Jihočeská univerzita v Českých Budějovicích

Pedagogická fakulta – Katedra fyziky

Návrh a řešení serverovny pro 200 uživatelů

Proposal and implementation of a server for 200 users

Bakalářská práce

Vedoucí práce: RNDr. Petr Bartoš, Ph.D.

Autor: Lukáš Melena

Anotace

Tato práce se zabývá problematikou serveroven, principem jejich činnosti a popisem funkcí jednotlivých zařízení a jejich návrhem. Práce je rozdělena na dvě části, kdy první část se věnuje obecné problematice návrhu serveroven, kdy je popsán návrh umístění a lokality serverovny, její zabezpečení, dále je popsán postup návrhu napájení a chlazení a nakonec se práce věnuje návrhu síťové infrastruktury, kde jsou popsány možnosti volby pasivních síťových prvků, aktivních síťových prvků a nejčastěji používaných serverů. Druhá část se zabývá popisem serverovny realizované ve středně velkém výrobním podniku, kdy je na konkrétním příkladu objasněn základní princip fungování celého systému a jednotlivých zařízení.

Abstract

This work is focused on problematic of data centres, their principles and description of functions of every apparatus and their concept. The work is divided into two parts. The first part consists of general problematic of data centres proposal – the description of location and place of data centre, its security system, process of supply system and cooling system. It also consists of concept of net infrastructure, where choice capacities of passive net components, active net components and mostly used servers are described. The second part deals with description of data centre used in middle-sized manufacturing corporation, where is presented the basic principle of functioning of the whole system and particular components on concrete example.

Prohlášení:

Prohlašuji, že předloženou práci jsem vypracoval samostatně, pouze s použitím uvedené (citované) literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění, souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě fakultou, elektronickou cestou ve veřejně přístupné části databáze STAG, provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

V Českých Budějovicích, dne 23. prosince 2009 ……

Poděkování:

Touto formou děkuji svému vedoucímu práce RNDr. Petru Bartošovi, Ph.D. za pomoc při zpracování této práce, dále svému vedoucímu IT oddělení Ing. Jiřímu Neumannovi za umožnění studia v pracovní době a svým kolegům Tomáši Sýkorovi, DiS. a Milanu Křenkovi, DiS. za odborné konzultace a cenné rady a připomínky při zpracování mé práce.

Obsah

1 Úvod

Tato bakalářská práce se zabývá obecnými problémy a zásadami se kterými se můžeme potkat při návrhu počítačové serverovny a realizací konkrétní serverovny, kdy jsou popsány jednotlivé technologie a systémy, jejich princip a funkce. Toto téma jsem si vybral z důvodu profesního zaměření a zájmu o pro mne dosud neznámé technologie.

Přínosem této práce by mělo být vytvoření komplexního pohledu na tyto složité systémy, jakými jsou datová a informační centra. Tento text je určen především pro méně zkušené, nebo začínají správce sítě, případně čtenáře zajímající se o danou problematiku a měl by poskytnout základní přehled o fungování a principech většiny středně velkých serveroven postavených na moderních technologiích s využitím především systémů firmy Microsoft, VMware a Citrix.

Práce je zpracována pomocí mých praktických zkušeností, studiem množství odborné literatury a konzultacemi se zkušenými administrátory.

Jelikož by podrobné popsání jednotlivých technologií a zařízení většinou svým rozsahem zabralo na samostatné bakalářské práce, byl kladen důraz na poskytnutí především nejdůležitějších informací potřebných pro pochopení celkového principu serverovny a jednotlivých zařízení. V práci se mohou vyskytovat prvky, které jsou věcí osobního názoru a je pouze na čtenáři, zda je bude akceptovat.

Práce je rozdělena do dvou částí. První část se zabývá obecnou problematikou návrhu datového centra a je rozdělena do několika logických celků, které se postupně zabývají návrhem lokality a umístění datového centra, zabezpečením, napájením a chlazením, síťovou infrastrukturou, která je potřebná pro zajištění základních síťových a serverových služeb a nakonec možnostmi návrhu datového úložiště. Druhá část se zabývá již konkrétním řešením, které bylo realizováno ve firmě. Zde bylo využito podobné struktury jako v první části.

Na závěr se pokusím zhodnotit realizované řešení a popsat problémy zjištěné při praktickém provozu a možnosti jejich odstranění.

2 Historie

Na začátku počítačového průmyslu mají své kořeny i počítačová datová centra, která byla většinou využívána pro vojenské účely. Tyto systémy byly umístěny ve velikých počítačových místnostech a brzy se stávaly velice složitými na obsluhu a údržbu. Vzhledem k velmi vysoké pořizovací ceně byla požadována i vysoká bezpečnost těchto center a byla zavedena přísná pravidla pro řízení vstupu k zařízení. K zjednodušení obsluhy a údržby těchto systémů se začaly vytvářet standardizované regály, kabelové žlaby a zdvojené podlahy pro organizaci počítačového zařízení a kabelových rozvodů.

Kolem roku 1980 se začala rychle rozrůstat výroba mikropočítačů, které začaly pronikat do všech odvětví. Tento vývoj měl za následek vznik velkého množství různých „datových center“ většinou s počátečními nízkými požadavky na provoz, které se ovšem postupem času stávaly opět čím dál složitější, čímž značně zvyšovaly i provozní požadavky. V průběhu roku 1990 se začínají mikropočítače nazývat servery a vzniká vztah mezi serverem a mikropočítačem, nazvaný klient-server. V této době začínají být dostupná levná síťová zařízení a společně se servery se začíná vše přesouvat do specializovaných místností. Výraz „datové centrum“ se v té době využíval především pro speciálně konstruované počítačové učebny.

Skutečný rozmach datových center přišel společně s rozvojem internetu po roce 1990, kdy především velké telekomunikační společnosti začínají budovat velké zařízení nazývané Internetová datová centra (IDCs). Tyto společnosti specifikují požadavky na datová centra, na jejich instalaci a provoz. Díky novým technologiím a postupům se začínají rozšiřovat datová centra do všech průmyslových i soukromých oblastí, díky jejich velikému praktickému využití.

V dnešní době jsou datová centra běžnou součástí veškerých možných společností, lze je nalézt prakticky ve všech průmyslových firmách, ve zdravotnictví, ve státní sféře, na školách, v bankovním sektoru a v mnoho dalších organizacích. Datová centra poskytují nepřeberné množství služeb, které lze využít k práci, vzdělání, výzkumu, nebo zábavě a bez jejich existence by nebylo možné využívat například internetu v takovém rozsahu služeb, jak jej známe dnes. [1]

3 Návrh datového centra

Rozhodneme-li se v dnešní době obrovského množství počítačových technologií zrealizovat výstavbu nového, nebo zmodernizovat stávající datové centrum, postavíme se s největší pravděpodobností před velmi nelehký úkol. Finanční investice do takového projektu obvykle bývá velmi značná a je tedy samozřejmou snahou, aby byla co možná nejefektivnější. Z toho důvodu je zapotřebí věnovat návrhu centra velikou pozornost.

S největší pravděpodobností se realizace většího projektu datového centra neobejde bez spolupráce se specializovanou firmou, aby však výsledek projektu dopadl podle našeho očekávání, je dobré mít určitou vlastní představu a přehled o jednotlivých úskalích a možnostech projektu a ty poté za pomocí odborné firmy realizovat.

Rozhodně není možné popsat všechny možné varianty datových center a jejich návrhy, jelikož na každý takový systém jsou kladeny různé požadavky a musí plnit odlišné úkoly. Lze ovšem specifikovat některé parametry a požadavky, které se ve většině případů podobají. Budeme-li se danou problematikou zabývat pouze ze stránky technického hlediska a vynecháme administrativní záležitosti týkající se výběrových řízení, možností dotačních programů, smluv a jim podobných záležitostí, dá se problematika návrhu rozdělit do několika částí.

3.1 Účel a typ datového centra

Prvním krokem při návrhu je ujasnění si účelu, typu a velikosti datového centra. Můžeme definovat tři základní typy datových center, jsou jimi korporátní datová centra (pro vlastní potřebu), nebo hostingová (pronajatá) datová centra, nebo případně mobilní centra.

Mobilní varianta je nejméně častá. Využívá se v případě akutní potřeby datového centra s výhledem na budoucí realizaci stabilního centra, nebo v případech, kdy není možná běžná výstavba. V takovém případě bývají veškeré potřebné komponenty a zařízení umístěny v mobilním kontejneru a mohou v některých případech nahradit i stabilní datová centra pro malé a střední firmy, kdy řeší například problémy týkající se výstavby nové budovy.

Poměrně elegantní řešení nabízí možnost vybudování hostingového datového centra. Tuto možnost nabízejí velké telekomunikační a technologické firmy, které nabízejí pronájem hardwarových a síťových prostředků k provozování vlastní serverovny. Pokud však již disponujeme potřebným hardwarem, je umožněno pronajmutí místa v profesionálně zařízeném datacentru, kam je možné umístit vlastní rackové skříně s vybavením. Spravovat chod takového hostingového centra může buď sám majitel, nebo lze přenechat správcovství specialistům

hostingové společnosti. Tímto způsobem lze tedy provozovat firemní aplikace a služby se špičkovým zabezpečením bez potřeby budování mnohdy velmi nákladných serveroven.

Nejčastějším typem datového centra je však korporátní datové centrum, obvykle vybudované v rámci firmy, organizace, či státní instituce. Tato varianta je obvykle finančně nejnáročnější, vyžaduje vhodné prostory a kvalifikovanou obsluhu, umožňuje ovšem vybudování datového centra přesně podle představy a potřeb jejího provozovatele.

Každá serverovna slouží k jinému účelu a vyžaduje různý přístup k zabezpečení. Je zapotřebí si určit, jak vysoká musí být míra zabezpečení centra, kolik vlastních a cizích uživatelů, nebo firem bude mít přístup do prostorů datového centra a bude se v rámci serverovny pohybovat a jak moc citlivá data se zde budou nacházet. Z toho je následně zapotřebí vycházet při celkovém návrhu všech bezpečnostních prvků, které budou v datovém centru využity.

Dalším důležitým parametrem je předpokládaná velikost centra. Zajímá nás především, jaké bude obsahovat množství zařízení, kolika uživatelům bude poskytovat služby a jakého charakteru dané služby budou a jaký je předpoklad růstu centra v následujících letech. Především otázku růstu společnosti je zapotřebí dostatečně diskutovat s managementem firmy, jelikož tento parametr je velmi důležitý především pro zajištění dostatečného napájení, navržení dostatečně rozšiřitelného systému s dostatečně velkou a škálovatelnou diskovou kapacitou a možností zajištění dostatečného chlazení i v následujících letech. V neposlední řadě je třeba myslet a i na dostatek prostoru v případě rozšíření serverovny o další rackové skříně. [2]

3.2 Umístění datového centra

Návrh umístění datového centra lze rozdělit do dvou kategorií. První kategorií je návrh lokality, ve které bude umístěna budova a druhou kategorií je umístění serverovny v budově. Ve většině případů je již lokalita daná, kdy se serverovna buduje v rámci podniku, či organizace a je k její stavbě využito volných prostor, avšak v některých případech, je výstavba serverovny spojena i s výstavbou, nebo výběrem nového objektu, ve kterém se bude serverovna nacházet.

3.2.1 Návrh lokality

V případě výstavby, nebo výběru nového objektu, je zapotřebí se při výběru vhodné lokality zaměřit na určitá kritéria, která by měla daná lokalita splňovat. V první řadě je zapotřebí zjistit dostupnost inženýrských sítí, kdy je důležité věnovat pozornost distribuci elektrické energie a dostupnosti připojení serverovny k síti internet. V případě elektrické energie je za-

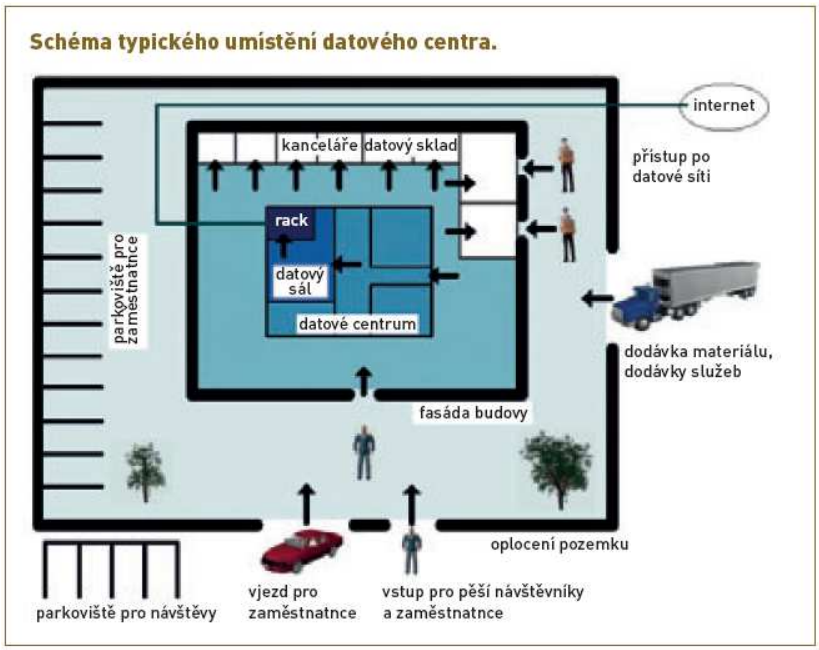
potřebí v tomto momentě znát přibližný elektrický příkon datového centra a ověřit, zda výkon transformátoru má dostatečnou rezervu i pro případ rozšíření serverovny v následujících letech. Dále ověříme počet a parametry silových přívodů. Při ověřování dostupnosti připojení k internetu je dobré zjistit možnosti připojení pomocí optické sítě, případně možnosti bezdrátového připojení.

Při určení lokality je také velmi důležité ověřit různá bezpečnostní rizika. Především je potřeba se vyhnout pokud možno záplavovým oblastem, kde hrozí riziko povodní a místům se zvýšeným výskytem nebezpečných jevů (především požáry, otřesy, sesuvy půdy, častý výskyt vichřic). Zjišťujeme i vzdálenost a dojezdovou dobu policie, záchranné služby, hasičů možnosti napojení požární signalizace na centrální dohledový systém hasičů. Dojezdová doba hasičů nám pomůže vhodně navrhnout objem zásobníků hasiva, aby v případě požáru dostačovalo do jejich příjezdu. Dále je vhodné ověřit předchozí využívání lokality, zda není například v místě bývalých dolů, zda není kontaminována zemina například předešlou chemickou výrobou a zda se v blízkosti nenacházejí potenciální cíle teroristických útoků například letiště, výškové budovy apod. Podle účelu, ke kterému bude serverovna sloužit je také vhodné při výběru lokality zohlednit dostupnost městského centra, například pro zákazníky, nebo naopak v případě požadavků na utajení vyhledat diskrétní umístění. Je také zapotřebí brát v úvahu dopady datového centra na okolí, kdy je zapotřebí zohlednit případné limity hluku a z klimatizačních jednotek, nebo zplodin z motorgenerátorů v blízkosti obytných objektů, zdravotnických zařízeních atd. [2]

3.2.2 Návrh místnosti v budově

Při výběru vhodného umístění serverovny v budově je zapotřebí vycházet z předpokládané velikosti serverovny. U větších serveroven je vhodné rozdělit serverovnu na dvě části a ty umístit do různých požárních zón v budově. V ideálním případě toto rozdělení provedeme v rámci dvou od sebe vzdálených budov. V případě využití záložních zdrojů elektrické energie, kterými mohou být motorgenerátory, velké UPS (Uninterruptible power supply) a baterie, je zapotřebí zajistit vhodné místnosti, u kterých dbáme na dostatečné nosnosti podlah, šířce a zatížitelnosti přístupových tras. U serverových místností počítáme s celkovým zatížením veškerého technologického zařízení včetně zdvojených podlah. Prostor musí disponovat také dostatečnou výškou, aby při použití zavěšených podhledů a dvojité podlahy, dosahovala výška minimálně 210 cm. Pro splnění bezpečnostních požadavků je zapotřebí posoudit možnosti únikových tras.

