0
DHCP: Relay IP Address (giaddr) = 0.0.0.0
DHCP: Client Ethernet Address (chaddr) = 08002B2ED85C
DHCP: Server Host Name (sname) = <Blank>
DHCP: Boot File Name (file) = <Blank>
DHCP: Magic Cookie = [OK]
DHCP: Option Field (options)
DHCP: DHCP Message Type = DHCP ACK

DHCP: Renewal Time Value (T1) = 8 Days, 0:00:00
DHCP: Rebinding Time Value (T2) = 14 Days, 0:00:00
DHCP: IP Address Lease Time = 16 Days, 0:00:00
DHCP: Server Identifier = 192.168.48.151
DHCP: Subnet Mask = 255.255.255.0
DHCP: Router = 192.168.48.1
DHCP: NetBIOS Name Service = 192.168.16.154
DHCP: NetBIOS Node Type = (Length: 1) 04
DHCP: End of this option field

Klient musí před uplynutím doby zapůjčení z DHCPACK obnovit svou IP adresu. Pokud lhůta uplyne aniž by dostal nové potvrzení, klient musí IP adresu přestat používat.

Protokol definuje roli i tzv. DHCP relay agenta. Používá se v situaci, kdy existují dvě nebo více sítí oddělené směrovačem a jen jedna síť obsahuje DHCP server.

V takovém případě správce na směrovači zapne relay agenta a nastaví jej tak, aby všesměrové (broadcast) DHCP dotazy ze sítí bez DHCP serveru přeposílal DHCP serveru. Agent k přeposílanému dotazu přidá číslo sítě a masku sítě, na které klienta zaslechl, aby DHCP server poznal, ze kterého adresního rozsahu má klientovi adresu přiřadit.

3.3.2 Možnosti přidělení IP adresy

IP adresa může být stanici přidělena několika způsoby:

Ruční nastavení

V tomto případě správce sítě nevyužívá DHCP serveru a konfiguraci jednotlivých stanic zapisuje jednotlivě přímo do konfigurace jednotlivých stanic.

Statická alokace

DHCP server obsahuje seznam MAC adres a k nim příslušným IP adres. Pokud je žádající stanice v seznamu, dostane vždy přidělenu stejnou pevně definovanou IP adresu.

Dynamická alokace

Správce sítě na DHCP serveru vymezí rozsah adres, které budou přidělovány stanicím, které nejsou registrovány. Časové omezení pronájmu IP adresy dovoluje DHCP serveru již nepoužívané adresy přidělovat jiným stanicím. Registrace dříve pronajatých IP adres umožňuje DHCP serveru při příštím pronájmu přidělit stejnou IP adresu.

3.3.3 Řešení vazby soustav DHCP a DNS

Služba DHCP je přirozeným zdrojem událostí (změna konfigurace uzlu sítě, vznik nového uzlu atd.), které v konečném důsledku vedou na nutnost provedení změny v informačním obsahu soustavy DNS.

Ze snahy co nejvíce omezit celkovou náročnost správy IP sítě na jednotlivé manuální zásahy lidské obsluhy logicky vyplývá vhodnost podchycení tohoto aktualizačního zdroje specifickým automatizačním nástrojem.

3.3.4 Souvislost soustav DHCP a DNS

Soustava (služba) DNS je technickým nástrojem pro plošné poskytování aktuálních informací o reálné struktuře IP sítě. Jako taková je závislá na včasné a přesné aktualizaci obsažených údajů v závislosti na změnách reálného prostředí.

Služba DHCP naproti tomu zasahuje do stavu technické reality IP sítě přidělováním konfiguračních informací jednotlivým stanicím (uzlům) této sítě.

V důsledku této činnosti dochází k automatickému vzniku, zániku nebo přesunu jednotlivých uzlů sítě. Tyto změny musí být co nejrychleji promítnuty do obsahu soustavy DNS, aby tak došlo k potlačení vzniklé nekonzistence mezi realitou a informacemi v soustavě DNS.

Je zřejmé, že nejlepšího stavu (co nejkratší doby mezi změnou reality a úpravou obsahu soustavy DNS) lze dosáhnout jedině automatizací přenosu informací mezi soustavou DHCP a DNS.

