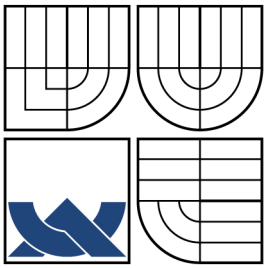
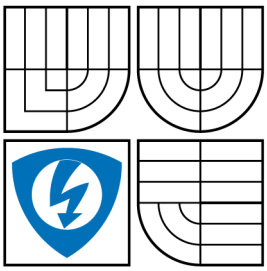


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

RELIZACE VÍCEÚČELOVÉHO SERVERU NA BÁZI WINDOWS

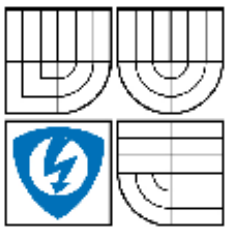
IMPLEMENTATION OF MULTI-PURPOSE SERVER BASED ON WINDOWS

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — PETR DEPIAK
AUTHOR

VEDOUCÍ PRÁCE — Ing. VÁCLAV PFEIFER
SUPERVISOR

BRNO 2008



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Depiak Petr ***ID:*** 78034
Ročník: 3 ***Akademický rok:*** 2007/2008

NÁZEV TÉMATU:

Realizace víceúčelového serveru na bázi WINDOWS

POKYNY PRO VYPRACOVÁNÍ:

Nastudujte problematiku a současné možnosti serverů na bázi WINDOWS a LINUX. Vzájemně srovnejte systémy na bázi WINDOWS (XP, 2000, NT, Server 2003) a zvolte nejvhodnější systém. Nastudujte problematiku služeb běžně poskytovaných servery – FTP, IMAP, NOVELL, Mysql, Apache. Na základě teoretických znalostí realizujte pracovní server založený na Vámi doporučeném systému, který bude sloužit jako veřejné úložiště dat pro akademické účely. Server musí poskytovat všechny běžné služby jako FTP, E-mail, MySQL, Apache apod.. Server musí umožňovat vzdálenou správu přes vhodného klienta a musí podporovat systém NOVELL.Server musí být navržen tak, aby bylo možno v budoucnu implementovat další služby, jako např. E-learning. Vzhledem k současným možnostem navrhněte vhodnou HW konfiguraci serveru pro plynulý běh serveru.

DOPORUČENÁ LITERATURA:

[1] Osif, M.:Windows Server 2003. Nakladelství GRADA, 2003. ISBN 80-247-0395-5
[2] Matas, J.: Linux jako brána do sítě Internet. [Bakalářská práce]. Ústav Telekomunikací □EKT VUT v Brně. 2007.

Termín zadání: 11.2.2008 ***Termín odevzdání:*** 4.6.2008

Vedoucí práce: Ing. Václav Pfeifer

prof. Ing. Kamil Vrba, CSc.
předseda oborové rady

UPOZORNĚNÍ:

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Petr Depiak
Bytem: Ondrova 63/69, 63500, Brno - Kníničky
Narozen/a (datum a místo): 19.5.1986, Brno

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií
se sídlem Údolní 244/53, 602 00, Brno
jejímž jménem jedná na základě písemného pověření děkanem fakulty:
prof. Ing. Kamil Vrba, CSc.

(dále jen „nabyvatel“)

Článek. 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - □ disertační práce
   - □ diplomová práce
   - ✓ bakalářská práce
   - □ jiná práce, jejíž druh je specifikován jako .....

(dále jen VŠKP nebo dílo)

Název VŠKP:	Realizace víceúčelového serveru na bázi WINDOWS
Vedoucí/ školitel VŠKP:	Ing. Václav Pfeifer
Ústav:	Ústav telekomunikací
Datum obhajoby VŠKP:	

VŠKP odevzdal autor nabyvateli v:

- ✓ tištěné formě – počet exemplářů 1
- ✓ elektronické formě – počet exemplářů 1

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - ✓ ihned po uzavření této smlouvy
   - □ 1 rok po uzavření této smlouvy
   - □ 3 roky po uzavření této smlouvy
   - □ 5 let po uzavření této smlouvy
   - □ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: …….