Další součástí celkového návrhu je určení vhodného umístění zhášecích nádob, klimatizačních jednotek, kanceláře personálu, či operátorského stanoviště. Je zapotřebí brát v úvahu i potencionální hrozby, kterými mohou být například voda z přívalových dešťů, nebo z kuchyně či umývárny, zpětný tok odpadních vod, nebo obtížné odvětrávání plynu, či kouře. Na obr. č. 1 je schéma typického umístění datového centra v budově.[2]



Obr. č. 1 – Typické umístění datového centra v budově

3.3 Určení úrovně zabezpečení

„Bezpečnost IT má mnoho podob. IT, to je vše od programového kódu (aplikace) přes technické vybavení (servery, datová úložiště, kabely) až po prostředí, kde je technika umístěna (datové sály, objekt datového centra). Vedle datové a softwarové oblasti, která se týká informačních toků při provozu IT zařízení, k bezpečnosti IT rovněž patří fyzická ochrana hardwarových prostředků, která se mnohdy podceňuje. Průzkumy a statistiky však ukazují, že opomenutí řádného fyzického zabezpečení se velmi výrazně podílí na bezpečnostních incidentech IT – patří sem poruchy hardwaru, chyby obsluhy, krádež zařízení nebo dat, vnitřní nepovolený přístup, zneužití zařízení, přírodní katastrofa, požár a další jevy. Principiálně se jedná o narušení technických prostředků v místě jejich instalace.“[3]

Zabezpečení bezproblémového chodu hardwarových zařízení – k zajištění bezpečnosti bezproblémového chodu hardwarového zařízení, je zapotřebí navrhnout kvalitní infrastrukturu napájení bez rušivých signálů, zajištění optimální teploty a vlhkosti v rackových skříních a v místnosti. Dále je zapotřebí zajištění ochrany proti dalším rušivým vlivům, například elektromagnetického záření. Tyto zařízení se souhrnně označují zkratkou *NCPI* (Network Critical Physical Infrastructure), neboli síťová kritická fyzická infrastruktura.

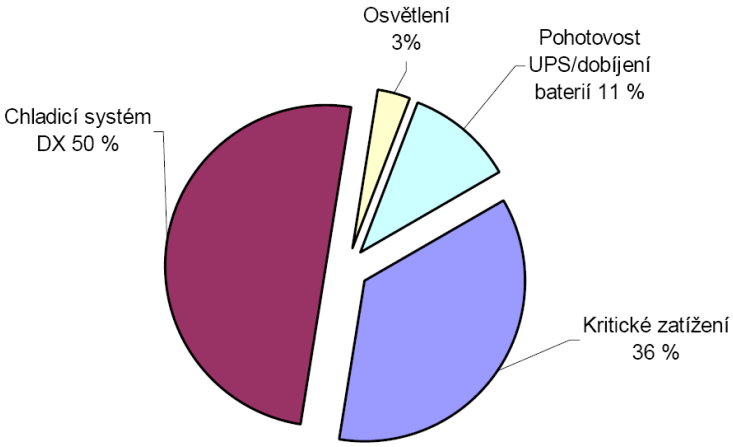
Fyzická bezpečnost hardwarového zařízení – v této oblasti bezpečnosti je zapotřebí eliminovat především možnost krádeže zařízení, nebo mnohdy cennějších dat. Dalším nebezpečím mohou být chyby obsluhy, zneužití zařízení, nepovolaný přístup osob, požár či jiná přírodní katastrofa.

Datová a softwarová bezpečnost – tato oblast je obvykle vnímána jako hlavní zdroj hrozeb pro datová centra. Zde je zapotřebí navrhnout ochranu proti počítačovým virům, spamu, softwarovým chybám, chybám sítí LAN a WAN, vnějšímu nepovolenému přístupu a zneužití dat. [2]

3.4 Napájení a chlazení datových center

3.4.1 Napájení

Jednou z velmi důležitých součástí návrhu serverovny je vybudování kvalitní napájecí a chladící infrastruktury. V případě větších serveroven je zapotřebí spočítat předpokládaný maximální příkon serverovny, který by neměl přesáhnout 75 % výkonu transformátoru, z kterého serverovna bude napájena, z důvodu zajištění dostatečné životnosti transformátoru. V ideálním případě je výhodné mít serverovnu napájenou dvěma na sobě nezávislými silovými kabely, pro případnou redundanci napájení. Do výpočtu celkového příkonu je třeba zahrnout veškeré spotřebiče, kdy sice největší část energie spotřebují chladící zařízení a IT zařízení, ale je zapotřebí počítat s napájením osvětlení v serverové místnosti, s telefonní ústřednou, požárními ventilátory, evakuačními výtahy atd. S těmito zařízeními je zapotřebí počítat i v případě návrhu hierarchie připojených zařízení na záložní zdroje. Obvyklé rozložení celkové zátěže napájení jednotlivými druhy zařízení je na obr. č. 2.



Obr. č. 2 – Rozdělení požadavků datového střediska na elektrickou energii

K dostatečnému zajištění ochrany systému proti výpadku napájení je zapotřebí záložních zdrojů. Tuto roli plní záložní zdroje UPS a motorgenerátory. Zařízení UPS by mělo vydržet napájet kritická zařízení minimálně po dobu dvaceti minut, případně do spuštění motorgenerátorů.

Při výběru UPS záložního zařízení je možné vybírat z pěti různých typů, kterými jsou ***offline***, ***line interaktiv***, ***offline s izolačním transformátorem***, ***online s dvojí konverzí***, nebo ***online s delta konverzí***.

Nejjednodušším z těchto typů je UPS typu offline. Tento typ je však pro využití na místě záložního zdroje v serverovnách nevhodný a využívá se jako záložní zdroj osobních počítačů. V případě malých podniků, webových a střediskových serverů, bývá nejčastěji navrhován typ line interaktivní, který je výhodný pro svojí nízkou cenu a vysokou účinnost, avšak není nevhodný pro oblast výkonu nad 5kVA. Ve výkonové oblasti mezi 3-15kVA je možné použít typ UPS offline s izolačním transformátorem, který se vyznačuje vysokou spolehlivostí a výbornou filtrací, tento typ je však značně nestabilní při použití s moderními počítači. Pro střední a velké serverovny je možno vybírat ze dvou zbývajících typů online, a to buď s dvojí konverzí, nebo s delta konverzí. Výhodou typu s dvojí konverzí je snadné použití při paralelním zapojení, typ s delta konverzí zas vyniká vysokou účinností a snižuje energetické náklady v rozsáhlých instalacích. Oba typy se dále vyznačují výbornou úpravou napětí a jsou vhodné pro provozování ve výkonové oblasti nad 5kVA, jelikož provoz pod touto hranicí je značně nehospodárný. [4]

Při návrhu motorgenerátoru, je zapotřebí znát potřebný příkon všech spotřebičů, které bude motorgenerátor v případě výpadku proudu napájet. Pro případ plánovaného rozšíření

serverovny, je vhodné volit motorgenerátory s dostatečnou výkonovou rezervou. Dalším důležitým parametrem je spotřeba paliva a objem palivových nádrží, které nám určují dobu, po kterou budou schopny motorgenerátory dodávat potřebnou elektrickou energii bez zásahu obsluhy.

Aby bylo využití záložních zdrojů co nejefektivnější, je zapotřebí rozdělit jednotlivá elektrická zařízení podle úrovně zabezpečení do čtyř skupin:

„Kritická zařízení napájená ze zdroje UPS – jde například o IT zařízení v datovém sále, datové knihovny, prvky pro síťovou konektivitu. U těchto zařízení předpokládáme, že mohou být provozována všechna najednou (soudobost 1,0).

Ostatní zařízení napájená ze zdroje UPS – například osvětlení v datovém sále, zálohovaný rozvod napájení pro kanceláře, zařízení mající vlastní nouzovou baterii – přístupový systém, ústředna SHZ, telefonní ústředna, nouzové osvětlení atd.

Zařízení napájená z náhradního zdroje elektrické energie (z motorového generátoru) – např. záložní zdroj UPS včetně výkonových ztrát a výkonu potřebného pro nabíjení baterie, stejnosměrné napájecí systémy, klimatizační jednotky pro datový sál, kompresory, čerpadla, ventilace, požární technologie-evakuační výtahy, požární ventilátory atd.

Nezálohovaná spotřeba budovy – elektrický příkon zařízení mimo datový sál (zátěže uvedené v bodech 2, 3, 4) počítáme se soudobostí podle předpokládaného využití příslušných skupin zařízení (osvětlení místností, výtahy, klimatizace kanceláří apod.).“ [5]

Díky tomuto rozdělení předejdeme, v případě výpadku napájení, zbytečnému plýtvání drahocennou energií, kdy nám nebude například klimatizace kanceláří, či jejich osvětlení, zkracovat dobu běhu kritických zařízení využívajících záložních zdrojů. Především u středních a velkých datových center je vhodné vybudovat kompletně redundantní systém napájení, kdy po celé trase tohoto systému napájení nesmí vzniknout žádné místo, které by nemělo vytvořenou záložní alternativu, označované jako SPOF „Single Point of Failure“ – selhání v jediném bodě.

3.4.2 Chlazení

Většina elektrické energie, kterou spotřebovaná IT zařízením se přemění na teplo. Toto teplo je zapotřebí odvést od zařízení pryč a zajistit přívod chladného vzduchu, aby byla zajištěna ochrana zařízení proti možnosti jeho přehřátí. Pro serverové místnosti je doporučené teplotní rozmezí 20 – 25 °C s vlhkostí 40 – 45 %.

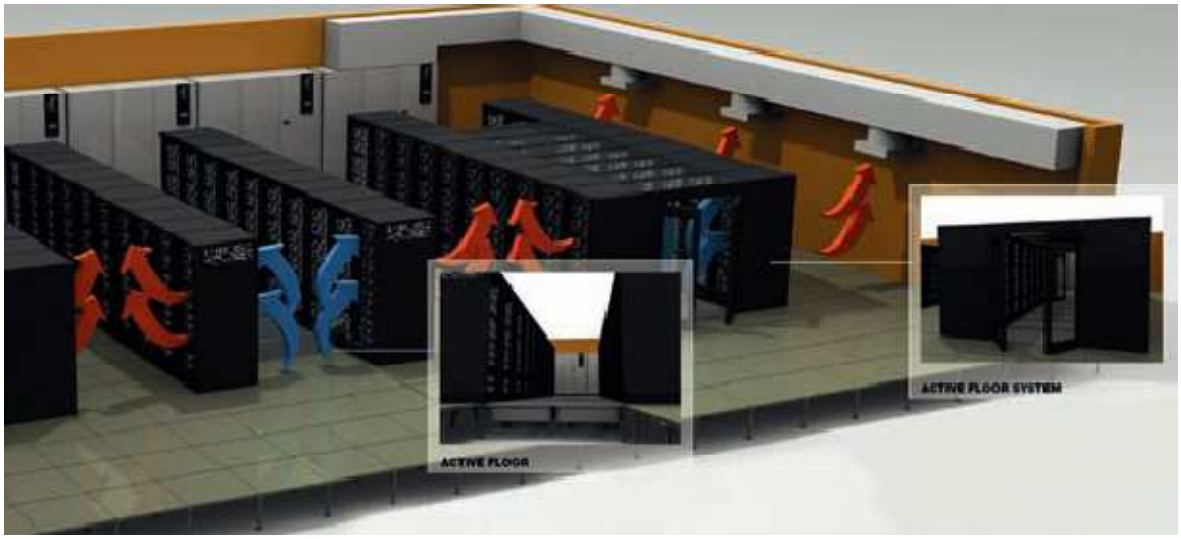
Při návrhu chlazení je rozhodující velikost a hustota IT zařízení v místnostech a stojanech. Při návrhu chlazení je zapotřebí se zaměřit na pět oblastí:

3.4.2.1 Průtok vzduchu ve stojanu

S touto oblastí chlazení se musíme zabývat jak u malých, tak i velkých datových center. V případě velké hustoty zařízení v rackové skříni je důležité zvolit skříň umožňující dostatečný průchod vzduchu, kdy například nevhodně navržené umístění jednotek PDU(power distribution unit) může tomuto průchodu zabraňovat. Kvalitní rackové skříně jsou vybaveny flexibilními vzduchovými přepážkami, které zabraňují zpětnému toku vzduch ze zadní části do přední. Dalším důležitým prvkem je například kartáčové těsnění otvorů pro kabeláž umístěných pod stojanem, zajišťující stálý tlak ve stojanu. Při výběru stojanu je také třeba klást důraz na dostatečnou hloubku stojanu, kdy příliš mělké stojany neumožňují kvalitní cirkulaci vzduchu způsobenou například překážejícími kabely. Přední a zadní dveře stojanu je vhodné volit perforované oproti méně vhodným skleněným dveřím.[4]

3.4.2.2 Rozmístění stojanů

Další důležitou oblastí, především ve velkých serverovnách, je rozmístění stojanů v místnosti. V případě menších serveroven, kde je umístěno pouze pár stojanů, stačí zajistit, aby proudil chladný vzduch k nasávací straně stojanů a ze strany vyfukovací byl odveden teplý vzduch tak, aby se pokud možno nemísil s nasávaným vzduchem. K tomu většinou stačí správné umístění klimatizační jednotky. U větších serveroven je problém o něco složitější, jelikož počet skříní může dosahovat několika desítek a je zapotřebí docílit efektivního a rovnoměrného chlazení všech těchto skříní. Nejosvědčenější způsob vychází z použití systému teplých a studených uliček, kdy jsou stojany postaveny do jednotlivých řad tak, aby byly nasměrovány do uličky proti sobě buď stranami vyfukovacími, nebo nasávacími, jak je naznačeno na obr. č. 3. [4]



Obr. č. 3 – Princip teplých a studených uliček

3.4.2.3 Určení vhodné polohy větracích otvorů

Aby byla zajištěna co nejvyšší efektivita větracích otvorů, je zapotřebí umístit vyfukovací větrací otvory pokud možno co nejblíže k nasávacím otvorům zařízení a zajistit udržení studeného vzduchu ve studených uličkách. V případě stropního rozvodu je zapotřebí zajistit vyfukování studeného vzduch kolmo do studených uliček, nikoli do boku. Byla-li zvolena varianta s podpodlahovým rozvodem, umístíme děrované dlaždice pouze do studených uliček. V případě umístění výdechových otvorů v místě, kde není v provozu žádné zařízení, je zapotřebí tyto otvory uzavřít z důvodu zamezení návratu vzduchu do chladícího zařízení s nižší teplotou, čímž se nám může zvýšit odvlhčování a snížit výkonnost chladícího zařízení.

Pro rozmístění nasávacích otvorů teplého vzduchu platí prakticky stejná pravidla, jen se jejich umístění nebude týkat studených uliček, ale uliček teplých. [4]

3.4.2.4 Nastavení chlazení

Při návrhu chlazení je zapotřebí předem určit, jakým způsobem bude regulováno chladící a zvlhčovací zařízení. Problémy mohou nastat především při použití chladících jednotek, které používají vlastní řízení vlhkosti, kdy může docházet k situacím, že do různých chladících jednotek je nasáván vzduch s rozdílnou teplotou a vlhkostí. V tomto případě může nastat případ, kdy jedna jednotka začne vzduch zvlhčovat a druhá odvlhčovat. Tím dochází ke značnému plýtvání elektrické energie a vody. Tento problém lze vyřešit centrálním řízením vlhkosti, nebo koordinací řízení vlhkosti mezi chladícími jednotkami. [4]

3.4.2.5 Rozložení příkonů

Dalším faktorem, který je dobré při návrhu chladicího systému zohlednit, je rozložení příkonu jednotlivých stojanů. Návrh je zapotřebí realizovat tak, aby bylo zamezeno koncentraci například výkonných serverů v jednom, nebo několika vedle sebe postavených stojanech. Tyto stojany nám budou v takovém případě vyzařovat více tepla než stojany ostatní, čímž nám může vzniknout teplé místo, k jehož uchlazení by bylo zapotřebí celkového navýšení výkonu chladicího systému. Tento výkon ovšem nebude v ostatních částech dostatečně využit a bude docházet ke zbytečnému plýtvání. [4]

3.5 Návrh infrastruktury IT technologií

Všechny předešlé kroky návrhu jsou potřebné k zajištění bezpečného a bezproblémového chodu samotných IT technologií, které jsou klíčovým prvkem datových center. Stejně jako při stavbě osobního počítače je základem výběr správné základní desky, která nám zajistí efektivní a bezproblémové propojení všech komponent, je pro datové centrum základním stavebním pilířem síťová infrastruktura.

Návrh celkové síťové infrastruktury můžeme rozdělit na tři části, kterými jsou pasivní prvky, aktivní prvky a servery. Jednotlivé části jsou na sobě do jisté míry závislé, s čímž je zapotřebí při návrhu počítat.

