ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

PROVOZNĚ EKONOMICKÁ FAKULTA

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ

NOVÉ TECHNOLOGIE V INFRASTRUKTUŘE FIREMNÍCH SÍTÍ

DIPLOMOVÁ PRÁCE

Vedoucí práce: **Ing. Jiří Vaněk, Ph.D.**

Autor práce: **Alexandr Krátký**

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Akademický rok 2008/2009

ZADÁNÍ DIPLOMOVÉ PRÁCE

Alexandr Krátký

obor Informatika

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 17 odst. 2 určuje tuto diplomovou práci.

Název tématu: **Nové technologie v infrastruktuře firemních sítí**

Struktura diplomové práce:

1. Úvod
2. Cíl práce a metodika
3. Úvod do problematiky rozsáhlých firemních sítí
4. Služby DNS a DHCP
5. Topologie firemních sítí
6. Komunikační technologie
7. Závěr
8. Seznam literatury
9. Přílohy

Rozsah původní zprávy: 50 - 60 stran

Seznam odborné literatury:

KAILASH, Jayaswal: Administering Data Centers: Servers, Storage, and Voice over IP. Indianapolis, Wiley Publishing, 2006. ISBN-13: 978-0-471-77183-8

SCHUDEL, Georgg; SMITH, David: Router Security Strategies: Securing IP Network Traffic Planes. Indianapolis, Cisco Press, 2007. ISBN 978-1-58705-336-8

RULE, David; DITTNER Rogier: The Best Damn Server Virtualization Book Period. Burlington, Syngress Publishing, 2007. ISBN 13: 978-1-59749-217-1

INFOBLOX: Powering Nonstop Core Network Services. [online]. < http://www.infoblox.com/library/l-genLibrary.cfm?section=l-whitepapers >

Vedoucí diplomové práce: **Ing. Jiří Vaněk, Ph.D.**

Termín odevzdání diplomové práce: duben 2010

L.S.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE - Provozně ekonomická fakulta

.....
Vedoucí katedry

.....
Děkan

V Praze dne: 15.12.2008

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Nové technologie v infrastruktuře firemních sítí" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D. za jeho cenné připomínky, odborné vedení, trpělivost a ochotu při vedení této diplomové práce. Dále chci poděkovat své rodině, za poskytnuté zázemí, podporu a pochopení v čase, kdy jsem se věnoval studiu na úkor své ženy a synů.

Nové technologie v infrastruktuře firemních sítí

Souhrn

Práce pojednává o trendech a nových technologiích v prostředí rozsáhlých firemních počítačových sítí. V prvních třech kapitolách je uvedena problematika výstavby a provozu geograficky rozsáhlých sítí. Jsou nastíněny ekonomické požadavky na infrastrukturu a jim odpovídající technická řešení. Čtvrtá kapitola charakterizuje služby DNS a DHCP a zhodnocuje problematiku jejich nedostupnosti. Pátá kapitola představuje změny v topologii velkých počítačových sítí a uvádí přínosy těchto změn pro chod podniku. Kapitola číslo šest zhodnocuje přínos nových komunikačních technologií, představuje podrobněji některá možná řešení IP telefonie a videokonferencí a zhodnocuje jejich přínos na korporátní úrovni. Závěr diplomové práce sumarizuje přínosy nových technických řešení a jejich použití ve firemní infrastruktuře, dále je predikován možný budoucí vývoj v této problematice.

Klíčová slova: Síťová infrastruktura, LAN, WAN, DNS, DHCP, Virtualizace, Cloud computing, VoIP, Videokonference, SLA

New technologies in infrastructure of corporate networks

Summary

This thesis analyses the new trends and technologies in the area of large-scale corporate computer networks. The first part (comprising the first three chapters) deals with the issues of the construction and the maintenance of geographically extensive networks, examining the economic implications of establishing such an infrastructure and evaluates the technical solutions that have been developed. Chapter four of the thesis analyses DNS and DHPC services, and considers the problems that arise when these are unavailable. Chapter five details the modifications in the topology of large-scale computer networks and demonstrates the benefits of these for the effective running of major corporations. Chapter six analyses the benefits of new communication technologies, presents in detail the possible solutions offered by IP telephony and video-conferencing and evaluates their added value at the corporate level. In its final chapter, the thesis summarises the benefits offered by new technologies and their use in corporate infrastructure. It concludes by outlining the possible future developments in this area.

Keywords: Network infrastructure, LAN, WAN, DNS, DHCP, Virtualization, Cloud computing, VoIP, Videoconferencing, SLA.

Obsah

Obrázky

1 Úvod

Počítačové sítě jsou v dnešní době zcela nepostradatelnou součástí všech podniků, téměř veškerá agenda zaměstnanců je zpracovávána na počítačích. Elektronicky jsou zpracovávány objednávky, evidence zákazníků, archivace faktur, bankovní převody, mailová komunikace, controllingové reporty a mnoho dalších činností. Počítače řídí výrobní linky, expedici i příjem zboží od dodavatelů. Automatizované systémy monitorují spotřebu elektrické energie, řídí vzduchotechniku, monitorují pohyb osob v budovách, obsluhují hasicí systémy. Aby bylo možné fungování všech těchto zařízení, je třeba vybudovat IT infrastrukturu odpovídající potřebám daného podniku. IT zázemí malé společnosti a mezinárodní korporace působící v desítkách státu bude samozřejmě z technického hlediska diametrálně odlišné. Důvod této odlišnosti, ale není primárně technický nýbrž ekonomický. Velká společnost může mít při výpadku některého systému velké ztráty, a proto vynakládá více peněz na eliminaci možných problémů a implementuje tomu odpovídající technická řešení. Stupeň složitosti roste spolu s velikostí podniku, zatímco celou počítačovou síť malé firmy může tvořit jediné zařízení, korporátní řešení jich může obsahovat desítky tisíc. IT infrastruktura nezahrnuje pouze počítačové sítě, ale jedná se o smysluplné propojení uživatelských stanic, serverů, databází, monitorovacích a komunikačních systémů i celých data center, přičemž robustnost této infrastruktury odpovídá rozumnému poměru investičních nákladů, provozních nákladů a ztrát v případě nefunkčnosti.

Ze strany velkých společností je vyvíjen značný tlak na snížení rozpočtu IT oddělení a současně zlepšení, zrychlení a zefektivnění služeb, které IT pro podnik zajišťuje. S nástupem „hospodářské krize“ v roce 2008 tento tlak ještě mnohonásobně zesílil a nároky na chod ICT jsou stále větší. Je třeba hledat nové technologie a přístupy tak, aby implementace byla rychlejší a potřebný počet zaměstnanců v IT co možná nejnižší. Právě tyto technologie a jejich možnosti jsou předmětem řešení diplomové práce.

2 Cíl práce a metodika

Hlavním cílem této práce je zhodnotit přínos nových technologií v informační a komunikační infrastruktuře velkých firem. Záměrem práce je i predikovat budoucí směr vývoje používání technologií v prostředí velkých sítí, kdy tyto technologie mají za úkol především zlepšovat dostupnost služeb a snižovat náklady na údržbu a náklady na personál (obecně i v IT oddělení).

Budou zde představeny některé trendy v nasazování informačních technologií. Přínosy implementace těchto technologií budou demonstrovány na konkrétních příkladech jejich nasazení. Dále bude představena problematika rozsáhlých firemních sítí a nezbytnost služeb DNS a DHCP, bude zhodnocen jejich význam a nové způsoby jejich implementace.

Jedním z dílčích cílů bude zhodnocení produktu DnsOne od společností Infoblox. Budou představeny možnosti tohoto řešení a budou uvedeny možnosti implementace a výhody v případě Disaster Recovery.

Dalším z dílčích cílů diplomové práce bude zhodnocení významu videokonferenčních řešení a jejich použitelnosti pro každodenní práci zaměstnanců.

Jednotlivé etapy práce:

Teoretická část:

- Studium a shromažďování informací o nových trendech v infrastruktuře ICT.
- Vlastní práce na projektech týkajících se daného tématu.
- Návrh struktury obsahu práce.
- Generalizace zkušeností získaných při nasazení IT řešení v prostření mezinárodní společnosti
- Vlastní tvorba teoretické části práce.

Praktická část:

- Volba technologií, na kterých bude demonstrován přínos pro podnik.
- Vymezení požadavků na zvolené technologie
- Celkový přínos zhodnocených řešení pro oddělení IT a zbytek podniku

3 Úvod do problematiky rozsáhlých firemních sítí

Počítačové sítě jsou obrazně řečeno páteří dnešních firem, propojují pobočky, národní centrály, dodavatele, odběratele, státní správu i zaměstnance na služebních cestách či pracujících z domova. Jejich role je z dlouhodobého a někdy i z krátkodobého hlediska naprosto klíčová pro fungování podniku. V dnešní době si lze jen těžko představit fungování banky bez možnosti elektronické komunikace s ostatními subjekty.

Téměř žádná rozsáhlá počítačová síť nevznikne v rámci jediného projektu, často je to výsledek mnoha let, kdy dochází k jejímu růstu a úpravám jako reflexi na požadavky podniku. Živý a dynamický podnik neustále expanduje, pohlcuje další společnosti, inovuje nabízené služby nebo nasazuje technologie sloužící k podpoře obchodu a zaměstnanců. Tyto podněty pak realizuje oddělení mající na starosti ICT. Geneze počítačové sítě je pak sledem mnoha dílčích projektů menšího či většího rozsahu. Jestliže dojde k budování nových poboček, je třeba následně posílit i infrastrukturu na národní centrále a následně i na centrále mezinárodní tak, aby bylo možné všem garantovat požadovanou úroveň služeb.

3.1 Dohoda o úrovni poskytovaných služeb

Dohoda o úrovni poskytovaných služeb je známa spíše pod anglickou zkratkou SLA znamenající service level agreement. SLA vznikla potřebou co nejpřesněji definovat úroveň, intenzitu a rozsah poskytovaných služeb pro zákazníka, přičemž zákazníkem může být i jiný útvar v rámci jednoho podniku. Tato smlouva definuje pro obě strany jasná pravidla a jejich povinnosti tak, aby z dlouhodobého hlediska docházelo k efektivní spolupráci.

Porozumění tomu proč podnik chce a potřebuje SLA je naprosto zásadní pro to, aby mohlo dojít k úspěchu obou smluvních partnerů. Dohoda o úrovni poskytovaných služeb je především právním dokumentem, který obsahuje nejen rozsah poskytovaných služeb, ale i případné pokuty za její nedodržení. Cílem dokumentu není penalizace outsourcingového dodavatele služby, ale předcházení výpadků služeb, jenž může ohrozit dobré jméno a obchodní záměry obou partnerů. Smlouva tak zamezí tomu, aby nedocházelo k chybám při poskytování služeb vycházejícím z rozdílnosti ve vzájemném očekávání.

„SLA by mělo být zaměřeno na tři klíčové oblasti. První bychom mohli nazvat „zárukou infrastruktury“, v praxi sem patří zejména charakteristiky typu vybavenost, konektivita, spolehlivost hardware a schopnost integrace různých technologií. Pro druhou klíčovou oblast se všeobecně vžil pojem „procesní záruky“, kde se nejčastěji jako příklad uvádějí

změny v pracovních procesech, jako jsou například přidání nového uživatele, nového účtu atd. Třetí kategorii nazýváme „vzrůstající záruky“. Úkolem této oblasti, jak již sám název napovídá, je především růst záruk a jistot, které dodavatel poskytuje svému zákazníkovi před možným selháním a nezdary.„ [1]

Záruky spolehlivosti služeb se uvádějí v číslech typu 97%, 99% nebo 99,999% a tato čísla charakterizují garantovanou dostupnost služeb. Číslo bývá vztaženo na kalendářní měsíc nebo rok. Jen pro představu si uveďme, co tyto hodnoty ve skutečnosti znamenají.

Dostupnost služeb na úrovni 97%

Rok má 365 dnů, což je možné zapsat jako 8760 hodin nebo také 525 600 minut. Jestliže je garantována dostupnost na úrovni 97%, zbylá 3% času pak mohou být služby nedostupné či v nedostatečné kvalitě. Tříprocentní výpadek pak představuje čas přibližně 21,6 hodiny měsíčně. Analogicky spočítané hodnoty jsou uvedeny v následující tabulce.

Garantované SLA	**maximální čas nedostupnosti služby za rok** (zaokrouhleno)
97%	15 768 minut (11 dnů)
99%	5 256 minut (3,7 dne)
99,9%	526 minut (8,8 hodiny)
99,99%	53 minut
99,999%	5 minut

Tabulka 1 - Maximální doba nedostupnosti služeb

Z předchozí tabulky je patrné, že splnitelnost SLA na úrovni 99,999% je velmi obtížná a bereme-li v potaz čas potřebný pro údržbu serverů nebo aktivních síťových prvků a jejich případný restart je tento čas téměř nesplnitelný. Přesto jsou na této úrovni spolehlivosti schopny pracovat například některé telefonní ústředny.

Další z klíčových oblastí SLA je měření. Běžně je tento úkol svěřován interním zaměstnancům odběratele služeb, ale v některých případech je vhodnější nechat tento úkol na třetí straně. Výsledky nezávislých kontrol jsou pak v definovaných časových intervalech předkládány smluvním stranám a ty pak na základě reportů provádějí vzájemné vyúčtování.

V rámci péče o zákazníka dochází v SLA i ke stupňování záruk, které se primárně zaměřují na neočekávané události, které mohou nastat. viz. HORA, Michal [1] *“SLA může obsahovat rejstřík možných chyb, jejich klasifikaci, frekvenci a způsoby jejich řešení. Příkladem může být, že 80 % problémů bude vyřešeno okamžitě a efektivně on-line a budou definovány*

jako problémy klienta. Tyto problémy mohou nastat z neznalosti jednotlivých uživatelů, a stačí tedy pomoc, např. po telefonu, k jejich rychlému vyřešení. Ostatních 20 % problémů může být závažnějších, a je tedy zapotřebí delší časové období k jejich vyřešení i možné další testování, aby byl problém úplně zažehnán. Pokud jsou problémy takto definovány a jsou správně a včas řešeny, potom dochází ke vzájemné důvěře mezi poskytovatelem a zákazníkem outsourcingových služeb, jejich lepší spolupráci, která následně vede i k maximální efektivitě obou smluvních partnerů. „

3.2 Jediný bod selhání

Jediný bod selhání je termín převzatý z anglického výrazu „single point of failure" (SPOF), je to označení kritického místa v systému. Jestliže dojde v tomto bodě k poruše, bude vyřazen z provozu celý systém. Tato místa jsou nežádoucí v kterémkoliv systému vyžadujícím vysokou dostupnost, ať už se jedná o počítačovou síť, softwarovou aplikaci nebo jiný průmyslový celek. Systém se stává robustnějším pomocí přidání redundance do všech možných SPOF. Redundance lze dosáhnout na úrovni vnitřních komponent počítače, na úrovni systému (více serverů, síťových přepínačů, …), nebo na místní úrovni (replikace). Vyhodnocení potenciálních míst selhání identifikuje kritické komponenty komplexního systému, které by v případě poruchy vyvolaly výpadek celého systému. Vysoce spolehlivé systémy nemusí spoléhat na žádné takové jednotlivé součásti.

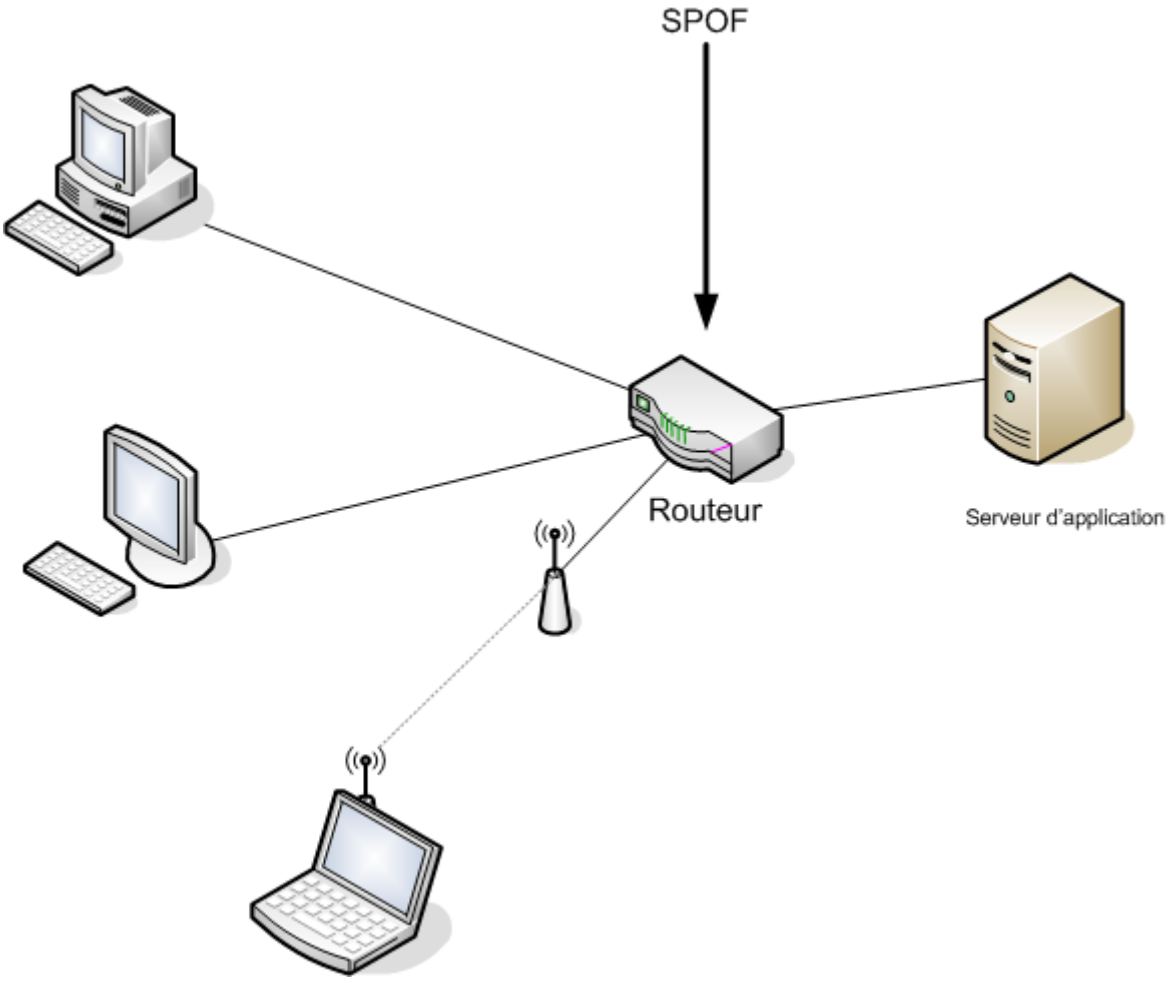
Z ekonomického hlediska každé redundantní řešení představuje nadbytečnou kapacitu, která není plně vytížena a generuje zvýšené náklady. Požadavky na redundanci, ale nevycházejí primárně z potřeb IT oddělení, ale jsou reakcí na požadavky podniku tak, aby mohl plnit své ekonomické cíle. Je tedy vždy na zvážení zodpovědného managementu, zda jsou ochotni akceptovat možné poruchy a čas potřebný k jejich odstranění, nebo investice potřebné k jejich předcházení.

Na obrázku 1. je znázorněn bod selhání v prostředí malé LAN sítě, kdy při selhání směrovače dojde k selhání celé počítačové sítě. V případě potřeby eliminace tohoto celkového selhání, je třeba přidat dodatečná zařízení a cesty a upravit nastavení serverů. V praxi lze postupovat následujícím způsobem:

- Každý důležitý systém je do počítačové sítě připojen pomocí dvou a více kabelů tak, aby každý z nich vedl do jiného síťového přepínače, dochází tak k eliminaci poruch způsobených síťovou kartou nebo nedostupností přepínače
- Všechny distribuční síťové přepínače jsou napojeny na vyšší vrstvu přepínačů opět tak, že každý prvek má spojení alespoň na dva další prvky a jestliže to situace

umožňuje je switch s každým prvkem propojen pomocí dvou cest, vylučuje se tak možná porucha na spojích mezi prvky

- Hlavní přepínače jsou také propojeny pomocí více cest na několik směrovačů, tato dodatečná spojení eliminují poruchy způsobené přepínačem, směrovačem, jejich propojením nebo komunikační linkou v prostředí WAN
- Směrovače pak mohou pro WAN nebo Internetovou konektivitu používat vetší počet tras či alternativních operátorů.

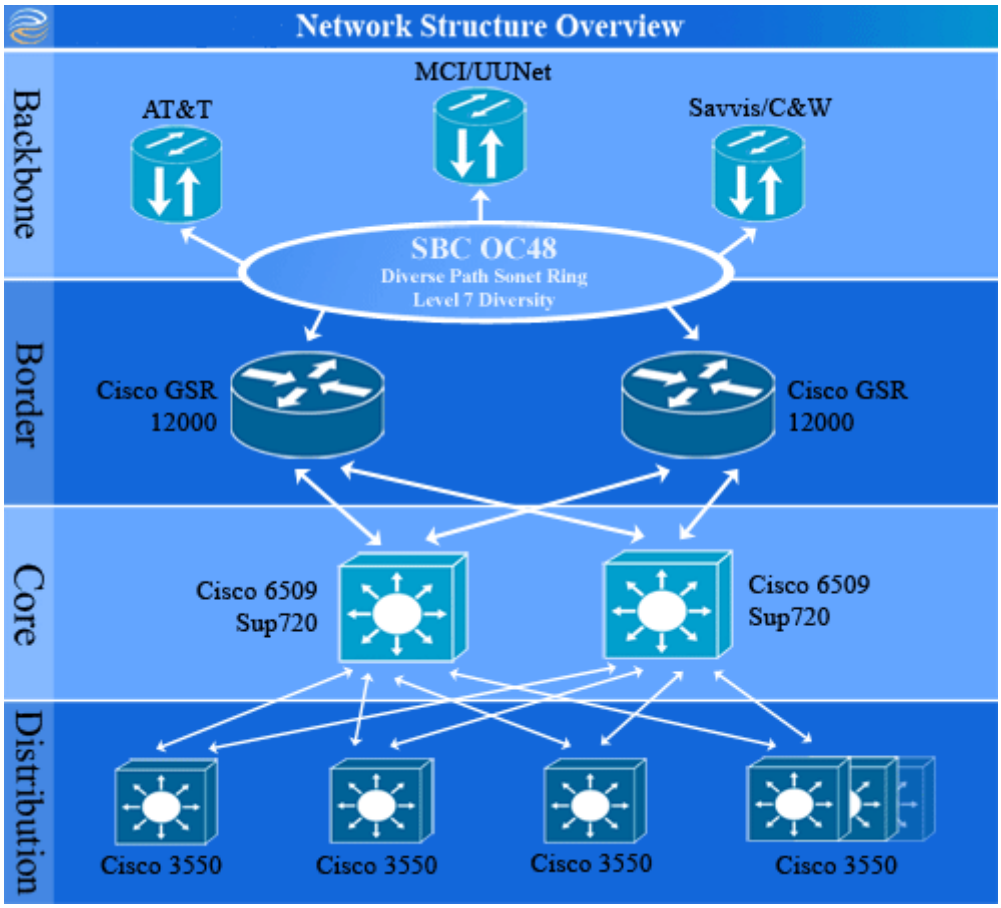


Obrázek 1 – SPOF, zdroj [1]

Jedno z mnoha možných řešení popisované redundance v prostředí robustnější sítě LAN je zobrazeno na obrázku 2.