…… ……

Nabyvatel Autor

ABSTRAKT

Práce je věnována poznatkům o síťových službách, které se často vyskytují na serverových systémech. Tyto služby zejména souvisí s úschovou, přenosem a interpretací dat. Jedná se o služby přenosu, které využívají protokoly FTP a SMB, kde jsou popsány jejich principy a možnosti zabezpečení. Následující část rozebírá problematiku elektronické pošty a vysvětluje její principy a možnosti nasazení. Popsány jsou její stěžejní protokoly SMTP, POP3 a IMAP. Důležitou část práce tvoří služba WWW využívající protokol HTTP. V této kapitole jsou referována témata spojená s relační databází MySQL a skriptovacího jazyka PHP pro tvorbu dynamické prezentace elektronického dokumentu. Předešlá teorie je uvedena do praktické části práce, ve které jsou tyto služby implementovány na serverovou platformu MS Windows 2003 Server Enterprise Edition R2. Hlavním záměrem implementace je využití nejvýše možného zabezpečení dat v rámci možností dostupného programového vybavení. Rovněž obsahem práce je úvod do problematiky hostování služby eDirectory sítě Novell, která je v praktické části aplikována na použitou platformu Windows. Součástí realizace služby eDirectory je řešení její správy, tvořenou explicitním nástrojem umožňujícím konfiguraci, pomocí webového rozhraní.

KLÍČOVÁ SLOVA

Windows 2003 Server Enterprise R2; FTP; Elektronická pošta; E-mail; SMTP; POP3; IMAP; instalace; nastavení; Novell;

ABSTRACT

This thesis puts brain to the pieces of knowledge of the network services which are occurred in the server systems. These services are related to data storing, transport and data interpretation. Basically there are transport services which are used by FTP and SMB protocols. These protocols define them generally and their security too. Next section describes principles and application possibilities of electronic mail. It is based on SMTP, POP3 and IMAP protocols. The important part of this thesis is the World Wide Web service exploiting the HTTP protocol. It also refers to creation of dynamic presentation of electronic document by using the MySQL relational database and PHP script language. Practical part goes out of the theoretical part discussed above and all services are implemented on the MS Windows 2003 Server EE R2 platform. The main scope is oriented to the highest usage of data security within the available software. Other part presents the introduction to hosting of the Novell eDirectory service. It is practically applied on the MS Windows platform. This application also includes the administration of eDirecroty service by using the standard tool. This tool allows the administration though the web interface.

KEYWORDS

Windows 2003 Server Enterprise R2; FTP; File Transfer Protocol; Electronic mail; E-mail; SMTP; POP3; IMAP; installation; setting; Novell;

DEPIAK, P. *Realizace víceúčelového serveru na bázi WINDOWS.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008. 49 s. Vedoucí bakalářské práce Ing. Václav Pfeifer.

Prohlášení

Prohlašuji, že svou bakalářskou práci na téma „Realizace víceúčelového serveru na bázi WINDOWS“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení §11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení §152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

(podpis autora)

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Václavu Pfeiferovi za vstřícnou metodickou pomoc a za poskytnutý hardware pro vypracování praktické části bakalářské práce.

Dále děkuji Jaroslavu Meixnerovi, správci sítě Ústavu telekomunikací, za poskytnutí informací o počítačové síti VUT.

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Tato práce je věnována problematice a zprovoznění služeb souborového serveru, elektronické pošty a HTTP serveru. Tyto služby tvoří značný podíl v počítačových sítích a často se aplikují na specializovaný hardware.

Teoretická část práce se věnuje základním principům jednotlivých služeb a základním rozdílům mezi OS Linux a Windows. Líčena je problematika služeb a možnosti, se kterými je nutno vlastní seznámení před praktickým nasazením. U služeb přenosu souborů pomocí protokolu FTP jsou popsány možnosti zabezpečení. Jsou zde obsaženy i základní poznatky protokolu SMB, který je rozšířen mezi produkty IBM a Microsoft.

Součástí běžné administrátorské práce je i konfigurace webového serveru a elektronického poštovního systému. Kapitoly, pojednávající o těchto službách, jsou představeny z administrátorského pohledu pro jejich pochopení a implementaci.

Zmíněné služby jsou v praktické části popisovány z hlediska jejich instalace a konfigurace. Uveden je i důvod výběru jednotlivých programových prostředků a jejich omezení. Praktická část řeší určité problémy eDirectory spojené se sítí Novell, stanic využívající její služby, omezení těchto stanic a omezení možností pro hostující platformu Windows.