3.4 NTP

NTP (Network Time Protocol) je protokol pro synchronizaci vnitřních hodin počítačů po paketové síti s proměnným zpožděním. Tento protokol zajišťuje, aby všechny počítače v síti měly stejný a přesný čas. Byl obzvláště navržen tak, aby odolával následku proměnlivého zpoždění v doručování paketů.

NTP klient používá Marzullův algoritmus pro stanovení času z (nepatrně) se lišících odpovědí časových serverů. Používá se čas UTC se speciálními příznaky pro přestupné sekundy. NTP obvykle dovede po internetu udržovat čas s chybou pod 10 milisekund (1/100 s), v lokální síti může při ideálních podmínkách dosáhnout přesnosti až 200 mikrosekund (1/5000 s).

Počítač, který chce synchronizovat své hodiny, pošle pár dotazů několika NTP serverům a ty mu v odpovědi pošlou svůj, přesný čas. Klient z odpovědí nejprve vyloučí servery se zřejmě nesmyslným časem (s odchylkou 1000 sekund a více). Poté ponechá skupinu serverů s největším společným průnikem.

Běžně se jím dosahuje přesnosti hodin v řádu milisekund.

4. NÁVRH ŘEŠENÍ

V návrhu řešení budu vycházet ze získaných teoretických poznatků a zjištěných výsledků analýzy. Důležitým kriteriem jsou i požadavky organizace, které budou při rozhodování zohledněny.

V návrhu se zaměřím i na kritická místa, která jsem zjistil při analýze. Zejména zajištění obnovy služeb v případě havárie serveru. Ve stávajícím prostředí tento scénář zcela chybí.

4.1 Požadavky organizace

Stávající IT infrastruktura v podobě jaké je dnes, funguje již několik roků. Sjednocením hardwarových zařízení a softwarového vybavení bylo dosaženo jednotného prostředí, které v té době přineslo také zjednodušení správy a údržby celého serverového prostředí..

Hlavním požadavkem organizace tedy je zachovat dodavatele software a hardware, pokud to bude umožňovat navrhovaný scénář.

Důvody jsou zřejmé: možnost pokračovat v zaběhnutém systému záručních oprav hardwarových zařízení a zachování uživatelského prostředí pro správu a údržbu nového systému. Přechod na zcela novou platformu, by přinesl další náklady na zaškolení a zaučení administrátorů systému.

4.2 Návrh služeb sítě

Návrh služeb sítě vychází z použití již existující domény tsit.cz a z funkční struktury AD. Oproti stávajícímu stavu budou implementovány dva nové řadiče domény v jednotlivých pobočkách a budou zapojeny do jejich lokálních sítích. Na těchto serverech dojde k implementaci popisovaných služeb. Provoz active directory umožňuje pokročilou konfiguraci a vzájemnou synchronizaci dat mezi radiči domény čehož využívají některé z popisovaných služeb.