Podniky při řešení záložních tras v prostředí počítačových sítí zacházejí ještě dále a dbají na to, aby záložní spoje mezi aktivními prvky vedly po jiných kabelových trasách, nebo aby každé zařízení bylo připojeno do elektrické sítě současně z několika nezávislých napájecích okruhů. Některé velké firmy jdou až tak daleko, že dopodrobna zkoumají topologii sítě

svých dodavatelů WAN konektivity, aby bylo možné eliminovat možný souběh vedení linek, kdy by při poruše jednoho bodu v síti došlo k výpadku na straně obou dodavatelů této konektivity.



Obrázek 2 - Eliminace SPOF v prostředí větší sítě LAN, zdroj [2]

Problematikou budováním vysoce dostupné síťové infrastruktury se zabývají následující zdroje [6] a [14].

3.3 Administrace a standardizace

Firmy, jež mají díky své velikosti pobočky v mnoha státech a jejichž oddělení zaměřená na podporu ICT musí mnohdy napomáhat udržovat a rozvíjet síťovou infrastrukturu obsluhující i stovky tisíc zaměstnanců. Již dávno došlo v podnicích k rozštěpení IT na oddělení aplikační, projektové, help desk, správu operačních systémů a sítí. Dále docházelo ke vzniku zcela nových oddělení, jejnž mají na korporátní úrovni na starosti

například centrální nákup hardwaru, vyhodnocování nových strategií a technologií, a standardizaci. Právě standardizace je pro kooperaci v IT velice důležitá, neboť harmonizované prostředí umožňuje rychleji implementovat nové technologie v mnoha zemích současně. V praxi je toho dosahováno díky liniové organizační struktuře v IT, fungování této struktury je možné nastínit na následujícím přikladu oddělení IT Networking:

Korporátní úroveň – určuje strategii celé společnosti, dodavatele hardwaru, typy používaných zařízení, nároky na redundanci, implementační scénáře, požadavky na zabezpečení, technicky schvaluje požadavky na nákup nových zařízení v jednotlivých dceřiných společnostech a jejich pobočkách ve všech státech.

3rd level support – udržuje „v chodu“ to, co bylo schváleno na korporátní úrovni, spravuje autorizační servery, řídí expanzi, řeší závažnější technické problémy, které nejsou schopni vyřešit administrátoři na nižších úrovních (z hlediska nedostatečného know-how, nebo nedostatečných oprávnění), generuje konfigurační šablony

Monitoring – operátoři pracující v 24 hodinovém provozu, zpravidla vyhodnocují automaticky reportované incidenty jako výstupy z monitorovacího softwaru, dle druhu incidentu informují jiné skupiny, nebo externí společnosti.

2nd level support – fungují na národní úrovni a podporují síťovou infrastrukturu v rámci tohoto státu, musí se řídit nařízeními nadřazených složek a reagovat na podněty od monitoringu a help desku.

Help Desk – zpracovává nahlášené požadavky od uživatelů a předává je dále, dělá pouze jednoduché úkony typu „propoj zásuvku a počítač“.

Nastíněný koncept má nesporné výhody, v případě odchodu pracovníka na lokální úrovni může dojít rychle k zablokování jeho účtu pro správu aktivních prvků a díky konfiguračním šablonám mohou být práva rychle delegována na nového zaměstnance. Model je výhodný i z ekonomického hlediska. Monitoring je prováděn ze zemí s levnou pracovní silou pro mnoho států současně a rovněž není třeba na lokální úrovni platit drahé síťové experty, jež nemůže firma plnohodnotně využít.

Dalším příkladem standardizace v prostředí síťové infrastruktury je správa moderních firewallů. Díky pokrokům v oblasti softwaru pro centrální správu je nyní možné spravovat několik tisíc firewallů pouze malým týmem pracovníků. Moderní firewallová řešení pracují jako distribuovaná architektura. Kdy je možné nasadit různé úrovně šablon a ty pak při změně konfigurace automaticky distribuovat napříč celou firmou. V mnoha případech tedy není nutné konfigurovat ručně jednotlivá zařízení. Dodavatelem takového řešení je například společnost CheckPoint.

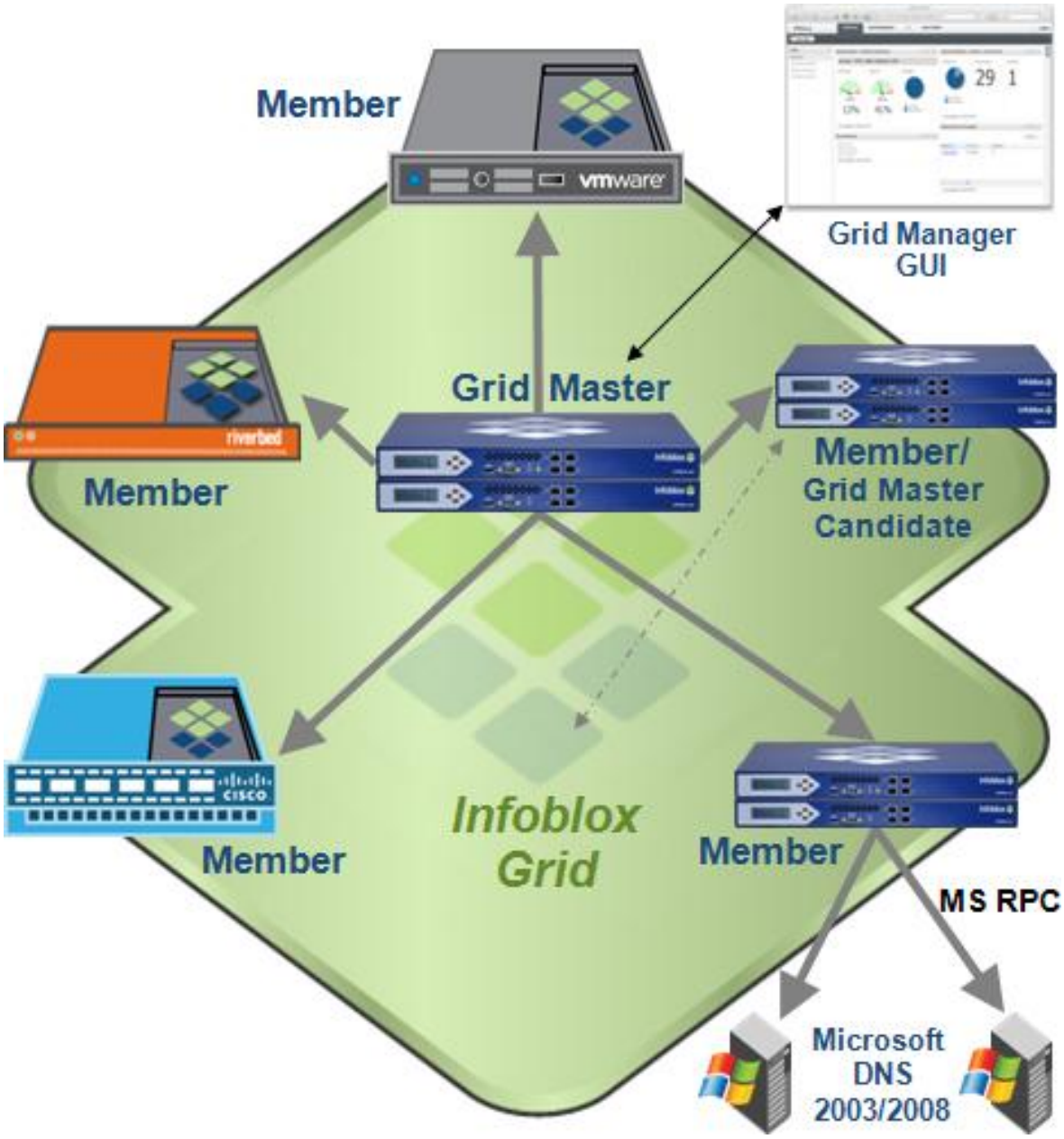
4 Služby DNS a DHCP

Pojmy DNS a DHCP rozhodně nepatří mezi novinky v síťové infrastruktuře, cílem této kapitoly tedy není hlubší seznámení s těmito protokoly, ale spíše zhodnocení významu pro počítačové sítě a nových způsobů jejich implementace. Pro úvod do problematiky komunikačního protokolu TCT/IP lze doporučit knihu Rity Pužmanové „TCP/IP v kostce“ [15]. Implementaci DNS a DHCP v prostředí Windows Server 2003 popisuje zdroj [16]. Protokol DNS pak velice podrobně popisuje kniha od Cricket Liu “DNS and BIND (5th Edition)“ [17].

4.1 DNSone

DNSone je produktem společnosti Infoblox, jedná se o síťové zařízení poskytující služby DNS, DHCP, NTP, FTP, SFTP a IP Address Management (IPAM). Zařízení je dodáváno v několika verzích v závislosti na požadovaném výkonu a počtu současných přístupů. DNSone box je schopen pracovat zcela samostatně jako běžný server, ale jeho hlavní výhodou je tzv. GRID. Grid je distribuovaný systém, kdy dochází k ovládání mnoha zařízení přes jeden jediný centrální bod. Tento bod je tvořen výkonnostně silnějšími boxy zapojenými do „HA pair“ což je pouze jiné pojmenování pro cluster. Grid si udržuje v databázi veškeré informace o podřízených boxech a jejich konfiguracích, provádí se přes něj veškeré změny v konfiguraci na podřízených boxech a umí provést i vzdálený online upgrade integrovaného operačního systému (IOS) na boxech. Skutečnost, že box používá vlastní databázi s konfigurací služeb a záznamů a současně tyto informace synchronizuje se zařízeními v jiné geografické lokalitě činní toto řešení velmi výhodným pro Disaster Recovery. V následujícím textu bude nastíněn postup při havárii DNS a DHCP služeb na DNSone boxu, přičemž tato havárie nebude mít díky použité architektuře žádný dopad na dostupnost služeb v síti a práci uživatelů.

1. Monitorovací systém nahlásí nedostupnost DNSone boxu na vzdálené pobočce.
2. Helpdesk po telefonu prověří, zda v lokalitě nedošlo k výpadku elektřiny apod.
3. Problém je předán od oddělení podpory síťové infrastruktury, je prověřeno nastavení aktivních prvků v lokalitě a na Gridu, lokální zaměstnanec se pokusí restartovat box. Obrázek je uveden v Příloze 1.
4. DNSone box stále nereaguje, je tedy připraven a odeslán náhradní box. Příprava boxu zahrnuje pouze nastavení IP adresy, masky sítě, výchozí brány, IP adresy gridu a heslo pro připojení, celá operace nezabere více než 5 minut.
5. Kurýrní služba doručí na pobočku náhradní box.



Obrázek 3 – DNSone, zdroj [3]

6. Zaměstnanci na pobočce odpojí porouchaný box a zapojí místo něj náhradní. Nový box po připojení do sítě začne komunikovat s gridem na centrále, zcela automaticky dojde k případnému upgradu integrovaného operačního systému a k nahrání konfigurační databáze. Jelikož grid, obsahuje vždy úplnou zálohu všech konfiguračních parametrů, není třeba provést žádnou další úpravu konfigurace. Synchronizace trvá 2 až 15 minut v závislosti na nutnosti provést upgrade IOSu a velikosti konfigurační databáze.
7. Porouchaný box je odeslán na centrálu a pak dále do servisu.

Aby výpadek služeb nepostihl uživatele v dané lokalitě je třeba, mít v konfiguraci DNS a DHCP nastaveny záložní servery. O těchto nastaveních se zmiňují následující kapitoly.

Implementace zařízení jako je DNSone, zapadá do současné strategie podniků v oblasti IT. Jak již bylo zmiňováno, firmy implementují nové technologie z důvodů větší robustnosti a odolnosti proti výpadku, zlevnění provozu a snížení nákladů na administraci. Zjednodušením obsluhy dochází k posunutí rutinních úkolů na nižší úroveň administrátorů a operátorů v dohledových centrech a tím k dalšímu snížení nákladů na provoz.

DNSone je nyní možné implementovat i jako virtualizovanou aplikaci na platformě VMware bez nutnosti zakoupení fyzického boxu viz obrázek 3.

4.2 DNS

Zkratka DNS pochází a anglického Domain Name System což lze volně přeložit jako hierarchický systém doménových jmen. Hlavním úkolem DNS je převod doménových jmen na IP adresy. Jedná se o distribuovanou databázi síťových informací realizovanou pomocí DNS serverů.

Pro potřeby budoucího výkladu je třeba objasnit několik pojmů:

Primární server – je DNS server na kterém vznikají záznamy, jestliže je v doméně nutné udělat změnu, tato změna musí být udělána na primárním serveru, každá doména má pouze jeden primární server.

Sekundární server – obsahuje kopii dat primárního serveru, data s primárním serverem průběžně synchronizuje, slouží k odlehčení zátěže primárního serveru a jako záloha v případě jeho výpadku.

Pomocný (caching only) server – slouží jako vyrovnávací paměť a odlehčuje tak zatížení dalších DNS serverů, ukládá si odpovědi na dotazy a poskytuje je při opětovných dotazech do doby, než vyprší jejich životnost.

Reverzní dotazy – převádí doménová jména zpět na IP adresy.

Dynamický update – tento druh úpravy DNS záznamů používají například klientské stanice, jejichž IP adresa je konfigurována pomocí DHCP protokolu. Protože se IP adresa může měnit, mění se tedy dynamicky i její přiřazení v DNS.

Bez možnosti překladu IP adres na doménová jména je funkce dnešních počítačových sítí takřka nemyslitelná. Stroje se bez DNS mohou v některých případech obejít, ale člověk jen

těžko. Lze si jen těžko představit nutnost pamatovat si IP adresy serverů v Internetu nebo firemní síti. DNS přináší mnoho výhod majících vliv na úroveň poskytovaných služeb, které je možné nastínit na následujících jednoduchých příkladech.

Příklad 1. Firma provozuje webový server, ale chce změnit poskytovatele Internetové konektivity. Tato změna představuje nutnost změnit i IP adresu, protože ta současná patří našemu současnému poskytovateli konektivity. Bez DNS by to znamenalo nutnost upozornit všechny obchodní partnery na novou IP adresu a nutnost předělat veškeré odkazy na náš server v internetu. S DNS „stačí“ pouze upravit záznam na DNS serveru a IP adresa může být změněna.

Příklad 2. Bez DNS je možné provozovat na jedné IP adrese pouze jeden webový server

Příklad 3. IP adresu verze 6 2001:0db8:85a3:0000:0000:8a2e:0370:7334 si je schopný zapamatovat opravdu jen málokdo.

Předcházející příklady jsou pravděpodobně až příliš triviální, ale jejich cílem bylo ukázat, že překlad IP adres na doménová jména je dnes chápán jako samozřejmost a uživatelé počítačových sítí si neuvědomují problémy spojené s nedostupností těchto služeb.

4.2.1 Rozložení zátěže DNS serverů

Mezinárodní společnosti používají pro své potřeby velké množství domén, přičemž většina jich slouží pro potřeby komunikace uvnitř podniku. Důvodem vzniku těchto často složitých struktur je potřeba rozčlenění zařízení do různých hierarchických celků, majících za cíl seskupit počítače dle dceřiných společností, států, lokálních poboček, typů zařízení v síti atd. viz následující tabulka.

Koncern	Řetězec	Stát	Pobočka	Druh zařízení
Metro AG	Kaufhof Media-saturn Metro	cn.metro.net cz.metro.net de.metro.net sk.metro.net	ho.sk.metro.net store21.sk.metro.net store22.sk.metro.net	printers.sk.metro.net computers.sk.metro.net maintenance.sk.metro.net

Tabulka 2 - Strom DNS

Replikace takto rozsáhlé databáze doménových názvů by byla značně problematická, docházelo by k velkému počtu aktualizací a byla by příliš zatěžována WAN konektivita. Řešením tohoto problému je distribuovaná architektura DNS, kdy dochází ke značné redukci zátěže sítě a zjednodušení správy DNS. V následující kapitole bude představena konkrétní implementace distribuované architektury DNS pomocí serverů s operačním systémem MS Windows a zařízení DNSone od společnosti Infoblox.

4.2.2 DNSone a služby DNS

Tato kapitola uvádí konkrétní příklad distribuované architektury služeb DNS v prostředí mezinárodní společnosti Metro AG, kde hlavní centrála společnosti je jediným přístupovým bodem do Internetu. Jelikož je vyžadována vysoká dostupnost služeb a rychlá obnova po haváriích, je pro jiné než serverové systémy použit pro poskytování služeb DNS box DNSone.

Hlavní zodpovědností při poskytování DNS služeb je:

Externí DNS:

- rozlišování doménových jmen v sítích společností Metro Group
- rozeznávání DNS pro Internet
- rozhraní z interního DNS do DNS celé skupiny Metro Group a Internetového DNS

Interní DNS:

- Je poskytováno pomocí DNSone
- Autoritativní pro všechny domény interních systémů
- Odpovídá na dotazy všem klientům
- Přímé interakce s DHCP

Microsoft DNS pro služby Active Directory:

- kořenové domény Active Directory hostované na serverech s Microsoft DNS z důvodu technické podpory

Autoritativní nastavení DNS viz Příloha 7.

Centrální DNS Server (umístěný v mezinárodní centrále)

- **Sekundární pro všechny zóny Metro Group**
- **Překládá doménová jména pro síť Metro Group a Internet**

DNSone HA pair (DNSone cluster umístěný v prostorách národní centrály)

- **Primární pro interní domény**
- **Primární pro clients.<cc>.madm.net (cc = country code)**
- **Primární pro reverzní zóny na národní centrále společnosti (HO = Head Office, národní centrála společnosti)**
- **Sekundární pro <cc>.madm.net**
- **Sekundární pro madm.net**
- **Přeposílání dotazů na externí DNS**

MS DNS Server (umístěný v prostorách národní centrály)

- **Primární pro <cc>.madm.net**
- **Sekundární pro madm.net**
- **Sekundární pro clients.<cc>.madm.net**
- **Přeposílání dotazů na DNSone HA pair**

DNSone na pobočce

- **Primární pro reverzní zóny na obchodě**
- **Sekundární pro clients.<cc>.madm.net**
- **Sekundární pro <cc>.madm.net**
- **Sekundární pro madm.net**
- **Přeposílání dotazů na DNSone HA pair na národní centrále**

DNS resolving viz Příloha 8.

Centrála

- **MS AD Servery**
  - **K překladu DNS na IP se používají pouze MS DNS servery**
  - **DNSone na centrále společnosti je možné použít k překladu pouze v případě, že MS DNS servery jsou nefunkční**
  - **Všechny relevantní DNS dotazy jsou zodpovězeny pomocí MS DNS serverů**
  - **Pro zodpovězení dalších dotazů je použito přeposlání**
- Všechna další zařízení připojená do počítačové sítě
  - **DNS překlad zajistí DNSone na centrále společnosti**

Obchod

- MS AD Server
  - **K překladu DNS na IP se používají pouze MS DNS servery**
  - **Alternativní překlad DNS zajišťuje DNSone na obchodě**
- Všechna další zařízení připojená do počítačové sítě

- DNS překlad zajistí DNSone na obchodě
- Alternativní překlad DNS zajišťuje DNSone na centrále

Jak je patrné z vizualizací v Příloze 7. a 8., jedná se ve své podstatě o velice efektivní řešení hierarchie DNS. Každé síťové zařízení má několik možných cest jak docílit překladu doménového jména na IP adresu. Přidaná hodnota, díky použití DNSone boxu v Grid konfiguraci, přidává takto řešené infrastruktuře na robustnosti a minimalizuje možnosti nedostupnosti služeb DNS.

4.3 DHCP

DHCP má jako dynamický protokol pro přidělování IP adres velký význam především pro klientské počítače, neboť díky tomuto protokolu není třeba konfigurovat síťová nastavení ručně. Servery, přepínače, směrovače a rozhraní pro administraci dalších zařízení připojených do počítačových sítí mají síťová nastavení konfigurována na pevnou hodnotu. Protokol DHCP nenastavuje pouze IP adresu nebo DNS server, ale i další parametry, které se dají využít například pro start operačního systému ze sítě. Jak již bylo zmíněno dříve, popis fungování DHCP protokolu není obsahem této práce, která si klade za cíl spíše poukázat na nové možnosti v jeho implementaci s cílem předejít možným výpadkům služeb, zjednodušení správy a zrychlení obnovy služeb v rámci Disaster Recovery. Pro úvod do problematiky DHCP lze proto znovu doporučit zdroje uvedené na začátku této kapitoly.

V lokálních sítích se nejčastěji používají DHCP servery běžící na serverech Microsoft Windows nebo operačním systému Linux. I když se tyto verze serverů neustále vylepšují, mají i svá omezení, což je příležitost pro zařízení jako je DNSone.

4.3.1 DNSone a služby DHCP

Hojně používaný DHCP server běžící na Microsoft Windows 2003 serveru má několik základních nevýhod:

- Není schopen jednoduše a automaticky replikovat svá nastavení na jiný server.
- Při instalaci oprav operačního systému a jeho následném restartu dochází k výpadku služeb.
- Činnost DHCP serveru mohou ovlivnit jiné služby poskytované serverem.

- V případě havárie serveru trvá jeho opětovné zprovoznění příliš dlouho.

DNSone box od společnosti Infoblox má oproti tomu následující výhody:

- DHCP není ovlivňováno žádnou jinou aplikací.
- Není nutné provádět restarty z důvodů údržby hostitelského operačního systému.
- Je možné konfigurovat „Failover Associations“, kdy při výpadku jednoho boxu převezme jiný jeho práci.
- GRID konfigurace skupiny boxů zmiňovaná v kapitole 4.1 zaručuje online zálohování všech nastavení z jednotlivých boxů na centrální cluster zvaný „HA pair“.
- Rychlá obnova služeb po hardwarovém selhání, blíže viz kapitola 4.1.

Jelikož bez správné konfigurace nejsou klientské systémy schopny komunikovat, je třeba nastavit procesy umožňující dostupnost těchto služeb i v případě havárie primárního DHCP serveru v dané sítí. Protože žádost o přidělení adresy DHCP serverem je zasílána jako broadcast v dané síti, je třeba mít v každé takovéto síti umístěn DHCP server, což je neekonomické a zbytečně administrativně náročné, nebo pomocí modifikace parametrů sítě změnit broadcast na unicast a odesílat požadavky na konkrétní server v jiné síti. Detailním popisem fungováním TCP/IP protokolu se zabývá Rita Pužmanová v knize „TCP/IP v kostce“ [15], fungování DHCP objasňuje například zdroj [16].

Aby bylo možné zaslat DHCP request mimo virtuální síť, ve které se daný počítač nachází, je třeba upravit konfiguraci této sítě, viz následující výpis z konfigurace přepínače.