„Rozhodneme-li se vytvořit si vlastní počítačovou síť, musíme se nejdříve rozhodnout, který síťový standard zvolíme. Každý standard přesně specifikuje použitelnou topologii, způsob a rychlost komunikace v síti. Nejčastěji používaným je dnes Ethernet, v některých případech však lze použít, Token Ring, ATM, 100VGA, Arcnet nebo další...“ [6]

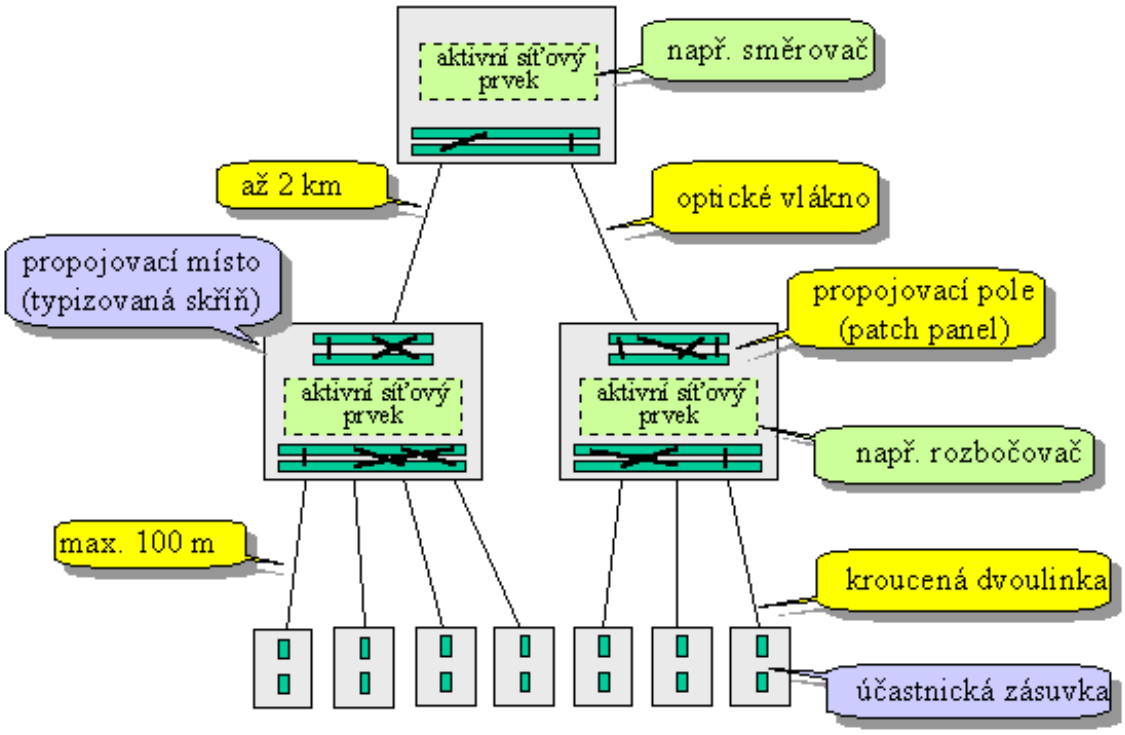
Nejdůležitějšími požadavky na síťovou infrastrukturu jsou především vysoká spolehlivost, propustnost, bezpečnost a modularita.

Vysoké spolehlivosti lze dosáhnout především pořízením kvalitních prvků a to jak aktivních, tak pasivních a dále redundancí sítě. Vše je samozřejmě zapotřebí navrhovat s ohledem k velikosti centra, kdy v případě malých center, kde síť tvoří pouze pár počítačů a její výpadek nemá takové fatální následky, jako u středních a velkých datových center, není striktně zapotřebí dodržovat například uvedenou redundanci. Chceme-li se ovšem vyhnout problémům například s rušením, či častými výpadky, je zapotřebí zvolit minimálně kabeláž přiměřené kvality o specifikaci alespoň CAT5e.

3.5.1 Pasivní prvky

U středních a velkých datových center je v dnešní době takřka nutnost při budování sítě použít systém strukturované kabeláže.

Strukturovaná kabeláž je univerzální a hierarchicky vybudovaná síť kabelů a pasivních prvků řídící se řadou norem a doporučení. Výhodou strukturované kabeláže je především dlouhá životnost, snadná rozšiřitelnost, univerzálnost a vysoká přenosová rychlost. Životnost kabeláže je zajištěna určitými postupy a normami, které specifikují, jakým způsobem musí být jednotlivé rozvody realizovány (např. rádius ohybu UTP kabelu nesmí být menší než čtyřnásobek jeho průměru) a kvalitou použitých prvků. Struktura kabeláže mívá obvykle stromový charakter, kdy základ tvoří obvykle páteřní síť, která obvykle propojuje jednotlivá patra budov, jednotlivé budovy, nebo pobočky. Páteřní síť je realizována ve většině případů pomocí optických kabelů, které jsou připojeny do aktivních prvků jednotlivých částí sítě, které tvoří samostatné moduly celé struktury. Další rozvody realizované obvykle v rámci jednoho patra budovy, jsou tvořeny UTP kabely, kdy udávaná délka kabelu by neměla přesáhnout 90 m, rozvody optikou jsou vzhledem k vysokým nákladům méně časté. Místo kabeláže lze využít i bezdrátového přenosu, což bývá obvykle nejlevnější metoda, v jejíž neprospěch ovšem mluví nízký dosah signálu uvnitř budov a nižší kvalita linky. Jelikož je model strukturované kabeláže univerzální, lze s její pomocí vytvářet různé topologie sítě a lze využít i jako telefonní síť, což může značně spořit náklady. Strukturovaná kabeláž se vytváří značně předimenzovaná, může se tedy zpočátku zdát výše investice do strukturované kabeláže vysoká, rozhodně se však do budoucna tato investice vyplatí, jelikož na rozdíl od většiny ostatních prvků má kabeláž životnost i několik desítek let. [7]



Obr. č. 4 – Topologie strukturované kabeláže

3.5.2 Aktivní prvky

Další součástí síťové infrastruktury jsou aktivní prvky. Zde je opět rozhodující velikost zamýšlené sítě a počet uživatelů. V případě malé sítě čítající několik připojených zařízení si ve většině případů, vystačíme s volně stojícími desktopovými aktivními prvky. Příkladem může být například kancelář, nebo domácnost o více počítačích propojená pomocí jednoho zařízení, které v sobě integruje jednoduchý router, switch a případně firewall. V případě středních a velkých center už musíme volit aktivní prvky montované do rackových skříní, které jsou vybaveny systémy pro organizaci kabelů, zajišťující jejich přehlednost a systémem chlazení, jelikož i tyto prvky jsou zdrojem tepla.

Mezi základní aktivní prvky patří především routery, firewally a switche. Některá z těchto zařízení, například router, nebo firewall, mohou být realizovány, buď softwarově za pomocí služby běžící na některém serveru, nebo hardwarově pomocí specializovaného zařízení. Hardwarové řešení obvykle poskytuje vyšší výkon a kvalitu poskytovaných služeb, což je ovšem vykoupeno vyššími finančními nároky. Výběr aktivního prvku závisí na mnoha sku-

tečnostech a je zapotřebí pečlivě zvážit, které funkce a parametry od aktivních prvků očekáváme.

Jedním z nejdůležitějších parametrů těchto zařízení je jejich propustnost. Zde je zapotřebí, aby prvky splňovaly doporučené rychlostní standarty. Pro páteřní síť je v dnešní době doporučeno využívat rychlosti 1 Gb/s a vyšší a pro připojení koncových zařízení alespoň 100Mb/s. S tím souvisí například i možnost zvážení výběru switchů, které jsou vybaveny optickými porty, což může ušetřit následnou potřebu koupě media konvertorů, které jsou zapotřebí při změně metalického vedení na optické a naopak.

V případě velkých sítí volíme zařízení s dostatečnou úrovní správy a možností monitoringu. Pokud to finanční možnosti umožňují, upřednostníme zařízení s podporou protokolu SNMP (Simple Network Management Protocol). Tento protokol umožňuje komunikace mezi zařízením a softwarem pro vyhodnocování údajů z těchto zařízení a jejich správu. Oblíbený softwarem pro toto využití může být například open source systém Nagios. Levnější variantou správy, je možnost konfigurování zařízení pomocí webového rozhraní, nebo pouze pomocí sériového portu RS232. Taková zařízení lze doporučit spíše v případě menších sítí, nebo při omezeném finančním rozpočtu.

Dalším kritériem výběru je úroveň bezpečnosti, kterou prvky poskytují. Zde jde především o možnosti šifrování, možnosti detekce a prevence narušení označované zkratkou NIPS (Network Intrusion Prevention Systems) a možnosti autentizace. V případě routerů a firewallů, na kterých plánujeme vytvářet VPN tunely, je vhodné se zaměřit především na zařízení s podporou hardwarového šifrování metodou SSL, nebo IPSEC. V případě autentizace je vhodné volit zařízení s řízením přístupu podle standartu 802.1x a s možností nastavení přístupu zařízení podle MAC a IP adresy.

Aktivní prvky mají také různé možnosti napájení. Lze zde volit například zařízení s vnitřním zdrojem, nebo s externím zdrojem. Externí zdroje nalezneme spíše u levnějších variant, lze však pořídit i zařízení obsahující dva integrované zdroje pro možnost redundantního napájení. Další možností je napájení zařízení pomocí ethernetového kabelu, které nese označení PoE (Power over Ethernet). Opačnou možností je možnost napájení jiného zařízení z aktivního prvku, příkladem může být například napájení průmyslové kamery ze switche.

Při výběru switchů určených především pro rozsáhlejší sítě, je vhodné volit switche s možností vytváření virtuálních sítí VLAN, kterými lze vytvářet další virtuální podsítě, umožňující přehlednější členění sítě. Dále zjišťujeme možnosti nastavování jednotlivých portů, zda switch podporuje tzv. QoS(Quality of Service), kdy je možné řídit datové toky na jednotlivých portech. V případě větších sítí, kde je využito redundance síťových cest, je zapotřebí

volit switche s podporou STA (Spanning Tree Algorithm), který zajistí zamezení problémů při vytváření smyček. [8|]

3.5.3 Servery

Návrh serverů v datovém centru je velmi individuální a je velmi složité pro něj stanovit obecná pravidla, jelikož datová centra poskytují různé druhy serverových služeb a mají různé nároky na použitý software i hardware. Z tohoto důvodu, zde uvedu pouze některá obecná pravidla a doporučení k výběru hardware a některé z nejpoužívanějších možných softwarových produktů.

„Na začátku, je důležité určit jakou práci má server zastávat. Je třeba dopředu vědět, jak rychlá linka bude k dispozici, jaká bude návštěvnost, u fileserverů mít představu o množství dat, ... Je také třeba vědět, jaká může být perspektiva do budoucna.

Při výběru hardware i software je vždy dobré myslet na to, že spolehlivost a dostupnost serveru bývá v drtivé většině případů mnohem cennější než extrémní výkon či pokročilé vlastnosti a schopnosti.“ [9]

V případě malých serveroven lze na místě serveru využít například i běžný osobní počítač, v případě větších serveroven je už ovšem vhodné volit značkové serverové sestavy, které zajistí vyšší spolehlivost a dostupnost. Je také zapotřebí zvážit možnosti využití virtualizace, kdy je možné na jednom fyzickém serveru provozovat více serverů virtuálních, což může přinést značné výhody, především v lepším využití výkonu fyzických serverů, možnostech zálohování a obnovy, nebo migrace.

Dalším parametrem při výběru serveru je jeho provedení podle jeho způsobu montáže, či umístění v serverovně. Servery je možno volit ve třech základních provedeních, kterými jsou servery volně stojící (Tower), montované do rackových skříní, nebo bladeové servery. Servery v provedení Tower lze doporučit pouze do menších serveroven, kde není počítáno s velkým počtem serverů. Do větších serveroven čítajících několik serverů je nohem výhodnější volit ze zbylých dvou řešení. V moderních datových centrech, kde se nachází velké množství serverů a je zapotřebí brát v úvahu i velikost obsazeného prostoru servery, je nejvýhodnější použít právě technologie blade, kdy jsou použity ultratenké servery montované do specializovaných blade skříní.

Výběru serverového softwaru, je především závislý na velikosti a účelu datového centra a jím provozovaných služeb. Některé typy těchto služeb jsou však pro většinu datových center shodné. Jedná se především o serverové služby určené pro správu počítačové sítě, síťové

služby, e-mailovou komunikaci, databázové servery a aplikační servery. Nejčastěji jsou tyto služby zajišťovány programy, které jsou určené pro operační systémy Microsoft Windows, nebo Unix/Linux.

Jedním ze základních serverů v každé větší serverovně je doménový řadič, na kterém je provozována část, nebo celá databáze adresářových služeb. K realizaci tohoto serveru je nejčastěji využíván systém Windows Server se službou Active Directory, případně multiplatformním OpenLDAP. Dalším významným systémem pro poskytování adresářových služeb je Novell 's Identity Manager. Na místě doménového řadiče lze také využít Unixový systém Samba, který umožňuje především sdílení souborů a tiskáren mezi systémy Windows a Linux.

V každé síti je zapotřebí zajistit základní síťové služby, kterými jsou především DNS, DHCP, routovací služby, VPN, firewall. Jak bylo popsáno v předchozí kapitole, většinu těchto služeb lze provozovat pomocí serveru, nebo pomocí specializovaných aktivních síťových prvků. Službu DNS lze na systémech Windows zajistit pomocí Windows serveru, případně pomocí programu BIND, který je velmi často využíván i v případě nasazení na Linuxových systémech. Ostatní služby jsou obvykle implementovány v rámci jedné aplikace, jako je tomu například u softwaru Kerio Winroute Firewall, který zabezpečí jak funkci firewallu, tak routovací a VPN služby pro systémy Windows. Pro systémy Linux lze implementovat v roli firewallu například nástroj IPtables, kterým lze vytvořit různé druhy pravidel, či programy na tomto nástroji založené. Pro vytváření VPN lze také využít rozšířený program Open VPN, který lze provozovat na obou systémech. Pro Linuxové systémy lze dále použít například program Poptop, či SSL-Explorer.

Dalšími servery nacházejícími se ve většině datových, centrech jsou poštovní servery a webové servery. Nejčastěji nasazovaným softwarem pro poštovní servery na platformě Microsoft je MS Exchange server. Pro Linuxové systémy jsou to především Sendmail a Postfix společně například s programy Dovecot, SpamAssassin, nebo Amavisd. Pro webové servery je možné využít integrovanou roli Windows serveru IIS, nebo na Linuxu postavený Apache HTTP Server.

3.5.4 Datová úložiště

Posledním nezbytným krokem k návrhu kompletního datového centra je návrh datového úložiště. Při návrhu datového úložiště můžeme vybírat ze tří nejčastěji používaných technologií.

3.5.4.1 DAS (Direct attached storage)

Nejlevnější řešení vhodné pouze pro malé serverovny, kde nejsou kladeny vysoké nároky na kapacitu a škálovatelnost. Datové úložiště zastává prakticky jeden, nebo více serverů, ke kterým jsou připojeny interní, nebo externí pevné disky, případně jiná zálohovací zařízení většinou zapojená do některého druhu pole RAID, díky kterému se jeví více disků jako jeden. K datovému úložišti v tomto případě přistupujeme pomocí serveru. V případě poruchy tohoto serveru se stává datové úložiště pro ostatní zařízení nedostupné, což je značná nevýhoda tohoto řešení. Další nevýhody spočívají v malé rozšiřitelnosti, kdy k jednomu serveru nelze přidávat příliš mnoho zařízení. Tuto nevýhodu lze řešit přidáním dalšího serveru, zde však vznikají další komplikace v zálohování a přenosu dat mezi servery, která značně zatěžuje síť LAN.[1]

3.5.4.2 NAS (Network attached storage)

Z pohledu rozšiřitelnosti a dostupnosti datového úložiště je výhodnější využití technologie NAS. Tato technologie je založena na využití diskových zařízení, která lze připojit přímo do sítě, kdy každé z těchto zařízení disponuje IP adresou. Každé zařízení obsahuje jednoúčelový operační systém, který zprostředkovává komunikaci mezi klientem a diskovým polem. Je-li zapotřebí rozšířit kapacitu úložiště, stačí přikoupit další zařízení NAS a připojit k síti. Je-li ovšem zapotřebí mezi jednotlivými zařízeními provádět zálohování a přenosy dat, vzniká stejný problém, jako v případě technologie DAS a to nadměrné zatěžování sítě. [1]

3.5.4.3 SAN (Storage area network)

Samostatná datová síť určená speciálně pro připojení datových zařízení, kterými jsou disková pole, zálohovací zařízení, nebo páskové knihovny. Tato technologie je v současné době nejčastěji využívána při výstavbě moderních datových center. Pro komunikaci je v SAN nejčastěji využito vysokorychlostního rozhraní Fibre Channel, u levnějšího řešení může být použito iSCSI(Internet Small Computer Systems Interface) rozhraní komunikující přes gigabitový ethernet pomocí TCP/IP protokolu. Tato síť je nezávislá na ostatních sítích a přistupuje se k ní pomocí serverů. Místní zálohování probíhá pouze v rámci této sítě, nezatěžuje tudíž ostatní sítě LAN a WAN. Výhodou těchto sítí je snadná rozšiřitelnost, vysoká spolehlivost a nízké provozní náklady. Nevýhodou je především vysoká pořizovací cena, z tohoto důvodu se využívá především u větších datových center. [1]

4 Realizace serverovny

S velmi rychlým rozvojem informačních technologií a rozvojem firmy se zvyšují i nároky na provozovaná datová a informační centra, která hlavně díky zastaralým technologiím přestávají splňovat výkonové a bezpečnostní požadavky. Do této situace se dostala i naše firma, která se rozhodla pro vytvoření zcela nového datového a informačního centra, které zajistí vysoký výkon v poskytování informačních technologiích uživatelům a maximální možné zabezpečení velmi cenných firemních dat před jejich ztrátou či odcizením.