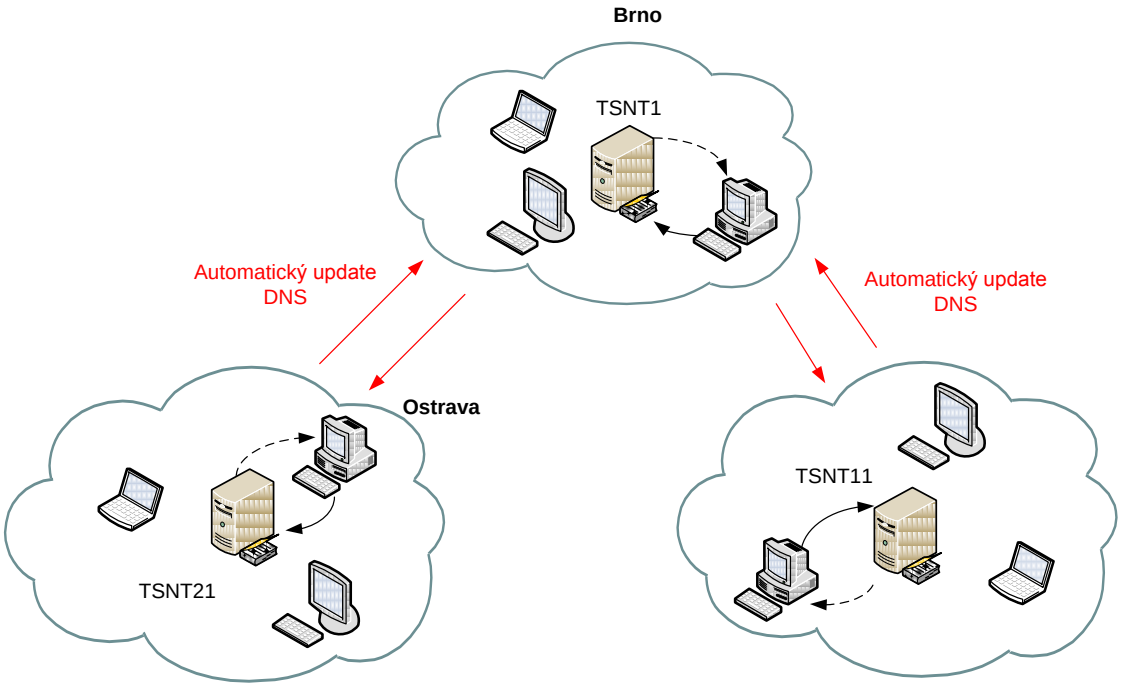
4.2.1 DNS

DNS bude provozováno na doménových řadičích, umístěných na jednotlivých lokalitách, přičemž bude nastaven režim provozu, Active Directory integrated – tedy jako multimaster replikace, kde každý server funguje jako primární a vzájemně si (v rámci replikace AD) vyměňují změny.

Fyzický model

Fyzickým modelem pro implementaci soustavy DNS rozumíme takovou volbu uspořádání serverů DNS, jejichž umístění v konkrétní topologii přenosové infrastruktury a přiřazení funkčních rolí v soustavě zabezpečí optimální chod soustavy jak z hlediska robustnosti, tak z pohledu výkonnostního.

Soustava autoritativních serverů DNS



Obrázek 3: Soustava DNS

Nově budovaná soustava DNS se opírá o existující server, tvořící její jádro. Tento server bude potřeba upravit pro provoz v integrovaných sítích Techniserv IT s.r.o. Jedná

se úpravy konfiguračního charakteru na serveru umístěném v centrále a instalaci a konfiguraci na serverů, které budou umístěny na pobočkách .

Následující tabulka shrnuje současné servery a jejich úpravy:

SERVER	UMÍSTĚNÍ	ZMĚNY
TSNT1	Techniserv IT s.r.o. Brno	Stávající DNS a Active Directory struktura firmy.
TSNT11	Techniserv IT s.r.o. Praha	Konfigurace proběhne automaticky v rámci replikace Active Directory
TSNT21	Techniserv IT s.r.o. Ostrava	Konfigurace proběhne automaticky v rámci replikace Active Directory

Tabulka 4: Úpravy stávajících serverů.

Jádro soustavy bude ještě tvořeno DC Techniserv IT s.r.o. Tato koncepce umožní zajistit:

- distribuci replik informací DNS pomocí replikace AD,
- dostupnost informací DNS i v případě výpadku komunikace v síti IS Techniserv IT s.r.o.,
- pozdější delegování pravomoci za správu soustavy DNS,
- snížení náročnosti budované soustavy DNS na množství administrativní práce a vyloučení trvalé potřeby vysoce kvalifikovaných lidských zdrojů mimo prostor centra.

Jako servery jádra soustavy DNS budou použity servery na bázi mikroprocesoru Intel s operačním systémem Microsoft Windows Server. K realizaci funkcí soustavy DNS bude využito programové vybavení, které je součástí operačního systému Microsoft Windows Server.

Kromě realizace soustavy DNS budou uvedené servery využity k zajištění infrastrukturních funkcí AD v rámci privátní IP sítě.