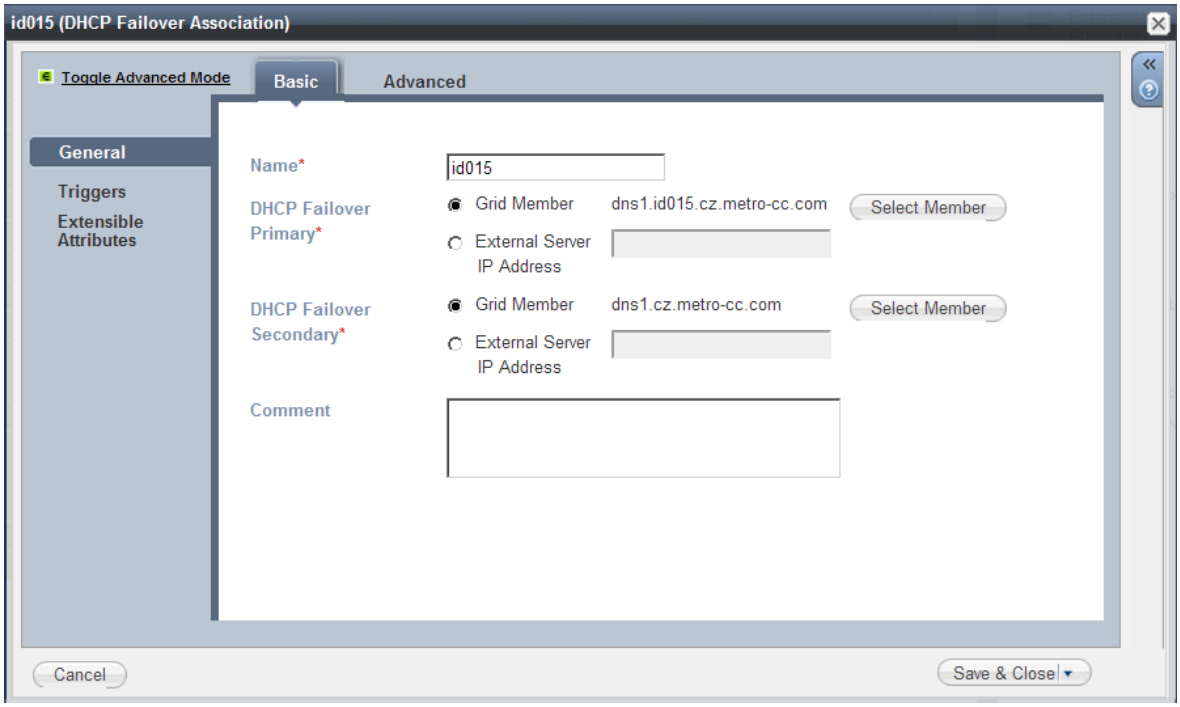
```
interface Vlan100
 description Wired Clients + Printers
 ip address 10.234.49.124 255.255.255.128       výchozí brána a maska sítě
 ip helper-address 10.234.48.19           DHCP server v LAN síti
 ip helper-address 10.234.48.17           PXE server v LAN síti
 ip helper-address 10.143.196.235         DHCP server na jiné pobočce
end
```

Díky této konfiguraci je žádost o přidělení adresy zaslána na tři uvedené adresy. PXE server odpoví pouze v případě, že má pro počítač s danou MAC adresou „bootovat“ ze sítě, což se řídí nastavením tohoto serveru. Odeslání DHCP reqestu na dva DHCP servery v různých lokalitách má své výhody. V případě nedostupnosti prvního serveru například z důvodu poruchy, začne IP adresy přidělovat záložní server, který má identickou konfiguraci. Je tak schopen přidělovat jak statické tak dynamické adresy.

Veškerá nastavení DHCP na všech boxech ve všech lokalitách jsou prováděna centrálně pomoci Grid Manageru, který je následně předává jednotlivým boxům. Nastavení je možné zálohovat, exportovat, předávat z boxu na box, nebo se z nich dají dělat šablony a ty následně znovu používat pro generování konfigurací. Konfigurace DHCP podporuje hierarchickou dědičnost nastavení, řazeno od nejvyšší úrovně:

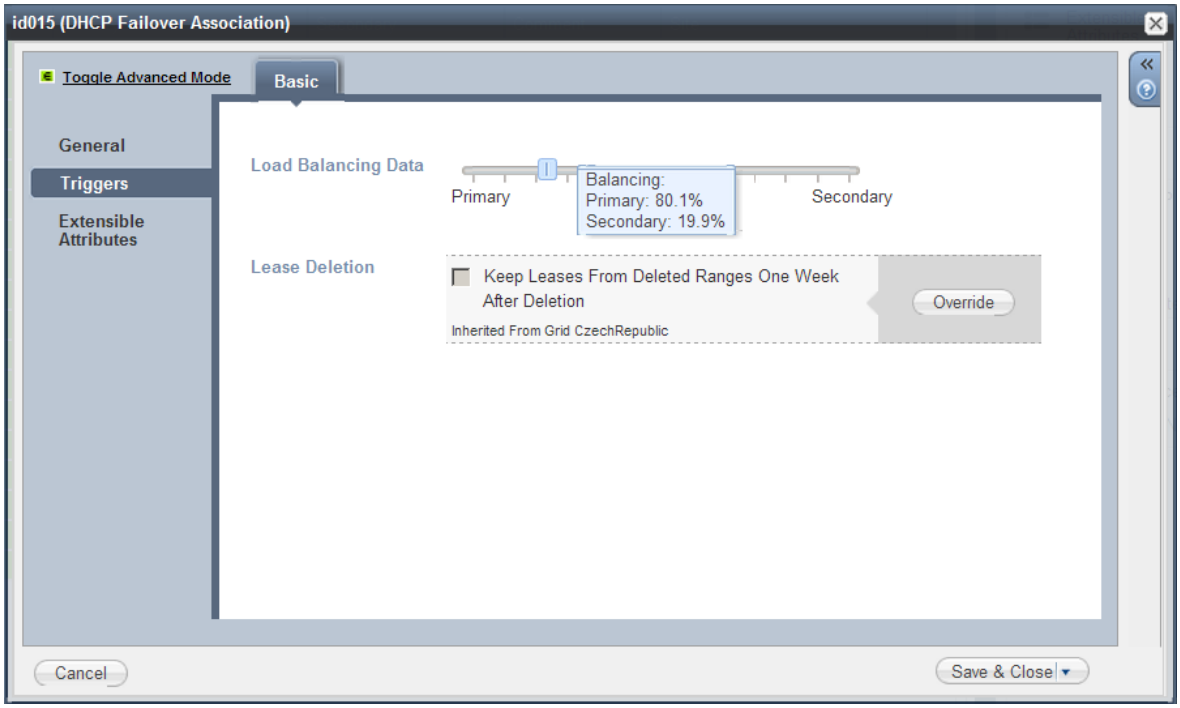
- Grid
- DNSone box
- Virtuální síť
- Rozsah dynamických adres v rámci jedné virtuální sítě
- Pevná rezervace

Dědičnost lze v libovolném místě přerušit a upravit jeden nebo více parametrů nastavení. Jak vypadají zmiňované možnosti nastavení z pohledu administrativní konzole Grid Manager bude zobrazeno na následujících obrázcích.



Obrázek 4 - DNSone Failover Association – Members

Obrázek 4. zobrazuje nastavení „Failover Associations“ toto nastavení umožňuje členům skupiny obsluhovat dynamický rozsah pro přidělování adres. Primární člen bývá v LAN síti sekundární v jiné geografické lokalitě dostupný pomocí sítě WAN. Oba servery sdílejí stejnou konfigurační databázi, obsahující i záznamy o přidělených adresách včetně času jejich exspirace. Aby byla většina DHCP reqestů zasílána na lokální server je pro dynamický rozsah adres v dané síti VLAN nastaven i Load Balancing. Toto nastavení určuje, v jakém poměru si mají jednotlivé boxy rozdělit žádosti o přidělení IP adresy viz orázek 5.

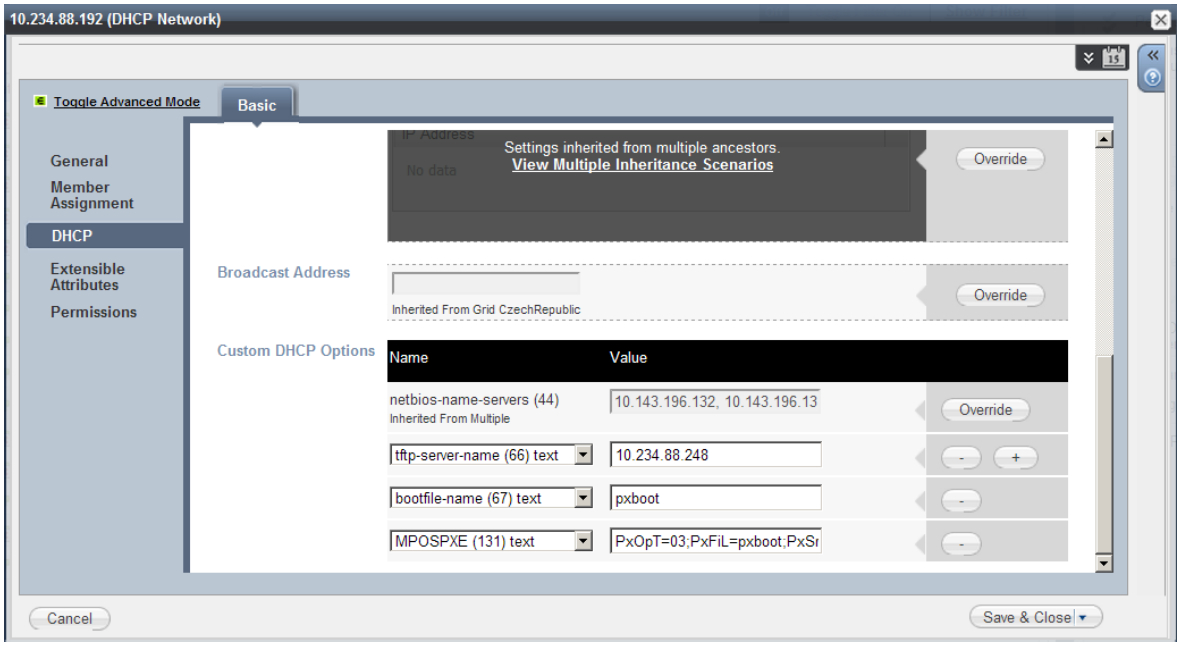


Obrázek 5 - DNSone Failover Association – Load Balancing

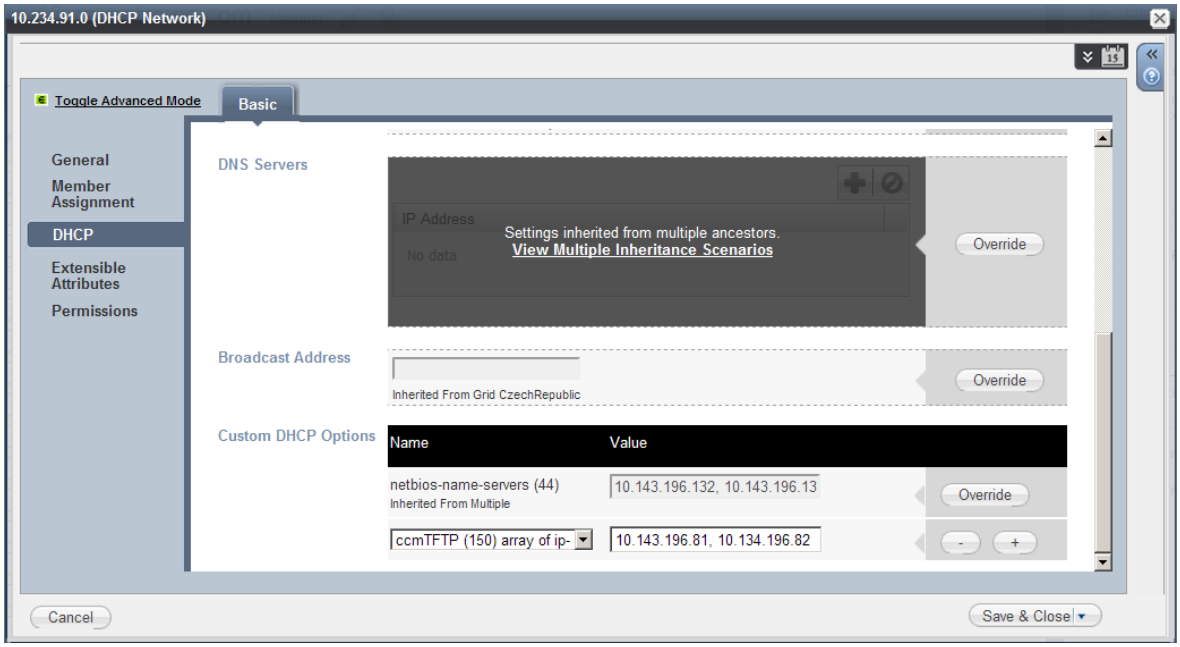
Některá síťová zařízení využívají speciálních nastavení. Konfigurace těchto parametrů je v Gridu velice snadná a díky nastavení dědičností a replikací je možné mít identické nastavení ve stovkách podsítí během několika málo vteřin. Custom DHCP options lze využít k řešení následujících úkolů:

- Startování operačního systému z počítačové sítě pro terminálové počítače.
- Image Deployment čili hromadnou reinstalaci počítačů
- IP telefonii, kdy Custom Options upozorňují telefon na umístění TFTP serverů
- atd.

Příklady těchto nastavení jsou na obrázcích 6. a 7. V přílohách 4., 5. a 6. jsou zobrazeny některé další výstupy z konfigurace Grid Manageru při správě DHCP.



Obrázek 6 - DNSone Failover Association – Custom Options PXE



Obrázek 7 - DNSone Failover Association – Custom Options VoIP

DNSone poskytuje velké množství pokročilých funkcí pro správu DNS, DHCP a NTP serverů. Svojí softwarovou architekturou umožňuje provádět hromadné operace na mnoha geograficky vzdálených lokalitách a současně bezpečné uchovávat konfigurační data. Administrace služeb pomocí tohoto produktu poskytuje oproti jiným řešením velkou časovou úsporu a v rozsáhlých sítích tato časová úspora zaručí brzkou návratnost investičních nákladů do poměrně drahého zařízení.

5 Topologie firemních sítí

Na topologii počítačové sítě je možné nahlížet z mnoha úhlů pohledu v závislosti na tom, co je cílem našeho zkoumání. Prvním z možných pohledů je vnímání počítačové sítě pouze z pohledu síťového administrátora, tedy jako prosté fyzické propojení aktivních prvků pomocí kabeláže.

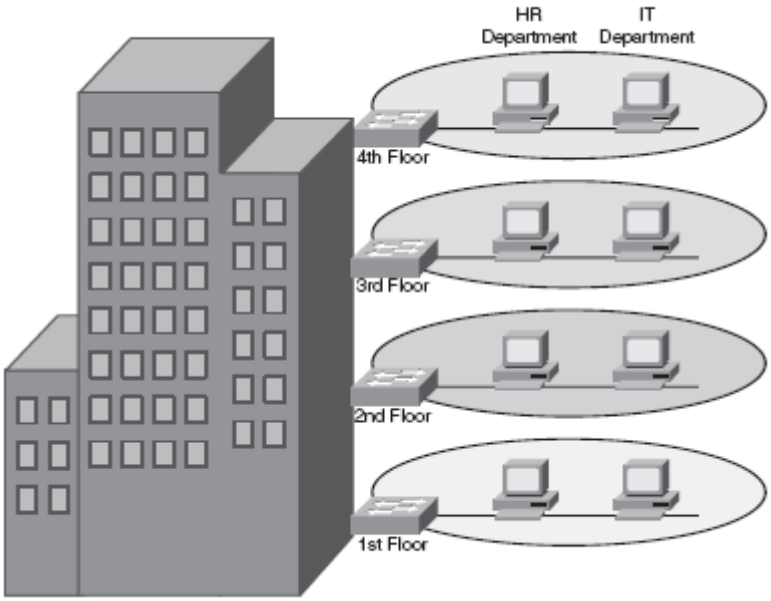
Tato část diplomové práce předpokládá znalost problematiky počítačových sítí, protokolu TCP/IP a ISO/OSI modelu, jejichž představení není náplní této práce. K úvodu do této problematiky lze využít následující zdroje.

[6] ODOM, Wendell, HEALY, Rus, METHA, Naren. Směrování a přepínání sítí

[7] DONAHUE, Gary. Kompletní průvodce síťového experta

[15] PUŽMANOVÁ, Rita: TCP/IP v kostce

[22] DEAN, Tamara: Network+ Guide to Networks Fifth Edition

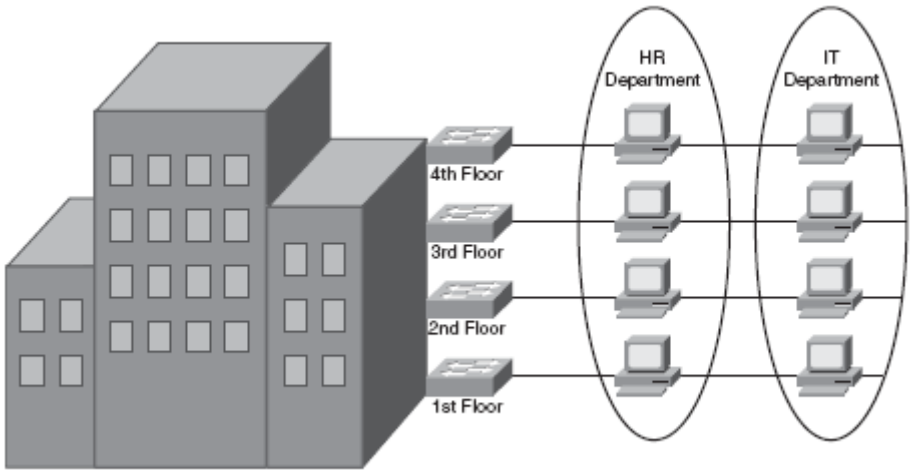


Obrázek 8 - Lokální virtuální sítě (Local VLANs), zdroj [8]

Základní topologická schémata jako je hvězda, kruh, sběrnice nebo strom v rozsáhlých sítích neplní nároky na redundanci spojení pro případ poruchy. Mimo toho, že dochází na

fyzické úrovni k přidání záložních tras, dochází ke konfiguraci sítí virtuálních a virtualizovaných. Virtuální sítě označované jako VLAN umožňují logické propojení nezávislé na fyzické vrstvě, které fungují na druhé vrstvě ISO/OSI modelu viz. obrázek [8] a [9].

Virtualizovaná síť vznikla z potřeby pokročilých síťových služeb uvnitř rozsáhlých virtualizovaných řešení postavených na platformách od firem VMware a Microsoft. Firma Cisco virtualizovala IOS (Internetwork Operating System) svého přepínače a umožnila tak vytvářet plnohodnotná logická propojení uvnitř virtuální infrastruktury, bez nutnosti fyzické potřeby síťových přepínačů a datové kabeláže. Z tohoto řešení plynou mnohé výhody, za ty hlavní lze uvést nižší náklady na pořízení, lepší škálovatelnost a v neposlední řadě i nižší spotřeba elektrické energie. Například Síťový přepínač Cisco 6509 určený pro datacentra má příkon 8000W, to znamená roční spotřebu okolo 70MWh. Za předpokladu, že se fyzický přepínač podaří zcela nahradit virtualizovaným přepínačem, může úspora na elektrické energii pouze na tomto zařízení činit i několik desítek tisíc korun ročně.



Obrázek 9 - End-to-End VLANs, zdroj [9]

Malé data centrum obsahující 100 serverů, datové pole, aktivní prvky a klimatizační jednotky má příkon 50kWh, roční spotřeba elektrické energie je 438MWh. Cena této energie činí přibližně 2.000.000,-Kč. Jestliže dojde k virtualizaci těchto serverů, je možné ušetřit 50% dle některých studií až 80% elektrické energie. Tyto úspory pak mohou představovat velice rychlou návratnost investic do virtualizace. Blíže se tímto tématem zabývá například zdroj [4], který ve své studii u popisovaného projektu prokázal návratnost investic (ROI) ve výši 237,8%.

Dalším pohledem na topologii počítačových sítí je pohled aplikační. V minulých letech bylo zcela běžné, že při přechodu na novou verzi programů nebo CRM systémů bylo nutné posílit HW serverů a komunikační trasy. Nová softwarová řešení však umožňují optimalizaci výkonu například pomocí SSL akcelerace a inteligentní kompresí dat, kdy dochází ke snížení objemu přenášených dat na 1/4 až 1/8 původního objemu. Není tedy nutné posilovat propustnost datových linek, jejich kapacita může být použita i pro jiné aplikace nebo může být snížena. Aplikační Caching snižuje zátěž aplikačních serverů a to díky neregenerování opakovaně vyžádaného obsahu viz. [23].

5.1 Virtualizace

Virtualizace a konsolidace je aktuální směr v oblasti IT, slibující sjednocení správy, zvýšení kontroly dat, podporuje ekologické cíle společností a snižuje energetickou náročnost. Virtualizovaná infrastruktura je snadno modifikovatelná a může se od té fyzické značně lišit.

Na fyzický hardware je instalován tzv. Hypervisor což je software umožňující instalaci virtualnizovaných operačních systémů a aplikací. Mezi hlavní dodavatele těchto řešení patří například VMware, Microsoft, Citrix a XEN. Hypervisor přiřazuje virtuálním strojům zdroje v podobě počtu procesorů, paměti, místa na disku, síťové karty atd.

Při virtualizaci tedy dochází k jisté agregaci a na jednom fyzickém serveru je možné dle použitého hardwaru, provozovat i několik desítek virtualizovaných strojů. Tomu, zda půjde o poměr fyzických ku virtuálním serverům 1:2 nebo 1:20 musí nejprve předcházet důkladná analýza. Nástroje pro tuto analýzu dodává Microsoft, VMware i další. Měří se využití procesoru, pamětí, počet I/O operací při zápisu na disk a další parametry. Po vyhodnocení těchto parametrů je pak možné nedoporučit či doporučit virtualizaci serveru a stanovit podmínky nutné pro udržení požadovaného výkonu a odezev serveru. Nebezpečí přetížení fyzických serverů plynoucí z příliš velkého počtu serverů virtuálních se lze vyhnout pomocí následujících pravidel [26]:

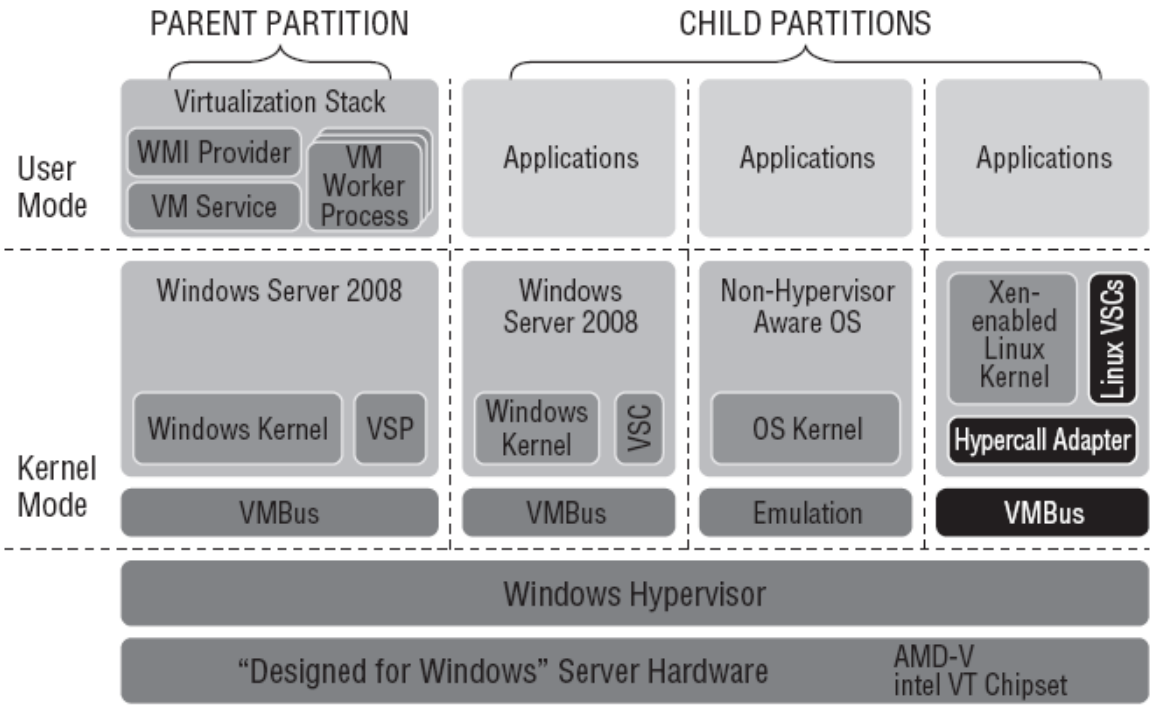
- Virtualizace začíná analýzou kapacity
- Nepřetržitý monitoring výkonu
- Testování stability aplikací
- Získávání výsledků zátěžových testů z reálného provozu od podobných subjektů

Blíže o tomto tématu pojednává například Daniel Ruest v knize Virtualizace podrobný průvodce [2] nebo David Rule spolu s Rogierem Dittnerem v knize The Best Damn Server

Virtualization Book Period [3]. Z ekonomického hlediska je zajímavý článek Zbyszeka Lugsche [4], jedná se o případovou studii virtualizace 29 serveru, kde dochází po třech letech od realizace k podrobnému vyčíslení nákladů a úspor. Návratnost investic (ROI) u popisovaného projektu dosáhla 237,8%.