Dosavadní řešení poskytování informačních technologií ve firmě spočívalo v rozmístění malých serveroven, založených převážně na unixových systémech, do jednotlivých poboček firmy. Tento systém vyžadoval vyšší náklady na zajištění provozu a vykazoval značné nedostatky v zabezpečení dat a možnosti jejich sdílení mezi jednotlivými pobočkami. Z tohoto důvodu bylo rozhodnuto o vybudování moderní centrální serverovny, která umožní poskytování služeb všem pobočkám a zajistí komfort a bezpečnost díky využití moderních technologií.

Prvním krokem k realizaci projektu bylo stanovení základních požadavků, které musí nová serverovna splňovat. Těmito požadavky byly především způsob, jakým budou poskytovány služby uživatelům, rozsah těchto služeb, nároky na úložný prostor a způsob zajištění vysoké bezpečnosti dat a zařízení. Na základě těchto požadavků byla zpracována zadávací dokumentace a vyhlášeno výběrové řízení, ve kterém byla vybrána firma zajišťující dodávku hardware, software a kompletní montáž a zprovoznění datového centra.

4.1 Umístění a zabezpečení serverovny

4.1.1 Výběr lokality

Výběr lokality pro umístění nového datového centra byl v tomto případně značně zjednodušen, jelikož firma disponovala volnými prostory v jedné z poboček, která se nachází v průmyslové oblasti, ve které není vyšší pravděpodobnost živelných pohrom a která disponuje kvalitní energetickou infrastrukturou. Jediným problémem byla dostupnost připojení k optické datové síti, kdy nejbližší přípojné místo bylo vzdálené skoro 1 km a bylo by třeba tento úsek na náklady firmy vybudovat, což znamená značné finanční prostředky a velké časové období pro vyřízení veškerých potřebných formalit. Z tohoto důvodu bylo dočasně využito bezdrátové připojení.

4.1.2 Umístění a zabezpečení serveroven v budově

V našem případě se serverovna skládá ze dvou hlavních částí a to z primární serverovny a sekundární serverovny. Obě tyto serverovny by bylo velmi výhodné umístit do dvou od sebe vzdálených budov, kde by byla zajištěna daleko větší míra bezpečí před současným poškozením a ztrátě dat v obou serverovnách najednou. Tato varianta ovšem nebyla v našem případě možná, proto je jak primární, tak sekundární serverovna umístěna do jedné budovy. Jednotlivé místnosti jsou od sebe vzdálené 150 m a nacházejí se ve dvou různých požárních zónách. Vzhledem k velikosti serveroven a počtu zařízení nebylo zapotřebí výrazným způsobem řešit nosnost stávajících podlah. Místnosti disponovaly dostatečnou výškou a bylo tedy možné bez problémů instalovat dvojité podlahy. Umístění bylo také vybráno s ohledem na možné elektromagnetické rušení z výrobních strojů a obě serverovny jsou od těchto zdrojů rušení v dostatečné vzdálenosti.

Aby bylo zamezeno vstupu do obou serveroven nepovolaným osobám, které by mohly poškodit, nebo zcizit nákladné zařízení, případně cenná data, byly obě serverovny vybaveny bezpečnostními dveřmi. Jelikož se v primární serverovně nachází jedno okno, byla na toto okno namontována ochranná mříž a okno bylo polepeno speciální bezpečnostní folií zajišťující jeho nerozbitnost. Dále je primární serverovna vybavena kamerovým systémem, který je připojen k dohledovému systému NetBotz.

Obr. č. 5 – Bezpečnostní kamera systému NETBOTZ

4.1.3 Dohledovým systém - NetBotz

Aby bylo možné monitorovat ohrožení serverovny, je v primární serverovně instalován dohledový systém NetBotz. Díky tomuto systému je možné včas informovat správce o možných hrozbách, nebo případných problémech, které mohou nastat, a tím případně těmto

hrozbám předejít a včas provést nápravná opatření. V našem případě je použito modelu NetBotz 420, který je vhodný pro malé a střední serverovny. Tento model je vybaven čidly na monitoring teploty, vlhkosti, proudění vzduchu, rosného bodu, a dále je k němu připojena IP kamera, kterou je možno online monitorovat prostor serverovny. V případě detekce pohybu kamerou je zaslána série snímků na administrátorem přednastavené emailové adresy, které mají k dispozici odpovědné osoby pro posouzení, zda se jedná o skutečné riziko, či planý poplach. Tyto osoby jsou dále informovány pomocí SMS zprávy zaslané SMS bránou. Zařízení NetBotz komunikuje pomocí IP protokolu, ale v případě potřeby umožňuje tento systém pojení i k alternativním sítím 802.11a/b/g, GSM/GPRS wireless, dial-up. [15]

Obr. č. 6 – Zařízení NETBOTZ 420

4.1.4 Zhášecí systém

Oddělení serveroven jejich polohou je pouze základní zabezpečení a bylo proto nutné instalovat další systémy na ochranu proti požáru. Hlavní důraz se kladl na zabezpečení primární části, kdy do prostoru serverovny je nainstalován samočinný zhášecí systém. Tento systém hasí na principu kombinace fyzikálních a chemických účinků, kdy prostor je v případě výskytu požáru zaplněn hasící látkou HFC 236fa (hexafluorpropan), která sníží obsah kyslíku ve vzduchu na úroveň, kdy již není umožněno hoření. V místnosti jsou umístěny nádoby s hasivem, které je rozvedeno teplocitnými plastovými hadicemi na nejrizikovější místa, jako jsou rackové skříně a rozvody elektrické sítě. Toto řešení má velkou výhodu oproti dřívějším metodám hašení, jelikož hasící látka nepoškozuje zařízení ani nosiče dat. Zároveň hasící látka není toxická a je dokonce možné se v hašeném prostoru i určitou dobu pohybovat, jelikož v prostoru zbývá přibližně 9 % kyslíku, což je ještě dostatečné množství pro dýchání člověka.

Celý systém je ovládán detekčně spouštěcí, hodnocovací a řídící jednotkou připojenou k samostatnému záložnímu zdroji napájení. K této jednotce jsou připojeny opticko-kouřová a teplotní čidla a v případě požáru spouští tato jednotka akustickou a optickou signalizaci. Při zaplavení prostoru hasivem není vypínána klimatizační jednotka, jelikož v tomto případě není nasáván žádný vzduch z venkovních prostor a klimatizační jednotkou cirkuluje pouze vzduch z místnosti, čímž se urychlí šíření plynu v místnosti. Celý systém je navíc doplněn samočinnými kouřovými hlásiči. [10]

Obr. č. 7 – Požární nádrže s hasící látkou HFC 236fa

Obr. č. 8 – Stropní kouřové hlásiče

4.2 Organizace zařízení, napájení

Pro zajištění přehlednosti a organizace serverů, síťových zařízení, kabelů a napájecích zařízení, je třeba vybudovat kvalitní infrastrukturu s kvalitním zálohovaným napájením. Základním prvkem této infrastruktury jsou čtyři serverové skříně (rack), kdy každá z těchto skříní je vybavena 2 kusy měřených RM PDU(Power distribution unit), což jsou jednotky zajišťující distribuci elektrické energie ve skříních. Tyto jednotky jsou schopné poskytnout 16A výkonu, umožňují zobrazování online informací o průtoku napájení a díky těmto informacím a správným uspořádáním zařízení ve skříni lze docílit rovnoměrného zátěže v jednotlivých v rackových skříních. Další neocenitelnou funkcí je možnost nastavení prahového hodnoty odebírané energie, kdy při překročení této hodnoty je obsluha informována e-mailem.

Obr. č. 9 – Rackové skříně v primární místnosti

Obr. č. 10 – Centrální UPS zařízení

K napájení skříní byly vybudovány dva na sobě nezávislé elektrické okruhy. Každý z těchto okruhů napájí jedno PDU zařízení, přičemž jeden okruh je jištěn navíc centrální, modulární UPS s výkonem 16 kW, která udrží datové centrum v provozu cca 30 minut od úplného výpadku elektrické energie. Toto UPS zařízení se skládá z několika menších modulů vzájemně se zajišťujících, kdy při poruše některého z modulů není ovlivněna funkčnost celého zařízení. Nejdůležitější zařízení ve skříních, kterými jsou především servery, jsou vybaveny dvěma zdroji, kdy každý ze zdrojů je zapojen do jedné PDU.

Jelikož nejsou na serverovnu kladeny nároky 365/7/24 a je při dlouhodobějším výpadku elektřiny akceptovatelná odstávka serverovny, nebyly instalovány záložní motorgenerátory.

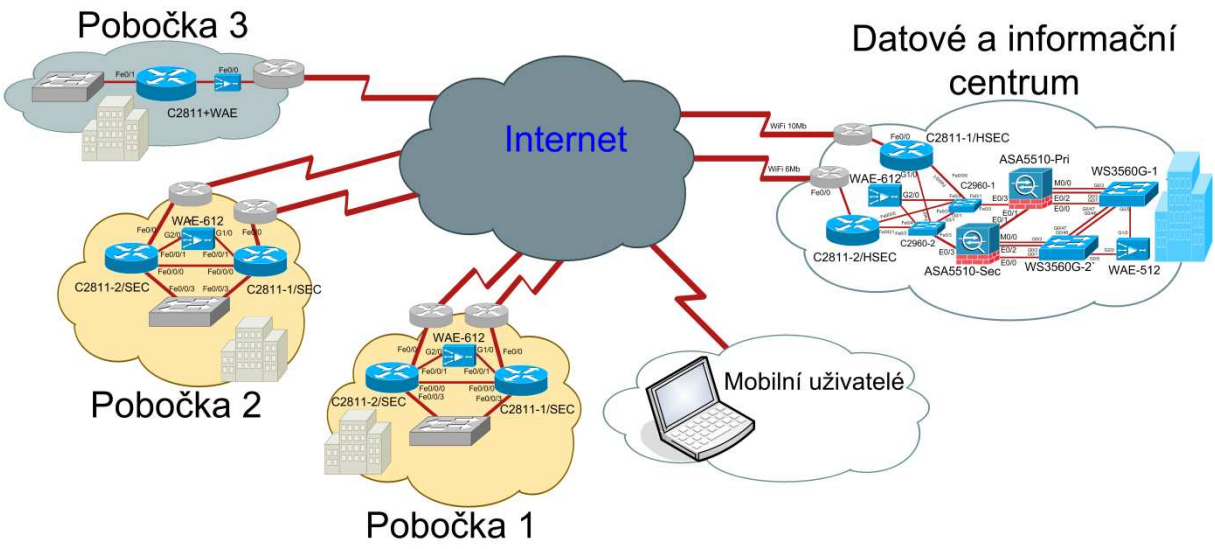
Záložní zdroje byly navrženy pro případ krátkodobějších výpadků, aby bylo umožněno, v případě přerušení napájení, bezpečného odstavení serverovny.

4.3 Topologie sítě

Původní řešení firemní sítě spočívalo v rozdělení celé sítě do několika na sobě nezávislých serveroven umístěných v jednotlivých pobočkách. Správa, komunikace a sdílení informací mezi těmito pobočkami bylo značně komplikované a neefektivní. Tento systém je zcela změněn a veškeré systémy jsou centralizovány na jednom místě a v pobočkách zůstávají pouze prostředky potřebné pro fungování vnitřní sítě.

4.3.1 Propojení datového centra a poboček

Hlavní myšlenka celého systému spočívá v poskytování vzdálené plochy uživatelům, kdy uživatelům je poskytován pouze obraz odpovídající situaci na serveru a od uživatele jsou přenášeny data udávající pohyb myši a informace o stisknutých tlačítkách na klávesnici. Tato komunikace, díky optimalizaci přenášených dat, není příliš náročná na šířku pásma, je zde však zapotřebí počítat s množstvím uživatelů, jejichž počtem se tyto nároky násobí. Pro zajištění plynulosti poskytované vzdálené plochy, je zapotřebí kvalitní linka, která umožní přenosy dat s minimem ztracených paketů a nízkou latencí. V případě nekvalitní linky dochází k časté ztrátě odezvy vzdáleného serveru a práce se stává značně nekomfortní. Z tohoto důvodu byla většina poboček připojena k síti WAN pomocí optické, nebo metalické (DSL) sítě a záložní konektivita byla řešena levnější bezdrátovou technologií v pásmu 10 GHz.

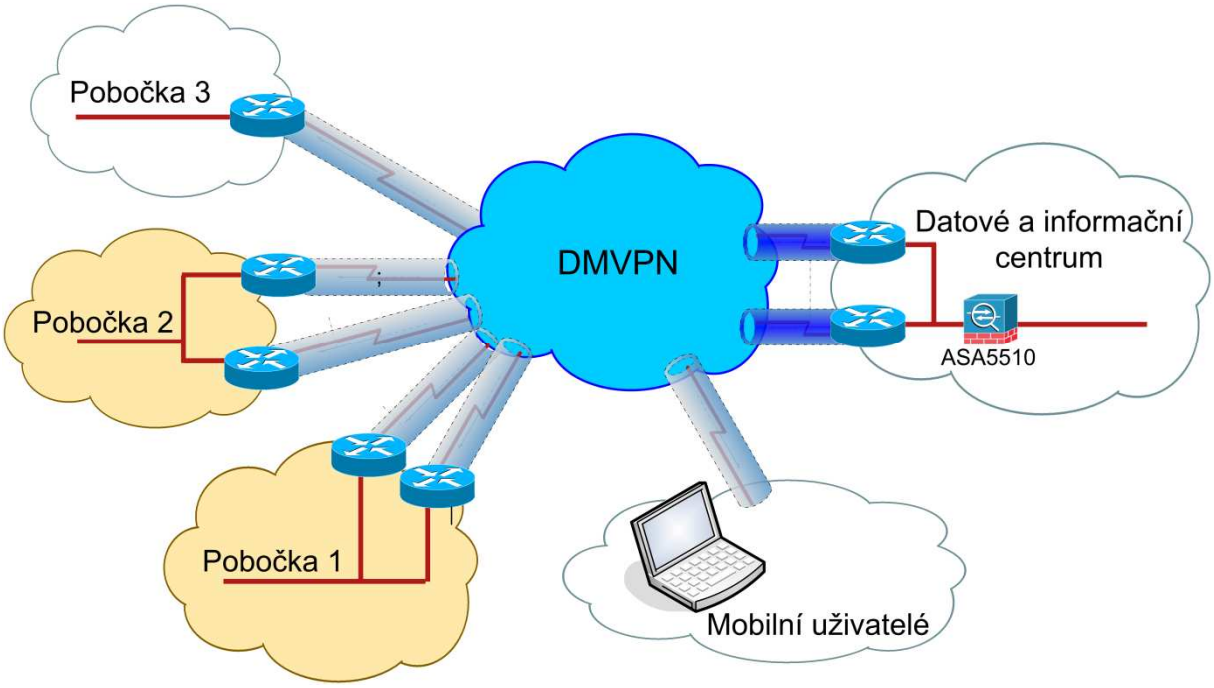


Obr. č. 11 – Propojení datového centra a poboček

4.3.2 VPN (Virtual Private Network)

Připojení poboček k datovému centru, bylo realizováno pomocí sítě WAN a VPN tunelů (Virtual Private Network-virtuální privátní síť). VPN tunely zajistí bezpečnost přenášených dat, podobně jako je tomu u vnitřní sítě LAN. Toho je dosaženo systémem autentizace pomocí certifikátů a šifrováním přenášených dat. Tyto tunely jsou vytvořeny pomocí routerů, jak na straně datového centra, tak na straně poboček, kdy se tento typ připojení nazývá Site-to-Site, nebo také Net-to-Net. Stejným způsobem je praktikováno i připojení uživatelů nacházejících se mimo vnitřní síť, kdy na straně uživatele se o vytvoření tunelu ve většině případů nestará router, ale sotwarový klient. Tento typ VPN tunelu je označován Host-to -Site.

Pro šifrování VPN tunelů je možné využít protokolu SSL (Secure Sockets Layer), nebo IPSec(Internet Protocol Security), využito bylo druhé možnosti z důvodu vyššího zabezpečení.

