UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

BAKALÁŘSKÁ PRÁCE

2017 Petr Čálek

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Nasazení a využití služby Active Directory na Windows Serveru 2016

Petr Čálek

Bakalářská práce

2017

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Petr Čálek**
Osobní číslo:	**I13104**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Nasazení a využití služby Active Directory na Windows Serveru 2016**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je podrobně představit službu DNS, DHCP a Active Directory pro nasazení v prostřední firmy střední velikosti. Autor práce podrobně představí služby DNS a DHCP, objasní pravidla navrhování a strukturování domén. V další části autor představí principy nasazení a využívání Active Directory. V praktické části autor zpracuje sadu úloh zaměřenou na konfiguraci DNS, DHCP a AD, jejichž řešení bude zpracováno ve formě videovýstupu.

Rozsah grafických prací:

Rozsah pracovní zprávy: **35**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

R. STANEK, William. Windows server 2016. 1. Seatle: Stanek&Associates, 2016. ISBN 9781535074094.

KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.

Vedoucí bakalářské práce: **Ing. Soňa Neradová, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2016**

Termín odevzdání bakalářské práce: **12. května 2017**

Univerzita Pardubice Česká republika

L.S.

Ing. Zdeněk Němec, Ph.D.
děkan

Mgr. Josef Horálek, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2017

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne

PODĚKOVÁNÍ

Chtěl bych poděkovat paní doktorce Soně Neradové za cenné rady nejen při tvorbě bakalářské práce, ale i po celou dobu studia. Dále bych chtěl poděkovat všem svým přátelům a rodině za podporu v průběhu studia.

ANOTACE

Cílem této bakalářské práce je návrh nasazení a využití služby Active Directory na Windows Serveru 2016 pro firmu střední velikosti.

V teoretické části budou vysvětleny základní služby, které WS poskytuje, jako jsou DNS, DHCP a AD. V této části bude také vysvětleno, jaké jsou pravidla pro návrh a strukturování domén a také principy nasazení a využití Active Directory.

Praktická část představuje ukázku konfigurace služeb, které budou představeny v teoretické části, a to formou několika videí.

KLÍČOVÁ SLOVA

DNS, DHCP, Active Directory, Windows Server 2016

TITLE

Deploy and use Active Directory on Windows Server 2016

ANNOTATION

The aim of this bachelor thesis is to deploy and use Active Directory on Windows Server 2016 for a medium-sized business.

In the theoretical part, the basic services provided by WS, such as DNS, DHCP, and AD, will be explained. This section also explains the rules for designing and structuring domains as well as the principles of deploying and using Active Directory.

The practical part presents a demonstration of the configuration of services that will be presented in the theoretical part, in the form of several videos.

KEYWORDS

DNS, DHCP, Active Directory, Windows Server 2016

OBSAH

Úvod....13
1. Windows server 2016....14
1.1 Změny oproti WS 2012....14
1.2 Jednotlivé edice Windows Server 2016....14
1.3 Systémové požadavky....15
1.3.1 Procesor....15
1.3.2 Paměť RAM....15
1.3.3 Místo na disku....15
1.3.4 Síťový adaptér....16
1.3.5 Ostatní požadavky....16
2. DHCP....17
2.1 Historie....17
2.2 Princip činnosti....17
2.3 DHCP zprávy....18
2.4 Parametry DHCP....19
2.5 Způsob přiřazování adres....20
2.6 Zabezpečení....20
2.6.1 DHCP snooping....20
2.7 Nastavení služby ve firmě....21
2.8 NAT....21
3. DNS....23
3.1 Princip činnosti....23
3.2 Zprávy a operace v DNS....23
3.3 Kořenové servery....24
3.4 DNS servery....25
3.5 Druhy mapování....25

3.6 Hierarchie domén 26
3.7 Parametry DNS serverů 26
3.8 Bezpečnost 27
3.9 DNSSEC 28
3.9.1 Fungování DNSSEC 28
3.10 Nastavení služby ve firmě 29
4. Active Directory 30
4.1 Struktura AD 30
4.2 Řadič domény 31
4.2.1 Řadič domény jen pro čtení 32
4.3 Globální katalog 32
4.4 Zásady skupiny 32
4.4.1 Dědění zásad 33
4.4.2 Nastavení zásad skupin 33
5. Praktická Část 35
5.1 Tvorba virtuálního stroje 35
5.1.1 Postup 35
5.2 Výukové video – Instalace OS WS 39
5.3 Výukové video – DNS a DNSSEC 39
5.4 Výukové video – DHCP 39
5.5 Výukové video – NAT 40
5.6 Výukové video – Group policy 40
6. ZÁVĚR 41
7. Použitá literatura 42
8. Přílohy 44

SEZNAM ILUSTRACÍ A TABULEK

Obrázek 1 - Komunikace DHCP serveru s klientem 18
Obrázek 2 - Tvorba virtuálního stroje - krok 1 35
Obrázek 3 - Tvorba virtuálního stroje - krok 2 36
Obrázek 4 - Tvorba virtuálního stroje - krok 3 36
Obrázek 5 - Tvorba virtuálního stroje - krok 4 37
Obrázek 6 - Tvorba virtuálního stroje - krok 5 37
Obrázek 7 - Tvorba virtuálního stroje - krok 6 38
Obrázek 8 - Tvorba virtuálního stroje – krok 7 38
Obrázek 9 - Tvorba virtuálního stroje – krok 8 38
Obrázek 10 - Tvorba virtuálního stroje – výsledek 39

Tabulka 1 Jednotlivé jmenné kořenové servery 24

SEZNAM ZKRATEK A ZNAČEK

ACL	Access Control List
AD SD	Active Directory Domain Services
AD	Active Directory
ATA	Advanced Technology Attachment
BIND	Berkeley Internet Name Domain
BOOTP	Boottrap Protocol
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
ECC	Error Checking and Correcting
EIDE	Extended Integrated Drive Electronics
EPT	Extended Page Table
ICANN	Internet Corporation for Assigned Names and Numbers
IDE	Integrated Drive Electronics
IP	Internet Protocol
ISO/OSI	International Organization for Standardization / Open Systems Interconnection
LAHF	Load Flags into AH Register
MAC	Media Access Control
NAP	Network Access Protection
NAT	Network Address Traslation
NPT	Nested Page Tables
PATA	Parallel Advanced Technology Attachment
PCI Express	Peripheral Component Interconnect Express

PXE	Preboot execution environment
SAHF	Store AH into Flags
TCP	Transmission Control Protocol
TLD	Top Level Domain
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WS	Windows server

ÚVOD

Žijeme v době, ve které se s počítačem setkáváme neustále. V osobním životě jsou to osobní počítače či notebooky, které využíváme pro své potřeby. Tyto počítače, v případě že jsou připojené k internetu, zpravidla vystupují jako jedna síťová IP adresa ve veřejné síti. V domácí síti však každé zařízení vlastní jedinečnou adresu, o rozdělení těchto adres v síti se stará služba DHCP Server. Tato služba včetně podrobností bude vysvětlena v průběhu práce.

V pracovním životě jsou to nejčastěji počítače, které jsou připojeny na firemní síť. Pro usnadnění správy se tyto počítače připojují k serveru. V této práci bude popsán Windows Server a konkrétně verze 2016.

Motivací a cílem této bakalářské práce je nastínit, získat a předat nabyté vědomosti. Pomocí práce bude nastíněno čtenáři využití jednoho z nejvíce využívaných síťových operačních systémů, tedy Windows Server.

Teoretická část seznámí čtenáře se základní charakteristikou systému Windows Server. Poté následuje rozsáhlá kapitola o službě DHCP, zde bude vysvětleno, jak probíhá získávání síťových parametrů, které dovolují vystupovat počítači na Internetu, ale i v samotné síti. Další kapitolou je popis služby DNS. Tato část vysvětlí, co se děje na pozadí, když uživatel zadá do adresního řádku webového prohlížeče adresu stránky (serveru) a očekává zobrazení. Poslední kapitolou teoretické části práce je seznámení čtenáře s Active Directory a nástin nastavení zásad skupin.

Praktická část je zpracována pomocí několika videí. V prvním bude popsáno, jak probíhá samotná instalace služby Windows Server včetně základních nastavení. Následovat bude konfigurace služeb DNS a DHCP pro potřeby imaginární firmy. Poslední částí bude obsahovat konfigurace uživatelů, skupin a ostatních objektů pomocí Active Directory.