Funkční model soustavy

Návrhem funkčního modelu soustavy DNS rozumíme volbu mezi základními variantami vestavěných mechanizmů vyhledávání hodnot k zadaným klíčům. Stěžejními aspekty je funkční, resp. obsahová integrace se soustavou DNS sítě Internet.
Vlastní jádro soustavy je řešeno jako soustava DNS serverů provázaných službou Active directory.

Všechny servery budou provádět aktualizaci záznamů dynamicky přímou cestou, záznamy stanice bude zavádět automaticky DHCP server. V nastavení DNS budou povoleny autorizované dynamické updaty.

Počítáme s jedinou doménou Active Directory *tsit.cz* (rozšíření stávající domény o další řadiče)..

Struktura jmenného prostoru

Návrhem struktury jmenného prostoru soustavy DNS rozumíme konkrétní volbu hierarchického uspořádání jmen primární struktury klíčů pro přímé vyhledávání, resp. primární struktury klíčů pro zpětné vyhledávání a potenciálních struktur pomocných soustav klíčů přímého vyhledávání.

Primární struktura klíčů pro přímé vyhledávání

Základními hledisky zvolenými pro konstrukci klíčů primární struktury přímého vyhledávání privátní autonomní DNS soustavy IS Techniserv IT s.r.o. jsou:

- promítnutí hierarchické organizační struktury Techniserv IT s.r.o.,
- umožnění aplikace automatické vazby na soustavu DHCP.

Konvence tvorby jmen aktivních prvků IP sítě

Při začleňování informací o aktivních prvcích privátní IP sítě Techniserv IT s.r.o. do datového obsahu soustavy.

DNS bude pro tvorbu jmen prvků (částí bez plné kvalifikace domény) užívána následující systematická konvence:

<DNS_jméno> :- <poř_číslo>
<první písmeno> :- <router_ch> | <switch_ch> | <hub_ch> | <ups_ch>
<router_ch> :- "r"
<switch_ch> :- "s"
<hub_ch> :- "h"
<ups_ch> :- "u"

Zde dále platí:

<poř_číslo> udává číslo instance daného typu aktivního prvku v příslušné lokalitě; je vyjádřeno jako přirozené číslo z intervalu hodnot *<1, nekonečno>*.

Administrativní model

Administrativním modelem rozumíme využití technických možností soustavy DNS pro delegaci pravomocí pro správu jednotlivých částí jejího jmenného prostoru.

Rozdělení pravomocí pro správu soustavy DNS můžeme sledovat ve dvou rovinách:

- organizační, tj. jakou měrou dochází k rozdělení jednotlivých správních úkonů na jednotlivé pracovníky organizace spravující vlastní soustavu DNS,

- technologické, jež je dána využitím vlastních technických prostředků soustavy DNS, které podporují reálnou dělbu práce při její správě.

Rozdělení pravomocí pro správu DNS

Ačkoliv za optimální stav považujeme předání pravomoci a zodpovědnosti za určitý subsystém na ten správní subjekt, z jehož iniciativy vzniká potřeba provádění příslušných změn, lze pravomoci delegovat jen pro rutinní provoz soustavy DNS.

Rozdělení pravomocí nelze aplikovat v rané fázi jejího budování. Proto doporučujeme ponechat minimálně v počátečních etapách výstavby správu striktně centrální. Tím bude zajištěna dostatečná operativnost potřebná k udržení vysokého tempa implementace.

Teprve po přechodu na stabilní provoz bude žádoucí přezkoumat vhodnost případné delegace pravomocí ke správě jednotlivých částí soustavy DNS/DHCP.

Jako vhodný model lze zvolit centrální správu, kdy všechny delegované zóny budou spravovány na hlavním primárním serveru.

Taková soustava je funkčně plně připravena i na pozdější předání části administrativních kompetencí mimo centrum, avšak až po adekvátním doškolení odpovědných pracovníků.

Primární data všech zón pro vnitřní soustavu DNS Techniserv IT s.r.o. budou umístěna na DNS serverech sítě IS Techniserv IT s.r.o.. V rámci sítě Techniserv IT s.r.o. budou DNS informace mezi jednotlivými servery distribuovány pomocí Active Directory. Do sítě Techniserv IT s.r.o. z něj budou přebírány všemi servery na úrovni centra a poboček (z důvodu automatického updatu z DHCP).