1 TEORETICKÉ ŘEŠENÍ

1.1 Windows, Linux

V dnešní době se nepřestává spekulovat o tom, který systém je lepší, a proto jsou v následující kapitole shrnuty charakteristické rysy. V současnosti existuje mnoho variant pro každý typ zmíněných systémů. Na linuxové (unixové) bázi ale počet převyšuje konkurenci. Hlavní příčinou jsou fakta, že většina linuxových systémů je vydávaná pod veřejnou licencí GNU GPL.

1.1.1 Linux

Výhoda linuxových systémů spočívá v možnosti širokého uživatelského nastavení. Existuje nespočet internetových stránek, kde je možné získat mnoho linuxových variant a potřebných balíčků. Uživatel si může vytvořit vlastní kompilaci specifikovanou pro jediný účel, např. domácí bránu. Linux díky své efektivnosti a případnému účelovému zaměření má nízké požadavky na hardware. Nepotřebuje grafické rozhraní, které zvyšuje nároky. Takovou zmíněnou domácí bránu je možné postavit třeba na staré x486 s 16 MB RAM, která neobsahuje pevný disk. Systém je zaveden přímo z diskety, CD nebo flash paměti. Problém vzniká tehdy, jestliže se uživatel příliš neorientuje v jeho prostředí a příkazech. Výhodou systému linuxového typu je minimální výskyt virů. Na Linuxu vyvíjejí i společnosti jako je Novell, jiné ho zase implementují do svých výrobků (např. Linksys). Ovšem některé společnosti se brání přijetí Linuxu pro svůj firemní server. Důvodů je hned několik. Jeden z nich je, že na klientských stanicích převládají systémy od Microsoftu, jenž by přišly o možnost využití veškeré vzájemné spolupráce. Výjimky tvoří sítě s několika druhy OS nebo servery poskytující funkce společné pro všechny systémy (www, e-mail, FTP…). Většinu distribucí Linuxu a dalších balíčků lze pořídit zdarma, ale uživatel přichází o určitou důvěryhodnost, než tomu je u komerčního software. Podstatné pro Linux je, že jeho kód je volně modifikovatelný, a proto může více vyhovovat zkušeným správcům, kteří si ho dokáží přizpůsobit dle svých požadavků. V některých případech volně šiřitelných verzí je zpracování tak kvalitní, že ani komerční software nedokáže konkurovat (např. značné využití FreeBSD)

1.1.2 Windows

Serverové řešení Windows se poslední dobou značně zlepšují a expandují. Jedná se o integrovanou platformu několika variant zaměřené na různé oblasti IT. Hlavní předností je jejich „jednoduchá“ obsluha, která spolu s klientskými OS (WinXP,W2k,Vista) tvoří jednu z nejlepších síťových platforem. Zaměřuje se na komerční oblast a jeho cílem je stanovit takové postupy a technologie, které zvyšují produktivitu práce s využití IT. Specifické pro sítě s doménou založené na produktu W2k, Windows 2003 je archi-

tektura *Active Directory*. Při vývoji byl zejména kladen důraz na výkonnost systému. Starší Windows NT nebyly příliš dokonalé a konkurence schopné stávajícím síťovým řešení Unix, Linux a FreeBSD. Nicméně byl to nutný krok, aby Microsoft posílila svoje postavení v oblasti serverových systémů.

"Náš cíl byl jasný, vytvořit řešení navržené s ohledem na přání zákazníků, které přinese dosud nevídanou kvalitu, nejvyšší výkonnost a nebývalou hodnotu pro firmy všech velikostí," řekl Bill Veghte, viceprezident divize Windows Server ve společnosti Microsoft. "První zákazníci potvrzují, že Windows Server 2003 snižuje celkové náklady na IT a přináší nejvyšší úroveň výkonnosti a spolehlivosti. Kvalita tohoto produktu je výsledkem neocenitelné podpory našich zákazníků a partnerů, kteří se podíleli na vývoji Windows Server 2003."