1. WINDOWS SERVER 2016

Windows Server 2016 je síťový operační systém vyvinutý firmou Microsoft. Stejně jako předešlé verze WS patří do skupiny Windows NT operačních systémů. Svým uživatelským rozhraním se vizuálně velmi podobá Windows 10, dosud nejnovějšímu operačnímu systému pro osobní počítače. Tento operační systém je nástupcem síťového operačního systému Windows Server 2012, oproti předchůdci má však několik změn, které budou představeny v následující podkapitole. První vydání tohoto systému se datuje na 1. 10. 2014, ačkoliv to byla pouze ukázková verze. Plnohodnotná verze byla vydána 26. 9. 2016 a veřejnosti dostupná 12. 10. 2016. (DigdarshanKavia@TWC, 2016)

1.1 Změny oproti WS 2012

Windows Server 2016 poskytuje mnoho vylepšení či novinek. Mezi vylepšení se může zařadit poskytnutí vyšší fyzické i virtuální paměti, zvýšení bezpečnosti a plná podpora výměny disků a pamětí serverů za běhu. Jako novinku lze považovat ukončení podpory zastaralé služby NAP. (Microsoft, 2017)

1.2 Jednotlivé edice Windows Server 2016

Další z rozdílů, ve srovnání s předchozími verzemi, je i v množství možných edicí. Systém WS 2016 má na výběr ze 3 edicí:

- Edice Windows Server Essentials je určena pro účely menších společností. Umožňuje pouze 25 uživatelů s 50 zařízeními a má pouze omezené možnosti. Další vhodné užití je použití jako primární server ve více serverové malé firmě. (Microsoft, 2016)
- Edice Windows Server Datacenter Edition zahrnuje pokročilé schopnosti softwarově definovaného datacentra, které bylo vytvořeno pro vysoce virtualizovaná privátní a hybridní cloudová prostředí.
- Edice Windows Server Standard Edition je určena pro malé a střední podniky, které však potřebují pokročilé funkce. Tato edice je omezena limitem v podobě oprávnění k virtualizaci, povolené jsou maximálně 2 virtuální prostředí.

Při instalaci každé z těchto edicí je možnost instalace s grafickým prostředím (Full-server Installation) i instalace bez grafického prostředí (Server-core Instalation). (DigdarshanKavia@TWC, 2016)

1.3 Systémové požadavky

Následující požadavky jsou uváděny jako minimální systémové požadavky. V praxi to tedy znamená, že pokud počítač neobsahuje alespoň tyto parametry, může to zapříčinit nesprávné fungování, či dokonce úplnou nefunkčnost.

1.3.1 Procesor

U procesoru nezáleží pouze na jeho frekvenci, ale také na počtu jader procesoru a velikosti vyrovnávací paměti cash. Následující parametry jsou minimální požadované:

- alespoň 1.4 GHz 64bitový jedno jádrový procesor / 1,3 GHz 64bitový více jádrový procesor;
- kompatibilita s x64 instrukční sadou;
- podpora technologií NX a DEP[1];
- podpora technologií CMPXCHG16b, LAHF/SAHF a PrefetchW[2];
- podpora překladu adres druhého řádu (EPT[3] nebo NPT[4]).

1.3.2 Paměť RAM

U požadavků na velikost paměti RAM záleží na volbě instalace. Následující parametry jsou minimální požadované:

- alespoň 512 MB pro Server-Core Installation / 2 GB pro Full-Server Installation;
- podpora ECC či podobné technologie.

1.3.3 Místo na disku

Počítače, na kterých má běžet Windows Server 2016, musí obsahovat paměťový adaptér, který je kompatibilní s architekturou PCI Express. Windows Server 2016 nepovoluje architektury ATA/PATA/IDE/EIDE pro zavádění systému. Minimální požadovaný parametr je alespoň 32 GB místa pro systémový oddíl.

V případě instalace systému přes síť, bude potřeba vyšší velikost oddílu. U počítačů, které obsahují více než 16 GB paměti RAM, je také třeba zvýšit velikost systémového oddílu, protože tyto počítače potřebují více místa pro stránkování, hibernaci a dočasné soubory.

[1] Jsou to technologie pro CPU sloužící k oddělení paměti pro instrukce procesoru a pamětí pro data.
[2] Jsou to služby zrychlující provedení a zvyšující bezpečnost Windows a 64bitových aplikací.
[3] EPT je druhá generace x86 virtualizační technologie od firmy Intel, sloužící pro jednotku správy paměti.
[4] NPT je druhá generace virtualizační technologie vázané na hardware od firmy AMD, sloužící pro jednotku správy paměti.

1.3.4 Síťový adaptér

Síťový adaptér používaný u serverového počítače by měl mít tyto minimální parametry:

- ethernetový adaptér schopný alespoň gigabitové propustnosti,
- kompatibilitu s architekturou PCI Express,
- podporu služby PXE (Pre-boot Execution Enviroment).

1.3.5 Ostatní požadavky

V případě, že se provádí instalace z optického disku, je nutné, aby serverový počítač obsahoval optickou mechaniku. Pokud se instaluje ze sítě, je nutné zajistit internetové připojení. Dále pro obsluhu serveru je potřebné mít monitor schopný rozlišení minimálně 1024x768. Další z vhodných periferií je klávesnice a v případě grafické instalace i myš. (ONDRUSEK, 2016)

2. DHCP

Dynamic Host Configuration Protocol, zkráceně DHCP, je standardizovaný síťový protokol pracující na principu klient/server. Tento protokol rozšířil služby, které poskytoval protokol BOOTP. Jeho hlavní využití je na IP sítích v podobě DHCP serveru, který klientům v síti dynamicky poskytuje potřebné parametry. Jedná se o IP adresu, masku podsítě, adresy DNS serverů a adresu výchozí brány. (PRESS, 1999) a (DROMS, 1997)

DHCP server je služba, která využívá protokol DHCP. Pokud je v síti povolen a nakonfigurován, poskytuje server klientům síťové parametry.

DHCP klient je služba běžící na klientském počítači, která slouží k získání síťových parametrů např. síťové adresy.

2.1 Historie

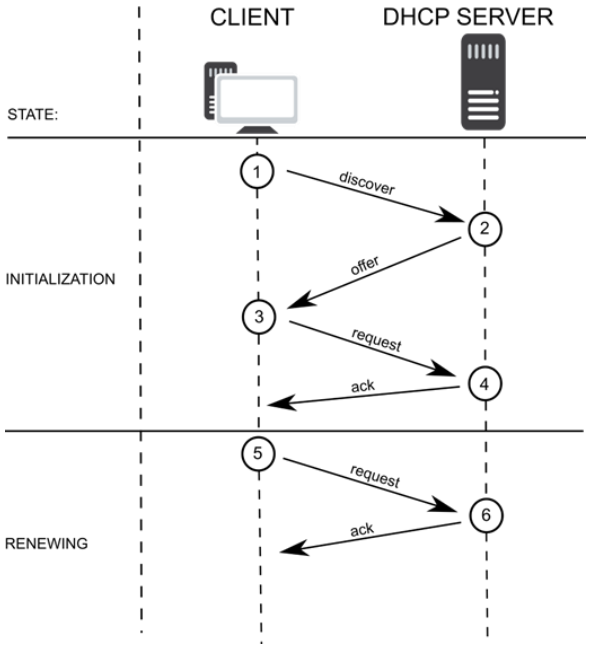
Standard DHCP vznikl v roce 1993. V této době vystupovalo na Internetu malé množství společností, proto nebyl kladen takový důraz na bezpečnost. Jde o rozšíření a vylepšení protokolu BOOTP. Hlavní rozdíl je v tom, že BOOTP nastavoval síťové parametry ručně, což vedlo k častým chybám v komunikaci na síti. Oproti tomu DHCP přiděluje adresy dynamicky, čímž se docílilo jedinečnosti adres v síti. (PUŽMANOVÁ, 2009)

2.2 Princip činnosti

Služba DHCP pracuje na principu výměny zpráv. Klient nejdříve osloví DHCP servery pomocí zprávy DHCPDISCOVER, která obsahuje klientovu MAC adresu a je odeslána na všeobecnou adresu a UDP port 67. Servery mu zpětně nabídnou IP adresu, masku podsítě, adresu serveru (výchozí brány) a také dobu zapůjčení. Tyto informace obsahuje zpráva DHCPOFFER, která je už odesílána na konkrétní klientovu adresu a UDP port 68.

Následně si klient vybere DHCP server a tím i IP adresu, kterou mu server nabízel a odpoví zprávou DHCPREQUEST, kterou odešle na všeobecnou adresu, tak aby ostatní DHCP servery věděly, že nejsou vybrány. Poté vybraný server odešle na konkrétní klientskou adresu zprávu DHCPACK a tím se celá transakce uzavírá. Klient má platné údaje pouze na časový úsek, který se nazývá **doba zapůjčení**. Po tuto dobu může používat pronajatou IP adresu, než bude dostupná pro jiné klienty. Pokud si klient nezažádá do 7/8 této doby o prodloužení, ztrácí IP adresu a musí žádat o novou.