Dalším příklad úspěšné konsolidace data centra je popsán v článku Petra Vlasatého [24]. „… V rámci programu náhrady hardwaru Sun nahradil 2915 kusů zařízení. Při poměru 2:1 pro servery (starý hardware ku novému) a 3:1 pro úložná zařízení jsme dosáhli 450% nárůstu výpočetního výkonu, 88% zmenšení prostoru potřebného pro tato zařízení a 61% snížení spotřeby elektrické energie. Celkově jsme snížili výdaje na výstavbu nového Data Centra o 9 milionů dolarů. Díky prostorovým a energetickým úsporám zde byla návratnost investic velmi rychlá.“

Za jednu z hlavních výhod virtualizace lze z technického pohledu považovat to, že dochází k oddělení operačního systému od hardwaru. Virtualizovaný operační systém tedy nepoužívá ovladače ke skutečným komponentám serveru, na kterém je instalován Hypervisor, ale používá ovladače pro komponenty prezentované hypervisorem. Změnu ovladačů by bylo možné považovat za nedůležitý detail, ale z praktického hlediska toto řešení přináší značné výhody. Virtualizovaný server je pak možné v rámci virtualizační platformy (ESX, Hyper-V, …) přenášet na jiné fyzické servery s rozdílnou konfigurací bez nutnosti dalších úprav. Na následujícím obrázku je schéma virtualizace na platformě Microsoft Hyper-V.



Obrázek 10 - Virtualizace Microsoft Hyper-V, zdroj [10]

5.1.1 Live Migration

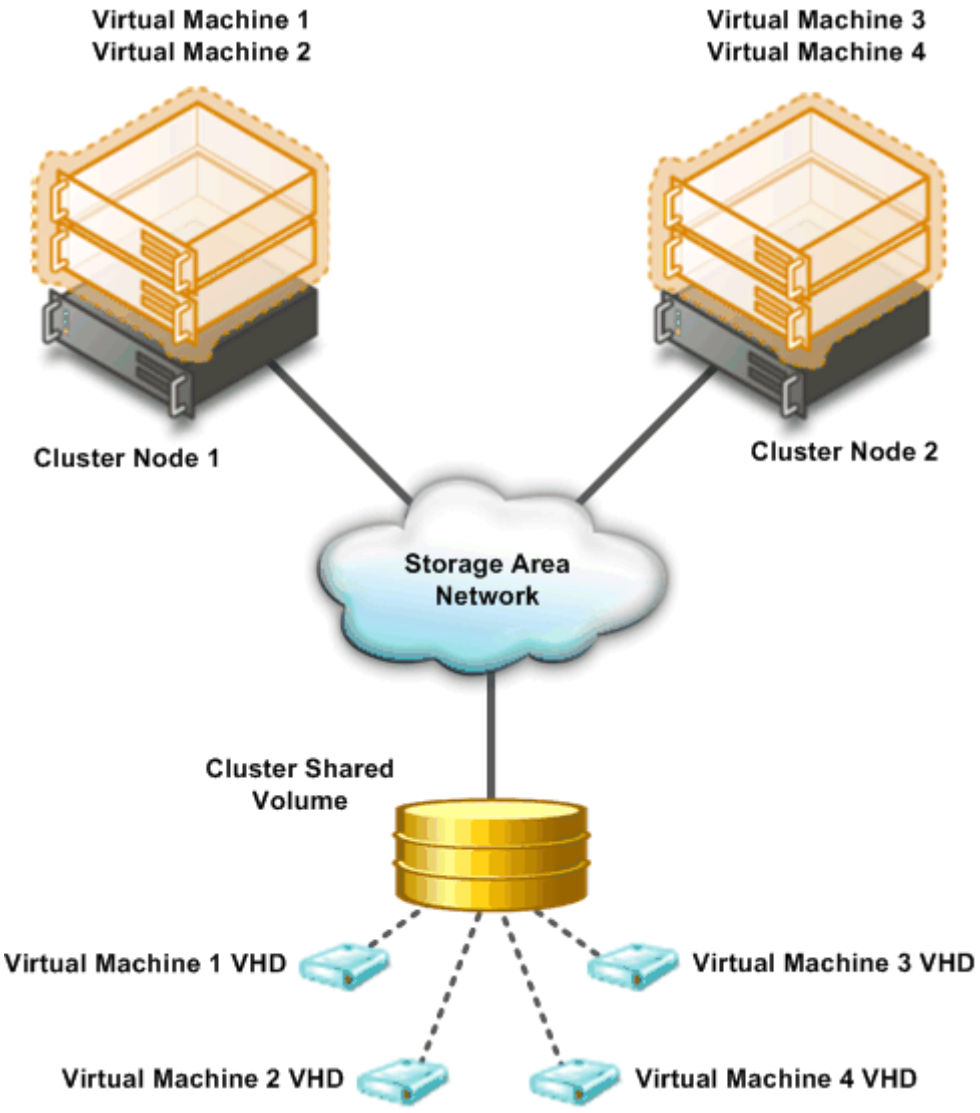
Tak jak různá řešení pro virtualizaci získávají na popularitě, opadá postupně i nedůvěra systémových administrátorů a jejich nadřízených. Přestože je většina virtualizačních projektů realizována pomocí VMware ESX serveru, zůstává zde prostor i pro jednodušší řešení. Firma Microsoft dodává svůj produkt Hyper-V zdarma jako součást řady operačních systémů Windows Server 2008. Tento produkt používají podniky pro nepříliš kritické servery a pro testovací prostředí, ale s příchodem verze Hyper-V 2.0 se začíná virtualizovat i produkční prostředí a popularita tohoto produktu rychle roste.

Nová verze tohoto produktu obsahuje funkci Live Migration neboli „živou migraci“, která umožňuje přesun virtuálního serveru za plného provozu na jiný server a to bez ztráty spojení s klienty připojenými na server. Funkce je využitelná v případě, že je nutné provést údržbu nebo opravu fyzického serveru a zároveň není možné provést odstávku virtuálního serveru. V následujícím textu bude uveden postup tohoto přesunu v prostředí Microsoft Windows Serveru 2008 R2, Hyper-V 2.0 jiné virtulazační platformy pracují na podobném principu.

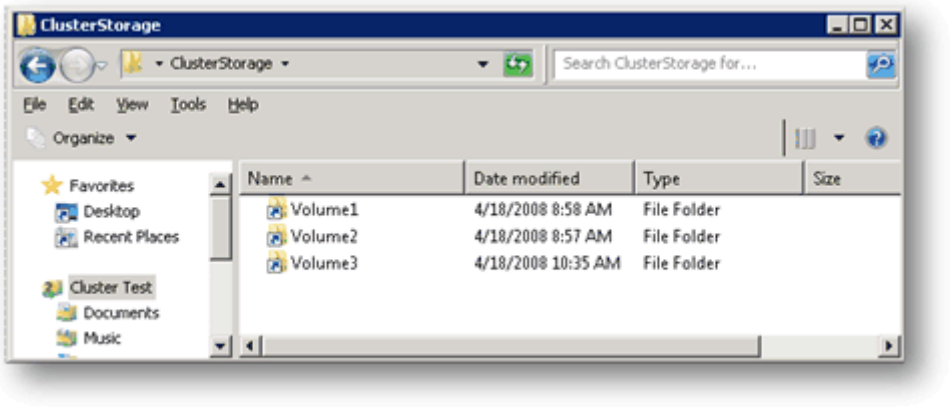
Následující text vyžaduje znalost problematiky virtualizace a datových polí, jejichž popis není předmětem této práce. Jako úvod do této problematiky mohou sloužit následující zdroje: [2], [14], [19], [20], [21], [27].

Live Migration používá nových funkcí clusterových sdílených svazků **(Cluster Shared Volumes - CSV)** spolu s funkcí Failover Clustering. CSV svazky umožňují více uzlům ve stejném failover clusteru souběžně přistupovat ke stejnému číslu logické jednotky (LUN). Z pohledu virtuálního stroje **(Virtual Machine - VM)**, každému virtuálnímu počítači se zdá, že skutečně vlastní LUN, avšak všechny *.VHD soubory pro jednotlivé VM jsou uložené na stejném svazku CSV, jak je znázorněno na obrázku 11.

Vzhledem k tomu, že CSV poskytuje konzistentní jmenný prostor do všech uzlů v clusteru, všechny soubory uložené na CSV mají stejný název a cestu z libovolného uzlu v clusteru. CSV svazky jsou uloženy jako adresáře a podadresáře pod kořenovou složkou ClusterStorage, jak je znázorněno na obrázku 12.



Obrázek 11 - Cluster Shared Volumes – CSV, clusterový sdílený svazek, zdroj [11]

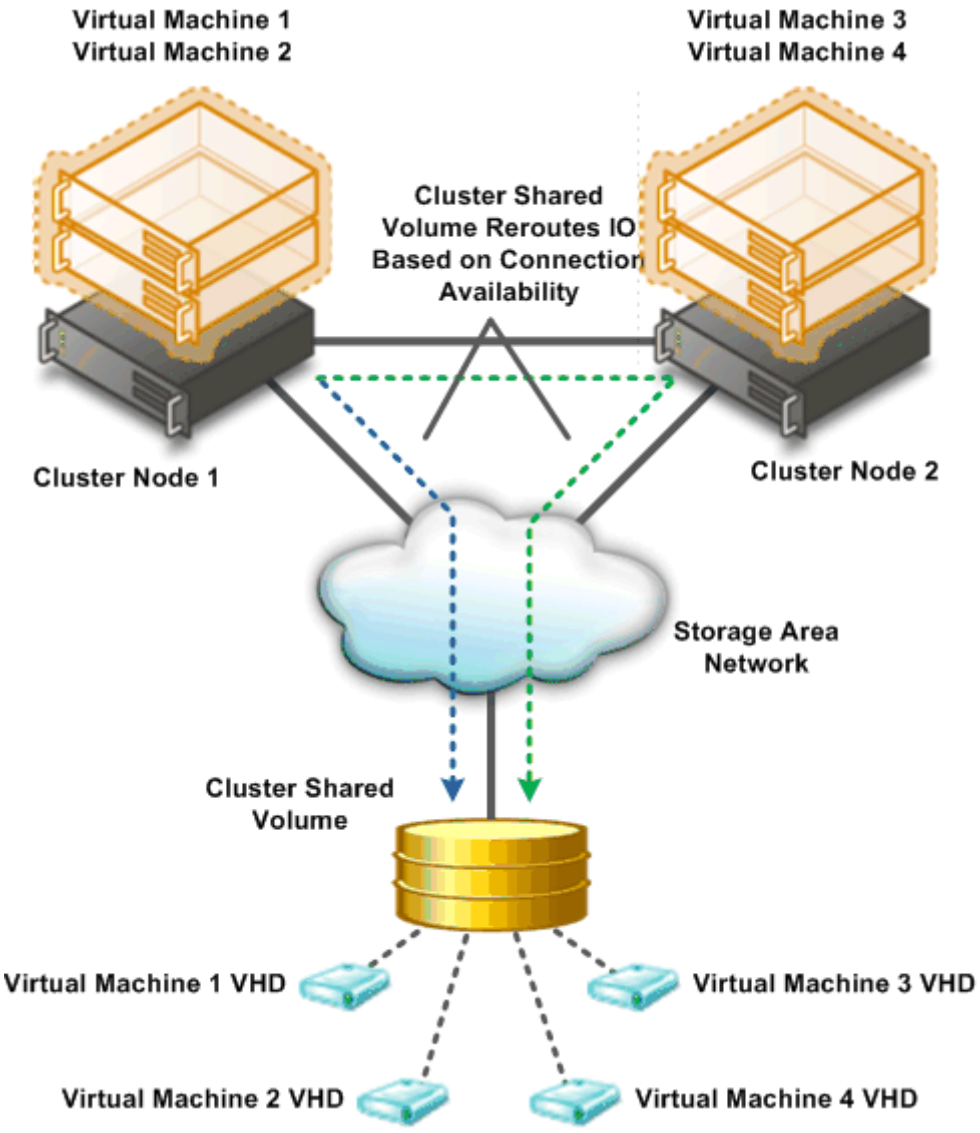


Obrázek 12 - Příklad jmenného prostoru na clusterovém sdíleném svazku, zdroj [12]

Jak je znázorněno na předchozím obrázku, jsou CSV svazky uložené ve složce ClusterStorage. Pokud je složka ClusterStorage umístěna na disku E:\, bude úplná cesta ke každému svazku CSV vypadat následovně:

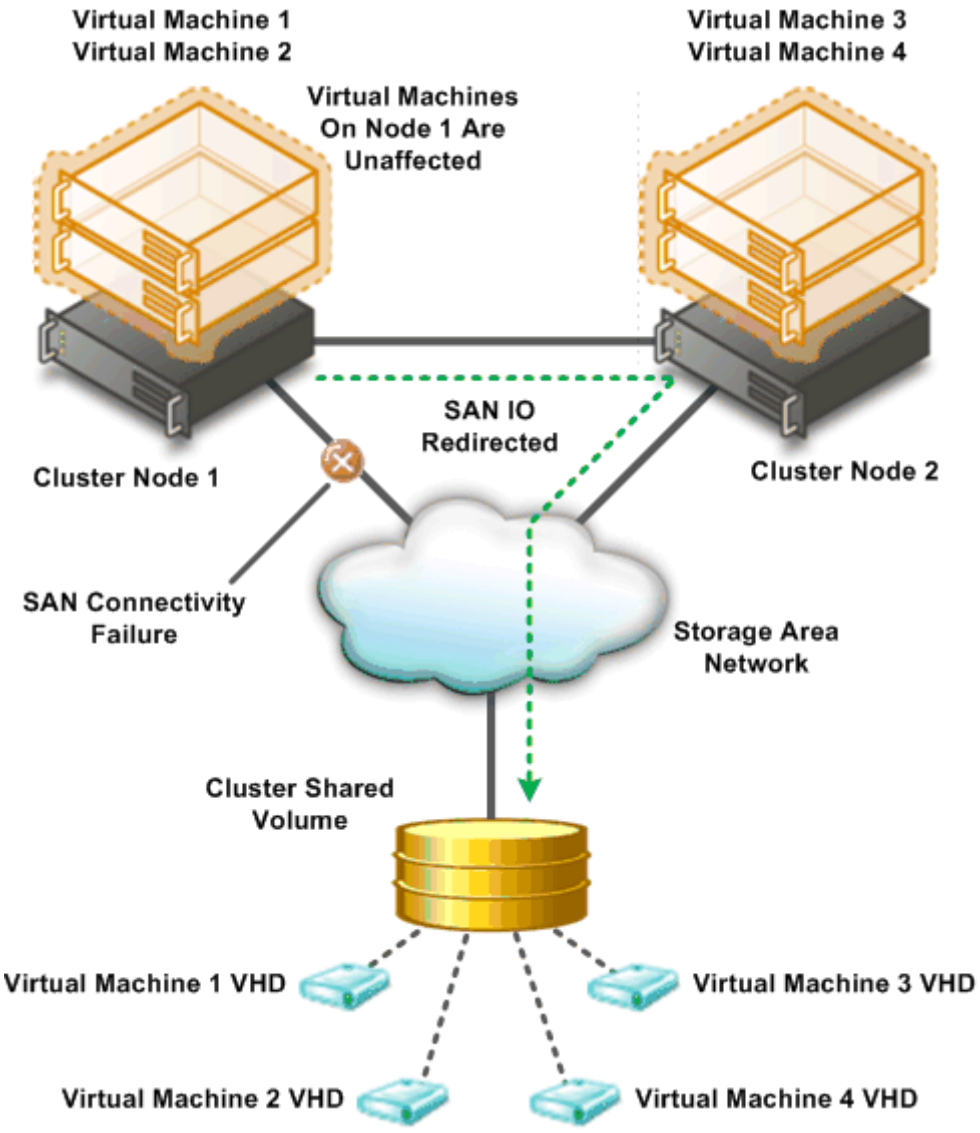
- E: \ ClusterStorage \ Volume1 \ root
- E: \ ClusterStorage \ Volume2 \ root
- E: \ ClusterStorage \ Volume3 \ root

Všechny uzly clusteru mají přístup ke sdíleným svazkům pomocí těchto plně kvalifikovaných cest. Vzhledem k architektuře CSV, je tak odolnější proti chybám, které se přímo dotýkají VM běžících na clusteru. Architektura CSV implementuje mechanismus, známý jako dynamické I/O přesměrování **(Input / Output)**, kde lze I/O přesměrovat do záložního clusteru na základě dostupnosti připojení, jak je znázorněno na obrázku 13.



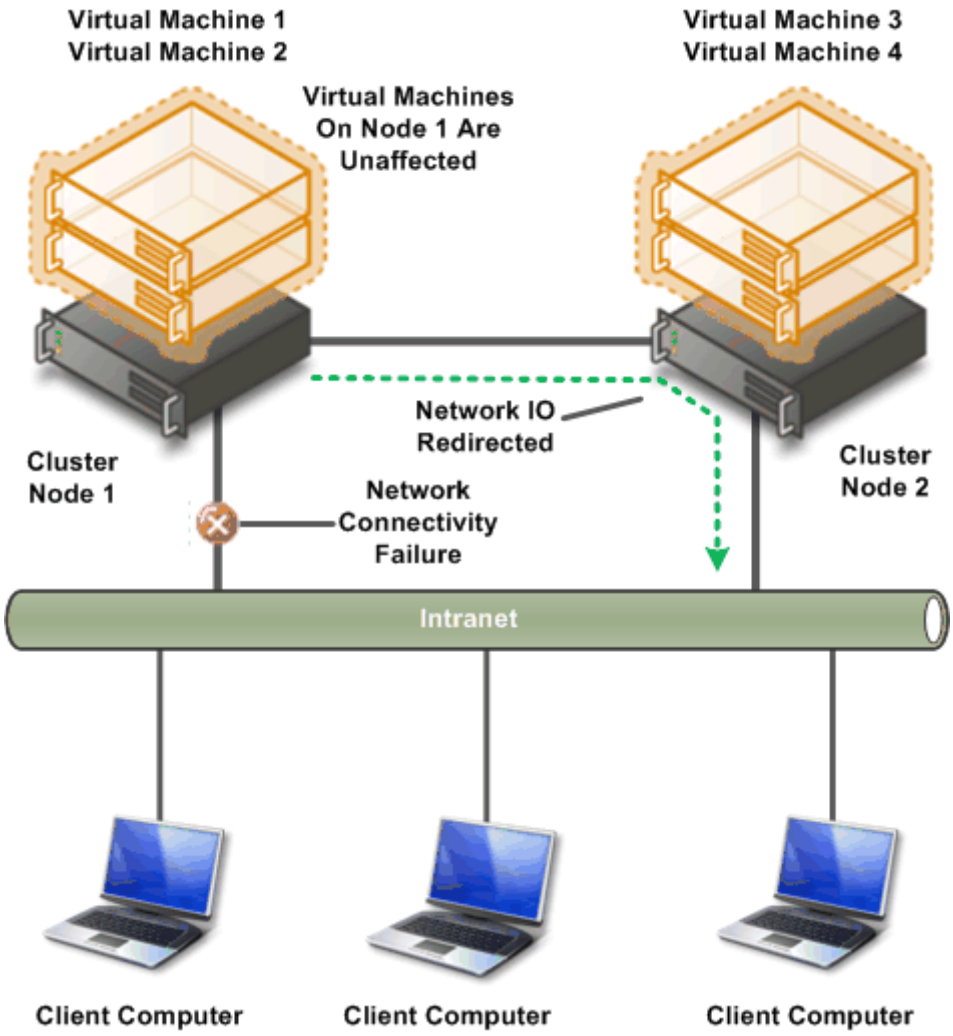
Obrázek 13 - Dynamické přesměrování I/O operací pro clusterový sdílený svazek na disku, zdroj [13]

První typ selhání, které může být přesměrováno, je selhání uzlu clusteru připojení ke sdílenému úložišti mezi uzly clusteru, typicky na Storage Area Network (SAN). Jak je znázorněno na obrázku 14., selže-li SAN připojení na uzlu 1, I/O operace jsou přesměrovány přes síť do uzlu 2. Uzel 2 pak provádí I/O operace do SAN. To umožní administrátorům udělat live migraci virtuálního serveru běžícího na uzlu 1 do uzlu 2.



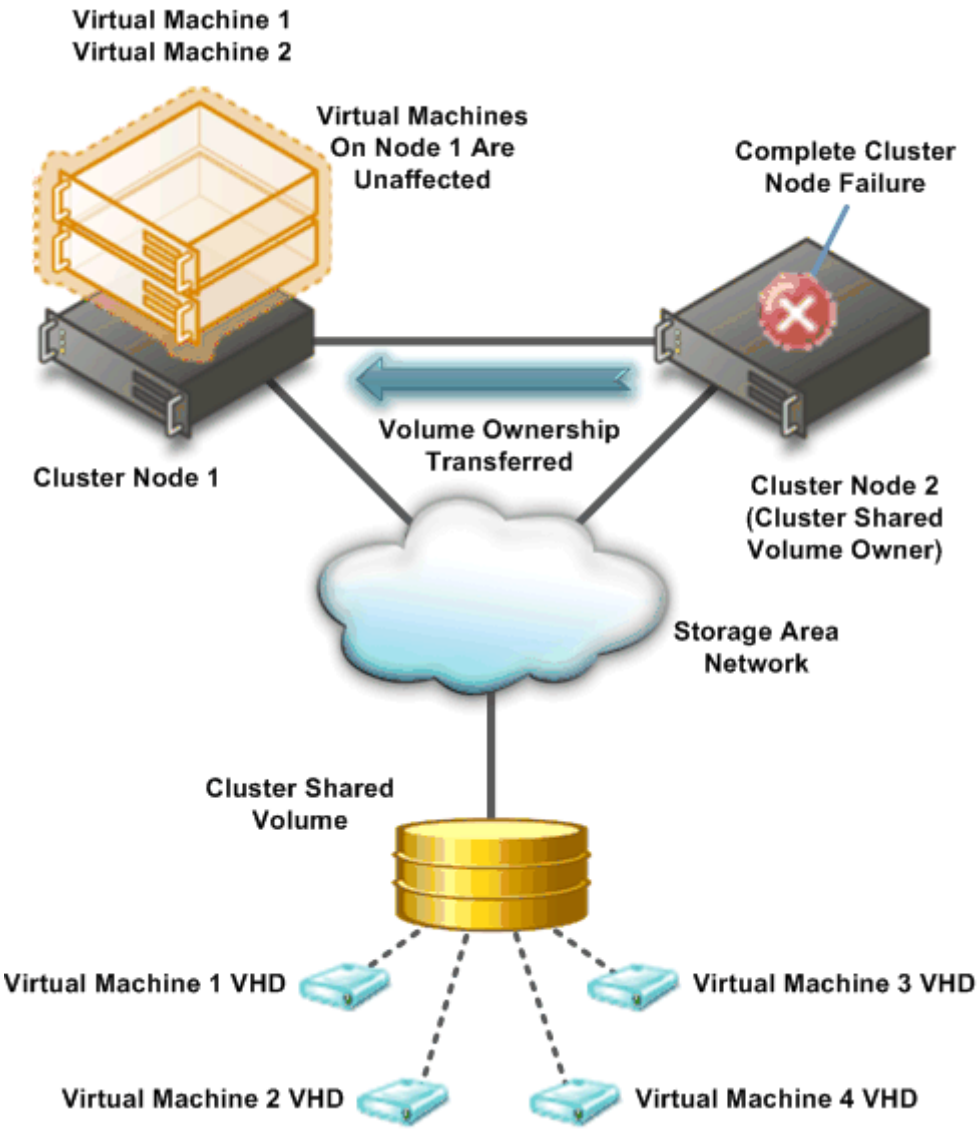
Obrázek 14 - input / output propojení odolné proti chybám, zdroj [14]

Dalším typem selhání, které může být přesměrováno, je selhání připojení k síti pro uzel clusteru. Jak je znázorněno na následujícím obrázku, primární síťové spojení mezi uzlem 1 a uzlem 2 selhalo. Uzel 2 automaticky přesměrovává provoz v síti přes redundantní připojení k síti a uzel 1 provádí síťové I/O operace.