Konfigurace klientů služby DNS

Důležitou součástí celého systému DNS jsou také klienti. Správná konfigurace klientů má stejně významný vliv na funkčnost celé soustavy jako konfigurace serverů.

Správa soustavy DNS

Veškeré změny v datovém obsahu soustavy DNS budou prováděny na primárním DNS serveru Techniserv IT s.r.o.. Manuální aktualizace obsahu soustavy DNS v ostatních zónách by se měla týkat jen minimálního množství vkládaných informací - aplikačních serverů, prvků tvořících infrastrukturu sítě IS Techniserv IT s.r.o. (směrovače apod.), nebo specifických záznamů DNS (CNAME, MX apod.).

Vzhledem ke snaze co nejvíce omezit rozsah nutné rutinní údržby soustavy DNS (doplňování a aktualizace jejích obsahových dat), bude hlavním kanálem vzniku nových informací pro soustavu DNS soustava DHCP.

4.2.2 DHCP

Řešení soustavy DHCP

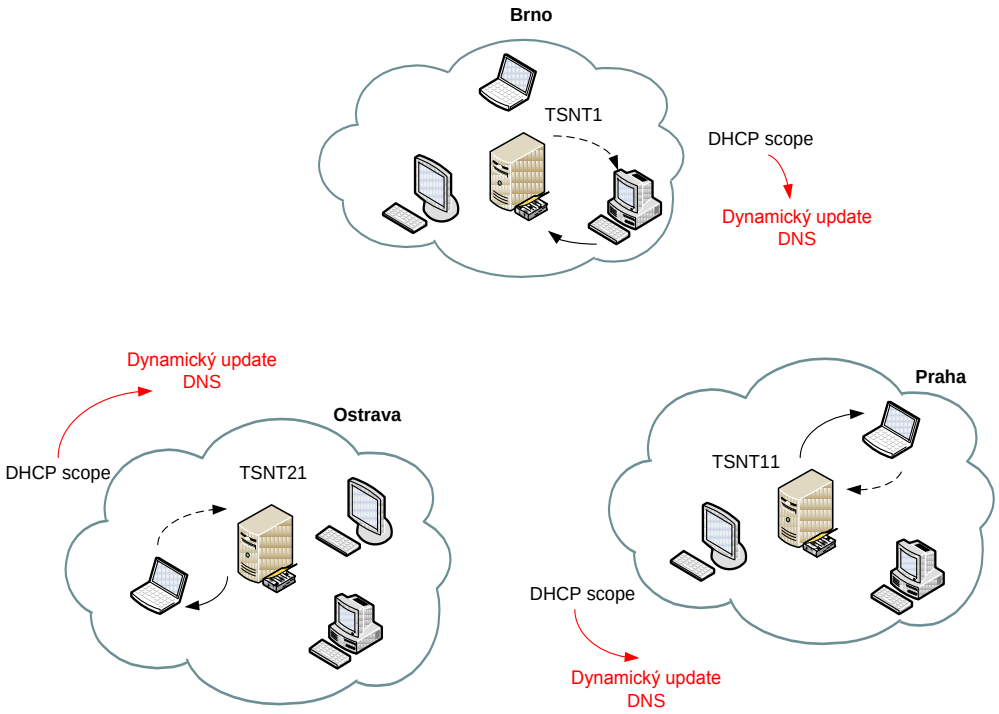
Následující odstavce popisují zásadní technologická východiska, která byla zvolena pro implementaci služby DHCP v privátní IP síti IS Techniserv IT s.r.o.

Soustava serverů DHCP

Pro implementaci služby DHCP v rámci IP sítě IS Techniserv IT s.r.o. je zvolena varianta, spočívající v použití služby DHCP na stávajících a nových serverech Techniserv IT s.r.o. s působností pro určenou pod část topologie sítě.