V případě, že klientovi vypršela dobu zapůjčení a žádá o její prodloužení, využívají se místo všech 4 zpráv pouze 2 a to DHCPREQUEST a DHCPACK. (PUŽMANOVÁ, 2009, s. 428–429)



Obrázek 1 - Komunikace DHCP serveru s klientem

Zdroj: (SKODA, 2016)

2.3 DHCP zprávy

Při komunikaci mezi nově připojeným klientem, či klientem s vypršenou platností výpůjčky a DHCP serverem se využívá několik různých zpráv, které jsou rozdílné obsahem a tím co představují. Protokol DHCP využívá zprávy protokolu BOOTP, to značí vzájemnou provázanost těchto dvou protokolů. BOOTP klient tedy může používat DHCP server a DHCP klient může využít BOOTP server. Zprávy jsou velmi malé, mají pouze kolem 400 B, proto je režie v síti malá. (PUŽMANOVÁ, 2009, s. 429)

- **DHCPDISCOVER** – zpráva, kterou zasílá DHCP klient na všeobecnou adresu do sítě, účelem je nalezení DHCP serverů v síti;
- **DHCPOFFER –** zpráva od DHCP serveru DHCP klientovi, který vysílal DHCPDISCOVER zprávu, pomocí této zprávy DHCP server nabízí klientovi parametry;
- **DHCPREQUEST** – klient přijme první nabídku, kterou obdržel, tato zpráva slouží k informování v síti o tomto rozhodnutí a zároveň jako žádost na vybraný DHCP server o poskytnutí parametrů;

- **DHCPACK** – tuto zprávu odesílá DHCP server jako potvrzení žádosti klienta.

Mimo výše zmíněné zprávy, které jsou součástí každé transakce mezi novým klientem a DHCP serverem, DHCP využívá i jiné zprávy, sloužící převážně k informování serveru, či naopak klienta.

- **DHCPNAK** – zpráva odesílaná DHCP serverem v případě, že IP adresa, o kterou klient žádal, je obsazená; po této zprávě musí klient znovu zahájit proces žádání o pronájem parametrů;
- **DHCPDECLINE** – zpráva, kterou odesílá DHCP klient, pokud zjistí, že nabídnuté parametry nejsou správné; poté musí následovat znovuzahájení procesu žádání o pronájem parametrů;
- **DHCPRELEASE** – zpráva odesílaná DHCP klientem na DHCP server; slouží jako oznámení serveru, aby uvolnil IP adresu, kterou měl klient zapůjčenou a zrušil zbylou dobu zapůjčení;
- **DHCPINFORM** – tuto zprávu využívá DHCP klient k získání informací o možnostech DHCP. (THOMAS, c2008-2017)

2.4 Parametry DHCP

DHCP server poskytuje nastavení síťových parametrů klienta. Nyní budou postupně vysvětleny jednotlivé síťové parametry.

IP adresa – 32bitová adresa, která je v dané síti unikátní. Tato adresa využívá IP protokol, v současné době je stále nejpoužívanější IPv4. Snaha o modernizaci a automatizaci zapříčiňuje neustálé navyšování počtu počítačů, a tím se i zvyšuje potřebné množství adres. DHCP server přiděluje klientovi adresu z určitého rozmezí adres, které má DHCP charakterizován. V případě, že DHCP vyčerpá adresy, které může přiřadit, klient se nepřipojí. Velikost rozmezí adres určuje maska podsítě. Každá adresa se skládá z klientské části a síťové části. Síťová část zůstává vždy v rámci jedné sítě stejná a klientská se mění podle daného počtu adres v rozmezí.

Maska podsítě – Má stejnou délku i formát zápisu jako IP adresa. Podle potřeby a druhu sítě se určuje potřebná velikost masky. V případě binárního zápisu jedničky představují síťovou část adresy, tedy neměnnou část IP adresy, a nuly značí klientskou část adresy, tedy část, která určuje jednotlivé klienty v síti. Například je dána IP adresa 192.168.12.0 s maskou 255.255.255.0. Maska ukazuje, že první 3 oktety, tedy 192.168.12, představují adresu sítě a poslední oktet bude nabývat hodnot 1-254 pro klienty.

Adresy DNS serverů - Jedná se o jednu, nebo dvě IP adresy serverů DNS, které poskytují překlad doménových jmen na IP adresy.

Adresa výchozí brány – Jedná se o IP adresu specifického směrovače, který je prostředníkem pro komunikaci s jinými sítěmi.

2.5 Způsob přiřazování adres

Nově připojená stanice se DHCP serveru dotáže na IP adresu, a ten následně využije jednu ze tří možností přidělení adresy:

- **manuální (statické) přidělení** – správce sítě přiděluje staticky adresu, protokol DHCP je využit pouze pro přenos síťových informací ke klientovi, v praxi pouze ojedinělé využití (např. firemní tiskárny);
- **automatické přidělení** – IP adresa je přidělena koncové stanici nastálo;
- **dynamické přidělení** – poskytnutí IP adresy klientovi na určitou dobu, adresa se vybírá z předem nastaveného rozmezí IP adres. Klienti, kteří se nepřesouvají, dostávají stále stejné adresy. (PUŽMANOVÁ, 2009, s. 428)

2.6 Zabezpečení

DHCP je protokol, který nevyžaduje ověřování, což znamená, že když se uživatelé připojují k síti, nemusí se identifikovat, aby získali zapůjčení parametrů. Tito neověření uživatelé tak mají možnost získat IP adresu, adresu DNS serveru apod.

Pro zvýšení bezpečnosti DHCP lze využít autentizace klienta i serveru. Toto rozšíření bylo publikováno v roce 2001, což bylo dlouho po vydání samotného protokolu, proto bylo mnoho DHCP klientů a serverů nepodporujících tento standard. Principem je zamezit nepovolenému klientovi získat pravé informace a nepovolenému DHCP serveru vstoupit do transakce a šířit nepravé informace. Vzhledem k tomu, že služba DHCP běží přes protokol UDP a IP, lze použít protokol IPSec na třetí vrstvě modelu ISO/OSI k ověření. (KOZIEROK, 2005?)

2.6.1 DHCP snooping

Jedná se o bezpečnostní funkci, která spočívá ve filtrování nedůvěryhodných DHCP zpráv. Princip je takový, že na začátku jsou všechny porty považovány za nedůvěryhodné. Postupně správce nastaví některé porty jako důvěryhodné, konkrétně port vedoucí do DHCP serveru a porty, přes které jsou připojeny přepínače. Pokud přijde DHCP zpráva z nedůvěryhodného portu, je ihned zahozena.

Zároveň se může vytvářet DHCP Snooping Binding Database, která obsahuje informace o všech přidělených IP adresách, času pronájmu, MAC adresách a informace o rozhraní. V případě, že přijde zpráva na nedůvěryhodné rozhraní, provádí se kontrola údajů oproti této databázi a neshodující se paket se zahodí. (BOUŠKA, 2008)

2.7 Nastavení služby ve firmě

Pro nastavení služby DHCP je nutné nejprve přidat (naistalovat) roli DHCP na Windows Serveru. Po přidání je nutné přidat DHCP rozsah (pool) adres, které budou službou přidělovány. Tento rozsah lze nazvat jakkoliv. Při přidávání se nastavuje několik údajů. Povinnými údaji jsou počáteční IP adresa, koncová IP adresa a maska podsítě. Dalším možným údajem je nastavení adresy výchozí brány.

Služba DHCP Snooping se nastavuje na přepínačích ve firemní síti. Po spuštění služby na přepínači se všechny porty na nedůvěryhodné a administrátor pak porty, do kterých jsou připojeny ověřené stanice, nastavuje jako důvěryhodné. Fungováním této služby se předchází nechtěným zásahům do sítě ze strany hackerů nebo jiných škůdců.

Pro povolení a konfiguraci služby NAT na Windows Serveru musí server obsahovat minimálně 2 síťové rozhraní, z nichž jedno bude propojeno na Internet. Prvním krokem je přidání role Vzdálený přístup na Windows Serveru. Po přidání se je nutné otevřít konfiguraci, vlevo zvolit daný server a následně vpravo kliknout na „Otevřít správu služby RRAS“. V nově otevřeném okně se vlevo klikne na jméno serveru pravým tlačítkem myši a v nabídce se zvolí první možnost. V dalším otevřeném okně se klikne na „Další“ a zvolí se služba zajišťující překlad adres, tedy NAT. V dalším kroku se v dialogovém okně zvolí rozhraní vedoucí na Internet, následně se prokliká až na konec.

Další informace viz praktická část bakalářské práce.

2.8 NAT

Služba zajišťující řešení nedostatku globálních IP verze 4 adres. Často je vnímána jako dočasné řešení do doby, než se plně přejde na IP adresy verze 6, která nabízí značně větší adresní prostor.

Každá síť, která je připojena k Internetu prostřednictvím NAT, musí mít alespoň jednu globálně platnou IP adresu. NAT zařízení, které může být implementováno softwarově (např. v jádře systému Linux pomocí služby iptables), či realizováno pomocí směrovače, překládá adresy v příchozích i odchozích datagramech. V odchozích datagramech nahrazuje

adresu zdroje svojí platnou globální adresou. Naopak v příchozích datagramech nahrazuje adresu cíle privátní adresou cílového zařízení.