Obrázek 15 - Síťové připojení odolné proti chybám, zdroj [15]

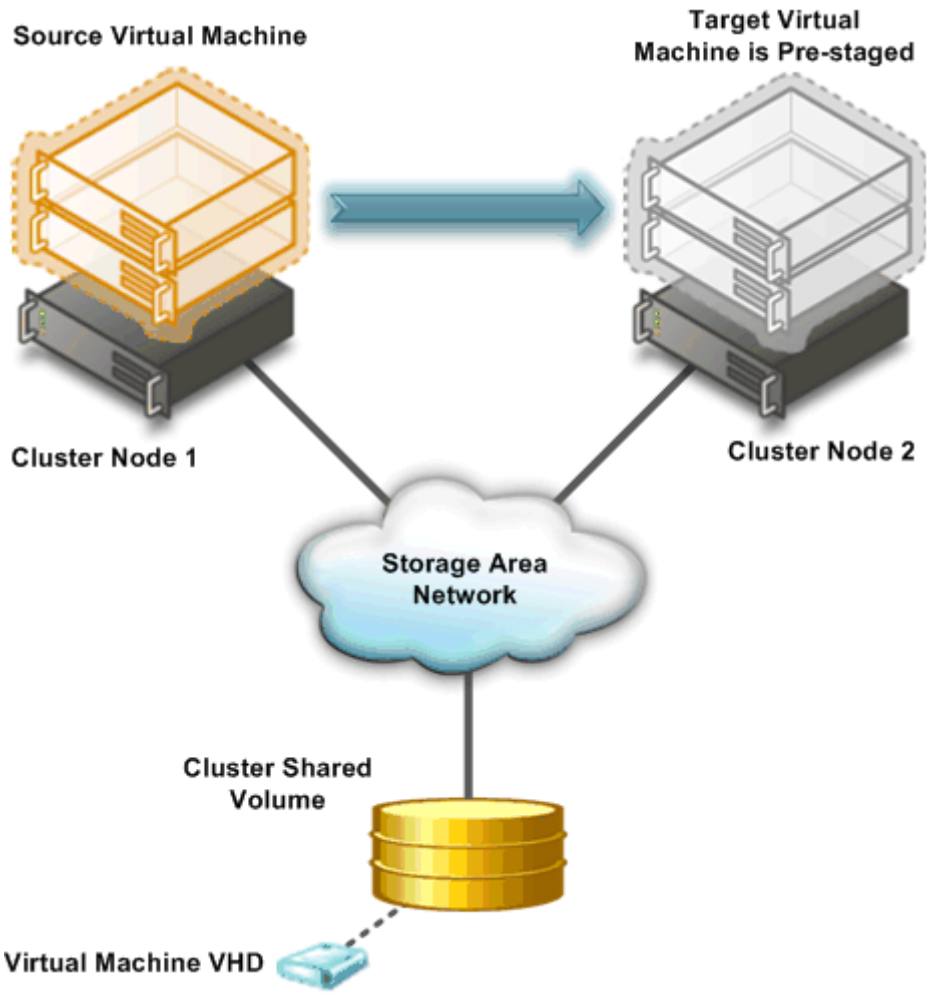
Dalším typem selhání, které může být přesměrováno, je selhání celého uzlu clusteru. Jak je znázorněno na obrázku 16., uzel 1 vlastní svazek, který je používán virtuálním serverem běžícím na uzlu 2. V případě úplného selhání uzlu 1, je vlastnictví svazku změněno na uzel 2 bez jakéhokoliv přerušení služby virtuálního stroje spuštěného na uzlu 2.



Obrázek 16 - Uzel clusteru odolný proti chybám, zdroj [16]

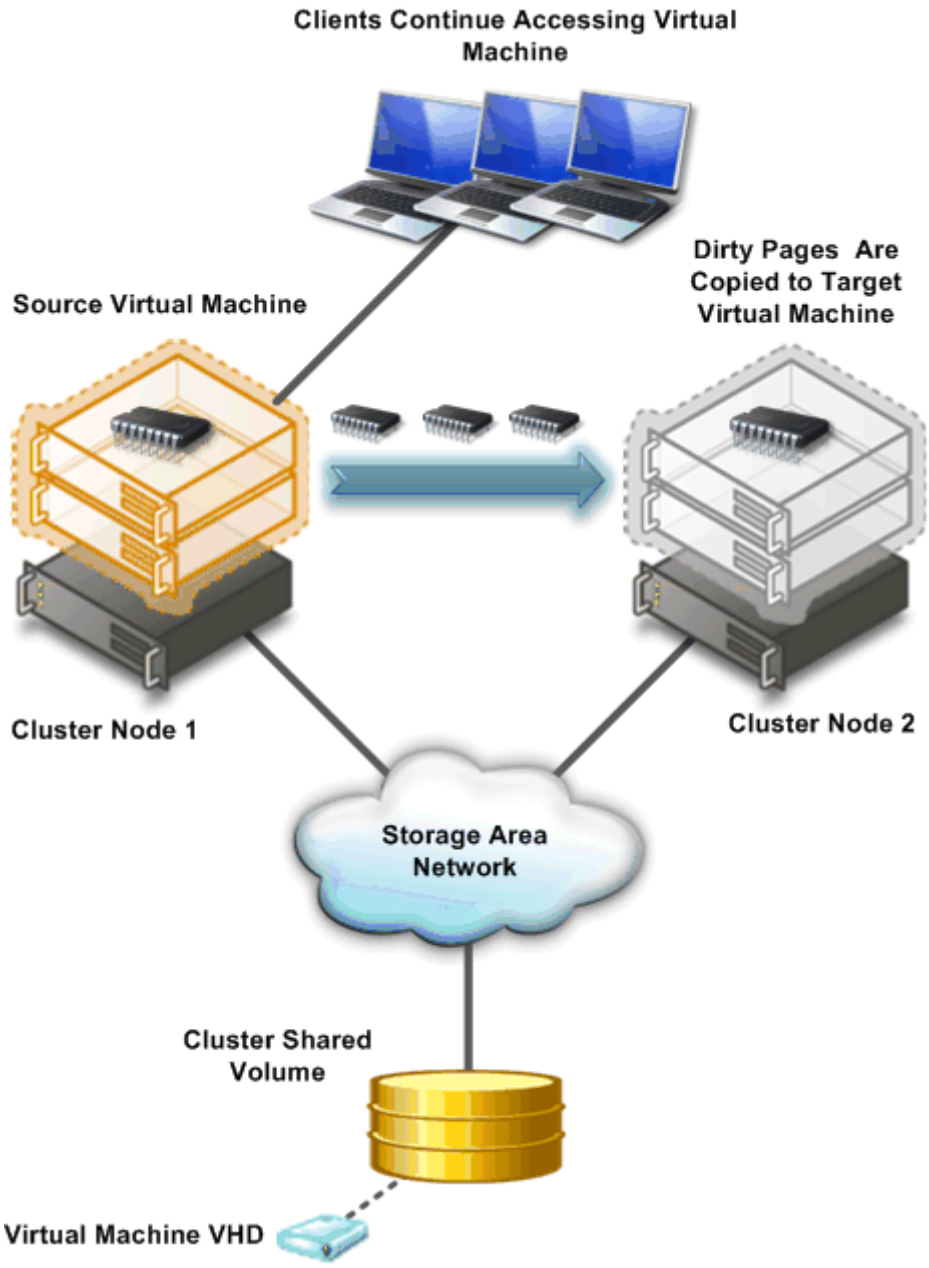
Administrátorem vynucený proces Live migrace je prováděn v následujících krocích:

1. Správce iniciuje „Live migraci“ mezi zdrojovým a cílovým uzlem clusteru.
2. Na cílovém uzlu clusteru je vytvořen duplicitní virtuální stroj, jak je znázorněno na následujícím obrázku.



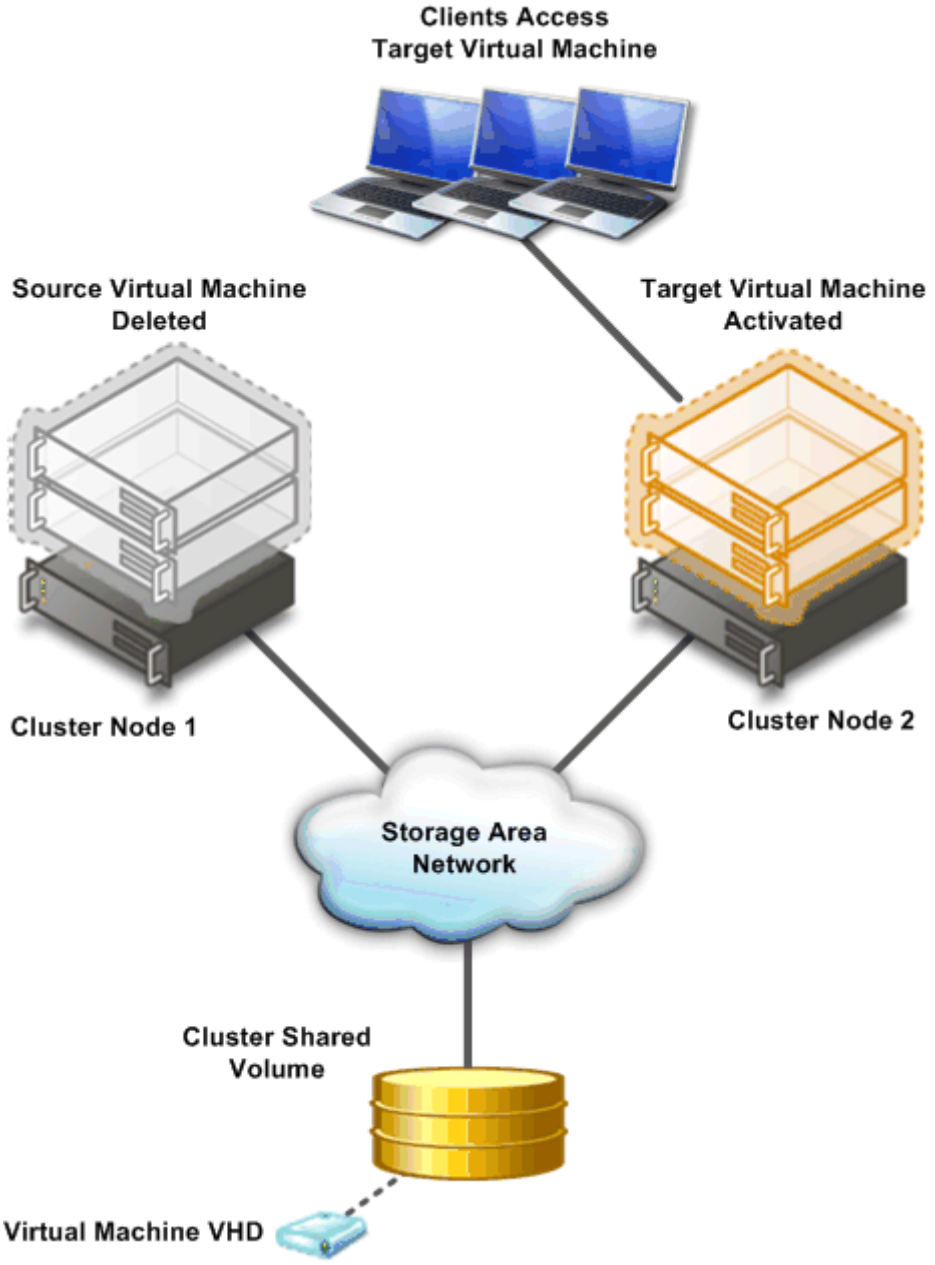
Obrázek 17 - Vytvoření cílového virtuálního serveru na cílovém uzlu clusteru, zdroj [17]

3. Veškerý obsah paměti zdrojového virtuálního stroje je zkopírován do cílového virtuálního stroje, jak je znázorněno na předchozím obrázku.
4. Klienti připojení ke zdrojovému serveru pokračují v práci, na zdrojovém virtuálním serveru a vytvářejí „špinavé stránky paměti“, jak je znázorněno na následujícím obrázku.
5. „špinavé stránky paměti“ jsou sledovány a pokračuje jejich iterativní kopírování, dokud se všechny paměťové stránky nezkopírují do cílového virtuálního stroje, jak je znázorněno na obrázku 18.



Obrázek 18 - Iterační kopie „špinavé paměti“ ze zdrojového do cílového virtuálního stroje, zdroj [18]

6. Když jsou všechny paměťové stránky zkopírovány do cílového virtuálního stroje, jsou klienti automaticky přesměrováni na cílový virtuální stroj a zdrojový virtuální stroj se zruší, jak je znázorněno na následujícím obrázku.



Obrázek 19 - Konečná konfigurace po ukončení procesu Live Migration, zdroj [19]

Verze Hyper-V 2.0 znamená pokrok ve snaze firmy Microsoft dodat zákazníkům vlastní virtualizační řešení, ale přesto kvalita a možnosti tohoto produktu ještě nejsou ani zdaleka na takové úrovní jako jsou produkty leadera v tomto oboru společnosti VMware. Například produkt VMware vSphere, který je určen pro virtualizaci celých data center a vytváření privátních cloud řešení, umožňuje zcela automatizovat přesuny virtuálních serverů. Data centra tak mohou v noci přesouvat virtuální servery na menší počet fyzických blade serverů a nevyužité servery vypínat. Ráno se vzrůstající zátěží dochází

opětovně k migraci serverů na vyhrazený hardware, aby výkon virtuálních serverů odpovídal požadavkům na jejich zátěž. Toto řešení se používá v rámci redukce nákladů za energie, přičemž je ušetřena energie potřebná k napájení fyzických serverů tak i energie potřebná k jejich chlazení. Zájemcům o informace o těchto pokročilých řešeních ve virtuální infrastruktuře datových center lze jako možný zdroj informaci doporučit alianci Vblock firem Cisco, VMware a EMC.

Tato kapitola byla zpracována za základě shrnutí informací z následujících zdrojů [21], [27], [28].

5.1.2 Virtual desktop infrastructure (VDI)

Pojem VDI představuje virtualizovanou infrastrukturu pro klientské počítače, hlavní myšlenkou tohoto řešení je konsolidace a virtualizace klientských operačních systémů do datových center, k nimž přistupují uživatelé pomocí protokolů pro vzdálený přístup.

Virtuální klientský počítač může existovat ve dvou režimech, tím prvním je režim permanentní, kdy má uživatel vždy svůj vlastní virtuální desktop. Toto řešení je vhodné především v případě, že uživatel používá nějaké speciální aplikace. V druhém režimu dochází k seskupování virtuálních počítačů do skupin, kde každý člen skupiny má identické nastavení. Uživateli se při pokusu o připojení přidělí aktuálně volný desktop ze skupiny. Předpokladem pro fungování takového řešení jsou samozřejmě i další nastavení například Group Policy v Active Directory, kdy je třeba nastavit uživatelům roamingové profily, přesměrování složek a připojení síťových disků a tiskáren. Výhodou druhého řešení je především homogennost daného prostředí, což snižuje nároky na správu a umožňuje rychle přidávat další virtuální desktopy. Při nasazení tohoto řešení pro velký počet uživatelů dochází k akumulaci úspory nákladů, kdy není třeba mít stejný počet počítačů jako zaměstnanců, vždy je totiž někdo nemocný, na dovolené, na služební cestě či na jednání mimo firmu.

Jedna z dalších technologií usnadňujících virtualizaci desktopů je Rapid Provisioning. Principiálně jde o to, že největší součástí virtuálního počítače je jeho virtuální disk s operačním systémem a aplikacemi. V případě virtualizace jednoho tisíce desktopů, by bylo třeba uložit přibližně 1000 x 10 gigabytů téměř shodných dat, což by představovalo 10 terabytů požadovaného diskového prostoru. V případě využití Rapid Provisioningu, který využívá rozdílové virtuální disky VHD, je oněch 10 gigabitů uloženo pouze jednou a tisíc virtuálních počítačů tato data sdílí a na své virtuální disky ukládají pouze rozdíly.

Pokročilou správu virtuálních desktopů umožňuje například řešení Citrix XenDesktop.

5.2 Cloud computing

Toto řešení je jakýmsi dalším krokem ve virtualizaci. Pojem není zcela specifikován, nejedná se totiž o jednu konkrétní technologii, ale spíše o způsob pohledu na poskytování výpočetního výkonu. Zákazník si „kupuje“ výpočetní výkon bez toho, aby musel rozumět infrastruktuře potřebné pro jeho realizace, je tedy zcela oproštěn od toho, že pro realizaci jím požadovaného řešení jsou potřeba nějaké servery, datová pole nebo to, kde jsou fyzicky umístěny.

Cloud, tedy pomyslný mrak obsahující potřebnou infrastrukturu, bývá zpravidla umístěn někde v internetu a zákazník dodavateli platí za pronájem prostředí sloužícího k uskutečnění následujících potřeb:

- webové servery
- matematické výpočty
- virtuální desktopy
- hostování aplikačních serverů
- atd.

V prostředí Cloud computingu tedy nedochází k implementaci řešení, která nejdou nasadit pomocí jiných metod např. pomocí virtualizace a hypervisorů. Hlavní výhodou tohoto řešení je jeho variabilnost. Zákazník si může pronajmout výpočetní výkon stovek serverů pro vědecké výpočty nutné pro vývoj nového produktu pouze na jím požadovanou dobu. Může se tak zprostit nákladů nutných pro vybudování vlastního data centra, které by po ukončení projektu nemělo další využití. Stejně tak „start up“ společnost působící na internetu nemusí investovat do vlastních serverů a místo toho si s rostoucími nároky na počet zákazníků a přístupů může od dodavatele pronajímat větší výpočetní výkon.

Existují i interní cloud implementace, ale dle [26] toto řešení používají pouze 2% firem. Interní cloudy mají několik významných vlastností, které přesahují standardní pojetí virtualizace. Pomocí samoobslužných portálů mohou vývojáři nasazovat aplikace bez zásahu administrátora serveru. Dále je zde implementován mechanizmus pro automatizovanou distribuci zátěže, kdy je díky neustálému monitorování docíleno optimálního rozložení virtualizovaných výpočetních prostředků na fyzický hardware.

Právě automatizace, je tedy považována za stěžejní potřebu pro implementaci interního cloud řešení. Hromadnému nasazení tedy zatím brání nedostupnost dostatečně kvalitních automatizovaných nástrojů pro ovládání tohoto prostředí. Cloud computing tedy nabízí

nové pohledy na fungování firemního ICT, ale to do jaké míry jde o řešení efektivní, bezpečné a ekonomicky výhodné ukáží následující roky, kdy bude možné zhodnotit realizované implementace této architektury.

Aby bylo možné cloud platformě důvěřovat, je nutný ještě další vývoj. ICT manažeři zatím nemají důvod těmto platformám příliš důvěřovat, neboť nemají skutečné záruky spolehlivosti a bezpečnosti provozovaných aplikací. Provozovatelé platforem nemají dostatečné nástroje, umožňující zákazníkovi garantovat správné fungování podnikových transakcí. Dalším nezbytným evolučním krokem v cloud computingu bude možnost přenositelnosti platformy tj. možnost přenesení platformy na vlastní infrastrukturu nebo k jinému poskytovateli služeb.

5.3 ICT řešení jako služba

Tento trend je patrný již několik let, ale s příchodem „hospodářské krize“ po roce 2008 značně sílí. Koncept tohoto řešení je známý z oblasti softwaru, anglická zkratka SaaS znamená Software as a Service. Výhoda řešení spočívá v jeho variabilnosti, firma využívá pouze aktuální počet potřebných licencí, bez toho aby si je musela sama kupovat, není třeba se starat o aktualizace na straně serverů nebo nákup aktualizací klientských programů. Vše zařizuje externí partner, který si tuto službu „pronájmu softwaru“ účtuje na měsíční bázi stejně, jako je účtován třeba pronájem datových linek. Jako službu je nyní možné pořídit datová pole, VoIP, servery i celá data centra. Výhody tohoto řešení nejsou většinou technické, ale spíše ekonomické. Podniky mají možnost inovovat infrastrukturu a zkvalitňovat služby bez velkých investičních nákladů. Není třeba uzavírat servisní kontrakty a platit drahé IT specialisty, neboť ti budou mnohem efektivněji pracovat pro našeho dodavatele, který je využije i u jiných zákazníků.

Toto řešení se v současnosti jeví jako velice efektivní cesta ke snížení nákladů na pořízení a provoz ICT. Výhodné je především pro menší a středně velké společnosti, kterým se nevyplatí zaměstnávat specialisty, jejichž služeb nejsou schopni plně a efektivně využít. Lze tedy předpokládat, že tímto způsobem nasazovaný outsourcing bude mít v blízké budoucnosti rostoucí tendenci.

5.4 Monitoring

Monitoring serverů, síťových prvků a dalších zařízení je dnes pro rozsáhlé sítě nutností. Možností a oblastí pro monitoring je velké množství a tak velkou roli hraje především technologie, na které je monitoring postaven. Monitorování může mít mnoho podob a je možné ho postavit na vlastních skriptech IT zaměstnanců daného podniku, na open source produktech i na velkém množství komerčních produktů.

Pro výběr toho správného produktu jsou rozhodující následující faktory:

- Náklady na pořízení monitorovacího programu.
- Spolehlivost.
- Čas potřebný na jeho nasazení.
- Technická náročnost nasazení.
- Technická náročnost správy.
- Možnosti konkrétního softwarového produktu.

Před výběrem a nasazením konkrétního produktu, je třeba provést detailní analýzu, která má za úkol zjistit:

- Co je třeba monitorovat.
- Kdo a jak bude vyhodnocovat výstupy z monitoringu.
- Bude monitoring sloužit k zobrazení historie o vytíženosti zdrojů?
- Bude monitoring upozorňovat na aktuální problémy nebo nedostupnost systémů?

Dále je třeba z obecnějšího hlediska zhodnotit jednotlivé oblasti monitoringu:

- Dostupnost serverů.
- Dostupnost služeb a aplikací, spolu s jejich odezvou.
- Události na serverech.
- Vytížení zdrojů (procesor, paměť, disk).
- Vytížení linek a měření přenosu dat.
- Statistiky síťového provozu.
- Analýza nestandardního chování v síti.
- Informace o portech směrovačů a přepínačů.
- Monitoring oblastí jako je Wi-Fi nebo IP telefonie.
- Bezpečnostní incidenty.