Jako hranice působnosti jednotlivých serverů DHCP jsou zvoleny jednotlivé pobočky. Soustava poskytující služby DHCP v privátní síti IS Techniserv IT s.r.o. v rámci projektu tedy bude tvořena serverem, umístěným v dané pobočce .

Jako servery soustavy DHCP budou použity stávající servery Techniserv IT s.r.o. na bázi mikroprocesoru Intel s operačním systémem Microsoft Windows Server. K poskytování služby DHCP bude využita služba dhcp, která je součástí instalace Windows serveru, která představuje implementaci serveru DHCP umožňující dynamické doplňování DNS.



Obrázek 4: Soustava DHCP

Podkladem pro počáteční konfiguraci jednotlivých serverů, poskytujících službu DHCP je seznam jednotlivých lokalit IP sítě Techniserv IT s.r.o., které budou službu využívat.

Správa soustavy DHCP

Veškeré změny v datovém obsahu adres soustavy DHCP budou prováděny na jednotlivých pobočkách Techniserv IT s.r.o. Aktualizace obsahu DHCP bude tedy plně ve správě místního informatika, který bude zodpovědný za všechny změny .

Konfigurace klientů služby DHCP

Konfigurace klientů služby DHCP se provede samočinně následkem nasazení nových serverů .

Následující tabulka ukazuje, kteří klienti používají DHCP:

Klient	Rezervace DHCP / Pevná adresa
Stanice	Dynamické DHCP (obvyklé) Statické DHCP (výjimka v případě potřeby)
Servery	Pevná IP adresa
Tiskárny	Pevná IP adresa
Aktivní prvky sítě	Pevná IP adresa

Tabulka 5: Klienti DHCP / Statické IP adresy

Parametry nastavené pomocí DHCP budou:

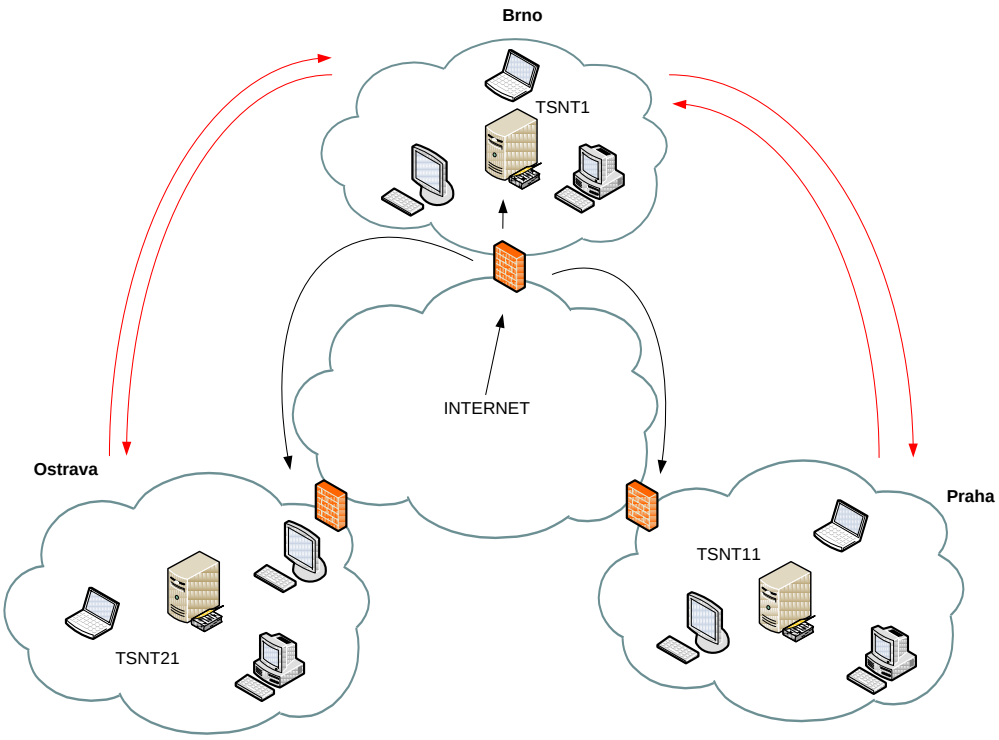
- IP adresa
- maska sítě
- brána (default gateway)
- DNS servery

4.2.3 NTP

Referenční časový zdroj lokání soustavy NTP bude realizován spuštěním služby NTP, na stávajícím firewallu organizace, umístěném v centrále firmy Techniserv IT s.r.o.