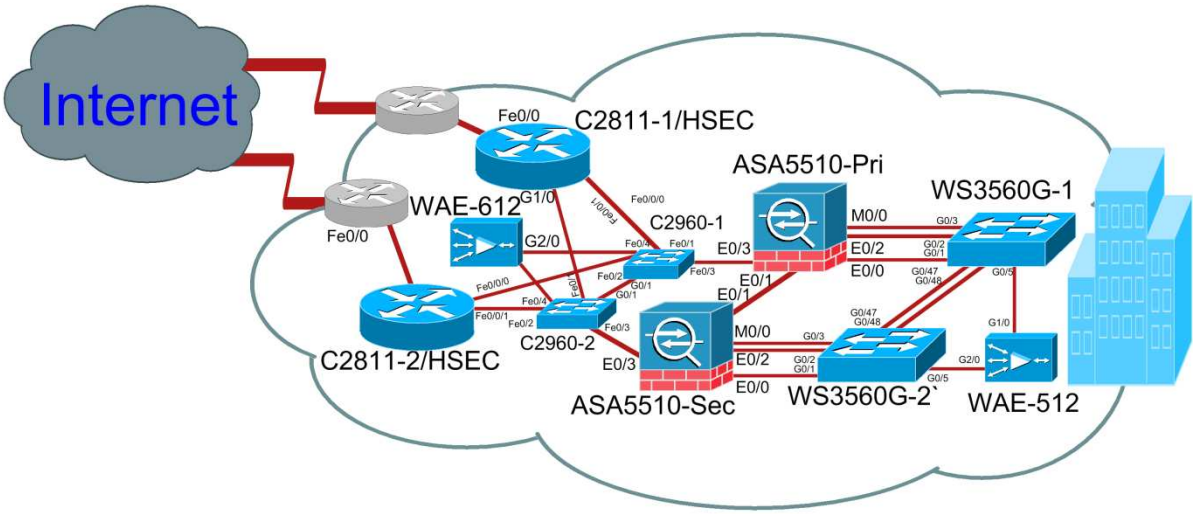


Obr. č. 12 – Schéma VPN tunelů

4.4 Topologie datového centra

Největší požadavky na kvalitu připojení k síti internet jsou samozřejmě kladeny na datové centrum, které je do sítě internetu připojeno pomocí dvou na sobě nezávislých symetrických internetových vedení s šířkou pásma 10Mb a 6Mb od dvou různých ISP (Internet Service Provider-poskytovatel internetového připojení).

Každé z těchto internetových připojení je přivedeno do jednoho ze dvou routerů (směrovačů) firmy Cisco C2811-1/HSEC, které zajišťují směrování paketů mezi sítí WAN a LAN a dále realizují VPN spojení. Tento typ routerů je výkonově vhodný pro menší až středně velké podniky, podporují kompletní sadu přenosových protokolů a vysoké zabezpečení komunikace. Tyto routery jsou dále zapojeny do dvou osmiportových switchů (přepínačů) Cisco C2960, které mají na starosti propojení routerů, firewallů a zařízení WAE612 .Všechna tyto zařízení se vyskytují v celém zapojení dvakrát. To je zapotřebí pro zajištění redundance z důvodu možné poruchy, či výpadku jednoho ze zařízení. V takovém případě přebírá veškerou komunikaci zařízení druhé a vždy je zajištěna záložní cesta pro přenášená data.



Obr. č. 13 – Topologie datového centra

4.4.1 WAE612,WAE512

Jak je patrné z obrázku č. 13, je ke switchům C2960 dále připojeno zařízení WAE-612. Jeho primárním úkolem je zajištění optimalizace přenášených dat po síti WAN a snížení nároků na šířku pásma internetového připojení. Toto zařízení v sobě obsahuje počítač s 3GHz procesorem Pentium 4, 2GB paměti SDRAM, 146GB SAS pevným diskem a může na něj být nainstalována jedna ze tří možných aplikací. Těmito aplikacemi jsou ACNS(Application and Content Networking System), WAAS(Wide Area Application Services), nebo WAFS(Wide Area File Services).

ACNS – tato aplikace je určena pro optimalizaci přenosu digitálních médií. Jedná se především o optimalizaci videí přenášených při videokonferencích, přenosech streamovaného videa, nebo e-lerningu, kdy je možné s vysokou kvalitou sledovat i dlouhotrvající video.

WAAS – aplikace WAAS je primárně určena pro optimalizaci a zvýšení efektivity při poskytování firemních aplikací uživatelům.

WAFS – aplikace určená pro optimalizaci přenosu souborů a souborových systémů, která se využívá při poskytování firemních dat a při zálohování.

V našem případě bylo využito technologie WAAS, jelikož serverovna je primárně určená pro poskytování aplikací a vzdálené plochy. Stejnou funkci jako zařízení WAE612 má i

zařízení WAE512, které je však určeno pro optimalizaci provozu po vnitřní síti LAN a jediný rozdíl najdeme pouze v absenci pevného disku, který plní u zařízení WAE612 funkci mezi-paměti. [11]

4.4.2 ASA5510,WS3560G

Mezi routery a switche WS3560G jsou zapojená redundantně dvě zařízení ASA5510, ve kterých je integrována řada bezpečnostních služeb, zajišťujících bezpečnou komunikaci a mezi sítí WAN a vnitřní sítí LAN. Jednou z nejdůležitějších funkcí je velmi výkonný firewall s propustností až 300 Mb/s, který je možno provozovat v podobě až pěti virtuálních firewallů. Toto zařízení je konfigurováno přes grafické rozhraní, které poskytuje pokročilé monitorovací funkce udávající přehled o stavu zařízení a firewallu.

Posledním zařízením podílejícím se na zprostředkování komunikace mezi uživateli a servery, zůstávají dva konfigurovatelné přepínače (switch) WS3560G.Tyto dva přepínače disponují 48 1Gbitovými porty RJ-45 a čtyřmi 1Gbit SX pro vláknovou optiku. Do těchto zařízení jsou redundantně připojeny všechny servery, virtuální cluster, skupina terminálových serverů a diskové pole SAN. [11]

4.5 Servery

4.5.1 Rozdělení serverů

Nejdůležitější částí serverovny jsou samozřejmě servery. V našem případě můžeme servery rozdělit na dvě kategorie a to servery fyzické (tzv. železa) a servery virtuální. Fyzické servery dále můžeme rozdělit do tří skupin a to na Citrixovou farmu,VMware cluster a Backup (zálohu).

Fyzické servery

Citrixová farma – obsahuje šest fyzických serverů s nainstalovaným operačním systémem Windows server 2008 standart edition 32bit a systémem Citrix XenApp Server.

VMware cluster – je tvořen třemi fyzickými servery, které jsou určené k virtualizaci serverů pomocí systému VMware ESX. Tyto fyzické servery poskytují hardwarové prostředky celkem devíti virtuálním serverům.

Backup server – jeden fyzický server určený ke správě zálohovacích procesů a skriptů.

Obr. č. 14 – Fyzické servery a konzole pro management

Virtuální servery

Na šesti virtuálních serverech je nainstalován operační systém Windows server 2008 enterprise 64bit, kdy dva z nich zastávají funkci doménové řadiče a tiskového serveru, dva jsou využity pro poštovní služby s nainstalovaným Exchange serverem, jeden server databázový na kterém je provozován systém MS SQL Server 2005, a na posledním je provozován Microsoft Office SharePoint Server 2007.

Na jednom, ze zbylých tří serverů, je na linuxovém operačním systému Fedora 12 provozován Proxy server, další linuxový stroj s distribucí CentOs, je využit na provozování monitorovacího a vizualizačního systému Nagios a poslední z virtuálních strojů je aplikační server běžící na systému Windows server 2003 standart edition 32bit.

4.5.2 Virtualizace-VMware ESX

Aby bylo možné lépe využít fyzických serverů a snížit tak jejich počet, tím pádem i finanční náklady, bylo využito možnosti virtualizace serverů. Virtualizace nám umožňuje provozovat několik virtuálních strojů na jednom fyzickém serveru, čím lze docílit lepšího využití jeho výkonu. Virtuální stroje jsou velmi snadno přenositelné a lze využívat na stejném hardwaru rozličná prostředí. Toho lze využít ke konsolidaci a izolaci serverů, nebo například k využití možnosti hostování starších aplikací na starších operačních systémech a k jejich migraci na nový hardware, čímž lze dosáhnout jejich vyššího výkonu.

Dále lze virtualizovaných strojů výhodně využít k testování a vývoji softwaru. Každý virtuální stroj představuje kompletní systém s procesory, pamětí, připojením k síti, úložištěm a systémem BIOS. Operační systém a softwarové aplikace tak lze ve virtuálním stroji nainstalovat a provozovat bez jakýchkoliv úprav. Dále jsou virtuální stroje od sebe zcela odděleny virtualizační vrstvou, díky níž se pád aplikace nebo chyba konfigurace v jednom virtuálním stroji neprojeví v ostatních strojích.

K virtualizaci bylo využito technologií firmy VMware. VMware ESX Server je samostatný virtualizační nástroj dodávaný s vlastním operačním systémem, ve kterém lze vytvářet, provozovat a spravovat virtuální stroje. Na tyto virtuální stroje lze instalovat různé operační systémy a aplikace, bez nutnosti jejich jakýchkoli úprav. VMware ESX si lze představit, coby virtualizační vrstvu instalovanou přímo na hardware nazývanou hypervizor, kdy operační systémy jednotlivých virtuálních strojů jsou touto vrstvou odděleny od hardwarových prostředků a o přidělování těchto prostředků se stará právě systém VMware ESX.

Systémy VMware ESX poskytují virtuálním strojům vestavěné funkce pro vysokou dostupnost, správu prostředků a bezpečnost, s nimiž dokážou softwarovým aplikacím poskytovat vyšší úrovně služeb než statická fyzická prostředí. Díky 64bitové technologii je možno využít až 1TB paměti RAM, virtuální stroje mohou využít až osm fyzických procesorů, kdy každý procesor může obsahovat 8 jader. Díky tomuto lze virtualizovat velké a výkonné stroje a na nich provozovat procesorově nejnáročnější aplikace, jako jsou databáze a informační systémy.

Kromě virtualizace strojů lze využít WMware ESX i pro síťové účely, kdy na každém virtuálním stroji lze nakonfigurovat až několik síťových karet s vlastní MAC a IP adresou a lze pomocí virtuálních přepínačů vytvořit simulovanou síť (VLAN) a tu využít například pro izolaci síťového provozu z bezpečnostních důvodů, nebo případného oddělení zátěže.

Další užitečnou vlastností je možnost bootování VMware systému z diskového pole, kdy fyzické servery nemusejí být vybaveny pevnými disky, čehož je využito i v případě naše-

ho datového centra. Tato možnost značně usnadňuje zálohování jednotlivých virtuálních pevných disků, jelikož všechna data se nacházejí na jednom centrálním úložišti a je tak značně zjednodušená jejich správa. Všechny tři fyzické servery, určené pro provozování virtuálních serverů, jsou zapojeny do clusteru s vysokým výkonem. [12]

4.5.3 Cluster

Anglickým slovíčkem Cluster označujeme propojení více počítačů v jeden celek obvykle pomocí počítačové sítě. Smysl tohoto spojování spočívá především ve zvýšení výkonu zařízení, nebo ve zvýšení spolehlivosti provozu. Jde o jakýsi druh spolupráce jednotlivých zařízení tvořící jeden celek. Clustery můžeme rozdělit na tři základní typy, které lze i mezi sebou do určité míry kombinovat.

Typy clusterů

1) ***Cluster s rozložením výkonu*** (Load ballancing nebo scallable)- propojení více zařízení, které poskytují stejné služby, mezi které se rovnoměrně rozkládá zátěž. Například klient, požadující službu, kterou poskytuje více serverů, bude obsloužen serverem s aktuálně nejnižším zatížením. Tímto lze zamezit případu, že na jednom serveru by pracovalo například dvacet lidí a na jiném jeden.
2) ***Cluster s vysokým výkonem*** (HPC, High-performance computing)- tímto clusterem lze například vytvořit velmi výkonný počítač spojením několika méně výkonných počítačů, což může být finančně výhodnější. Složitější úloha je rozdělena mezi jednotlivé počítače, které spolupracují na jejím výpočtu.
3) ***Cluster se zabezpečením dostupnosti*** (Failover ,High-availability)- zapojení, kdy každé zařízení může poskytovat odlišné služby, avšak v případě výpadku některého ze zařízení je zastoupeno jiným. V případě opětovného zprovoznění původního zařízení si toto zařízení přebírá služby zpět. Tento cluster je využíván pro zajištění redundance služeb.
4) ***Úložný cluster*** (Storage cluster)- umožňuje vícenásobný přístup ke sdílené paměti, která je tvořena více úložnými jednotkami. Využívá se například ke zvýšení výkonu u datových sítí SAN, nebo NAS a k vyššímu zabezpečení dat.[1]

V případě popisovaného datového centra máme vytvořeno několik clusterů. Prvním clusterem máme propojeny výše zmíněné tři fyzické servery, určené pro virtualizaci serverů. Dále bylo využito clusteru v případě citrixových serverů, kde bylo využito clusteru

s rozložením výkonu. Vzhledem k tomu, že se tento cluster skládá z většího počtu serverů, nazývá se obvykle pojmem farma. Clusteru se zabezpečením dostupnosti bylo využito v případě dvou virtuálních Exchange serverů a v síti SAN bylo použito principu úložného clusteru.

4.5.4 Windows server 2008

Na většině serverů našeho datového centra je použito nejnovější verze serverového operačního systému Windows server 2008 od firmy Microsoft. Tento operační systém vychází ze stejného kódu jako Windows Vista s jádrem Windows NT 6.0 kernel, se kterou má podobnou funkcionalitu a architekturu.

Windows server 2008 je dostupný v několika možných edicích, přizpůsobeným různým požadavkům a nasazením. Edici lze volit od nejlevnější verze Windows server 2008 Foundation, která je určená pro malé podniky a firmy, umožňující cenově výhodné nasazení pro základní činnosti, jako je například provozování méně náročných firemních aplikací, sdílení souborů, tiskáren a základní zabezpečení, až po edice určené pro nejnáročnější nasazení, kterou je například edice Enterprise.

Konfigurace serveru je řešena systémem přidělování rolí a služeb, které má server vykonávat. Po nové instalaci serveru nemá server přidělenu žádnou z možných rolí a tyto role je zapotřebí aktivovat. Je samozřejmě výhodné aktivovat pouze role a služby, které po serveru požadujeme z důvodu maximálního výkonu serveru. Základní role, pro které lze server konfigurovat jsou: Doménový řadič/Active Directory doména, DNS server, DHCP server, aplikační server, souborový server, tiskový a faxový server, terminálové služby, webový server, Update server -WSUS.

V našem datovém centru bylo využito edice Standart a Enterprise. Verze Standart byla instalována na fyzické citrixové servery, kdy je zapotřebí pouze role terminálové služby a webového serveru. Edice Enterprise byla využita k provozu výkonově náročných Exchange a doménových serverů, databázového a Microsoft Sharepoint serveru, kdy bylo využito výhodných licenčních podmínek, které umožňují provozovat až čtyři virtuální servery s jednou licencí, což není v případě fyzických serverů a pro každý stroj musí být zakoupena zvlášť licence.

Windows server 2008 je možné instalovat ve dvou verzích a to buď ve standardní verzi, nebo ve verzi Core Server, která postrádá Windows Explorer, Internet Explorer, NET Framework a další prvky. Tato verze se využívá v prostředí, kde je zapotřebí co nejvyšší míry

bezpečnosti a výkonu. Core Server lze konfigurovat pouze pomocí příkazové řádky (Windows Powershell), nebo vzdáleně pomocí MMC (Microsoft Management Console). [13]

4.5.5 Popis a funkce jednotlivých serverů

4.5.5.1 Technická specifikace serverů

Všech deset serverů se vyznačuje shodnou hardwarovou specifikací, byly využity servery HP DL380G5 se čtyřjádrovými procesory Intel Xeon X5450 na pracovní frekvenci 3,0GHz. Servery určené pro citrixovou farmu a Backup server jsou vybaveny 4GB paměti RAM a servery pro VMware cluster 16GB RAM. Servery obsahují duální gigabitový multifunkční síťový adaptér s technologií TOE, která snižuje odezvy v síti. Dalšími vymožeností těchto serverů je například 8 zásuvek SFF, ke kterým je možno připojit disky SATA za běhu počítače, nebo integrovaná správa Lights-Out 2 (iLO 2), která umožňuje hardwarově založenou vzdálenou správu, kdy je například umožněno vzdáleně zapnout server a konfigurovat BIOS. Všech šest citrixových serverů disponuje dvěma pevnými SAS disky o kapacitě 72GB. Ostatní servery využívají místo pevných disků datové sítě SAN.

4.5.6 Exchange server 2007

Microsoft Exchange Server 2007 je nástupcem o generaci staršího produktu Microsoft Exchange serveru 2003 a je jednou ze základních součástí firemních systémů. Jeho role spočívá ve zprostředkování příjmu a odesílání e-mailových zpráv, správy kalendáře a kontaktů, nebo například sdílení veřejných složek. Pro mobilní uživatele a uživatele pracující mimo firmu je možnost využít například přístup k e-mailu přes webové rozhraní (OWA – Outlook web Access) a přístupu pomocí mobilních zařízení. Po instalaci serveru je podobně jako u Windows serveru nutné přiřadit a doinstalovat serveru role, které má server zastávat. Výhodou tohoto systému je, že není třeba mít nainstalované všechny komponenty a docílit tak vyššího výkonu systému a také vyšší bezpečnosti. Další výhodou je, že každá role může běžet na jiném serveru, což využijeme většinou u větších firem, nebo mohou být všechny role na serveru jednom.