"Windows Server 2003 nabízí rychlost a stabilitu ve všech klíčových oblastech - ať už jako databázový server, aplikační server, webový server, souborový a tiskový server nebo jako poskytovatel adresářových a terminálových služeb. Podle výsledků nedávných testů uznávaného Transaction Processing Performance Council, patří Windows Server 2003 v žebříčcích TPC-C, TPC-H a TPC-W na první místo ve výkonnosti. Jakýkoliv zákazník může využít výhod Windows Serveru 2003 ke zlepšení ekonomického výsledku tím, že sníží náklady na hardware a administraci vzhledem nízké ceně a vysokému výkonu. Vysoké výkonnosti dosahuje Windows Server 2003 zejména na větších multiprocesorových systémech založených na 64 bitovém procesoru Intel Itanium 2."[8]

1.2 PŘENOS SOUBORŮ

1.2.1 FTP (File Transfer Protocol)

File transfer protokol je protokol určený pro přenos souborů v síťovém prostředí. Záměrem jeho vzniku bylo stanovení pravidel přenosu souborů, které budou společné pro odlišné druhy operačních systémů v heterogenních sítích.

Vznik protokolu FTP se přiřazuje do roku 1971. Do dnešní doby prošel řadou inovací a vylepšení. Soupis změn a přehled postupného vývoje standardů tohoto protokolu lze naleznout v dokumentu normy RCF 959. Tento dokument slouží jako opěrný bod, o něhož se opírají novější dokumenty, ať už doporučené postupy, diskuze nebo standardy (RFC 1579, RFC 2228, RCF 2428, RCF 3659). Ty doplňují protokol FTP o metody a funkce, bez jejichž uplatnění by byl v dnešní době jen těžko použitelný. Např. RFC 1579 pojednává o způsobu užití a chování protokolu, stojí-li v cestě firewall. Další RCF 2428 je standardem pro rozšíření protokolu FTP při použití protokolu IPv6 a překladu adres NAT.

V současnosti zastává tento protokol v síti Internet velice důležitou roli. Často se setkáváme s jeho implementací u hostingových služeb, kdy odesíláme zdrojové nebo datové soubory webových stránek aj. na server. Časté použití je nasazení FTP na systémy po-

skytující veřejnou distribuci dat. Samozřejmě se využívá i pro privátní přenos (často i velice „citlivých“) dat přes síť Internet. Ve druhém zmíněném případě bude objasněna nevhodnost tohoto použití dále v textu.

Protokol FTP patří v modelu TCP/IP síti do aplikační vrstvy. Zapouzdřuje se do nižší spolehlivé spojově orientované vrstvy TCP. V protokolu TCP obsazuje dva základní porty v rozsahu označovaném jako „dobře známe porty“, z anglického „Well known ports“. Konkrétně port č. 21, na kterém jako výchozím naslouchají FTP servery pro řídící spojení a port č. 20, ze kterého probíhá přenos souborů.

Datový přenos probíhá ve znakové nebo binární formě. Výhoda použití znakové formy spočívá v jednoduchém zajištění kompatibility různých operačních systémů, pro kterou byl mimo jiné FTP vytvořen. Znakovou formou mohou být korektně přesouvána data v textové podobě, která jsou automaticky konvertována do znakové sady cílového OS, aby znakové interpretace mezi OS byly ekvivalentní. V binárním režimu přenosu je soubor přenesen přesně bit po bitu.

Bezpečnost FTP

Samozřejmě princip znakového přenosu a její otevřenost má i své velké nevýhody. Jak je zmíněno dříve, není vhodné tuto technologii používat pro přenos citlivých dat, které by se mohly dostat do nepravých rukou. Data nejsou šifrována a mohou být zachycena 3. osobou mezi komunikujícími uzly sítě. Další nebezpečí hrozí, jestliže se k FTP serveru pomocí loginů a hesel připojují jen pověření uživatelé, hrozí odhalení jejich přihlašovacích údajů. Vysvětlení je jednoduché, protože řídící spojení pomocí kterého probíhá i výměna přihlašovacích údajů, funguje formou dialogu mezi uzly nechráněnými znakovými příkazy.