Každé NAT zařízení obsahuje tabulku překladu adres, která obsahuje záznamy o přeložených adresách ve formě dvojic: IP adresa zařízení na Internetu a interní IP adresa zařízení v privátní síti. Tato tabulka může být nastavena staticky, nebo dynamicky, musí však být nainicializována dřív, než přijde datagram z Internetu.

Služba NAT může také způsobovat problémy. Jsou často zapříčiněné tím, že NAT vyřazuje mechanizmus přímé komunikace mezi koncovými klienty. Ve výsledku to znamená, že některé aplikace nemusí fungovat přesně tak, jak byly navrženy. (PUŽMANOVÁ, 2009, s. 219-221)

3. DNS

V internetové síti je mnoho koncových klientů a je nemožné pamatovat si jejich adresy. Právě proto byla vyvinuta služba DNS Server. Tato služba využívá protokol DNS a zajišťuje převod názvů serverů na čísla (IP adresy) a naopak. Vazby mezi jménem počítače a IP adresou jsou definovány v databázi DNS, která obsahuje jednotlivé záznamy neboli „DNS věty“. Části této databáze se umisťují na tzv. jmenné servery, a ty zajišťují převod jména na adresu a naopak. (HORÁK a KERŠLÁGER, 2008, s. 62) a (KABELOVÁ a DOSTÁLEK, 2008, s. 255)

3.1 Princip činnosti

Každý klient DNS má v síťovém nastavení nastavenou adresu na DNS server, kterému posílá žádost o překlad (mapování) doménového jména na IP adresu. Tento server vždy nejprve prozkoumá soubor, který má uložený v paměti a zjistí, zda zná odpověď na žádost od klienta. V případě, že ji nezná, zeptá se jiného DNS serveru, který je autoritativní pro vrcholovou doménu. Na základě odpovědi odpoví klientovi a zaktualizuje si soubor v paměti. Pokud server nemá v paměti záznam s adresou DNS serveru zodpovědného za vrcholovou doménu, pošle žádost přímo kořenovému serveru. Ten následně odpoví zasláním adresy DNS serveru zodpovědného za TLD.

Když lokální DNS server zažádá DNS server zodpovědný za vrcholovou doménu, odpoví mu adresu DNS serveru zodpovědného za doménu druhého řádu. Následující dotaz tedy už vede k tomuto serveru. Tento server by měl být schopný zodpovědět původní dotaz. Lokální DNS server si následně odpovědi zaznamená do souboru v paměti a tím způsobí, že po dobu záznamu bude schopen sám řešit mapování (překlad) dané vrcholové domény TLD a dané domény druhého řádu. (PUŽMANOVÁ, 2009, s. 422-423)

3.2 Zprávy a operace v DNS

DNS využívá dva druhy zpráv, první slouží jako dotaz (query) a druhá je pro odpověď (response). Na rozdíl od jiných protokolů, tyto zprávy mohou být odesílány přes TCP, ale také pomocí UDP, který je používaný častěji.

Mezi operace, které DNS využívá, patří vyhledávání (domain lookup) a přenos zón (zone transfer). Tyto přenosy se využívají na popud sekundárních serverů, když potřebují informace, které primární obsahují.

3.3 Kořenové servery

Kořenové neboli root servery slouží kořenové zóně označované „.“. Jejich zónou je celý jmenný prostor, tedy celá stromová struktura jmen. Na těchto serverech se neukládají informace o jednotlivých doménách, ale IP adresy všech autoritativních serverů. To znamená, že zná všechny národní domény (ccTLD) i všechny schválené generické domény (gTLD). Pro správné fungování mapování v síti je nutné, aby každý jmenný server znal IP adresu kořenového serveru.

Ve světě existuje celkem 13 kořenových serverů, z toho 10 jich je umístěno na území Spojených států. Správu nad 2 americkými servery drží americká armáda, proto je o těchto serverech málo informací. Zbylé 3 servery jsou umístěny v Londýně ve Velké Británii, ve Stockholmu ve Švédsku a poslední se nachází v Tokiu v Japonsku. Pro rozpoznání kořenových serverů se označují písmeny a–m. Organizace, které budou mít na starost správu těchto serverů, vybírá organizace IANA.

Tabulka 1 Jednotlivé jmenné kořenové servery

Označení	URL adresa	IP adresa	Správa
A	a-root-servers.net	198.41.0.4	Verisign Inc.
B	b-root-servers.net	192.228.79.201	University of Southern California
C	c-root-servers.net	192.33.4.12	Cogent Communications
D	d-root-servers.net	199.7.91.13	University of Maryland
E	e-root-servers.net	192.203.230.10	NASA
F	f-root-servers.net	192.5.5.241	Internet Systems Consortium, Inc
G	g-root-servers.net	192.112.36.4	US Department of Defense
H	h-root-servers.net	198.97.190.53	US Army
I	i-root-servers.net	192.36.148.17	Netnod
J	j-root-servers.net	198.4.0.10	Verisign Inc.
K	k-root-servers.net	193.0.14.129	RIPE NCC
L	l-root-servers.net	199.7.83.42	ICANN
M	m-root-servers.net	202.12.27.33	WIDE Project

Zdroj: zpracováno dle (IANA)

Kořenový server A obsahuje hlavní databázi jmen domén nejvyšších úrovní. Kořen jmenného prostoru Internetu tvoří jediný soubor, ve kterém je popsáno delegování domén nejvyšších úrovní. Ostatních 12 kořenových serverů si tento soubor pouze kopíruje, přenos probíhá pomocí

mechanizmu transferu pro DNS, nebo za využití protokolu FTP. Zhruba jednou až dvakrát týdně soubor mění, z důvodů změn jmenných prostorů, které má na starost organizace IANA.

Pro předejití vypadnutí některého ze serverů se musí zajistit několik věcí. Mezi hlavní patři zajištění náhradního zdroje napájení v případě, že by byl přerušen přívod elektrického proudu. Další velmi důležitou věcí je nutnost kvalitní klimatizace v místnostech se servery a samozřejmě zajištění zálohy pomocí připojení k místní páteřní síti. A v neposlední řadě je třeba zajistit zabezpečení serverů, jednak softwarové, ale také fyzické zabezpečení čili dovolit přístup pouze autorizovanému personálu.

Kořenové servery obsahují pouze minimum běžících programů proto, aby se předešlo softwarovým hrozbám. Na kořenových serverech tedy běží pouze operační systém, protokol času v síti pro synchronizaci času v Internetu a program BIND. Použitý operační systém se liší, ale vždy je to variace systému UNIX. Jiné síťové služby by mohly působit jako hrozba, a proto se nepoužívají. (PUŽMANOVÁ, 2009, s. 423-424)

3.4 DNS servery

DNS servery se dělí na:

- **primární** – tyto servery ukládají soubory s informacemi o zóně, pro které jsou autorizované do své paměti; tento soubor nejen vytváří, ale také ho udržují a aktualizují;
- **sekundární** – servery, které přenáší informace o zóně jiného serveru a ukládají si příslušný soubor na disk; tyto soubory, ale neaktualizují, přesto slouží jako autoritativní záloha pro danou zónu; (PUŽMANOVÁ, 2009, s. 423)

a z jiného úhlu pohledu na:

- **autoritativní** – servery, které si na disku uchovávají záznamy k dané doméně či zóně; většinou bývají 2 (primární a sekundární), ale může jich být i více; autoritativní servery bývají provozovány registrátorem domény;
- **rekurzivní** – servery, které pomocí rekurzního mapování (dotazu) zjišťují informace o záznamu příslušného autoritativního DNS serveru a na určitou dobu si je uloží do paměti cash, tím zajistí rychlejší odpověď klientům a snížení zatížení autoritativních serverů; rekurzivní servery obvykle provozují poskytovatelé síťových služeb.

3.5 Druhy mapování

Mapování se provádí buď iterativně, nebo rekurzivně.

Iterativní mapování – Princip spočívá v tom, že dotázaný jmenný server vrátí klientovi, který se ptal, pouze tu nejlepší odpověď, nejlépe přímo požadovanou adresu. Většinou však odpovědí bývá pouze adresa jmenného serveru, který má „blíž“ k vyřešení žádané operace.

Rekurzivní mapování – Princip je takový, že jmenný server požádá jiný server o pomoc. Pokud nezná odpověď čili tento server není autoritativní pro danou doménu, pověří jiný jmenný server vyřešením mapování a takto se postupuje, až se narazí na autoritativní server. (PUŽMANOVÁ, 2009, s. 423)

3.6 Hierarchie domén

Všechny domény v Internetu jsou hierarchicky uspořádány do stromové struktury. Vrcholem je tzv. kořenová doména, Spravuje ji NIC. Nižšími patry této struktury jsou domény nejvyšší úrovně neboli Top Level Domain – TLD. Za nimi následují domény druhé, třetí a dalších úrovní.

Vrcholové domény se dále dělí na generické domény (gTLD) a národní domény (ccTLD).