4.5.6.1 Role Exchange serveru

Hub Transport Server Role (HUB)

Tato role má na starosti směrování emailů, kdy server přijímá požadavky od všech ostatních rolí a doručuje zprávy na místo určení. V případě využití pouze jednoho Exchange

serveru, kdy není možné využít roli EDGE, která musí být instalována samostatně, je možné doplnit tuto roli anti-spamovým softwarem z role EDGE a tím zajistit filtrování zpráv od nevyžádané pošty. V našem případě je však filtrování zpráv od spamu zajištěno pomocí externí firmy, čímž bylo dosaženo menšího vytížení serverů. [13]

Client Access Server Role (CAS)

Tato role zajišťuje komunikaci mezi emailovými klienty pomocí klientských protokolů. Jedná se především o klienty, kterými jsou Outlook Web Access (OWA), ActiveSync, nebo Outlook Anywhere.

Outlook Web Access – zajišťuje přístup k emailové schránce pomocí webového rozhraní, kdy prostředí je téměř totožné s prostředím v programu Outlook.

Exchange ActiveSync – je synchronizační protokol, který je navržen pro mobilní a bezdrátové připojení k Internetu, využívající jazyka XML(Extensible Markup Language – obecný značkovací jazyk) a protokolu HTTP (Hypertext Transfer Protocol – internetový protokol). Jelikož mobilní připojení pracuje s malou šířkou pásma a vysokou latencí, čímž jsou data přenášena pomaleji, než je tomu u vysokorychlostní sítě, je tento protokol navržen tak, aby přenášel informace mezi serverem Microsoft Exchange a mobilním zařízením co nejrychleji.

Outlook Anywhere – služba, která umožňuje připojení klientů Outlook 2007 a Outlook 2003 k serveru Exchange z Internetu pomocí síťové součásti systému Windows RPC over HTTP (Vzdálené volání procedur přes protokol HTTP). Takové řešení nevyžaduje připojení k firemní síti prostřednictvím sítě VPN (virtuální privátní sítě), a přesto poskytuje plné funkce aplikace Outlook. [13]

Mailbox Server Role (MBX)

Role starající se především o mailboxy uložené v databázi a o jejich neustálou dostupnost pomocí CCR (Cluster Continuous Replication -clusterová průběžná replikace), nebo pomocí LCR (Local Continuous Replication -místní průběžná replikace). V případě CCR je využito dvou serverů propojených do clusteru, kdy každý server má svojí vlastní databázi, která se průběžně replikuje. V druhém případě jde o zdvojení databáze na dvě různé diskové jed-

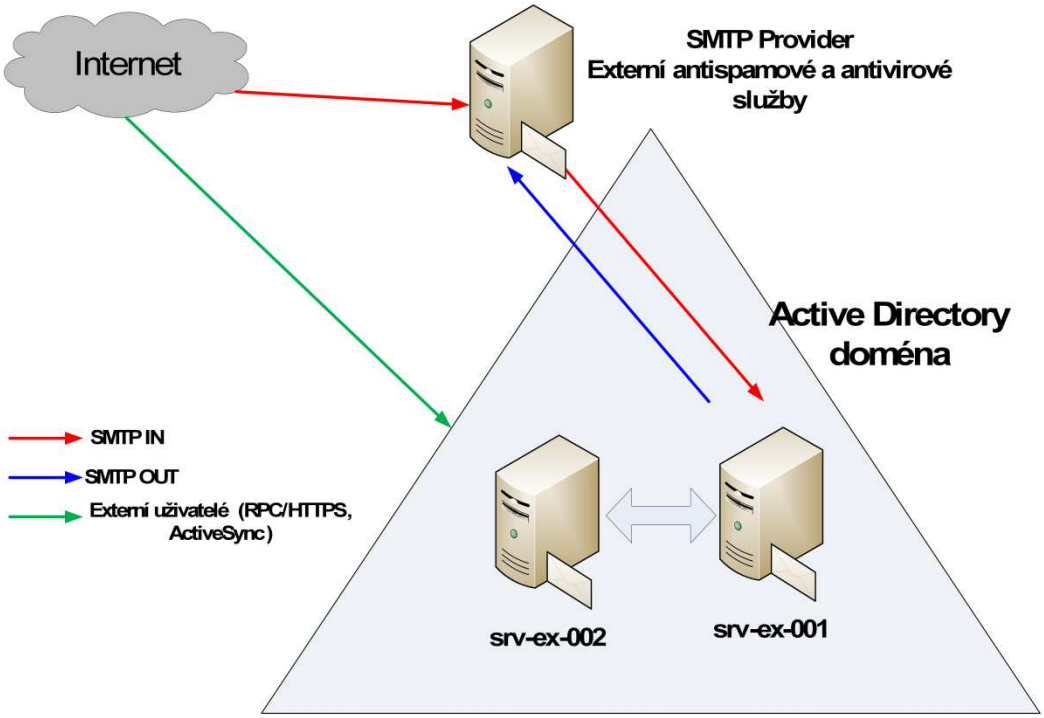
notky, kdy je jedna databáze hlavní a je aktivní a druhá záložní. Záložní databáze je průběžně replikována a je využita v případě poškození aktivní databáze. [13]

Unified Messaging Server Role (UM)

Jedná se o další možnost přístupu do emailové schránky, kdy je umožněna komunikace pomocí telefonu a je možno využít schránku jako hlasovou, nebo faxovou schránku. Při přístupu ke schránce pomocí telefonu je možno si přehrát hlasové záznamy, přečíst si emaily, nebo například přeorganizovat akce v kalendáři. [13]

Edge Transport Sever Role (EDGE)

Tato role je primárně určený pro příjem emailových zpráv podobně jako role HUB. Tato role se nedá kombinovat s ostatními rolemi a musí být instalována zvlášť na samostatný server. Tento server by si měl poradit s velkým množstvím spamových zpráv a virů, což někdy činí více než tři čtvrtiny veškeré komunikace. Z tohoto důvodu dostala tato role do vínku celou řadu anti-spam nástrojů a je předurčena pro instalaci antivirového softwaru. Jeho další funkcí je rozhodování se o tom, kam má přijatou zprávu, kterému serveru předat. Tato role nebyla v našem případě využita a byla nahrazena rolí HUB. [13]



Obr. č. 15 – Schéma propojení a komunikace Exchange serverů

4.5.7 Domain Controller

Domain Controller, neboli česky doménový řadič, je počítač, nebo server na kterém je umístěna buď celá, nebo část ***Active Directory.*** V případě popisovaného datového centra jsou vytvořeny dva virtuální stroje zapojené v clusteru s vysokou dostupností (failover), kdy v případě výpadku jednoho stroje je schopen druhý stroj převzít roli nefunkčního stroje, čímž je zajištěna větší spolehlivost celého systému.

Společně se službou Active Directory jsou na doménových řadičích provozovány důležité služby DNS, DHCP a WSUS.

4.5.7.1 Active Directory

Active Directory (dále pouze AD) je jedna z nejdůležitějších rolí Windows serveru, která má na starosti správu počítačové sítě s operačním systémem Microsoft Windows. Tento systém je založen na adresářové službě a protokolu LDAP (Lightweight Directory Access Protocol), který k této službě přistupuje. Hlavním úkolem AD je správa objektů, kterým poskytuje služby pro autentizaci a autorizaci a umožňuje administrátorům nastavovat pravidla, řídit tyto objekty, nebo například distribuovat centrálně programy na jednotlivé počítače. Objektem je libovolný uživatel, počítač, systém, služba spravovaná službou AD. Všechny tyto objekty jsou uloženy v centrální databázi, též nazývané adresář. Každý objekt je jednoznačně identifikován svým jménem a má definovanou sadu atributů (např. uživatel má atributy jméno, příjmení, členství ve skupině atd.). Tyto atributy jsou definované pomocí schématu určujícího také druh objektů, který mohou být uloženy ve službě AD.
AD vytváří kompletní strukturu sítě, která se dělí na dvě části a to fyzickou a logickou.

4.5.7.1.1 Fyzická struktura

A) Doménové řadiče (Domain Controller)
B) Sites (Sítě/podsítě) – v AD představují fyzickou geografickou polohu hostujících sítí. Mohou se skládat z podsítí a usnadňují vyhledávání informací a především řídí replikace doménového adresáře mezi doménovými řadiči.

4.5.7.1.2 Logická struktura AD

Doménový les *(Forest)* – vrchol struktury AD. Nachází se v něm veškeré objekty, jejich atributy a pravidla v AD. Les obsahuje jeden, nebo více doménových stromů a ty jsou propo-

jeny dvoucestným vztahem důvěry, což umožňuje nezávislým doménám uvnitř lesa mezi sebou komunikovat. Všechny domény sdílejí stejný globální katalog a schéma.

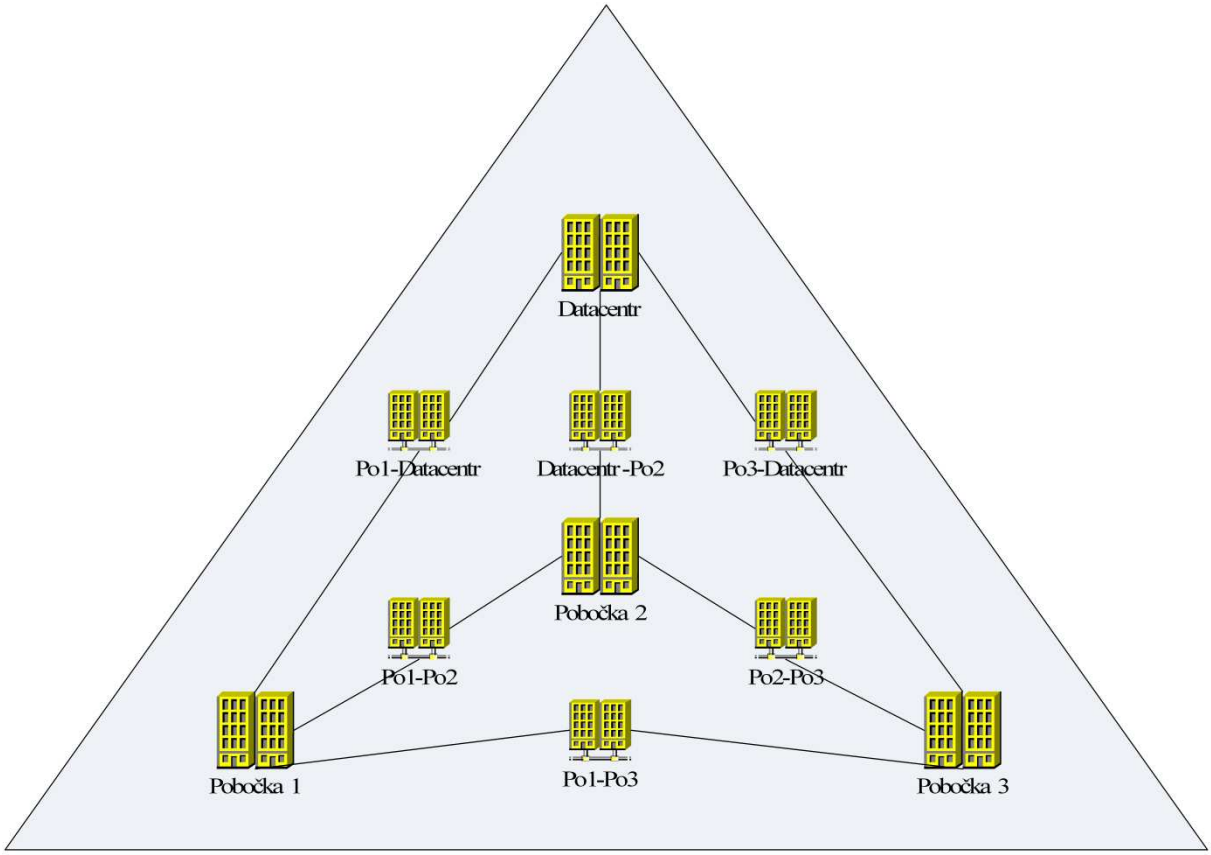
***Strom** (Tree)* – hierarchické spojení více domén sdílejících stejný jmenný prostor (namespace). Mezi doménami je vytvořen vztah rodič-potomek, kdy potomek dědí schéma podle hierarchicky výše postaveného rodiče.

***Doména** (Domain)* – Skupina počítačů sdílejících společnou adresářovou databázi. Každá struktura AD je tvořena minimálně jednou doménou. Doména je tvořena minimálně jedním doménovým řadičem a je základním prvkem AD. Ve většině případů pro firemní prostředí dostačuje jedna doména, která není omezená lokalitou firmy a může zahrnovat organizační jednotky všech poboček firmy. Doména tvoří bezpečnostní hranici, kdy nelze přenášet bezpečnostní nastavení mezi doménami a přístup k objektům v doméně je řízen pomocí ACL (Access Control List-atributy objektu určující operace, které lze s objektem provádět). Domény jsou pojmenovány podle DNS standardu, kdy doménové jméno potomka vznikne použitím jeho relativního jména doplněné za tečkou jménem jeho rodičovské domény.

Organizační jednotka (OU – Organizational Unit) – nejmenší jednotka AD umístěná uvnitř domény, kterou lze vytvářet logickou strukturu organizace, kdy vytvoříme OU například podle jednotlivých oddělení ve firmě a pro každou tuto OU lze poté nastavit specifická oprávnění a politiky. Organizační jednotka seskupuje objekty a bývá nazývána kontejnerem. Zjednodušeně by se dalo říct, že doména je kontejner pro organizační jednotky a organizační jednotky jsou kontejnerem pro objekty. Organizační jednotky mohou obsahovat více vnořených OU. Díky OU lze snadněji spravovat velké množství objektů, zefektivnit správu prostředků a lze stanovit rozsah práv jednotlivých správců v doméně. [1]

4.5.7.2 Replikace globálního katalogu

Aby bylo možné využívat ve všech pobočkách nastavených politik a pravidel AD a služby AD byly dostupné na pobočkách s dostatečným výkonem, je na každé pobočce umístěn doménový řadič se službou AD. Pro všechny tyto doménové řadiče je zapotřebí zajistit aktualizace globálních katalogů, kdy v případě změny v některém z katalogů se provede změna ve všech ostatních pobočkách. V případě provedení změn ve dvou katalozích najednou je při replikaci použit katalog s novější informací.



Obr. č. 16 – Schéma systému replikací globálního katalogu AD

4.5.7.3 DNS

Na doménovém řadiči je provozována mimo Active Directory také role DNS(Domain Name System). Princip DNS spočívá v hierarchickém přiřazování doménových názvů IP adresám přiřazených doménovým serverům. Tato role je zcela zásadní pro funkci Active Directory, jelikož každá doména vytvořená v AD má vlastní doménový název, např. firma.cz, Princip DNS spočívá v hierarchickém přiřazování doménových názvů IP adresám přiřazených doménovým serverům a naopak.

Pro názornost si lze předvést vytváření doménových názvů na uvedeném příkladu, kdy doména firmy se nachází v doméně cz a obsahuje dvě pobočky (pobočka1,pobočka2), které provozují další vlastní domény. V tomto případě bude doménový název pro pobočku1 ve tvaru *pobočka1.firma.cz* a pro pobočku2 obdobně *pobočka2.firma.cz*

DNS názvy jsou využívány z důvodu snadnějšího používání pro člověka oproti použití číselných IP adres. [14]

4.5.7.4 DHCP

Role zajišťující přidělování IP adres, masek sítě, brány, adres serverů DNS a dalších parametrů jednotlivým klientským počítačům, které se přihlašují do sítě. Přidělování adres může být statické, nebo dynamické. V případě statického přidělování je ke každé MAC (Media Access Control-jedinečné označení síťového prvku) adrese přidělena jedna definovaná IP adresa. V případě dynamického přidělování je udán rozsah adres, kdy volné adresy jsou náhodně přidělovány přihlašujícím se klientům. Z důvodu snadnější administrace je v našem případě využito dynamického přidělování IP adres, kdy již jednou přidělená IP adresa je uložena v seznamu. V případě nového požadavku stanice o IP adresu, je přidělena adresa stejná, čímž je dosaženo minimálních změn IP adres na jednotlivých stanicích.[14]

4.5.7.5 WSUS (Windows Server Update Services)

Služba, která nahrazuje automatické aktualizace přijímané operačními systémy Microsoft Windows zajištěné službou Windows Update. Přijímání automatických aktualizací z internetu jednotlivými stanicemi v případě velkého počtu, značně zatěžuje internetové připojení a administrátoři nemají kontrolu nad jednotlivými aktualizacemi, z tohoto důvodu je výhodnější využít tuto službu, která tyto problémy odstraňuje. Princip spočívá v jednom stažení aktualizací na server, odkud je rozeslána na jednotlivé stanice. Administrátor má možnost rozhodnutí, které aktualizace budou, či nebudou instalovány na dané stanice a vše probíhá již pouze v rámci vnitřní sítě. Další výhodou je možnost spolupráce se systémem Active Directory, kdy lze například při použití skupinových politik zamezit stanicím odmítnutí instalace aktualizací.