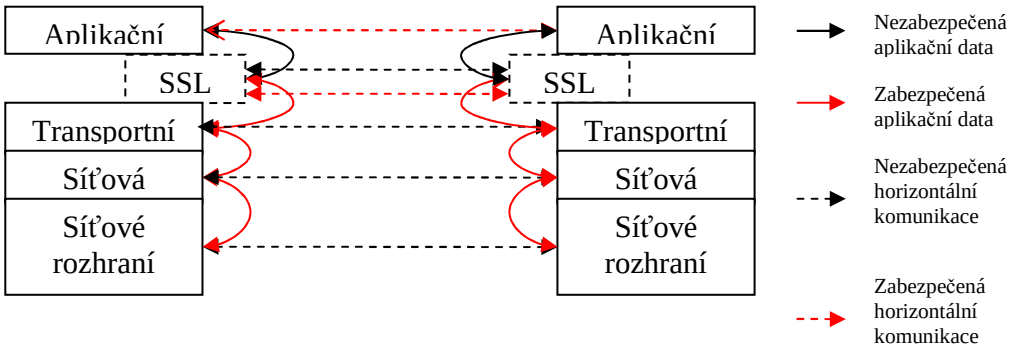
Metody zabezpečení

SSL/TLS

Pro splnění bezpečného přenosu pomocí FTP a ochranu dat šifrováním lze použít dodatečnou šifrovací vrstvu SSL nebo TLS. Spojení těchto bezpečnostních vrstev s FTP (server FTP s implementovanou podporou SSL/TLS) označujeme jako FTPS (nezaměňovat s SFTP!). Využití těchto vrstev je založeno na použití PKI (Public Key Infrastructure) a certifikátů dle X.509.

Certifikáty jsou použity nejen jako veřejné klíče pro autentizaci asymetrickou šifrovací metodou a vygenerování klíčů sezení, ale také jako podpis totožnosti. Záleží pouze na tom, jaká instituce certifikát vydala. Samozřejmě certifikát může vydat CA – Certifikační autorita, která je ve světovém měřítku respektována, nebo si certifikát můžeme vytvořit zcela sami na serveru, který tuto službu podporuje. Takto vytvořený certifikát se bude na klientské straně ve většině případů značit jako nedůvěryhodný.

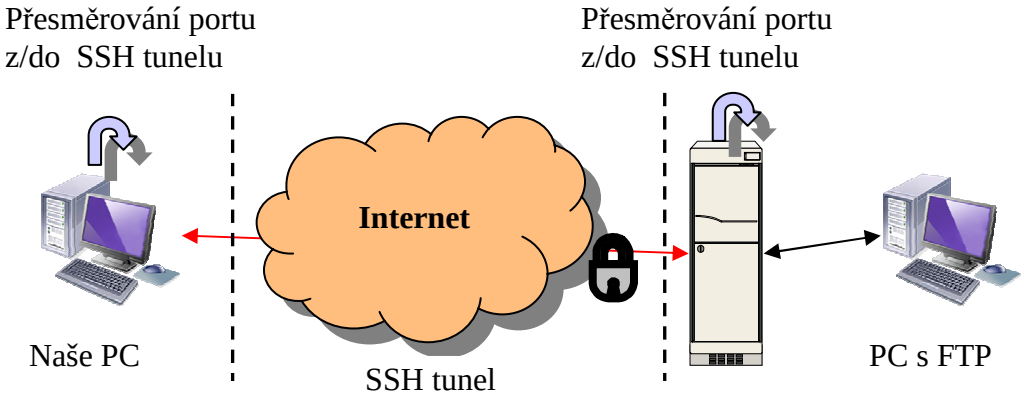
SSL nezabezpečuje veškerou komunikaci, ale pouze komunikaci klient-server (aplikační vrstvu). Pro připojení k FTP serveru zabezpečený SSL, budeme potřebovat na straně klienta program, podporující toto spojení. Např. program *DataFreeway*.



Obr. 1 *Princip komunikace přes zabezpečovací vrstvu SSL*

SSH tunelování

Další možností je využití tunelování přes zabezpečené spojení SSH. V takovém případě hovoříme o Secure FTP. Často se setkáme s označením Secure FTP, které pracuje s vrstvou SSL jako FTPS, ale prvotně je toto označení myšleno v kombinaci s SSH (FTP over SSH). Vytvoříme socket šifrovaný SSH, přes který spojujeme aplikační programy FTP. Princip je podobný jako v předchozím případě, ale jedná se o metodu, na které není nutné uzpůsobovat aplikační programy. Jednoduše vytvoříme „zabezpečený tunel“, do kterého směrujeme porty komunikace. Nevýhodou je, že na vzdáleném konci potřebujeme mít vytvořený SSH účet. Jedno z použití SSH tunelu viz Obr. 2.