Generické domény jsou nejčastěji třípísmenné. Patří mezi ně například .com (doména určená pro komerční organizace), .edu (doména určená pro vzdělávající organizace), .org (doména sloužící pro ostatní organizace), ale také .arpa (dočasná doména ARPANETu, velmi zastaralá doména).

Národní domény bývají nejčastěji dvoupísmenné, vyznačují příslušnost k určitému státu a jsou rozdělovány dle normy ISO 3166. Mezi národní domény se řadí například .cz pro Českou republiku, .sk pro Slovenskou republiku nebo .ru pro Rusko. Výjimku tvoří doména .eu, která nepřísluší konkrétnímu státu, ale celé Evropské unii.

Doména druhého řádu je doména, která následuje hned po vrcholové doméně (např. **seznam**.cz). Domény nižších řádu vznikají dalším členěním domén. (PUŽMANOVÁ, 2009, s. 422)

3.7 Parametry DNS serverů

Zóna dopředného vyhledávání – Je zóna, v níž se převádí jednotlivé názvy domén na IP adresy. Její součástí jsou složky domén, které spravuje a jejich záznamy. Pro IPv4 záznamy typu A a pro adresy IPv6 záznamy typu AAAA.

Zóna zpětného vyhledávání – Zóna, ve které se převádí IP adresy na názvy domén.

Záznam typu A – Je DNS záznam, který odpovídá IPv4 adrese a slouží k překladu doménového jména právě na IP adresu.

Záznam typu AAAA – Záznam, obsahující překlad názvu (doménového jména) na IP adresu, vztahuje se k IPv6.

Záznamy typu HINFO a TXT – Tyto typy záznamů jsou určeny pouze pro informování. HINFO obsahuje dva údaje. Prvním je informace o hardwaru a druhým je informace o softwaru. TXT obsahuje obecný textový řetězec.

Záznamy typu CNAME – Slouží k vytváření synonym k doménovým jménům, jde o vytváření tzv. aliasů k jménům počítačů.

Záznamy typu PTR – Záznam typu PTR slouží k překladu IP adresy na doménové jméno.

Záznamy typu MX – Záznam, který specifikuje poštovní server domény. Ukazuje, na který počítač má být pro doménu doručena pošta. V záznamu je i číselná priorita, která určuje počítače, na které může být pošta pro doménu odesílaná. Zasílá se od nejvyšší priority, když zasílání selže, posílá se na počítač s druhou nejvyšší prioritou.

Autoritativní zóna – Skupina jmenných domén, pro které je daný jmenný server autoritativní. (KABELOVÁ a DOSTÁLEK, 2008, s. 276-279)

3.8 Bezpečnost

Záznamy v systému doménových jmen a aktualizační zprávy v DNS musí být kvalitně zabezpečené proti vnějším útokům, platí to především u kořenových serverů. Typ útoku, který se u kořenových serverů nejvíce objevuje, se nazývá DoS neboli v češtině odmítnutí služby. V praxi to znamená, že útočník zasílá obrovské množství požadavků na server a tím dochází k zahlcení serveru. Velké riziko přináší užívání softwaru BIND, který je využíván na většině serverů DNS. Slabiny tohoto softwaru umožňují útočníkovi falšovat důvěryhodné webové servery a tím získávat důvěrné informace od uživatelů. V případě, že útočník získá informace o komunikaci mezi poskytovatelem internetových služeb a servery DNS, je riziko přesměrování provozu na falešnou URL, což vystavuje uživatele přímému útoku pod záminkou dotazu na hesla, nebo jiné citlivé informace. Vhodným řešením této situace je šifrování DNS zpráv, či využití bezpečnostního rozšíření systému doménových jmen DNSSEC. Dohled nad bezpečností kořenových serverů má společnost ICANN. (PUŽMANOVÁ, 2009, s. 425)

3.9 DNSSEC

DNSSEC je rozšíření systému DNS, které zvyšuje bezpečnost služby doménových jmen. Toto vylepšení zabraňuje podvržení falešných, pozměněných nebo neúplných údajů o doménových jménech a tím dochází ke zvýšení uživatelské bezpečnost při používání DNS. V případě že služba DNS není vhodně zabezpečena pomocí DNSSEC, je riziko že potencionální útočník může narušit komunikaci a následně zfalšovat údaje. Tímto narušením změní útočník údaje o doménových jménech, to ovlivní fungování dalších internetových služeb, a právě zde vzniká hrozba zneužití, o které uživatel většinou nemá vůbec tušení. Pro ukázku několik příkladů zneužití informací útočníkem:

- má možnost získat cizí e-maily;
- pomocí falešných webových stránek může získat uživatelská hesla, informace o platebních kartách apod.;
- může přesměrovávat a odposlouchávat telefonní hovory vedené přes internet.

3.9.1 Fungování DNSSEC

DNSSEC přináší DNS asymetrické kryptování, což znamená, že se využívá jiný klíč pro zašifrování než pro dešifrování. Je to podobný princip jako například u podepisování e-mailů elektronickým podpisem. U DNSSEC šifrování funguje tak, že si držitel domény vygeneruje dvojici klíčů, jeden soukromý a jeden veřejný. Pomocí svého soukromého klíče elektronicky podepíše technické údaje, které o své doméně vkládá do DNS databáze. Využitím veřejného klíče je možnost ověření pravosti podpisu. Pro dostupnost klíče ho držitel publikuje ke své doméně u nadřazené autority. Pro všechny .cz domény je touto autoritou registr domén .cz. Technická data v databázi DNS registru domén .cz jsou také zašifrována a správce registru poskytne veřejný klíč nadřazené autoritě. Vytváří se tak logický řetěz zajišťující důvěryhodnost údajů, který se nesmí v žádném svém článku porušit, aby všechny elektronické podpisy souhlasily. (CZ.NIC, 2017)

3.10 Nastavení služby ve firmě

Mezi hlavní nastavení patří vytvoření dopředné zóny vyhledávání a vytvoření zóny zpětného vyhledávání. Nejprve se vytváří a konfiguruje primární dopředná zóna. Při její tvorbě se zadá název domény, která bude v síti.

Následuje vytvoření primární reverzní (zpětné) zóny. Zde se zadává jednoznačné ID sítě, tedy část IP adresy, která se nemění. Po zadání se samo doplní celé jméno zóny, které má formát neměnná IP adresa zpětně, následuje tečka a jméno domény (např. 10.168.192.domena).

Nastavení DNSSEC je také vcelku snadné. Na dopřednou zónu se klikne pravým tlačítkem myši a najede se na možnost DNSSEC, poté se ukáže možnost podepsat zónu. Nabídka se nechá nastavená, jak je, do doby, dokud půjde pokračovat dále. Ve chvíli kdy se narazí na přidání podpisového klíče klíče, zde se klikne na přidat a v nově objeveném okně tlačítko OK. Pokračuje se dále, až bude potřeba přidat podpisový klíč zóny, zde se následně postupuje stejně jako u předchozího klíče. Postupuje se dál, než se dojde na okno zabývající se kotvami vztahů důvěryhodnosti, zde se zaškrtne políčko k povolení distribuování kotev vztahů pro danou zónu. A následně se jen prokliká do konce.

Další informace viz praktická část bakalářské práce.

4. ACTIVE DIRECTORY

Služba Active Directory Domain Services ukládá různé informace o klientech a jejich počítačích v síti. Díky této službě má správce serveru možnost spravovat tyto informace či sdílet prostředky. AD DS nabízí distribuované databáze, tyto databáze v sobě schraňují informace o síťových zdrojích i aplikacích. Správce serveru je díky tomu schopný uspořádat elementy sítě, jako jsou uživatelé, počítače či jiná zařízení, do speciální hierarchické struktury. AD DS se také využívá pro přidělování práv uživatelům a sdíleným počítačům, přiděluje přístupová práva na složky, soubory a jiné objekty v síti. Výsledkem je zjednodušení práce administrátora, kdy nemusí nastavovat práva jednotlivým uživatelům, ale nastaví je skupině, do které daní uživatelé patří. (BOUŠKA, 2008b)

4.1 Struktura AD

Jak již bylo zmíněno výše, služba Active Directory si do databáze ukládá informace o jednotlivých síťových prvcích. Termínový jmenný prostor označuje oblast, ve které může být umístěn síťový prvek. Například DNS je jmenný prostor, který řeší překlad názvů hostitelů na IP adresy. Služba Active Directory poskytuje jmenný prostor pro řešení názvů síťových objektů samotným objektům a dokáže vyřešit širokou škálu objektů, včetně uživatelů, systémů a služeb v síti.

Za objekt je v Active Directory považováno téměř vše, co služba sleduje. Objektem tedy může být jakýkoliv uživatel, prostředek nebo služba, kterou AD využívá.

Schéma – Sada atributů, které jsou dostupné pro libovolný typ objektu. Přesné informace o schématu, tedy informace o atributech objektů, se ukládají v rámci služby AD. To umožňuje upravovat atributy ve třídách objektů a následně je distribuovat do celé sítě.

Struktura AD se základně dělí na logickou a fyzickou strukturu.