4.5.8 Citrix server

V dnešní době, kdy stále více pracovníků pracuje různými způsoby na různých místech, například z domova, na notebookách, nebo ve vzdálených pobočkách, je čím dál obtížnější a nákladnější spravovat tradiční počítačovou infrastrukturu firmy, kdy aplikace jsou umístěny na jednotlivé koncové uživatelské zařízení. Tento přístup k distribuci aplikací je příliš statický a ve chvíli kdy je zapotřebí provést rozsáhlejší změny, je provedení velmi časově náročné a zvyšují se tak náklady na údržbu. Z tohoto důvodu je výhodné mít všechny aplikace a data uložené centrálně na serveru, kde je jejich správa značně zjednodušená. K tomuto účelu bylo využito infrastruktury Citrix pro poskytování Windows aplikací pomocí technologie vizualizace.

Tuto roli má na starosti šest fyzických serverů, na kterých je nainstalován operační systém Windows server 2008 standart edition 32bit a Citrix XenApp Server. Na klientských počítačích může být nainstalována buď aplikace Citrix XenApp, nebo rozšiřující plugin pro webový prohlížeč. Klient může využít buď kompletní vzdálené plochy, nebo spouštět jednotlivé streamované aplikace. Druhá varianta má velkou nevýhodu při spuštění několika programů najednou, kdy spuštění každé aplikace zabere určitou část šířky přenosového pásma. V případě vzdálené plochy je zabrána pouze jedna část a spouštění libovolného množství aplikací v rámci vzdálené plochy, nemá vliv na přenosové nároky a nezatěžuje zbytečně linku.

V případě, že klient využívá ke svojí práci pouze aplikace poskytované pomocí systému citrix, jsou na jeho lokální PC kladeny minimální hardwarové požadavky, jelikož veškeré výpočetní úlohy mají na starosti citrixové servery. V případě nutnosti zvýšení výkonu systému tudíž není zapotřebí řešit jednotlivé stanice a stačí zvýšit potřebný výkon serverů, což lze provést z pohledu uživatele zcela transparentně. Aplikace potřebné pro spuštění vzdálené plochy na klientských počítačích lze instalovat jak na operační systémy Windows, tak i na unixové systémy, které lze využívat zdarma, čímž lze dosáhnout finančních úspor při nákupu licencí operačních systémů.

Celý systém má však i jistá omezení a nevýhody. Značná nevýhoda může být značně omezená možnost přizpůsobení celého systému jednotlivým uživatelům, s různými nároky a požadavky. Dále vznikají problémy v případě provozu specifických aplikací využívajících například hardwarové klíče. V tomto případě je zapotřebí ponechat tyto aplikace na lokálních stanicích uživatelů, pro které může být snížen komfort obsluhy programů, jelikož část programů může být provozována pomocí systému citrix na vzdálených serverech a část na lokálním stroji. Uživatel je v tomto případě nucen přepínat mezi jednotlivými prostředími. Dále může vznikat problém s dostupností souborů, kdy uživatel může vytvořit soubory na lokálním stroji, které jsou zapotřebí přenášet na centrální úložný prostor, což může být v případě přenosu přes síť WAN značně zdlouhavé a může to značně vytěžovat přenosové pásmo. Tento problém může nastávat i v opačném případě, kdy se soubor nachází v datovém centru a je zapotřebí přenést jej na lokální stroj.

4.5.9 Databázový server

Databázový server je jeden z nejdůležitějších serverů pro firemní informační systémy. Tento server je určen pro správu a poskytování databází a databázových služeb. Vzhledem k požadavkům na rychlou práci s obrovským množstvím dat, je zapotřebí vybavit tento server především dostatečnou velikostí paměti RAM, která v našem případě činí 8GB. Server obsahuje několik databází, které využívají různé aplikace, kdy nejdůležitější aplikací je informační systém Evolution.

Jednotlivé databáze se skládají obvykle z velkého množství tabulek, do kterých se ukládají jednotlivé záznamy, které mají přesně definovanou strukturu. Obvykle je celá databáze se všemi v ní uloženými daty tvořena jedním, nebo několika málo soubory. Záznamy jsou nejčastěji strukturovaná textová data, mohou je ovšem tvořit i obrázky, videa, dokumenty a mnohé další soubory. Přístup k těmto záznamům je prováděn pomocí jazyka SQL, což lze realizovat buď přímo pomocí jednotlivých příkazů, nebo pomocí grafických aplikací. Databáze umožňují široké možnosti řazení dat, jejich filtrování, strukturalizaci, indexování, propojování a mnohé jiné operace, které v případě uložení dat běžným způsobem, mnohdy nejsou realizovatelné. S daty uložených v databázi může najednou pracovat více lidí, nebo aplikací a díky propracovaným autentizačním technikám lze zajistit vysoké zabezpečení těchto dat.

Na serveru se nacházejí dva databázové systémy, kterými jsou Microsoft SQL server 2005 a systém MySQL. Databáze systému MS SQL serveru 2005 využívá především informační systém, dále pak antivirový systém McAfee, systém Citrix a Sharepoint server. MySQL databáze jsou využívány docházkovými systémy, účetními programy a evidenčním systémem.

4.5.10 Proxy server

Proxy server byl v našem případě řešen pomocí služby Squid provozované na linuxovém systému. Tento server slouží jako dočasná paměť k uložení navštívených webových stránek. Při opakovaném požadavku na zobrazení stránky, která je již uložena na serveru, je klientovi poskytnuta stránka přímo z Proxy serveru, nikoli z webu, čímž se sníží objem přenášených dat z internetu. Nevýhodou tohoto systému může být poskytnutí klientovi neaktuálních stránek. Dobu uchování těchto dat na Proxy serveru má možnost ovlivnit programátor webových stránek, například zápisem meta tagu v načítané HTML stránce. Pomocí Proxy serveru lze také blokovat přístupy do internetu, stahování souborů, nebo například návštěvu adres s nevhodným, či erotickým obsahem. Tuto funkci zajišťuje služba SquidGuard, se kte-

rou lze službu squid propojit. Dále lze Proxy server využít pro skrytí IP adres vnitřní sítě. Také je možné umožnit přístup klientům pouze za pomocí uživatelského jména a hesla, což lze využít k určení klientů, kteří mají mít přístup a kteří nikoli.

4.5.11 Aplikační server

Server s instalovaným operačním systémem Windows Server 2003 sloužící k poskytování aplikací, které využívá jen malá část uživatelů a je nevýhodné je poskytovat pomocí citrixových serverů, kdy je zapotřebí instalovat každý program na všech šest serverů. Jedná se především o účetní programy, bankovní aplikace, mzdové a docházkové aplikace a další aplikace pro zcela specifické účely. Uživateli jsou tyto programy poskytovány jednoduchou formou nakopírování zástupce potřebného programu do jeho profilu.

4.5.12 Nagios server

Linuxový server pro provozování open source systému Nagios. Tento systém je navržen na automatické sledování počítačové sítě a v ní provozovaných služeb. Je možné monitorovat služby jak systému Linux, tak služby systému Windows. Lze například sledovat dostupnost zařízení pomocí služby ping, kterou lze kontrolovat síťovou dostupnost serverů v jiných pobočkách, nebo dostupnost internetu zasíláním pingů například na webový server google. Velmi praktické je sledování funkčnosti jednotlivých hardwarových komponent důležitých zařízení, kterými jsou především servery a aktivní síťové prvky. Je možné sledovat vytížení procesorů, jejich teploty, otáčky ventilátorů, využití paměti RAM, nebo zaplnění pevných disků. U všech sledovaných je možné nastavovat limity a hodnoty, při kterých systém automaticky zašle upozornění v podobě emailové zprávy. Tomuto nastavení je zapotřebí věnovat dostatečnou pozornost, jelikož špatné nastavení může vést k zasílání velkého množství zpráv, ve kterém lze přehlédnout důležité informace.

4.5.13 Sharepoint server

Server, na kterém je provozována řada aplikací softwarového balíku Microsoft Office SharePoint Server 2007, umožňující vytvoření prostoru určeného k týmové spolupráci v rámci firmy. Pro přístup k této službě je zapotřebí pouze internetového prohlížeče a funguje na principu intranetu.

Sharepoint je možné využívat ke sdílení kontaktů a elektronických dokumentů, kdy lze sledovat historii verzí, změn a lze také zjistit uživatele, který změnu provedl. Pro snadné a rychlé nalezení konkrétního dokumentu lze využít fulltextového vyhledávání. Pomocí Sharepoint serveru můžeme také plánovat a zadávat úkoly, sledovat průběh jejich řešení či týmově diskutovat nad tématem, či dokumentem, nebo spolupracovat na společných projektech. Snadno lze presentovat informace například o nových výrobcích, nebo tzv. vyvěšovat centrální oznámení na elektronické nástěnce.

Ke službě lze přistupovat buďto pomocí vnitřní sítě, nebo odkudkoli z internetu pomocí webového rozhraní.

4.5.14 Backup server

Server se systémem Windows server 2003 určený k provozu služeb zajišťujících zálohování a obnovu dat. K tomuto účelu je na serveru nainstalován program Backupexec od firmy Symantec a program SnapManager od firmy NetApp. Program Symantec byl zvolen především díky jeho komplexní ochraně dat a možnostem obnovení systému, kdy lze využít jak pro fyzické, tak virtuální servery a dále pak pro možnosti optimalizovaného zálohování pomocí protokolu NDMP, čehož je využito v případě zálohování na páskovou knihovnu. Program SnapManager byl součástí dodaného diskového pole FAS 3020HA od firmy NetApp a je určen především k zálohování databází SQL a Exchange. Dále jsou na serveru spouštěny skripty, pro spouštění zálohovacích úloh VMware zálohovacího nástroje.

4.6 Datové úložiště (Storage), zálohování

Nejdůležitějším úkolem IT specialistů je správa a zabezpečení důležitých a citlivých dat. Z osobní praxe vím, jak velký problém může vzniknout v případě ztráty těchto dat, ke které může dojít například kombinací havárie disku s nefunkčním zálohováním. V takovém případě se firma ocitá v situaci, kdy obnova ztracených dat je velmi nákladná a v některých případech i zcela nemožná. Z tohoto důvodu je zapotřebí klást velmi velký důraz na vybudování kvalitního datového úložiště kombinovaného se spolehlivým záložním systémem, aby data byla v bezpečí a dostupná v maximální možné míře všem uživatelům, kteří k nim mají mít přístup.

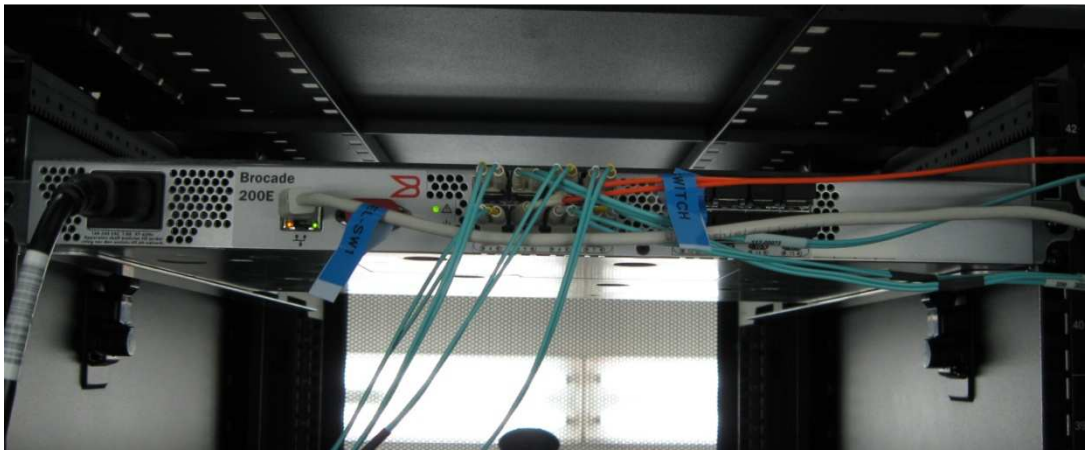
Celý systém datového centra byl navržen tak, aby se veškerá data a aplikace, nacházela na jednom centrálním místě a tím se značně usnadnila správa celé počítačové struktury. Díky tomuto systému není již zapotřebí hlídat zálohování velkého množství lokálních počítačů a

serverů v jednotlivých pobočkách. Další nespornou výhodou je také značné zamezení vzniku duplicitních souborů, které se mohly vyskytovat v neaktuální podobě na více místech najednou, čím mohlo docházet k chybám a zbytečnému snižování kapacity pevných disků. Samozřejmostí je i docílení velmi značného zjednodušení sdílení dat mezi uživateli nacházejícími se v různých pobočkách.

4.6.1 SAN (Storage Area Network)

Pro realizaci datového úložiště byla zvolena datová síť SAN. V našem případě bylo využito možnosti vybudování clusterového řešení, která nám zajistí potřebnou redundanci a zabezpečení datového úložiště. Datová síť byla rozdělena na dvě části, kdy jedna část je umístěna v primární serverovně a druhá část v sekundární serverovně. Síť SAN je tvořena diskovým polem, dvěma Fibre Channel switchi a páskovou knihovnou, kdy všechna zařízení mezi sebou komunikují pomocí protokolu Fibre Channel s výjimkou přenosů dat na páskovou knihovnu.

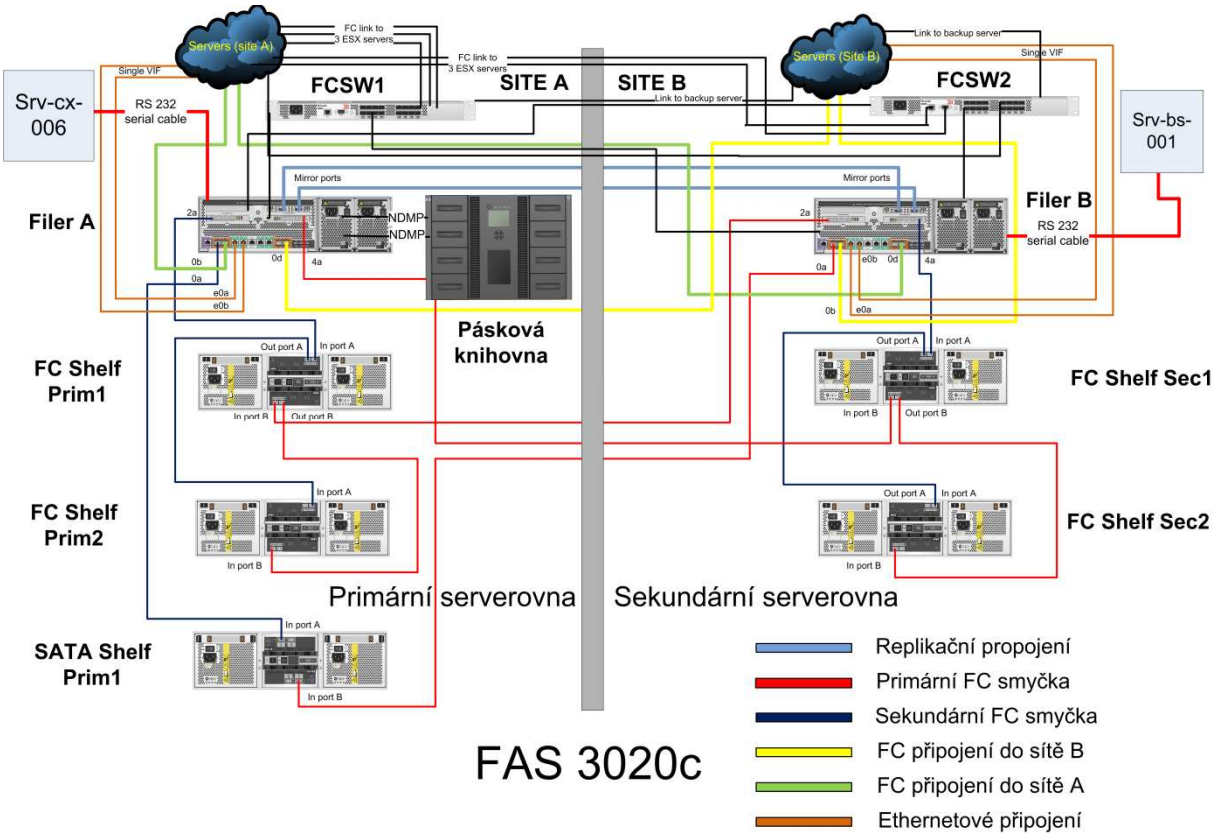
Použitím Fibre Channel switchů byla stanovena topologie Fabric, podle které jsou tyto zařízení též nazývané Fabric switch. Veškerá zařízení připojovaná k těmto switchům musí obsahovat speciální kartu HBA(Host Bus Adapter), která je obdobou síťových karet v běžné TCP/IP síti.