Tento zdroj bude synchronizován oproti skupině veřejných NTP serverů, dostupných prostřednictvím sítě internetu. Současně bude poskytovatelem informace o přesného času v rámci interní struktury organizace.

Klíčovým důvodem pro implementaci služby NTP je zajištění časové synchronizace všech prvků sítě od serverů, síťových prvků až po klientské stanice. Sjednocení časů na všech komponentách, je nutnou podmínkou pro efektivní sběr informací určených pro monitorování a detekci možných hrozeb, průniků či ladění systémů.



Obrázek 5: Soustava NTP

Nasazení služby

Distribuce času na jednotlivé systémy, které jsou začleněné v doméně je realizována automaticky, pomocí synchronizačních funkcí Active Directory.

Server TSNT1 s rolí PDC emulátor bude přebírat čas pomocí protokolu NTP z interního NTP zdroje na firewallu. Další synchronizace proběhne automaticky v rámci domény.

Taktéž aktivní prvky sítě, včetně firewallů na obou pobočkách, budou nakonfigurovány tak, aby pomocí NTP protokolu, byly schopny převzít informaci o přesném čase z centrálního firewallu.

Správa soustavy NTP

Funkce soustavy synchronizace času na bázi protokolu NTP je zcela automatizovaná.

Stávající konfigurace celé soustavy vytváří dostatečnou nezávislost konfigurace klientů na případných změnách vnějších podmínek.

4.3 Návrh hardwaru a softwaru

Na základě dřívějších dobrých zkušeností a takřka bezproblémového provozu stávajících serverů od firmy Hewlett Packard, rozhodl jsem se navrhnout hardware od stejného výrobce.

- 2 x server HP ProLiant DL320 G6, 4GB RAM, Xeon L5520, 4GB DDR3, SATA 500GB 7.2k, RAID 0, 1, DVD, 500W.

Porovnání cenové hladiny jiných výrobců mě v tomto rozhodnutí ujistilo, neboť rozdíly jsou vzhledem k výši investice minimální.

V softwarové časti jsem se rozhodl navrhnout použití operačního systému Microsoft Windows Server 2008, který obsahuje v základní ceně produktu všechny popisované služby.

4.4 Ekonomické zhodnocení

V případě, že společnost zrealizuje navržené změny, budou nutné vstupní resp. počáteční náklady za nákup nového hardware,operačního systému a implementaci řešení.

Na implementaci řešení se budou podílet 2 zaměstnanci, předpokládaná doba trvání je dva pracovní dny, takže celková časová dotace činí 4 člověk/den.

Ks	Název	Popis	Cena
2	**SERVER**	HP ProLiant DL320G6 rack 1U	43 007 Kč
2	**OS**	Microsoft Windows 2008 Server Standard OEM CZ 5 klientů CAL	17 339 Kč

Tabulka 6: Soupis HW a SW

Výsledná cena je odhadována na **120 692 Kč.**

V každém případě je možné říct, že se celkové náklady sestávají z nákladů na implementaci a nákladů na další úpravy, údržbu a správu. Náklady spadající do druhé skupiny lze výrazně snížit o důkladnou definicí požadavků před implementací (omezí se náklady na úpravy) a vhodně nastavenými pravidly používání (omezí se náklady na správu).

Ve firmě Techniserv IT s.r.o. pracují z větší části počítačově velmi gramotní IT specialisté. Instalace, implementace a úpravy budou proto řešeny vlastními silami, stejně jako administrace. To samozřejmě ve srovnání s externím řešením značně sníží náklady na správu a vedení infrastruktury. Z uvedeného důvodu je popsaný návrh řešení akceptovatelný.

5. ZHODNOCENÍ A ZÁVĚR

V mé bakalářské práci jsem vypracoval návrh služeb sítě pro firmu Techniserv IT s.r.o..