Logická struktura je chápána jako struktura skládající se z lesa, stromů, domén a organizačních jednotek. Na vrcholu této struktury je les, který má pod sebou jeden nebo více stromů. Strom obsahuje jednu či více domén, ve které se nachází už jednotlivé organizační jednotky. Součástí organizační jednotky jsou konkrétní objekty, tedy počítače, klienti, tiskárny apod.

Na druhou stranu fyzická struktura obsahuje doménový řadič a sítě či podsítě, tedy skupiny síťových adres v určitém rozsahu.

Les – Skupina doménových stromů a domén, které sdílejí stejný kořen jmenného prostoru. Komunikace mezi dvěma oddělenými lesy je standardně zakázaná, pokud je potřeba komunikovat, musí ji správce povolit.

Doménový strom – Seskupení jedné či více domén. Vytváří se přidáním podřízené domény (potomka) ke kořenové (rodičovské) doméně. Ty, které strom obsahuje, sdílejí schéma, jmenný prostor a hierarchické spojení doménových jmen. Dá se tedy říci, že doménový strom pracuje na principu potomek – rodič.

Doména – Základní prvek logické struktury Active Directory. Její součástí jsou objekty dané domény. Maximální počet objektů není daný, protože doména není nutně vázaná na jedno fyzické umístění. Active Directory může tvořit jedna, ale i více domén, jejich názvy však musí být jedinečné. Přístup k objektům domény se řídí pomocí ACL, což znamená pomocí povolení jednotlivých IP adres nebo určitého rozsahu IP adres.

Organizační jednotka – Kontejner sloužící k označení určitého pracovního týmu, oddělení, lokace apod. Díky sjednocení více klientů usnadňuje správu delegováním pravomocí. Organizační jednotka je nejmenší jednotka, na kterou je možné delegovat oprávnění.

Skupina – Logické seskupení několika uživatelů. Výhodou skupin je možnost hromadného přidělování práv a přístupů. Je to způsobeno tím, že každý člen skupiny dědí oprávnění skupiny, ve které se nachází.

Uživatel – Jako objekt uživatel je v AD brán uživatel, který má vlastní uživatelské jméno a heslo. Dalšími informacemi může být telefon, email, adresa a informace o skupinách, kterých je členem. (BOUŠKA, 2008b)

4.2 Řadič domény

Jako řadič domény se označuje počítač, na kterém je uložen adresář služby Active Directory. Je to velmi důležitý typ síťového serveru v sítích Windows. Pro chod bez problémů je nutné, aby byly tyto servery chráněné, stabilní, ale zároveň i dostupné. Ztráta řadiče domény v síti může vést k vážným problémům pro uživatele, servery i různé aplikace, které jsou závislé na ověření zásad skupin. (STANEK, 2009) a (STANEK, 2010)

4.2.1 Řadič domény jen pro čtení

Je to řadič domény, který se využívá v sítích s malou bezpečností. Dokáže odolat útokům hrubou silou, které se snaží získat hesla uživatelů, díky tomu, že databáze AD na daném serveru neobsahuje tato hesla. Dá se tedy říci, že řadič domény jen pro čtení slouží k zvýšení bezpečnosti. (STANEK, 2009) a (STANEK, 2010)

4.3 Globální katalog

Globální katalog je služba Active Directory, která obsahuje vybrané informace o objektech celého stromu či lesa. Globálním katalogem většinou bývá první nainstalovaný řadič domény. Využití této služby je při hledání objektu z jiné domény. Dalším velmi důležitým použitím je při přihlašování do sítě. Nutný je hlavně, pokud se v síti používají univerzální skupiny a v jedné lokalitě se připojují uživatelé z různých domén.

Součástí globálního katalogu jsou oddíly schématu a konfigurace, ale také Domain partition pro doménu, které jsou součástí či částečné doménové oddíly jiných domén v lese, tyto oddíly jsou ale pouze pro čtení. Lokalizace globálního katalogu probíhá pomocí služby DNS. (BOUŠKA, 2008b)

4.4 Zásady skupiny

Zásady skupiny neboli Group Policy je pojem popisující sadu pravidel, která se aplikují v prostředí firmy.

Motivací pro zavedení těchto pravidel je především rozličnost uvnitř firmy. Uživatelé se ve firemní síti dají rozdělit do skupin, které využívají jiné programy a mají povolení přístupu k odlišným firemním prostředkům. Díky zavedení zásad skupin se zjednodušila administrátorova práce, pouze spravuje tyto zásady a přiděluje je jednotlivým objektům v doménách.

Zásady se dají rozdělit na lokální a doménové.

Lokální ovlivňují jednotlivé lokální počítače a jejich uživatele. Využívají se, pokud není počítač připojen do domény. V praxi to tedy znamená, že pokud bude vytvořen uživatel na počítači administrátor mu nastaví omezení, a to jaké bude mít oprávnění vymezuje právě lokální zásady skupiny. Každý počítač má tyto zásady uloženy ve skrytém adresáři %systemroot%\system32\GroupPolicy.

Doménové se používají u počítačů připojených do domény. Aplikují tedy práva pro uživatele a počítače dané domény. Při založení nové domény se automaticky vytvoří dva objekty zásad skupiny: Default Domain Policy a Default Domain Controllers Policy.

Default Domain Policy slouží k propojení s celou doménou v Active Directory, které se provede automaticky. Uplatňuje se také pro výběr základních nastavení zásad, uplatňovaných na každého uživatele a počítače v dané doméně. Mezi tyto nastavení může patřit například určení zásad hesel (minimální délka, maximální doba stáří hesla, počet pokusů na zadání správného hesla apod.).

Default Domain Controllers Policy je automaticky vytvořený a propojený s organizační jednotkou, která se vztahuje na všechny řadiče domény v doméně. Hlavní využití tohoto objektu je pro ovládání bezpečnostních nastavení pro řadiče v dané doméně. (STANEK 2010)

4.4.1 Dědění zásad

V rámci aplikování zásad je implementovaný princip dědičnosti, to znamená, že zásady nastavené na rodičovském kontejneru se uplatní i na podřízený kontejner. Díky tomuto fungování každý uživatel a počítač v doméně je předmětem zpracovávání zásad skupin.

Zásady skupin mohou nabývat třech různých stavů, prvním je „nedefinováno“, který je výchozí. Druhým je stav „povoleno“, tento stav značí, že dané nastavení bude vynuceno a aplikováno na všechny uživatele a počítače, kterých se týká daná zásada (přímo, či děděním). Třetím stavem je stav „zakázáno“, který se aplikuje podobně jako předchozí, má však opačný význam.

To, jak má dědění fungovat je možné nastavit několika způsoby. Je možné změnit pořadí propojení objektů a tím i upravit jejich prioritu. Druhou možností je potlačit dědičnost, zde je však nutné, aby nebyla dědičnost vynucena. Další možností je úplné blokování dědičnosti. A v neposlední řadě je také možné vynutit dědičnost za účelem zamezení, blokování či potlačení dědičnosti. (STANEK 2010)

4.4.2 Nastavení zásad skupin

Obecně tyto nastavení slouží ke konfiguraci počítače, jeho operačního systému, skriptů, bezpečnosti a dalším podobným nastavením. Mezi hlavní druhy nastavení patří:

- **nastavení softwaru** – slouží k nastavení automatických instalací či případných možných upgradu;
- **šablony pro správu** – je určen ke změnám komponent Windows, aplikací a ke změnám konfigurace samotného operačního systému;

- **nastavení systému Windows –** je k nastavení a ovládání nastavení systému Windows, a to jak uživatelských, tak ale i týkajících se zabezpečení či využití skriptů.

Zásady počítače – Nastavení zásad pro počítače, které se nastaví při zapnutí počítače.

Zásady uživatele – Nastavení zásad pro uživatele, které se nastaví při přihlášení uživatele. (MAR-ELIA, 2006) a (STANEK 2010)

5. PRAKTICKÁ ČÁST

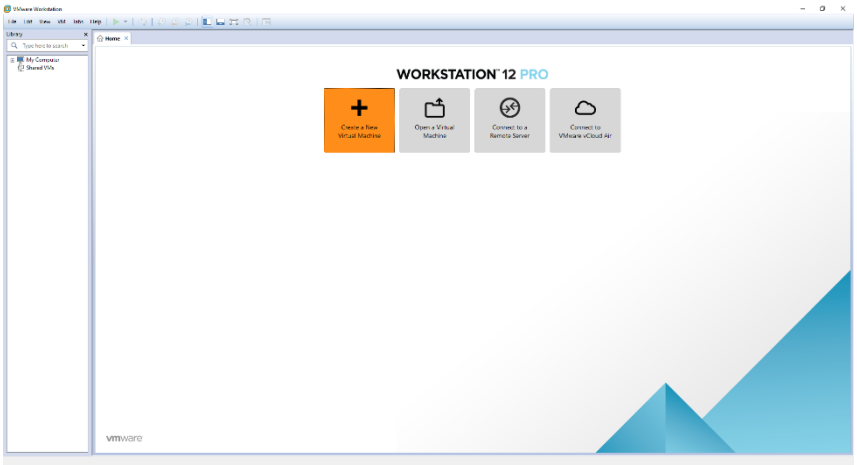
Obsah praktické části mohl být realizován jako samostatný server na libovolném počítači (splňujícím minimální požadavky) či pomocí instalace jako virtuálního stroje. Byl využit druhý způsob.