Obrázek 20 - Spotlight Server Activity Summary

Nástroje pro monitoring je možné dělit i z hlediska časového. Monitorovací software může být určen pro dlouhodobé sledování serverů a uchovává data i několik let zpětně, nebo může být určen pouze pro krátkodobé sledování. Příkladem takového typu programu je například Spotlight od společnosti Quest Software. Tento produkt je určen pro sledování provozních parametrů serverů při ladění výkonu aplikací a k odhalování výkonnostních problémů například z důvodu přetížení disků na datovém poli nebo síťových karet. Výstup z programu Spotlight je na předchozím obrázku a dále pak v příloze 9. a 10.

Z technického hlediska se používají dva základní způsoby monitoringu. Monitorování pomocí standardních protokolů jako je SNMP, WMI, IPMI. Monitorování s pomocí agenta, což je speciální softwarový klient, který musí být umístěn na konkrétním zařízení.

Server shromažďující data z monitorovaných systémů, musí být schopen tato data sumarizovat, kategorizovat, prioritizovat, vykreslovat historii v různých časových

intervalech nebo vyhodnocovat skutečnou příčinu problému na základě souběhu několika incidentů současně. V závislosti na důvodu monitorování je možné upozornit operátory, konkrétního administrátora nebo může být spuštěn předem připravený skript, jako reakce na konkrétní událost. Tento skript se může například pokusit restartovat službu na serveru.

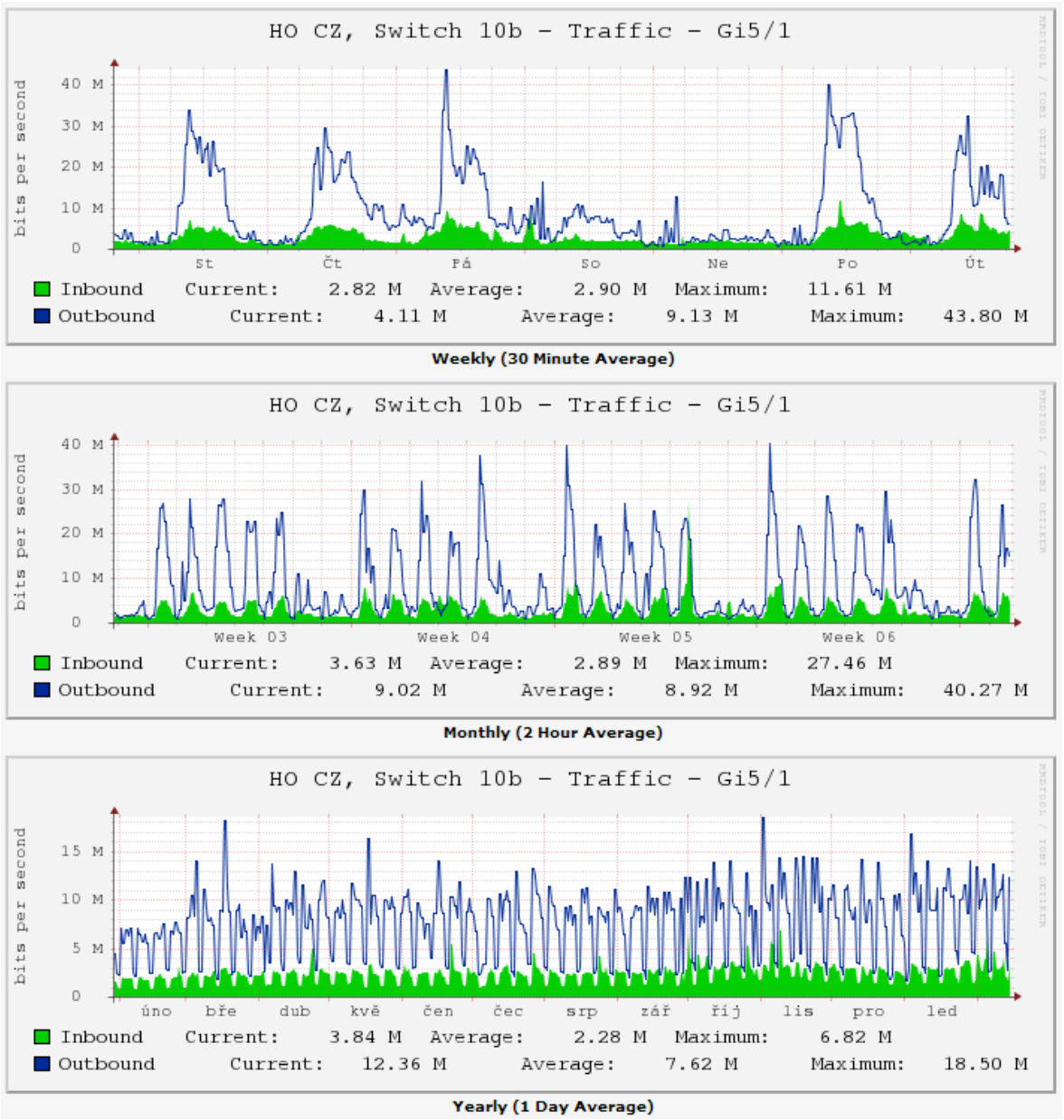
Jelikož málokterý monitorovací nástroj poskytuje v praxi stejné možnosti, použitelnost a funkčnost týmům zodpovědným na správu sítě, operační systémy i aplikace. Dochází k implementaci několika monitorovacích systémů současně s větším či menším přesahem monitoringu i do jiných oblastí.

Z konkrétních nástrojů lze uvést například open source systém **NAGIOS** sloužící primárně pro monitoring počítačových sítí, ale pomocí mnoha dostupných pluginů je možné jej využít i ke sledování operačních systémů a aplikací.

CA Spectrum Infrastructure Manager placený nástroj pro monitoring aktivních prvků, zvládající obsluhovat více než 18.000 zařízení.

Open Source nástroj **CACTI** slouží k zobrazení utilizace na jednotlivých portech síťových prvků a k jejich grafické sumarizaci za různá časová období. Výstup z tohoto programu je zobrazen na Obrázku 21.

Mezi další používané nástroje pro monitoring patří například CiscoWorks LAN Management Solution, IBM Tivoli Netcool nebo Big Brother a již zmiňovaný Spotlight od společnosti QUEST.



Obrázek 21 - Cacti – monitoring spojení s firewallem

6 Komunikační technologie

Komunikační technologie na bázi VoIP nebo Videokonference dnes otevírají cestu zcela novým způsobům komunikace, jejichž hlavním cílem je snižování celkových nákladů na vlastnictví TCO (Total cost of ownership) a zvyšování efektivity. Technologie dospěla do stádia mainstream adoption, došlo k všeobecnému přijetí trhem, přičemž hlavním důvodem k jejich nasazení je jejich přidaná hodnota v rámci sjednocené komunikace (UC - Unified communications).

6.1 IP telefonie

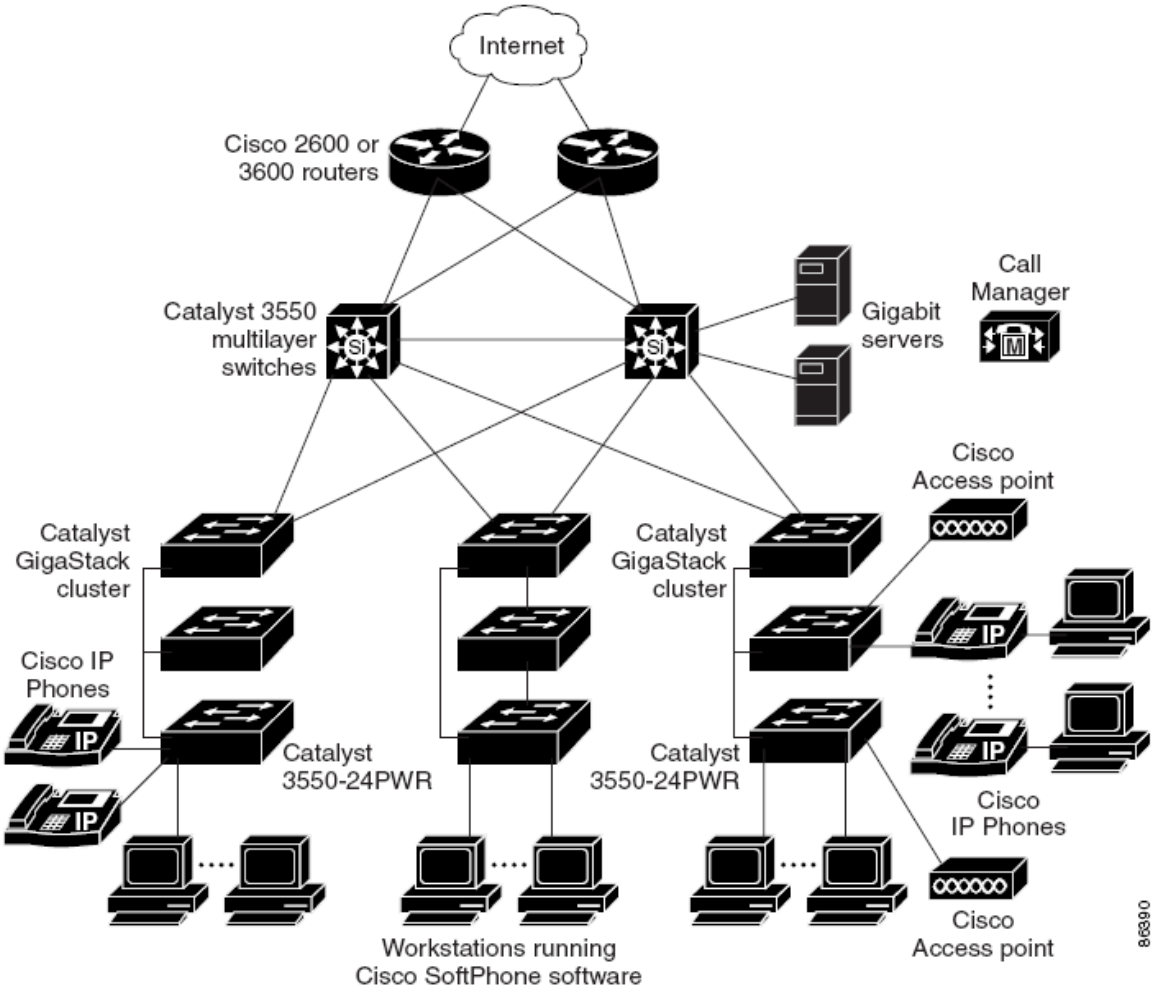
Voice over Internet Protocol, VoIP nebo také IP telefonie, je technologie pro přenos hlasu pomocí protokolů UDP/TCP/IP prostřednictvím počítačových sítí. Pro přenos digitalizovaného hlasu lze použít sítě LAN, WAN, Internet intranet, ale i datové služby mobilních operátorů. Pro zajištění dostatečné kvality a srozumitelnosti přenášeného hlasu využívají sítě tzv. QoS (Quality of Service) což jsou algoritmy sloužící k vyhrazení šířky přenosového pásma tak, aby nedošlo ke snížení kvality poskytovaných služeb.

Jelikož IP telefonie je samo o sobě velice rozsáhlé téma ICT, nebude tato práce charakterizovat technické aspekty jeho fungování ani používané komunikační protokoly a hardware. Cílem této práce je spíše poukázat na nové možnosti nasazení této technologie a její přidanou hodnotu v rámci sjednocené komunikace.

Pro úvod do problematiky počítačových sítí s přepínáním paketů lze doporučit následující zdroje [6], [14], [15], [18]. Pro objasnění fungování a zabezpečení VoIP, pak lze doporučit knihu Voice over IP Security od Patricka Parka [32].

Příkladem hybridní VoIP sítě a jejím postupným přechodem na síť plně fungující na IP, je článek „VoIP ve velkém a prakticky“ o nasazení IP telefonie na Západočeské univerzitě zdroj [31]. Článek popisuje evoluci telefonní sítě v průběhu let 2002 až 2010.

IP telefony mohou fungovat jako síťové přepínače a šetří tak množství požadovaných portů na přepínačích v přístupové vrstvě sítě. Jak může taková síť vypadat, ukazuje následující obrázek.



Obrázek 22 - Schéma páteřní sítě LAN, zdroj Cisco [22]

Výrazným krokem vpřed při implementaci IP telefonie ve firemním prostředí je nasazování softwarových klientů. Programy jako je Cisco IP Communicator umožňují zaměstnancům přijímat hovory bez ohledu na to, zda se nacházejí na svém obvyklém pracovním místě, nebo zda jsou na služební cestě v zahraniční centrále společnosti. Díky tomu, že IP telefonie není na rozdíl od analogových telefonních linek vázána na fyzické propoje mezi telefony a ústřednami. Je možné telefonní provoz přesměrovávat do jiných lokalit nebo dokonce států a to vše bez nutnosti měnit telefonní čísla. Této možnosti využívají především oddělení zákaznických služeb. Je tak zabezpečen 24 hodinový servis pomocí tří center na různých kontinentech. Vždy po osmi hodinách dojde k přesměrování provozu na další centrum a je tak využito časového posunu v těchto lokalitách. Pro mezinárodní společnosti je to jedna z mnoha efektivních cest jak ušetřit na nákladech na zákaznický servis a za telefonní poplatky.

Mezi nové trendy v této oblasti patří hostování telefonních ústředen. Výhodou tohoto hostování je model poskytování služeb SaaS, kdy firma nemusí investovat peníze do nové PBX ústředny, ale platí za virtuální ústřednu u svého poskytovatele telefonních služeb na bázi měsíčních plateb za počet linek. Podle některých odhadů je v České republice takto hostováno až 10.000 virtuálních pobočkových ústředen zdroj [30].

VoIP je postupně integrováno například do ERP nebo CRM systémů, takže obchodníci nebo zaměstnanci Call center vidí, ještě před přijetím hovoru, informace o zákazníkovi, jeho platební morálku a jiné důležité informace. Některé ústředny podporují propojení s externími kalendáři jako je MS Exchange nebo Google kalendář a jsou schopny inteligentně přesměrovávat hovory například na mobilní telefon.

Mezi nevýhody VoIP řešení patří například poměrně složitá implementace napříč rozsáhlou počítačovou sítí, nutnost speciální konfigurace pro možnost identifikace v rámci nouzových volání. Dále je třeba brát v úvahu nutnost zabezpečení hlasové komunikace proti případnému odposlechu a ochranu proti DoS útokům na VoIP infrastrukturu.

6.2 Videokonference

Videokonferenční řešení získávají v prostředí mezinárodních firem na popularitě. Hlavním motivačním faktorem pro jejich nasazení je úspora nákladů. Vyslání jednoho zaměstnance na jednodenní zahraniční jednání v Evropě stojí firmu 10.000 až 20.000 Kč. Je třeba počítat nejen s cenou letenky, ale i s časem a dalšími náklady na zaměstnance. Jestliže bude schůzka v zahraniční centrále společnosti trvat pouze dvě hodiny, zbytek pracovní doby zaměstnance strávený samotnou cestou letadlem, čekáním na letišti a dopravou na letiště, je pro zaměstnavatele strávený zcela neefektivně. Je možné namítnout, že při obchodní schůzce je třeba cítit kontakt s protistranou a musí být možné sledovat i gesta nonverbální komunikace, ale i to je dnes řešitelné. Technická řešení pro tyto požadavky dodává například společnost Cisco v podání produktu Telepresence a nebo firma TANDBERG (poznámka Společnost Cisco koupila v roce 2010 společnost TANDBERG, jedná se tedy v současnosti o dvě rovnocenná řešení od jedné společnosti).

TANDBERG dodává videokonferenční řešení v několika variantách, přičemž hlavním produktem je konferenční místnost pro 6 osob. Součástí celého řešení jsou LCD monitory o uhlopříčce 65 palců, Full HD kamery, ale i potřebný nábytek a řídící elektronika. Vizuální koncept těchto videokonferencí má působit tak, že monitory jsou na opačném místě stolů umístěny v takové vzdálenosti, že velikost obrazu osoby na monitoru je zobrazena 1:1 s jeho fyzickou předlohou. Na následujících obrázcích jsou zobrazeny videokonferenční místnosti.

Obrázek 23 - Cisco TelePresence System 3010, zdroj [23]

Konference je možné pořádat v mnoha režimech, z nichž budou uvedeny ty nejčastěji používané:

- 1 : 1 - pro 6 účastníků na každé straně
- 1 : 3 - pro 6 účastníků na jedné straně a 2 účastníky ve třech dalších lokalitách
- 1 : n - 2 nebo 4 účastníci na jedné straně a stejný počet účastníků až ve 42 jiných lokalitách, ale v tomto případě již nejsou účastníci videokonference zobrazeni v živé velikosti

Videokonferenční místnosti se umí spojit i se softwarovými klienty na počítačích a ti se mohou spojit i pouze mezi sebou.

K výrazným pokrokům v nabídce a rozvoji videokonferenčních řešení došlo především díky novým kompresním algoritmům pro přenos hlasu a obrazu a dále pak zvětšením přenosové kapacity datových linek. Předchozí generace videokonferencí používali kvůli

potřebným odezvám a datové propustnosti několik sdružených ISDN linek. Ovšem cena takto uskutečněné konference, byla díky poplatkům za mezinárodní hovory dost vysoká.

Přibližná cena vybavení videokonferenční místnosti na následujícím obrázku je 7.500.000 Kč a při výrazném omezení mezinárodních služebních cest se mohou náklady na její pořízení vrátit již v prvním roce. Skutečnou úsporu nákladů a efektivitu těchto řešení však žádná firma z pochopitelných důvodů nezveřejňuje.

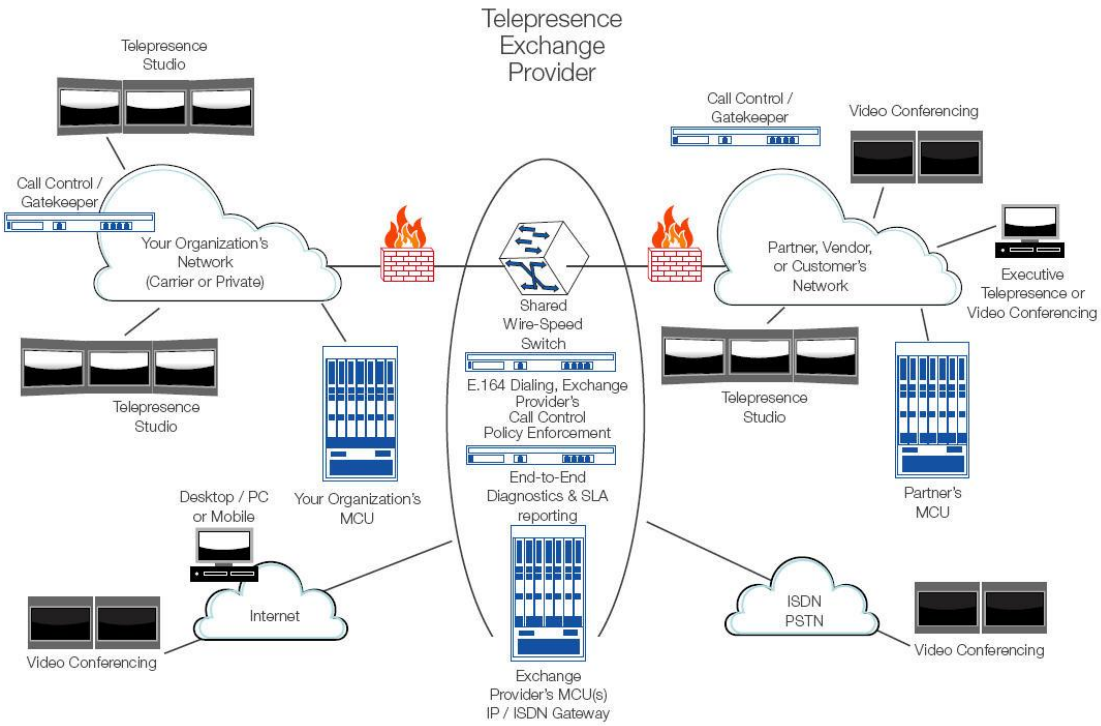
Obrázek 24 - TANDBERG Telepresence T3, zdroj [24]

Videokonferenční místnosti a softwarový klienti jsou pro jejich koncové uživatele jediné viditelné body poměrně složité infrastruktury potřebné pro chod těchto systémů. Pro jejich činnost je nutné konfigurovat QoS služby v rámci celých LAN a WAN sítí, dále pak firewally a výkonné servery sloužící k míchání zvukových a obrazových kanálů před jejich dalším přenosem. Zjednodušené schéma takovéto infrastruktury je zobrazeno na následujícím obrázku.

Videokonferenční místnosti nemusí být nutně používány pouze pro „běžné“ porady, ale lze je použít i z jiných důvodu viz následující:

- Jsou využívaný pro školení zaměstnanců na vzdálených pobočkách.

- Pohovory se zájemci na vedoucí místa v zahraničních pobočkách.
- Jednání s dodavateli v zahraničí, dodavatel je asistentkou zaveden do konferenční místnosti a pomocí videokonference se spojí s obchodníkem v jiném státě.



Obrázek 25 - Cisco Telepresence Exchange, zdroj [25]

Poněkud odlišným typem komunikačního nástroje je například software WEBEX od společnosti Cisco. Tento produkt totiž neumožňuje pouze přenos video hovoru a prezentace, ale i možnost sdílet či ovládat počítače účastníků. Během video hovoru je tedy možné ukázat protistraně nejen prezentaci v PowerPointu, ale i živou ukázku fungování prezentované aplikace či pomoci s řešením problému přímo na počítači protistrany. Produkty typu aplikace WEBEX tedy zapadají do konceptu řešení pro sjednocenou komunikaci, protože využívají audio, video, prezentace i služeb pro sdílení vzdálené plochy. Lze je tedy považovat za nástroje zvyšující výrazným způsobem efektivitu práce zaměstnanců.

6.3 Instant messaging

Instant messaging je nasazován jako součást sjednocené komunikace UC například pomocí Microsoft Office Communication Server (MS OCS) spolu s produkty MS Office a SharePoint. Integrací těchto produktů lze efektivněji komunikovat na sjednocené platformě tak, že komunikace může probíhat podle modelového scénáře. Uživatel obdrží e-mail od kolegy a potřebuje se dozvědět další informace, okno emailu přímo indikuje, zda je kolega online a nabízí zahájení chatu nebo navázání telefonního hovoru. Jedním kliknutím tak lze zahájit chat pomocí MC Office komunikátoru nebo uskutečnit hovor pomocí pevné linky.

Někteří vedoucí pracovníci jsou proti této formě komunikace zaujatí a brání se jejímu nasazení. Lze ale předpokládat, že díky tlakům na nasazování řešení pro zvyšování efektivity zaměstnanců dojde v brzké době k jejich prudkému rozvoji.

7 Závěr

S rostoucí složitostí počítačových sítí je třeba přicházet s nástroji a postupy usnadňujícími jejich efektivní správu. Ekonomické zájmy firem kladou vysoké požadavky na ICT a současně dochází k soustavnému snižování rozpočtů oddělení majících na starosti jejich správu. Oddělení informačních technologií přistupují k řešení těchto požadavků z několika možných úhlů pohledu a způsoby, jak se s jejich řešením vypořádají se tak různí. Pravděpodobně nejhorší možné řešení, plynoucí z požadavku na snížení rozpočtu IT je to, kdy dochází ke snížení úrovně poskytovaných služeb. Z dlouhodobého hlediska je tato strategie neudržitelná, podnik začne zaostávat za konkurencí, není schopen dostatečně flexibilně reagovat na nové příležitosti, začne ztrácet pozici na trhu či zcela zanikne. Další možností je outsourcing, kdy jsou určité činnosti vlastních zaměstnanců vykonávány zaměstnanci externího dodavatele. V některých případech, je tak možné efektivněji využít potřebné odborníky za předpokladu že, stávající zaměstnanci nejsou využiti na 100% nebo naopak, je třeba zajistit směnný provoz. Zlepšení efektivity lze dosáhnout i pomocí úpravy procesů uvnitř firmy, kdy na základě změny pracovních postupů, mohou být některé lidské zdroje přesměrovány na jiné činnosti nebo zcela eliminovány.