Obr. č. 17 – Fibre Channel switch

Aby bylo možné přidělit oprávnění přístupu k jednotlivým zařízením, jako jsou například jednotlivá disková pole, nebo páskové knihovny, je zapotřebí nakonfigurovat tzv. zóny (Nody). Tyto zóny se definují pomocí WWN adres (World Wide Name), což jsou fyzické adresy SAN zařízení, obdobné MAC adresám síťových zařízení v síti TCP/IP. Lze tedy definovat například pro konkrétní server přístup k diskovému poli, ale zakázat přístup k páskové knihovně.

Všechna zařízení v síti SAN se navenek chovají jako jeden velký disk. Aby mohlo být využíváno různých souborových systémů, je třeba tento celek dále rozčlenit na menší části, které se navenek chovají jako více disků. Každé této části je přiřazeno identifikační číslo tzv. LUN (Logical Unit Number), pomocí něhož se mapují tyto jednotky ke konkrétním WWN adresám.



Obr. č. 18 – Schéma zapojení datové sítě SAN

4.6.2 Diskové pole

V našem případě bylo k realizaci úložného systému vybráno diskové pole od firmy NetApp (Network Appliance) FAS 3020HA. Toto pole v sobě kombinuje funkce blokového a souborového přístupu protokoly Fibre Channel, iSCSI (Internet Small Computer System Interface – protokol vycházející ze dvou technologií a to ze SCSI, což je rozhraní pro připojování disků k serverům a TCP/IP protokolu), CIFS (Common Internet File Systém - linuxový souborový systém) a NFS (Network File Systém – síťový souborový systém umožňující vzdálený přístup k souborům přes počítačovou síť).

Toto pole obsahuje dvě řídící hlavy (Filer) označené na obrázku č.18 Filer A a Filer B. Řídící hlava je prakticky počítač, na kterém je nainstalován operační systém Data ONTAP vyvinutý firmou NetApp, speciálně navržený pro poskytování optimalizovaných datových přenosů a funkcí. K těmto hlavám je možné připojit disky s rozhraním SAS (Serial Attached SCSI), SATA, nebo Fibre Channel.

V našem případě každá část pole disponuje dvěma policemi (Shelf) o sedmi Fibre Channel discích velikosti 300GB. V primární serverovně se navíc nachází další police obsahující 14 SATA disků s velikostí 750GB, zastávajících funkci mezipaměti zálohovaných souborů, při přenosu do páskové knihovny LTO. Na disková pole obsahující Fibre Channel disky jsou kladeny nároky především na rychlou přístupovou dobu, která zajistí rychlé odezvy při práci uživatelů. V případě pole vytvořeného pomocí SATA disků je upřednostňována kapacita, nižší náklady a vyšší spolehlivost disků.

Obr. č. 19 – Diskové pole NetApp

Data se mezi diskovými policemi navzájem nepřetržitě synchronně replikují tak, aby byla fyzicky v obou částech pro případně selhání některého ze zařízení. V případě nedostupnosti síťového připojení, je umožněna správa obou řídících hlav přímým propojením fyzického citrixového serveru a backup serveru k oběma hlavám, pomocí sériového portu.

Na obr. č. 18 je vyfocené diskové pole umístěné v primární serverovně. Od shora je umístěná disková hlava, pod ní dvě police s FC disky, dále jedna police se SATA disky a ve spodní části se nachází pásková knihovna HP MSL8096.

4.6.3 Pásková knihovna HP MSL8096

V případě živelné katastrofy, která by měla za následek zničení kompletního datového centra, je přijato opatření pro zamezení kompletní ztráty dat. Toto opatření spočívá v uložení kompletních záloh do trezoru jedné z poboček firmy, které se provádí jednou týdně. Vzhle-

dem k velkému množství zálohovaných dat, pohybujících se řádově v terabajtech, není možné využít pro zálohování přenos dat pomocí sítě WAN a je tedy nutné přemístit tyto zálohy na nějakém fyzickém médiu. Pro tento případ je datové centrum vybaveno páskovou knihovnou, která využívá k uložení záloh magnetických pásek, které mají oproti jiným typům přenosných médií mnohem větší kapacitu.

V realizovaném řešení pásková knihovna disponuje 8 šuplíky (magazine), kdy každý šuplík obsahuje 12 slotů, které mohou sloužit pro datové pásky, čistící pásky a mailsloty. Vzhledem ke kapacitě pásky, která činí 1,6TB, lze dosáhnout maximální komprimované diskové kapacity 153TB při úplném využití páskové knihovny. Rozsah zálohovaných dat ovšem takové kapacity nedosahuje a pro potřebu datového centra je využito pouze čtyřiceti slotů, kdy 38 slotů obsahuje datové pásky, a dva sloty obsahují čistící kazety.

Pásková knihovna je určena pro připojení pomocí optického rozhraní využívající protokol Fibre Channel a spolu se zálohovacím systémem Openview Data Protector a protokolem NDMP(Network Data Management Protocol) umožňuje zálohovat data přímo z diskového pole NetApp FAS3020 na páskovou knihovnu. Pásková knihovna umožňuje selektivní i plnou zálohu dat, archivaci a obnovu dat v případě havárie nazývanou disaster recovery. Celá knihovna se spravuje pomocí webového rozhraní, není tedy pro konfiguraci zapotřebí používat a instalovat další software.

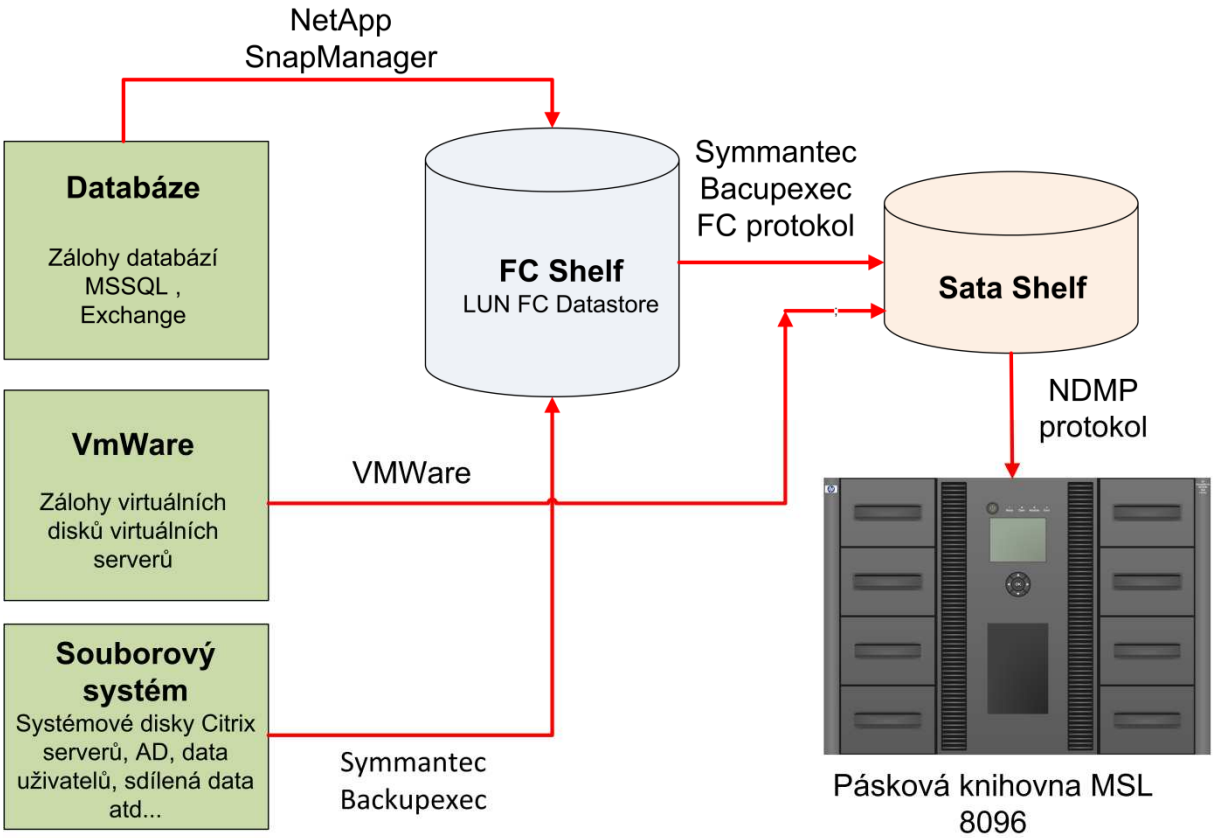
4.6.4 Systém zálohování

Jedním z velmi důležitých kroků k zabezpečení dat je vytvoření sytému zálohování. Zálohování probíhá v několika fázích, kdy jsou zálohovány tři různé typy zálohovaných dat, které jsou zálohované pomocí různých zálohovacích systémů. Prvním oblastí zálohování jsou databáze serverů Exchange a SQL server 2005, druhou jsou systémové disky VMwarových virtuálních počítačů a třetí oblastí je zálohování souborového systému, který obsahuje veškerá data Active Directory + data uživatelů.

V první fázi zálohování jsou data databází a souborového systému přesunuty na LUN Datastore vytvořený na FC diskovém poli. Databáze jsou zálohovány 3X denně a o zálohování se stará program SnapManager, instalovaný na Backup serveru. O zálohování kompletního souborového systému se stará program Backupexec, který vytváří plnou zálohu jednou týdně v sobotu. Poslední zálohovanou oblastí jsou systémové disky virtuálních serverů. Zálohování těchto dat je provedeno pomocí nástroje integrovaného v systému WMvare ESX, který pro-

vádí zálohy opět jednou týdně v sobotu. Jak je patrné z obr. č. 20, tak zálohy již nesměřují na FC pole, nýbrž přímo na LUN vytvořený na SATA diskovém poli.

Toto řešení je navrženo z důvodu usnadnění obnovy ztracených dat, kdy obnovy dat uživatelů a dat z databází jsou relativně časté, ovšem obnova systémových disků virtuálních strojů je výjimečná. Na FC poli se však udržuje pouze třetina posledních záloh, zbylé dvě třetiny se přesunují na pole SATA, odkud jsou všechny zálohy jednou týdně přesunuty na páskovou knihovnu. O přesun dat z pole SATA na páskovou knihovnu se stará opět program Backupexec, který využívá k přesunu dat protokol NDMP, který umožňuje přímý přenos dat mezi diskovým polem NetApp a páskovou knihovnou. Přenos záloh je opět prováděn jednou týdně o víkendu, kdy na začátku následujícího týdne jsou pásky s týdenní zálohou převezeny na jinou pobočku firmy a uschovány v trezoru, kde se vymění za předešlé pásky. Vyměněné pásky se opět vrátí do páskové knihovna a jsou přepsány novými zálohami. Pro databáze a souborové systémy byl navržen čtyřtýdenní cyklus, po který jsou zálohy udržovány, pro virtuální stroje je cyklus poloviční.



Obr. č. 20 – Principielní schéma zálohování

5 Závěr

První část bakalářské práce se zabývá návrhem datových center, nemá však za cíl vypracovat komplexní návod, podle kterého by mohlo být skutečně takové centrum navrženo, dává však přehled o jednotlivých okruzích a tématech, kterými je zapotřebí se při návrhu zabývat. Tyto informace lze využít i pro zamyšlení pro provozovatele již realizovaných datových center, zda jejich stávající systémy stále vyhovují požadavkům dnešní doby, případně zda není již zapotřebí vylepšit stávající centrum technologiemi novými. Dále tyto informace mohou být nápomocny při tvorbě zadávací dokumentace pro výběrová řízení.

V druhé části se práce zabývá konkrétním realizovaným projektem, který je v dnešní době úspěšně provozován ve výrobním podniku, ve kterém pracuji jako člen týmu IT specialistů, kteří mají na starosti chod a údržbu těchto systémů. Jelikož tento projekt nahradil zcela odlišné systémy, které firma původně používala, bylo zapotřebí se s novými technologiemi seznámit, kdy v první řadě bylo zapotřebí pochopit základní principy a účel jednotlivých zařízení. Studiem velkého množství literatury a konzultacemi s odborníky z firmy realizující zprovoznění zařízení, jsem značně rozšířil své znalosti a možnosti snadnější a efektivnější správy těchto systémů.

Realizovaný projekt se ve firmě velmi osvědčil a z mého pohledu to byl krok správným směrem, kdy se investice do těchto systémů v budoucnosti ukáže jako správná. I přes veškerou snahu se projekt nevyhnul některým problémům, se kterými se datové centrum v současné době potýká. Největším problémem je především nedostatečný počet citrixových serverů, kdy doporučený počet uživatelů pracujících na jednom serveru je 25, což je často značně překročeno a práce na těchto serverech je značně pomalá. Tento problém je velmi často zapříčiněn problémem a nutnou odstávkou některého ze serverů. Řešením by mohl být zajisté nákup dalšího zařízení, avšak mým dalším cílem je navrhnout a zkonzultovat možnosti migrace těchto fyzických serverů do virtuálního prostředí, kde by byla zjednodušená správa a možnost lepšího využití hardwarového zařízení. Dalším problémem, se kterým se celý projekt setkal, je chybné navržení licencování terminálových přístupů, kdy byly zakoupeny licence pro jednotlivá zařízení (tzv. per-Device), kdy mnohem výhodnější, v tomto prostředí, by bylo licencování pro jednotlivé uživatele (tzv. per-user). Tímto systémem licencování vzniká problém s nedostatkem jednotlivých licencí z důvodu přihlašování se některých uživatelů z více zařízení (například z domácích počítačů). Tyto licence je poté zapotřebí ručně odebírat, což je značně neefektivní a v této době probíhá jednání s firmou Microsoft o změně systému licencování.

6 Použitá literatura

[1] Wikipedia, the free encyclopedia – http://en.wikipedia.org

[2] Altron – http://www.altron.cz

[3] KROUPA, Tomáš. Datová centra v kostce (1.) : Návrh řešení a fáze budování. *Inside* [online]. 2008 [cit. 2009-11-13].

[4] APC by Schneider Electric – http://www.apcmedia.com

[5] KROUPA, Tomáš. Datová centra v kostce (2.) : Analýza zátěže. *Inside* [online]. 2008 [cit. 2009-11-13].

[6] DOUŠEK, Martin. *Jak vybrat aktivní prvek* [online]. 1.6.2007 [cit. 2009-11-20]. Dostupný z WWW: <http://www.pripojtese.cz/art_doc-77F1C2171349FE96C12572E90045BBA3.html>.

[7] Svět sítí – http://www.svetsiti.cz

[8] Intelekt – komponenty datových a telekomunikačních sítí – http://www.intelek.cz

[9] HOUŠTĚK, Petr. *Provozujeme linuxový server : hardware I* [online]. 17.1.2005 [cit. 2009-11-22]. Dostupný z WWW: <http://www.linuxsoft.cz/article.php?id_article=619>.

[10] Klika BP – Požární bezpečnost staveb – http://www.klika.cz

[11] Cisco systems – http://www.cisco.com

[12] VMware Business Infrastructure Virtualization – http://www.vmware.com

[13] Microsoft Corporation – http://www.microsoft.com

[14] Wikipedie, otevřená encyklopedie – http://cs.wikipedia.org

[15] Netbotz – monitorovací systémy – http://www.netbotz.com

7 Seznam obrázků

8 Seznam zkratek

100VGA	Asynchronous Transfer Mode
ACL	Access Control List
ACNS	Application and Content Networking System
ATM	Asynchronous Transfer Mode
CCR	Cluster Continuous Replication
CIFS	Common Internet File Systém
DAS	Direct Attached Storage
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
GSM	Global System for Mobile communications
GPRS	General Packet Radio Service
HBA	Host Bus Adapter
HPC	High-performance computing
HTML	HyperText Markup Language
IP	Internet Protocol
IPSEC	Internet Protocol Security
iSCSI	Internet Small Computer System Interface
ISP	Internet Access Provider
LAN	Local Area Network
LCR	Local Continuous Replication
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number
MAC	Media Access Control
NAS	Network-Attached Storage
NDMP	Network Data Management Protocol,
NFS	Network File System
NIPS	Network Intrusion Prevention Systems
RM PDU	Metered Rack Power Distribution Unit
PDU	Power distribution unit
PoE	Power over Ethernet
QoS	Quality of Service
RAID	Redundant Array of Independent Disks
RPC	Remote Procedure Call
SAN	Storage Area Network
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPOF	Single Point of Failure
SSL	Secure Sockets Layer

STA	Spanning Tree Algorithm
TCP/IP	Transmission Control Protocol/Internet Protocol
UPS	Uninterruptible power supply
UTP	Unshielded twisted pair
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAAS	Wide Area Application Services
WAFS	Wide Area File Services
WAN	Wide Area Network
WWN	World Wide Name
XML	Extensible Markup Language