Vytvoření virtuálního stroje umožňují např. programy VirtualBox nebo VMware Workstation. Pro tvorbu praktické části byl využit program VMware Workstation s licencí pro studenty.

5.1 Tvorba virtuálního stroje

Před zahájením je třeba ujistit se, že počítač má dostatečný výkon pro běh virtuálního stroje. V praxi to znamená, aby počítač běžel plynule, i když se uvolní např. 2 GB paměti RAM pro virtuální stroj. Následně je ještě třeba obstarat si obraz operačního systému, konkrétně Windows Server 2016. V tomto případně bylo využito spolupráce školy se společností Microsoft a kopie byla stažena z webové stránky Microsoft Imagine.

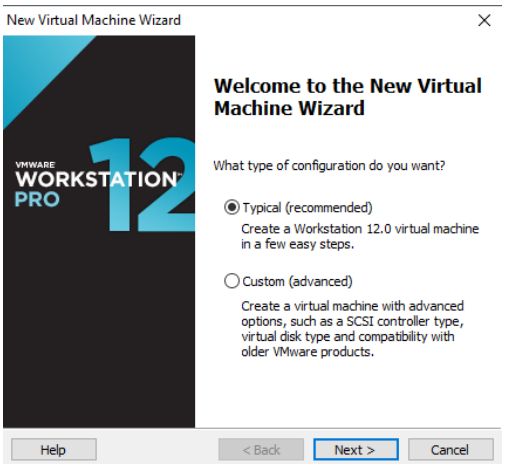
5.1.1 Postup



Obrázek 2 - Tvorba virtuálního stroje – krok 1

Zdroj: vlastní

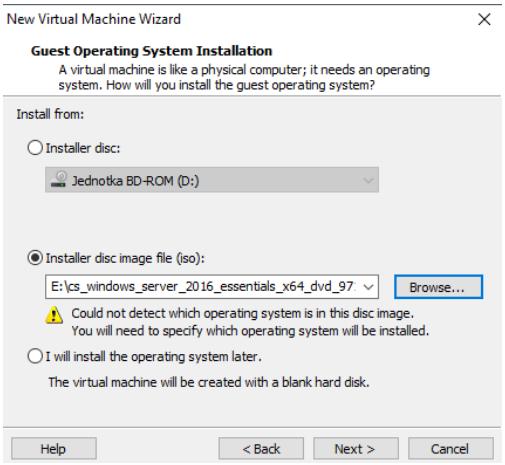
Prvním krokem je po spuštění programu VMware Workstation kliknout na **Create a New Virtual Machine.**



Obrázek 3 - Tvorba virtuálního stroje – krok 2

Zdroj: vlastní

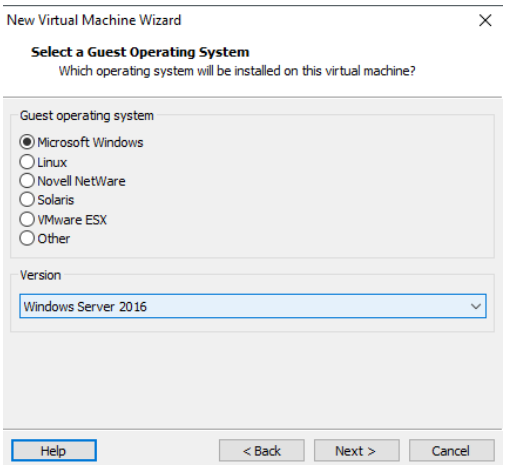
Následně se otevře okno konfigurace. Nechá se volba instalace **Typical** a pokračuje se dál tlačítkem **Next**.



Obrázek 4 - Tvorba virtuálního stroje – krok 3

Zdroj: vlastní

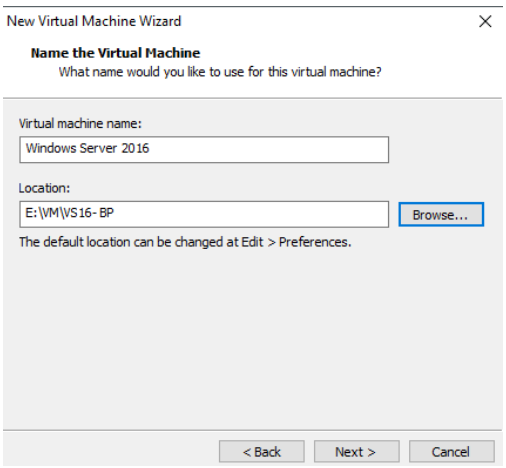
V následujícím kroku se vkládá obraz operačního systému. Je možné ho načíst z optického disku, nebo z pevného disku počítače. Další možností je obraz nevkládat, ale to znamená, že se bude muset vložit později.



Obrázek 5 - Tvorba virtuálního stroje – krok 4

Zdroj: vlastní

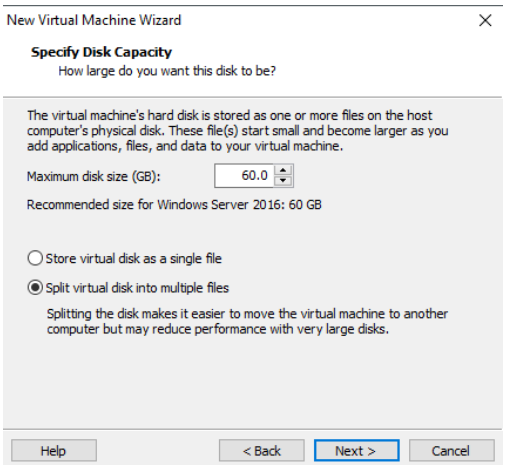
Dále je třeba upřesnit, o jaký operační systém se jedná.



Obrázek 6 - Tvorba virtuálního stroje – krok 5

Zdroj: vlastní

Následně se vyplní jméno virtuálního stroje a umístnění, kam bude stroj nainstalován.

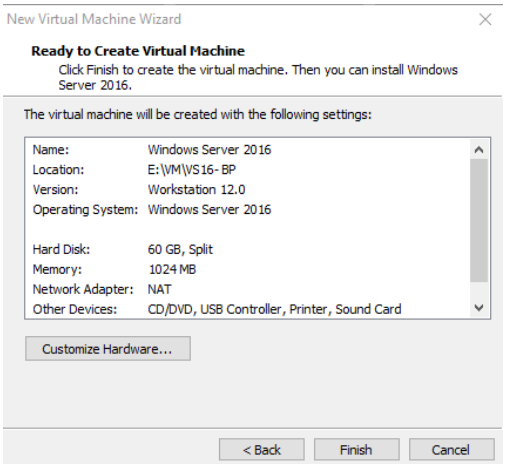


Obrázek 7 - Tvorba virtuálního stroje – krok 6

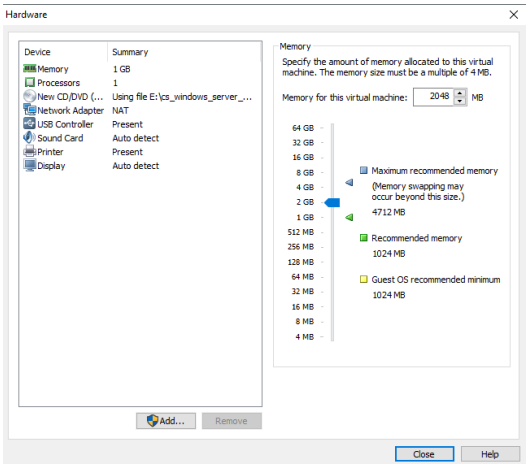
Zdroj: vlastní

V dalším kroku se upřesní velikost, která se poskytne stroji na pevném disku počítače.