Efektivnějšímu fungování IT oddělení pomáhají i „dohody o úrovni poskytovaných služeb“ (SLA - Service Level Agreement). SLA vznikla potřebou co nejpřesněji definovat úroveň, intenzitu a rozsah poskytovaných služeb pro zákazníka, přičemž zákazníkem může být i jiný útvar v rámci jednoho podniku. Tato smlouva definuje pro obě strany jasná pravidla a jejich povinnosti tak, aby z dlouhodobého hlediska docházelo k efektivní spolupráci. Nedochází tak k problémům v komunikaci a obě partnerské strany jsou si vědomy svých práv a povinností, což ve svém důsledku zlepšuje efektivitu jejich práce, neboť došlo k transparentnímu vymezení povinností.

Z technického hlediska dochází v rámci předcházení možným výpadkům služeb k odstraňování „jediných bodů selhání“ (SPOF - Single Point Of Failure). Při analýze infrastruktury jsou vyhledávána místa, která při své vlastní nefunkčnosti způsobí nefunkčnost celého systému. K odstranění SPOF pak dochází přidáváním záložních síťových spojení a aktivních prvků, redundantním napájením, přesunem dat na bezpečná datová pole, umístěním aplikačních serverů na servery zapojenými v clusteru a podobně. Z ekonomického hlediska každé redundantní řešení představuje nadbytečnou kapacitu, která není plně vytížena a generuje zvýšené náklady. Požadavky na redundanci, ale nevycházejí primárně z potřeb IT oddělení, ale jsou reakcí na požadavky podniku tak, aby mohl plnit své ekonomické cíle. Je tedy vždy na zvážení zodpovědného managementu, zda jsou ochotni akceptovat možné poruchy a čas potřebný k jejich odstranění, nebo investice potřebné k jejich předcházení.

Jedním z výrazných trendů v mnoha velkých firmách je tlak na redukci zaměstnanců majících na starosti podporu ICT. V reálném prostředí nejde vždy o to snížit absolutní počet zaměstnanců, ale vzhledem ke zvyšujícímu se počtu spravovaných systémů, zlepšit efektivitu jejich správy tak, aby tempo přijímání nových pracovníků bylo nižší než množství nově podporovaných technických řešení. Tohoto cíle je dosahováno pomocí standardizace používaných produktů jak na úrovni architektury, tak i u používaného hardwaru a softwaru. Díky nástrojům pro centrální správu dochází k velké úspoře času například při správě DNS, DHCP, Firewallů, hromadných instalací stanic nebo při podpoře virtuálních prostředí. Tyto nástroje umožňují snížení času potřebného na správu i o 90%. Způsob fungování takovýchto rozhraní vychází převážně z „Grid Computingu“, kdy jedno centrální rozhraní díky dědičnosti spravuje mnoho podřízených zařízení. Další možností úspory v oblasti personálních nákladů je implementace nástrojů zjednodušujících správu tak, že je možné přesunout operativní činnosti ze systémových inženýrů na operátory respektive help desk.

Součástí této práce byla i demonstrace možností zmiňovaných nástrojů pro centrální správu a to konkrétně produktu DNSone od společnosti Infoblox. Byl nastíněn model fungování rozsáhlé mezinárodní firemní sítě a tomu odpovídající architektura a správa poskytovaných síťových služeb DNS a DHCP. Bylo prokázáno, že pomocí moderních nástrojů pro centrální správu, je možné tyto služby spravovat mnohem efektivněji a současně je systém odolný proti výpadkům služeb a snadno obnovitelný po případné havárii.

Heslo „Green IT“ bylo ještě donedávna spíše módním trendem v oblasti marketingu, ale s nástupem „ekonomické krize“ v roce 2008 a tlakem na redukci nákladů, došlo k velkému rozvoji virtualizace. Mnoho publikovaných studií jednoznačně potvrzuje přínosy virtualizace v podobě úspory nákladů na nákup hardwaru, tak i v podobě nákladů na chlazení a napájení data center. Snížení ekologické zátěže, je tak vlastně až druhotným efektem při snižování nákladů firem v oblasti ICT, ale i přes tuto skutečnost se jedná o pozitivní přínos pro životní prostředí.

Cloud computing je v současnosti velice aktuální téma a z ekonomického hlediska přináší tento způsob nákupu výpočetního výkonu, pro určité typy aplikací, znatelný přínos. Analýzou dostupných informací, byla však objevena i negativa, která mohou pro firmu z dlouhodobého hlediska představovat téměř neřešitelný problém v podobě závislosti na jediném dodavateli. Může dojít ke stavu, kdy bude třeba přejít od jednoho poskytovatele cloud služeb k jinému, ale zatím nejsou k dispozici dostatečně kvalitní softwarové nástroje pro tuto migraci. Setrvání u stávajícího partnera se tak může stát jak ekonomicky, tak technicky nevýhodným. Technologii cloudu lze využít i interně uvnitř podniku, kdy díky automatizaci při alokaci zdrojů, dochází ke zvýšení efektivity práce a to především u zaměstnanců majících na starosti softwarový vývoj a testování. Automatizace je

považována za stěžejní potřebu pro implementaci interního cloud řešení. Hromadnému nasazení tedy zatím brání nedostupnost dostatečně kvalitních automatizovaných nástrojů pro ovládání tohoto prostředí. Cloud computing nabízí nové pohledy na fungování firemního ICT, ale to do jaké míry jde o řešení efektivní, bezpečné a ekonomicky výhodné, ukáží následující roky, kdy bude možné zhodnotit realizované implementace této architektury.

Dalším trendem v oblasti poskytování firemní infrastruktury pro ICT, je poskytování menších či větších technologických celků jako služby od externího dodavatele. Firma tak jedná pouze s jedním dodavatelem, na základě SLA je vymezena úroveň služeb, reakční časy pro běžné úkony i pro odstranění havárií. Hardware i případný software a licence jsou majetkem dodavatele, ten provádí i pravidelnou údržbu, upgrade, monitoring i zajištění případných oprav hardwaru od dalších dodavatelů. V reálném firemním prostředí dochází například k „pronájmu“ pokročilých datových polí, zaměstnanci IT tak „jen“ přidělují zdroje pole.

Monitoring IT zařízení se v současnosti využívá jako prevence celkového selhání zařízení nebo služby, ale i z důvodu účtování pro potřeby SLA. Především velkým podnikům lze monitorování jen doporučit, neboť mohou při použití správných nástrojů minimalizovat případné ekonomické ztráty plynoucí z odepření služeb, nebo v důsledku jejich snížené kvality. Mezinárodní společnosti budují dohledová centra s operátory pracujícími ve 24 hodinovém režimu v zemích s nízkou hodinovou mzdou, například v Rumunsku nebo Indii. Operátoři reagují na výstupy z monitorovacího softwaru a komunikují v případě problémů s odpovědnými zaměstnanci v daných zemích nebo přímo s poskytovateli služeb, například s dodavateli WAN konektivity.

IP telefonie není dnes preferovaným řešením pro hlasové služby jen kvůli možným finančním úsporám za komunikaci, ale především díky dodatečným službám, které klasické analogové a digitální ústředny neumožňují. VoIP je tak nasazována především díky výhodám v rámci sjednocené komunikace.

Videokonferenční řešení jako je TANDBERG Telepresence T3 jsou na takové úrovní, že mohou v mnoha případech nahradit osobní setkání. Implementace těchto řešení napříč celou mezinárodní korporací tak značně zvyšuje efektivitu zaměstnanců a úspor za cestování. Díky několikaletým zkušenostem s používáním videokonferenční místnosti TANDBERG Telepresence u zaměstnavatele autora, lze tuto formu komunikace doporučit jako funkční a efektivní řešení pro komunikaci, které lze díky softwarovým klientům propojit i s koncovými stanicemi zaměstnanců. Díky pořizovacím nákladům je však ekonomická návratnost možná pouze u opravdu velkých firem.

8 Seznam literatury

1. HORA, Michal. Tajemství zkratky SLA [online] 2011-01-15 <http://www.systemonline.cz/outsourcing-ict/tajemstvi-zkratky-sla-1.htm>
2. RUEST, Daniel, Ruest, Nelson. Virtualizace podrobný průvodce. Brno: Computer Press, 2010. 408 s. ISBN: 978-80-251-2676-9
3. RULE, David; DITTNER Rogier: The Best Damn Server Virtualization Book Period. Burlington, Syngress Publishing, 2007. ISBN 13: 978-1-59749-217-1
4. LUGSCH, Zbyszek. Jak je to s návratností investic do Virtualizace?, [online] 2011-02-10 < http://www.systemonline.cz/virtualizace/jak-je-to-s-navratnosti-investic-do-virtualizace.htm>
5. KAILASH, Jayaswal: Administering Data Centers: Servers, Storage, and Voice over IP. Indianapolis, Wiley Publishing, 2006. ISBN-13: 978-0-471-77183-8
6. ODOM, Wendell, HEALY, Rus, METHA, Naren. Směrování a přepínání sítí. Brno: Computer Press, 2009. 880 s. ISBN: 978-80-251-2520-5
7. DONAHUE, Gary. Kompletní průvodce síťového experta. Brno: Computer Press, 2009. 528 s. ISBN: 978-80-251-2247-1
8. SCHUDEL, Georgg; SMITH, David: Router Security Strategies: Securing IP Network Traffic Planes. Indianapolis, Cisco Press, 2007. ISBN 978-1-58705-336-8
9. INFOBLOX: Powering Nonstop Core Network Services. [online]. < http://www.infoblox.com/library/l-genLibrary.cfm?section=l-whitepapers >
10. BABARÍK, Martin. Windows Server 2008 Hotová řešení. Brno: Computer Press, 2009. 432 s. ISBN: 978-80-251-2207-5
11. RUSSEL, Charlie, CRAWFORD, Sharon. Microsoft Windows Server 2008. Brno: Computer Press, 2009. 1272 s. ISBN: 978-80-251-2115-3
12. STANEK, William. Mistrovství v Microsoft Windows Server 2008. Brno: Computer Press, 2009. 1368 s. ISBN: 978-80-251-2158-0
13. STANEK, William. Windows 7. Brno: Computer Press, 2010. 712 s. ISBN: 978-80-251-2792-6
14. INIEWSKI, Krysztof. Network infrastructure and architecture: designing high-availability networks. New Jersey: Wiley, 2008. 564 s. ISBN 978-0-471-74906-6
15. PUŽMANOVÁ, Rita: TCP/IP v kostce. České Budějovice: Kopp, 2004. ISBN 80-7232-236-2
16. MICROSOFT TEAM: Microsoft Windows Server 2003 Resource Kit. Brno: Computer Press, 2006. ISBN 80-251-1260-8
17. LIU, Cricket, ALBITZ, Paul: DNS and BIND (5th Edition). O'Reilly, 2006. 648 s. ISBN: 0596100574
18. VACHON, Bob, GRAZIANI, Rick: Accessing theWAN, CCNA Exploration Companion Guide. Indianapolis: Cisco Press, 2008. 696 s. ISBN: 978-1-58713-205-6

19. CERLING, Tim, BULLER, Jeff, ENSTALL, Chuck, RUIZ, Richard: Mastering Microsoft® Virtualization. Indianapolis: Wiley Publishing, 2010. 579 s. ISBN: 978-0-470-44958-5
20. BUFFINGTON, Jason: Data Protection for Virtual Data Centers. Indianapolis: Wiley Publishing, 2010. 530 s. ISBN: 978-0-470-57214-6
21. MICHAEL, Michael, LINERS, Hector: Mastering Virtual Machine Manager 2008 R2. Indianapolis: Wiley Publishing, 2010. 603 s. ISBN: 978-0-470-46332-1
22. DEAN, Tamara: Network+ Guide to Networks Fifth Edition. Boston: Course Technology, 2010. 901 s. ISBN-13: 978-1-423-90245-4
23. ŠÍMA, Horymír: Využívejte své technologie maximálně. Praha: Computerworld 12/2009. strana 10
24. VLASATÝ, Petr: ECO datová centra – ve znamení modularity. Praha: Computerworld 12/2009. strana 13
25. BRODKIN, Jon: Interní cloudy: Víc než jen virtualizace. Praha: Computerworld 06/2010. strana 22
26. GITELLENOVÁ, Sandra: Pozor na přetížení serverů. Praha: Computerworld 06/2010. strana 25
27. Whitepaper : Windows Server 2008 R2 Reviewers Guide. Microsoft 2008
28. PETRŽELA, Radim: Microsoft Hyper-V 2.0. Praha: MHM Computer Data v Péči 13/2009 strana 6 – 7
29. FIURÁŠEK, Antonín: VDI aneb Desktopy tak trochu jinak. [online] 2011-02-27 <http://www.systemonline.cz/virtualizace/vdi-aneb-desktopy-tak-trochu-jinak.htm>
30. KALÁB, Dalibor: IP telefonie znovu a silnější. Brno: Connect! 05/2010. strana 8
31. PETROVIČ, Michal: VoIP ve velkém a prakticky. Brno: Connect! 05/2010. strana 16
32. PARK, Patrick: Voice over IP Security. Indianapolis: Cisco Press, 2009. 383 s. ISBN: 978-1-58705-469-3

9 Přílohy

9.1 Seznam obrázků

19. Konečná konfigurace po ukončení procesu Live Migration, zdroj. whitepaper : Windows Server 2008 R2 Reviewers Guide. Microsoft 2008, strana 23.
20. Spotlight Server Activity Summary
21. Cacti – monitoring spojení s firewallem
22. Schéma páteřní sítě LAN, IP tel zdroj. společnost Cisco, Catalyst 3550 Switches in a Collapsed Backbone Configuration (Cisco IOS Release 12.2(44)SE), February 2008, strana 1-15
23. Cisco TelePresence System 3010, zdroj www.cisco.com
24. TANDBERG Telepresence T3, zdroj www.cisco.com
25. Cisco Telepresence Exchange, zdroj www.cisco.com

9.2 Seznam tabulek

9.3 Seznam příloh

9.4 Rejstřík pojmů

Active Directory - Implementace adresářových služeb firmy Microsoft v prostředí Windows

Cloud – Cloud computing, poskytování výpočetních zdrojů na vyžádání prostřednictvím počítačové sítě

CSV - Cluster Shared Volumes, clusterové sdílené svazky

DHCP - Dynamic Host Configuration Protocol

Disaster Recovery - Je proces politik a souvisejících postupů sloužících k přípravě na využití nebo pokračování technologické infrastruktury kritické pro organizaci po přírodní nebo člověkem vyvolané katastrofě.

DNS - Domain Name System

DoS - Denial of Service, distribuovaný útok s cílem přetížit server a způsobit tak odmítnutí poskytnout službu

ICT - informační a komunikační technologie (z anglického Information and Communication Technologies)

IOS – Integrovaný operační systém

IPv4 - Internet Protokol verze 4

IPv6 - Internet Protokol verze 6

IT - Informační technologie

LAN - Local Area Network, Lokální síť je označení pro počítačovou síť, která pokrývá malé geografické území

Outsourcing - vyčlení různé podpůrné a vedlejší činnosti a svěření této činnosti smluvně jiné společnosti čili sub kontraktorovi, specializovanému na příslušnou činnost.

PBX - Private branch exchange, pobočková ústředna

PXE - Preboot eXecution Environment, bootování počítačů ze sítě

QoS - Quality of Service, kvalita služeb

SaaS - Software as a Service, software jako služba

SAN - Storage Area Network, dedikovaná datová síť, sloužící pro připojení externích zařízení k serverům (disková pole, páskové knihovny, …)

SLA - Service level agreement, jedná se o část servisního kontraktu, kde je formálně definována úroveň poskytovaných služeb

SPOF - single point of failure, jediný bod selhání

TCO - Total cost of ownership, celkové náklady na vlastnictví

UC - Unified communications, sjednocená komunikace

VDI - Virtual desktop infrastructure, infrastruktura pro virtualizace desktopů

VHD - Virtual Hard Disk

VLAN - Virtual Local Area Network, virtuální lokální síť

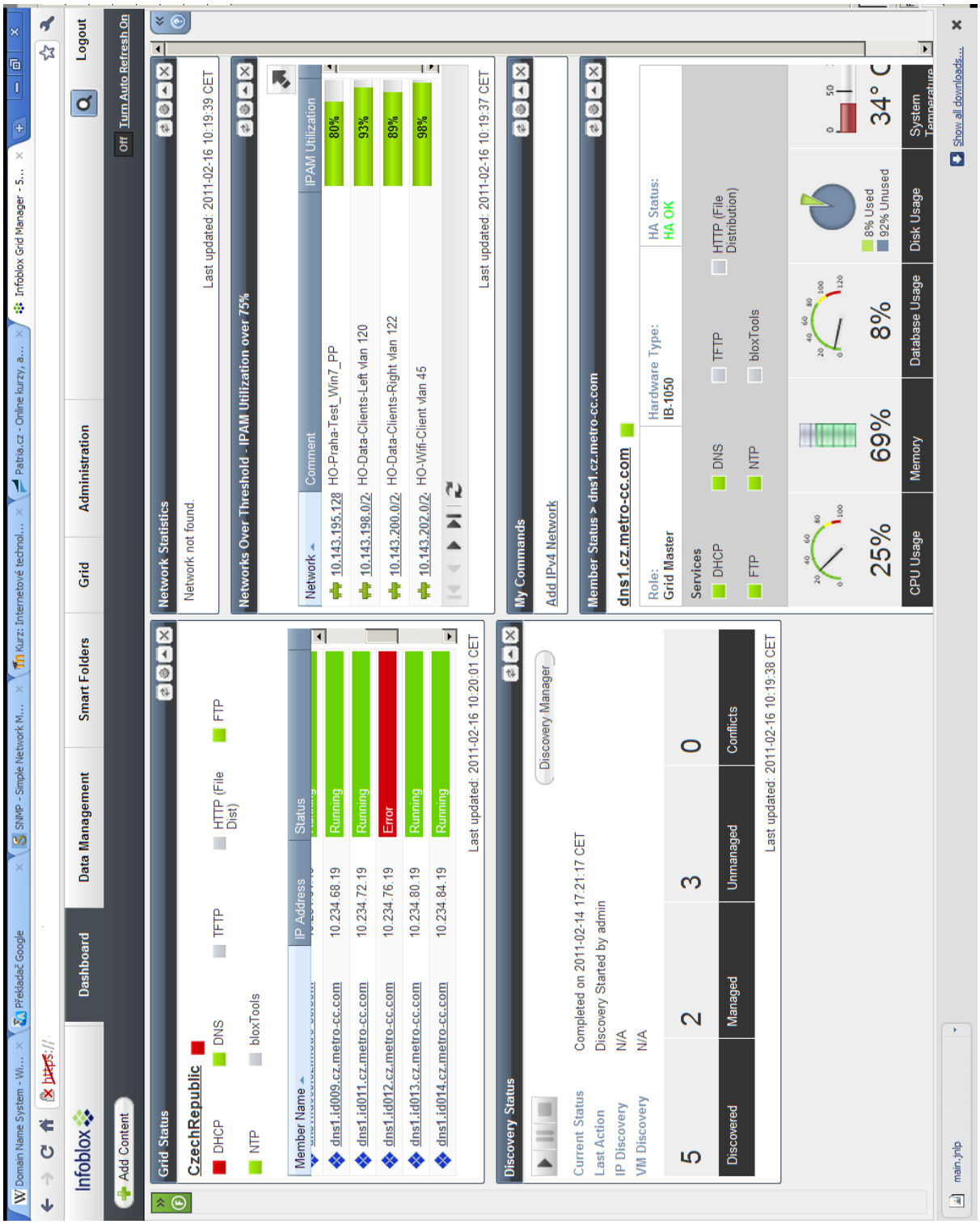
VM – Virtual Machine, virtuální stroj

VoIP - Voice over Internet Protocol

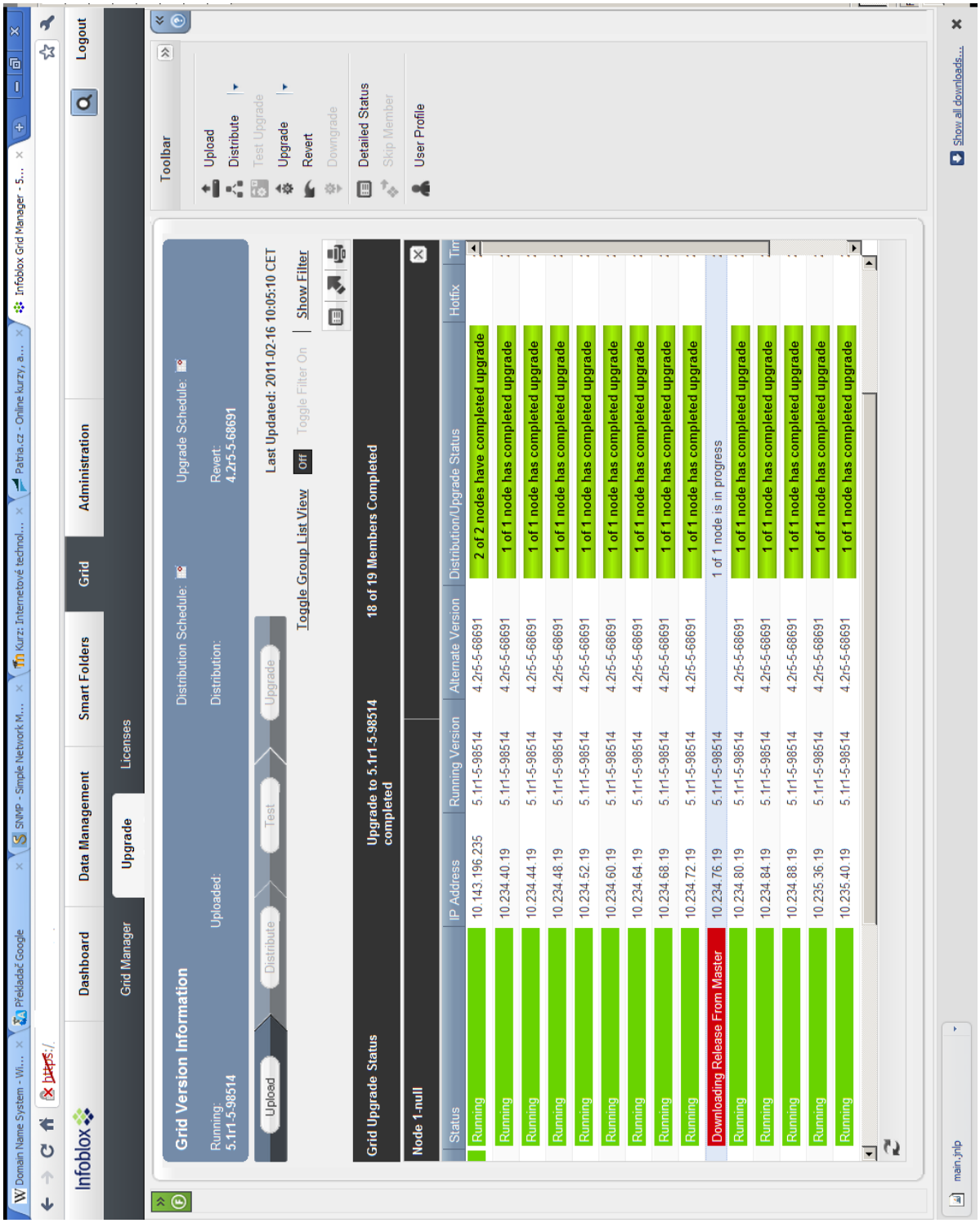
WAN - Wide Area Network, jedná se o počítačovou síť, která pokrývá rozlehlé geografické území (například síť, která překračuje hranice města, regionu nebo státu)