Navržené řešení poskytuje z hlediska služby DNS redundanci. Za pomocí služby DHCP na každé lokalitě bude přidělována klientským stanicím konfigurace DNS tvořena 3 servery, kdy jako primární bude zvolen lokální DNS server v rámci sítě dané pobočky. V případě výpadku primárního DNS serveru budou dotazy vyřizovány v dalšími servery v pořadí. Popisované řešení služby DHCP zajistí funkčnost nastavení protokolu TCP/IP na klientských stanicích na jednotlivých lokalitách i v případě výpadku spojení interních sítí firmy provázaných pomocí vpn prvků. Služba NTP umožní díky distribuci přesného času na všechny prvky firemní sítě, efektivní sběr informací určených pro monitorování a detekci možných hrozeb, průniků.

Navržené řešení je dále kompatibilní nejen se systémy typu Windows, ale také se všemi verzemi systému typu Unix či Linux, a to jak na straně klientských počítačů, tak na straně serverů. To samozřejmě značně zvyšuje možnost dalšího rozšiřování infrastruktury podle měnících se požadavků společnosti.

V návrhu jsem zahrnul požadavky na popisované služby jak ze strany vedení firmy, tak i s přihlédnutím ke stávajícím trendům a předpokládanému vývoji v oblasti IT. Jednotlivé služby jsou dimenzovány tak, aby pokryly současnou potřebu ale i neustále rostoucí nároky na složitost struktury počítačových sítí.

Během tvorby jsem jednotlivé části návrhu konzultoval s vedením firmy. Navržené změny by proto měly plně vyhovovat všem požadavkům ze strany vedení firmy.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

AD Active Directory

CAL Client Access License

DC Doménový řadič

DHCP Dynamic Host Control Protocol

DNS Domain Name (Server, System, Service)

FSMO Flexible single master operation

HP Hewlett-Packard

HW Hardware

IANA Internet Assigned Numbers Authority

IP Internet Protocol

IS Informační systém

IT Informační technologie

MAC Media Access Control

MS Microsoft

NTP Network time protokol

OEM Original Equipment Manufacturer

OS Operační systém

PDC Primary Domain Controller

RFC Request for Comments

SW Software

TCP Transmission Control Protocol

UDP User Datagram Protocol

VPN Virtual Private Network

WINS Windows Internet Name Service

SEZNAM POUŽITÉ LITERATURY

(1) BIGELOW, S. J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. 1.vydání. Computer Press. 2004. 990 s. ISBN 80-251-0178-9.

(2) MICROSOFT. *Setting Up the Microsoft DNS Server*. [online]. Dostupné z: http://technet.microsoft.com/en-us/library/cc723556.aspx

(3) MICROSOFT. *Windows Time Service Tools and Settings*. [online]. Dostupné z: http://technet.microsoft.com/en-us/library/cc773263(WS.10).aspx

(4) MICROSOFT. *Základní informace o službě DHCP*. [online]. Dostupné z: http://support.microsoft.com/kb/169289

(5) ODOM, W. *Počítačové sítě.* 1.vydání. Computer press. 2005. 384 s. ISBN 80-251-0538-5.

(6) SATRAPA, P. RANDUS, J. *Linux – Internet server*. 1.vydaní. Neokortex. 1996. 413 s. ISBN 80-902230-0-1.

(7) SAVILL, J. *The Complete Guide to Windows Server 2008*. 1.vydání. Addison-Wesley. 2008. 1752 s. ISBN: 0-321-50272-8.

(8) STANEK, W. R. *Active Directory: Kapesní rádce administrátora.* 1.vydání. Computer Press. 2009. 352 s. ISBN: 978-80-251-2555-7.

(9) STANEK, W. R. Microsoft *Windows Server 2008: Kapesní rádce administrátora.* 1.vydání. Computer Press. 2008. 704 s. ISBN: 978-80-251-1936-5.

(10) ŠETKA, P. *Mistrovství v Microsoft Windows Server 2003.* 1.vydání. Computer Press, 2008. 704 s. ISBN 978-80-251-1871-9.