Zdroj: vlastní

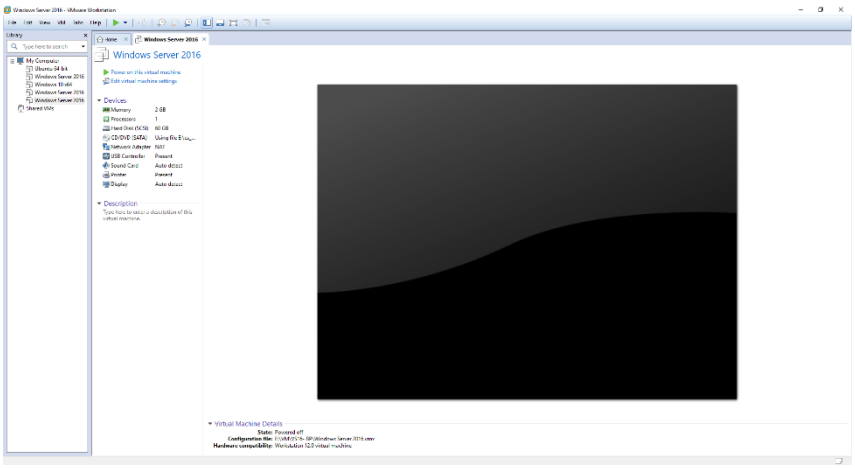


Obrázek 9 - Tvorba virtuálního stroje – krok 7



Obrázek 8 - Tvorba virtuálního stroje – krok 8

Následuje přehled nastavení. Pro plynulejší chod virtuálního stroje je vhodné zvýšit množství poskytnuté paměti RAM. Stiskem tlačítka **Customize Hardware…** se objeví okno, ve kterém se poskytnutá paměť zvýší.



Obrázek 10 - Tvorba virtuálního stroje – výsledek

Zdroj: vlastní

Posledním krokem je již výsledné okno, které ukazuje nastavení stroje, případnou možnost úpravy těchto nastavení a umožňuje spuštění virtuálního stroje. Při prvním spuštění se provede instalace.

5.2 Výukové video – Instalace OS WS

V prvním videu je ukázána instalace serverového operačního systému Windows Server 2016. Aby mohl uživatel podle tohoto videa zdařile naistalovat systém, potřebuje samotnou kopii operačního systému, buď ve formě oficiální DVD kopie, nebo formou optického obrazu. Dále je samozřejmě nutný licenční klíč, instalaci je možné dokončit i bez zadání tohoto kódu, systém však bude vyžadovat následnou aktivaci vložením klíče.

5.3 Výukové video – DNS a DNSSEC

Druhé video přibližuje postup při přidání role DNS server a její následnou konfiguraci. Pro možnost nastavení služby potřebuje uživatel vědět, jak má pojmenovat zónu dopředného vyhledávání a zóny zpětného vyhledávání. Čtenář zde také může vidět, jak se nastavuje bezpečnostní služba DNSSEC.

5.4 Výukové video – DHCP

Ve třetím videu je možné vidět přidání služby DHCP a vytvoření adresních rozsahů. Administrátor potřebuje mít rozmyšlenou síťovou architekturu, tedy jak velký rozsah adres potřebuje vytvořit. Dále je nutné, aby věděl, jakou adresou má začít. Při vytváření rozsahu adres může správce nastavit adresu výchozí brány, adresy DNS serverů či adresu WINS serveru.

5.5 Výukové video – NAT

Předposlední video pokrývá problematiku instalace a nastavení serverové role Vzdálený přístup, konkrétně služby NAT. Než správce začne konfigurovat, musí se přesvědčit, že server má minimálně 2 aktivní síťová rozhraní, z toho jedno musí vést přímo na internet.

5.6 Výukové video – Group policy

Poslední video nastiňuje aplikaci zásad skupin na serveru. Pro nastavení bez problémů by měl mít správce předem promyšlené, jaké objekty zásad vytvoří a jaké budou mít práva a možnosti. Špatné nastavení může vážně ovlivnit fungování firemní sítě, např. způsobení zahlcení sítě.

6. ZÁVĚR

Cílem této bakalářské práce bylo nastínit využití síťového operačního systému Windows Server 2016 a jeho služby Active Directory ve firmě střední velikosti. Ukázka nasazení byla předvedena ve výukových videích, která jsou náplní praktické části.

Na začátku teoretické části práce byl představen operační systém Windows Server 2016 a systémové požadavky pro možnost jeho využití.

Ve druhé části byla podrobně vysvětlena služba DHCP, její fungování a zabezpečení i jednotlivé zprávy, které se zasílají při komunikaci DHCP serveru s klientem na uživatelském počítači. V této kapitole bylo také vysvětleno fungování služby NAT.

Třetí část se zaměřila na službu DNS. Bylo zde nastíněno fungování služby a představeny jednotlivé druhy mapování i druhy úrovní domén. Značná část byla také věnována rozšiřující službě DNSSEC, která se stará o zvýšenou bezpečnost služby DNS.

Posledním tématem teoretické části byla služba Active Directory. Nejprve byla tato služba představena s vysvětlením její struktury. Dále byly objasněny pojmy: řadič domény, globální katalog a zásady skupiny.

Praktická část bakalářské se věnovala postupu při vytváření virtuálního stroje a formou videí dokumentovala postup instalace a nastavení služeb DNS, DHCP a Active Directory.

Obsah této bakalářské práce může sloužit jako podklad při výuce. Pomocí postupů ukázaných v praktické části může uživatel zprovoznit vlastní server, za podmínky že splňuje dané minimální hardwarové požadavky.

7. POUŽITÁ LITERATURA

DigdarshanKavia@TWC. Windows club: *Windows Server 2016 Editions, Pricing, Availability, Features* [online]. 2016 [cit. 2017-04-30]. Dostupné z: http://www.thewindowsclub.com/windows-server-2016-editions.

Microsoft. *Compare features in Windows Server versions* [online]. Microsoft, 2017 [cit. 2017-04-30]. Dostupné z: https://www.microsoft.com/en-us/cloud-platform/windows-server-comparison.

Microsoft. *Windows Server Evaluations* [online]. Microsoft, 2016 [cit. 2017-04-30]. Dostupné z: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016-essentials.

ONDRUSEK, Jaime. System Requirements. *Microsoft Technet* [online]. 2016 [cit. 2017-04-30]. Dostupné z: https://technet.microsoft.com/en-us/windows-server-docs/get-started/system-requirements.

PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 2., upravené a rozšířené vyd. České Budějovice: Kopp, 2009. ISBN 978-80-7232-388-3.

DROMS. R. *Dynamic Host Configuration Protocol* [online]. 1997 [cit. 2017-04-30]. Dostupné z: https://tools.ietf.org/html/rfc2131#page-43.

PRESS. *Živě.sk: Automatické přidělení IP adres pomocí DHCP serveru* [online]. 1999 [cit. 2017-04-30]. Dostupné z: http://www.zive.sk/clanok/4666/automaticke-prideleni-ip-adres-pomoci-dhcp-serveru.

SKODA, Martin. *Flowmon: DHCP MONITORING IN FLOWMON 8.0* [online]. 2016 [cit. 2017-04-30]. Dostupné z: https://www.flowmon.com/en/blog/dhcp-monitoring-in-flowmon-8-0.

THOMAS, Jajish. *OmniSecu.com: Dynamic Host Configuration Protocol (DHCP) Messages* [online]. c2008-2017 [cit. 2017-04-30]. Dostupné z: http://www.omnisecu.com/tcpip/dhcp-dynamic-host-configuration-protocol-messages.php.

KOZIEROK, Charles M. *The TCP/IP Guide: DHCP Security Issues* [online]. [2005] [cit. 2017-04-30]. Dostupné z: http://www.tcpipguide.com/free/t_DHCPSecurityIssues.htm.

BOUŠKA, Petr. *Samuraj-cz: Cisco IOS 13 - DHCP služby na switchi* [online]. 2008 [cit. 2017-04-30]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-ios-13-dhcp-sluzby-na-switchi/

HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 4., aktualizované a rozšířené vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2073-6.

IANA: Root Servers [online]. [cit. 2017-04-30]. Dostupné z: https://www.iana.org/domains/root/servers.

KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

CZ.NIC, z. s. p. o. *CZ.NIC: JAK FUNGUJE DNSSEC* [online]. 2017 [cit. 2017-04-30]. Dostupné z: https://www.dnssec.cz/page/444/jak-funguje-dnssec/.

BOUŠKA, Petr. *Samuraj-cz: Active Directory komponenty - domain, tree, forest, site* [online]. 2008b [cit. 2017-04-30]. Dostupné z: http://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/.

MAR-ELIA, Darren, MELBER, Derek, STANEK, William S. *Zásady skupin Microsoft Windows: Microsoft Windows Group Policy Guide,* Brno: Computer Press a.s., 2006. ISBN 80-521-1261-4.

STANEK, William R. *Group Policy – Zásady skupiny ve Windows: Kapesní rádce administrátora.* Brno: Computer Press a.s., 2010. ISBN 978-80-251-2920-3.

STANEK, William R. *Mistrovství v Microsoft Windows Server 2008.* Brno: Computer Press a.s., 2009. ISBN 978-80-251-2158-0.

8. PŘÍLOHY

Příloha A – Obsah CD Praktická část.....45

Příloha B – Obsah CD 46

Příloha A – Obsah CD

Na CD je přiložena praktická část bakalářské práce CalekP_NasazeniVyuziti_SN_2017.zip

Obsah:

Výukové video – Instalace OS WS

Výukové video – DNS a DNSSEC

Výukové video – DHCP

Výukové video – NAT

Výukové video – Group policy

Příloha B – Obsah CD

Na CD je přiložena bakalářská práce CalekP_NasazeniVyuziti_SN_2017.pdf