9.5 Obrázkové přílohy

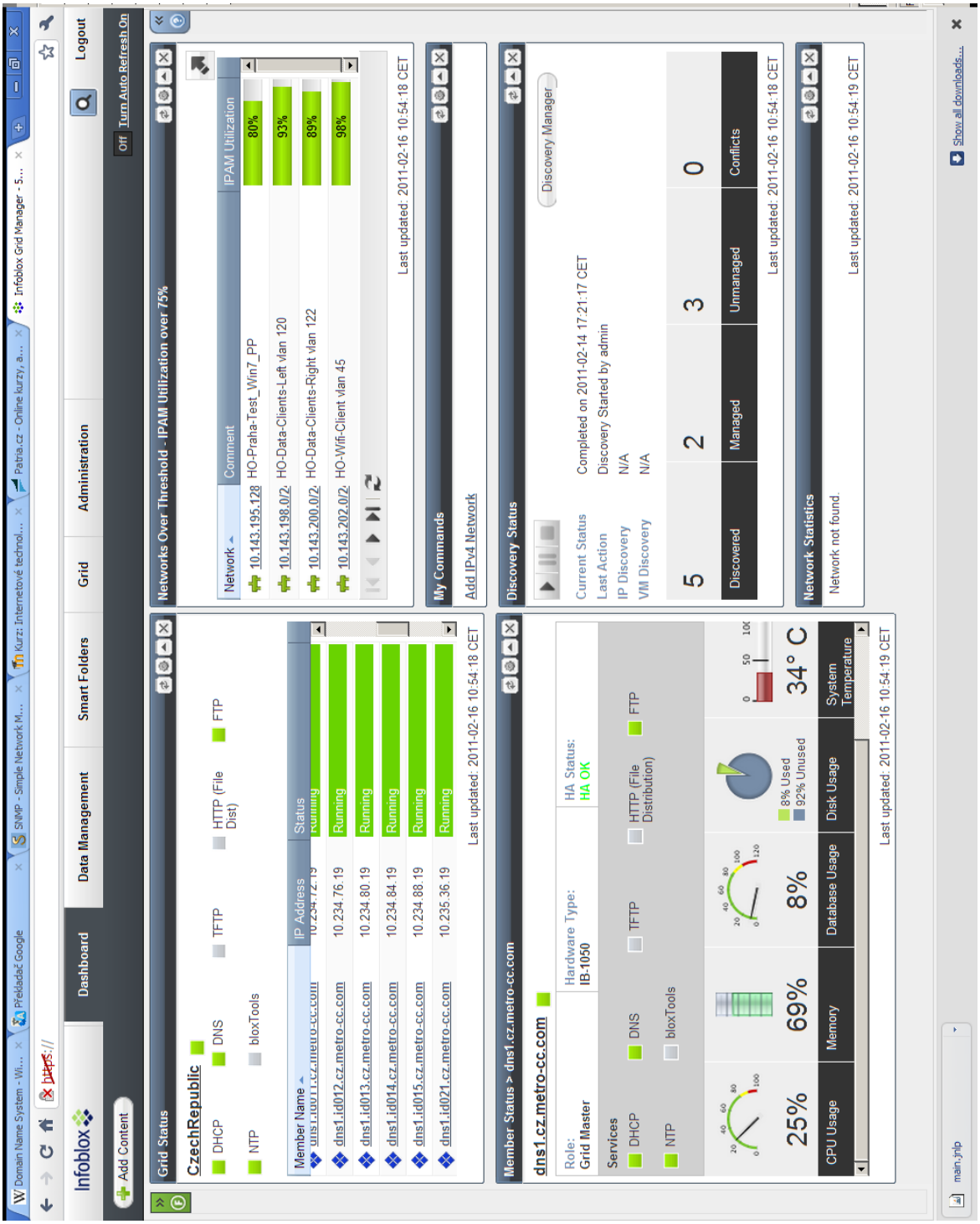
Příloha 1 - DNSone porucha boxu na pobočce podniku



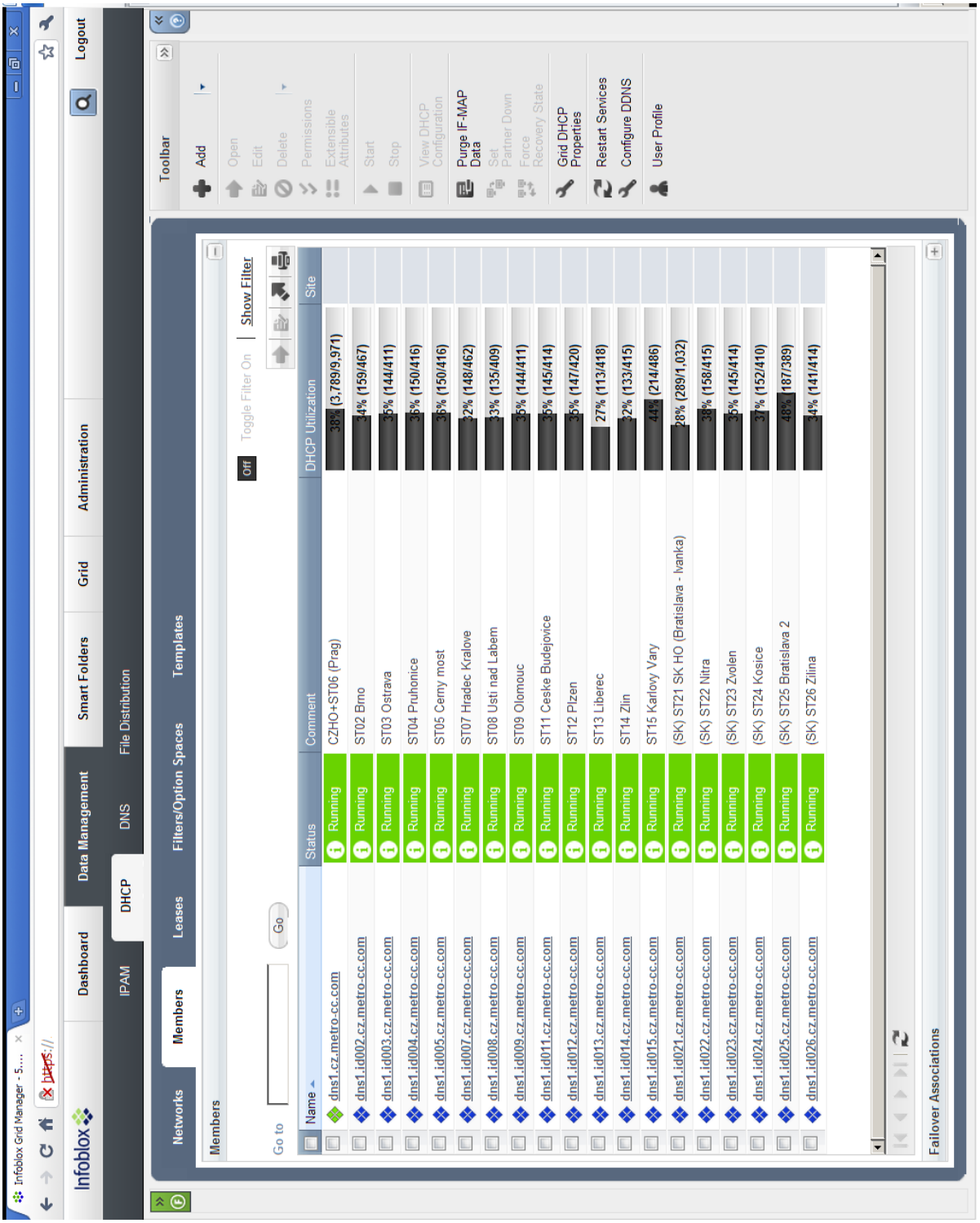
Příloha 2 - DNSone synchronizace verzí operačního systému



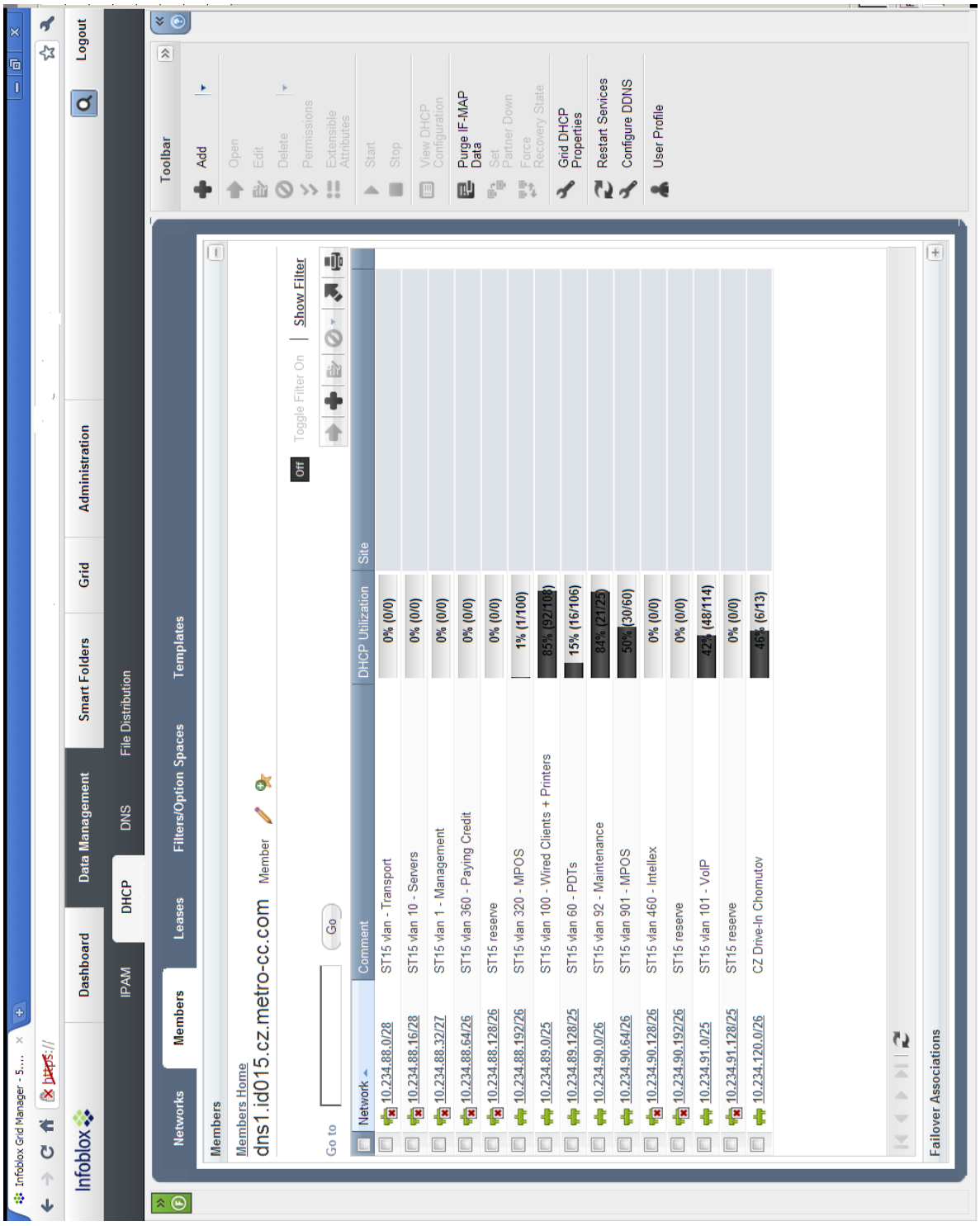
Příloha 3 - DNSone náhradní box je synchronizován a funkční



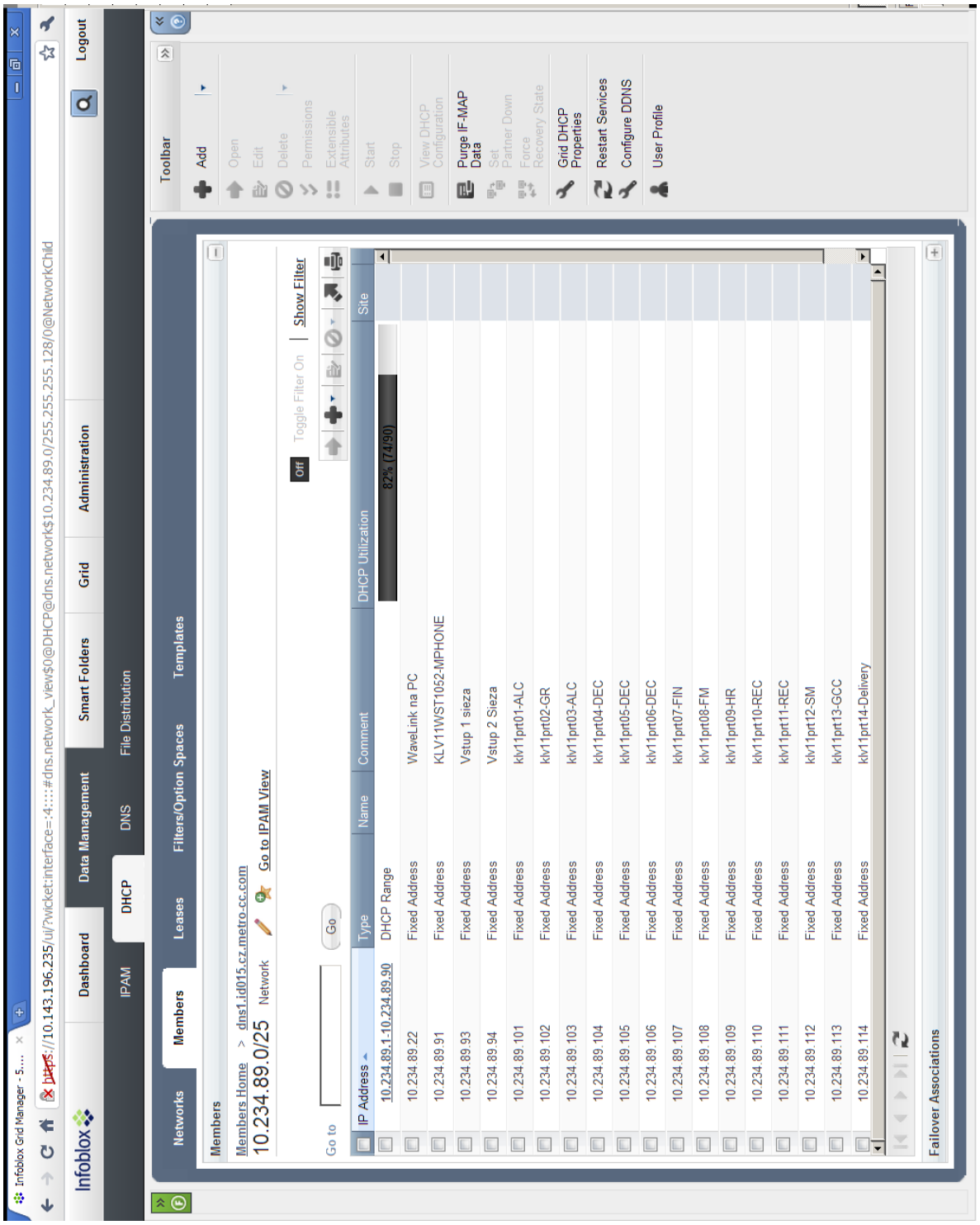
Příloha 4 - DNSone Boxy, které jsou součástí Gridu



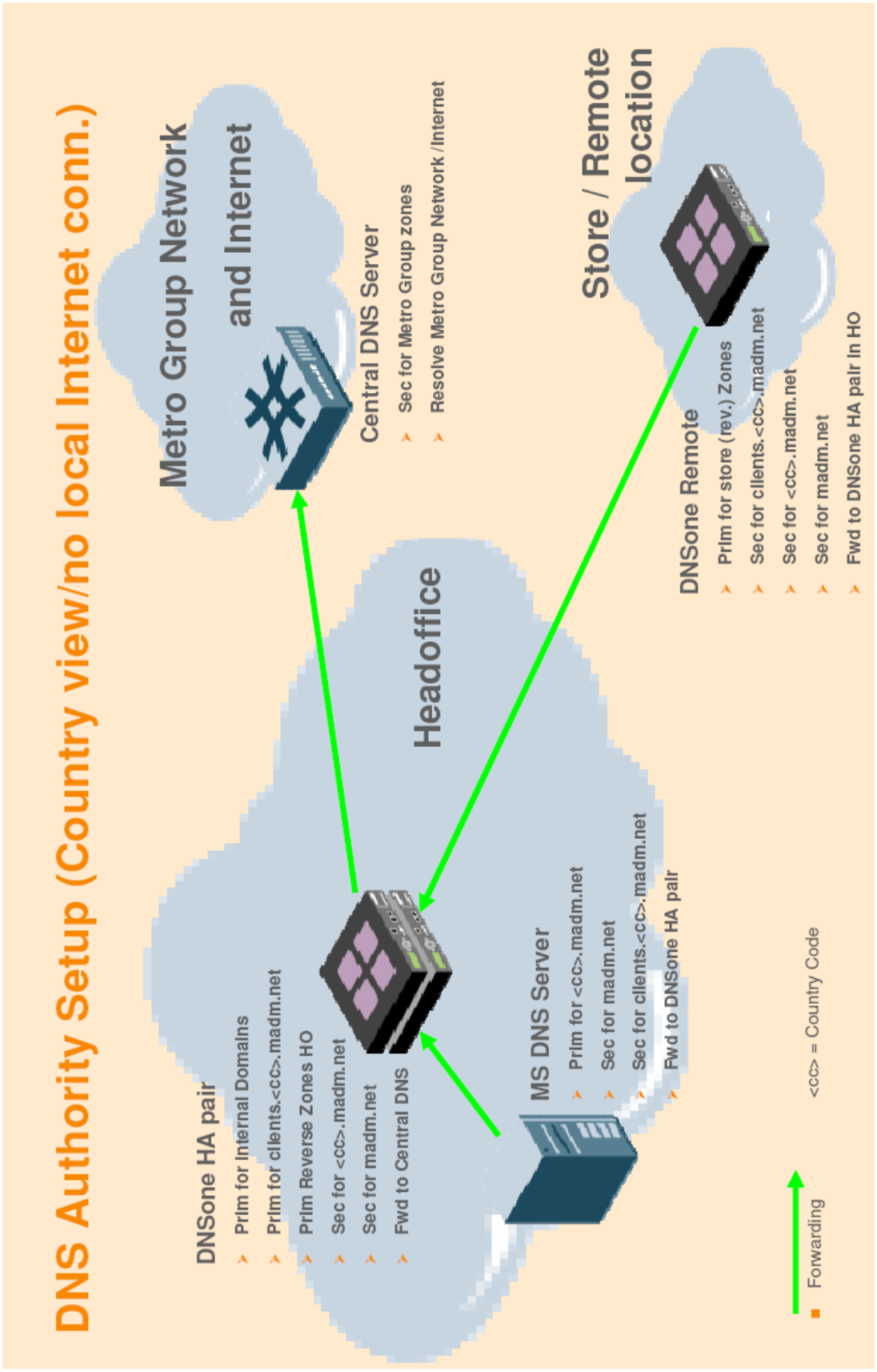
Příloha 5 - DNSone sítě obsluhované boxem na pobočce



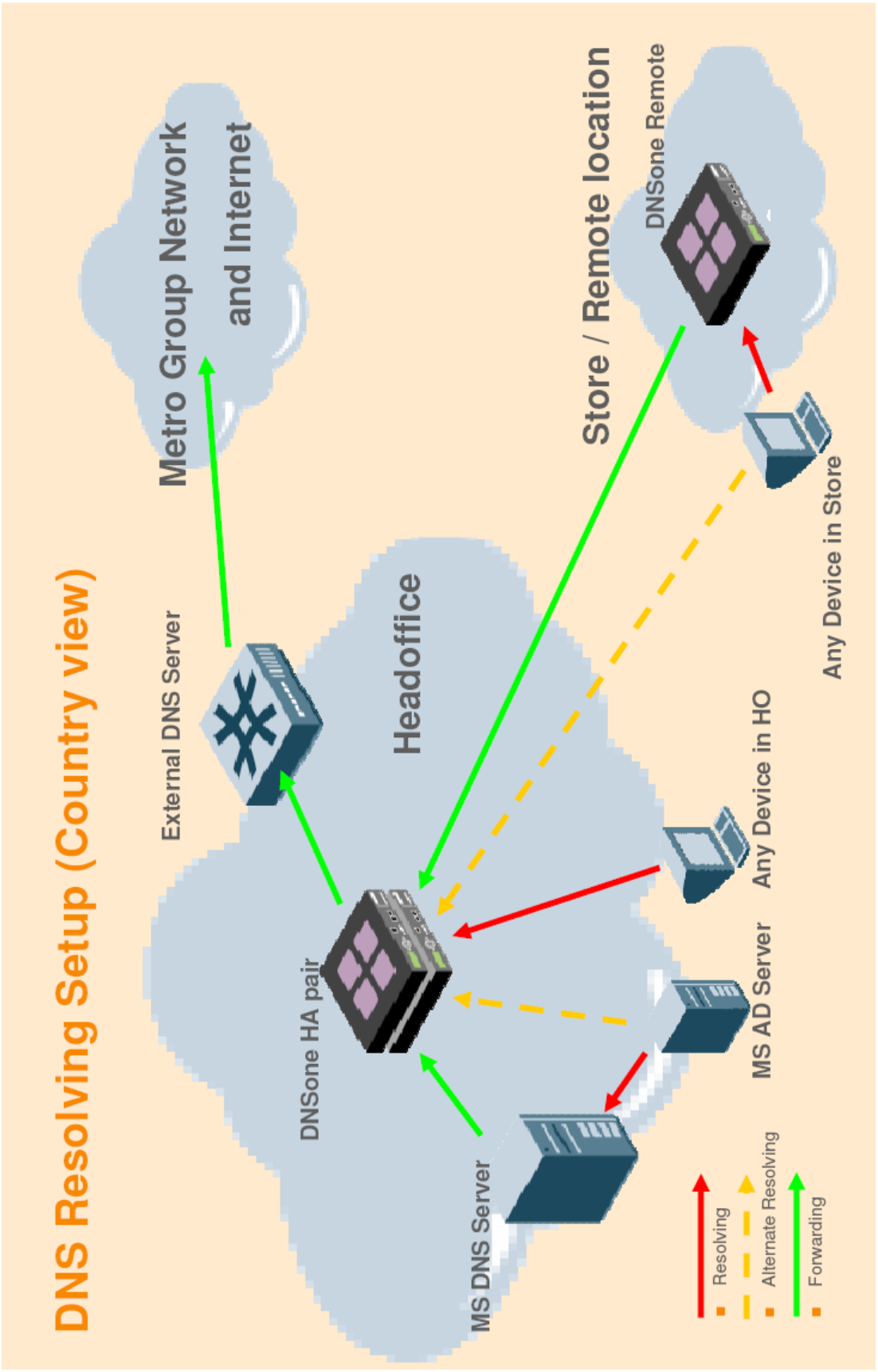
Příloha 6 - DNSone DHCP rezervace v jedné podsíti



Příloha 7 - DNSone Authority Setup, zdroj [7]



Příloha 8 - DNSone Authority Setup, zdroj [8]



Příloha 9 - Spotlight Server Monitoring Home Page

Příloha 10 - Spotlight Server Monitoring Physical Disk Activity