Obr. 2 *Možnost použití SSH*

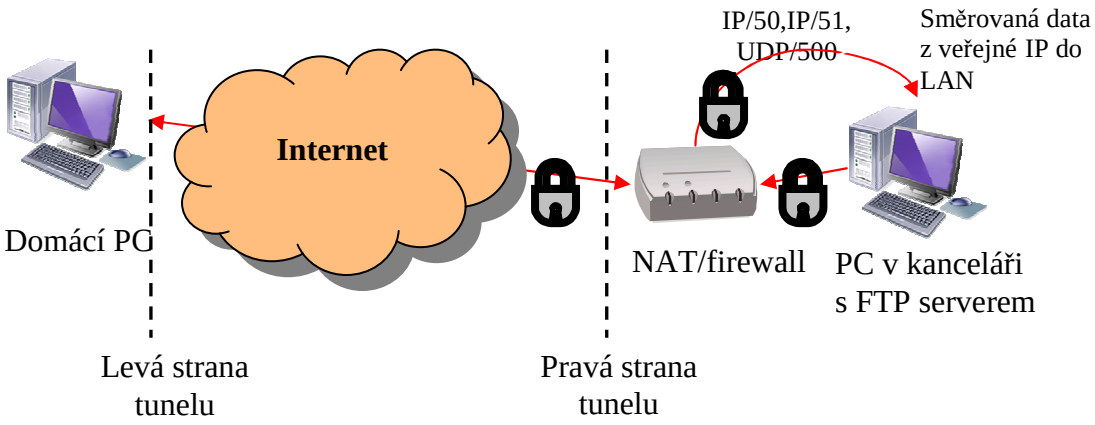
V konkrétním případě dle obrázku je vhodné vytvořit tunel pro porty TCP/20 a TCP/21, abychom uchránili datové i řídící spojení.

Další označení, se kterým se setkáme je SFTP, která není přímou nadstavbou FTP, ale programu SCP vycházejícího z Unixu. Tento program řeší SSH ve vlastní režii obdobně jako FTPS řeší SSL.

IP Sec

Poslední možností je využití protokolu IP Sec (Internet Security Protocol). Jedná se o nepovinné[1] rozšíření síťové vrstvy o bezpečnostní a kryptografické mechanismy. Výhoda oproti SSL je nezávislost protokolů vyšších vrstev. Tato metoda, nejen že zajistí vlastní šifrování, ale zajistí i směrování. V takovém případě se nejedná o příliš časté užití s FTP, protože IP Sec tunel je nutné nastavit na obou stranách pro každou komunikující dvojici. Konfigurace je náročná, proto se používá při komunikaci mezi statickými uzly přes veřejnou síť např. VPN sítě.

IP Sec zabezpečuje data pomocí šifrování na úrovni síťové vrstvy. Útočník z dat zachycených paketů nezjistí žádnou souvislost. Dokonce i IP hlavičky paketu může být zašifrována a nahrazena.[2]



Obr. 3 *IP Sec tunel pro zabezpečené spojení k FTP přes NAT*

Každá metoda zabezpečení je vhodná pro určité podmínky, ale můžeme říci, že pro veřejné služby a ochranu osobních údajů aplikací WWW, pošty nebo souborové služby je nejrozšířenější a nejvhodnější SSL.

Přístupové režimy

Protokol FTP ke svému provozu potřebuje dva datové kanály. Jeden kanál pro přenos souborů, který standardně využívá protokol TCP na portu č.20. Druhý kanál slouží k vlastní režii protokolu, která zahrnuje výměnu stavových informací a základní autentizaci uživatele přes TCP port č.21. Mohou nastat dva případy přístupu. Označujeme je jako „aktivní režim“ a „pasivní režim“.

Aktivní režim

Tato situace nastává, pokud klient vlastní veřejnou IP adresu na svém PC, která je dostupná pro server FTP. Spojení zahajuje klient z náhodného portu TCP/1023< na řídící port TCP/21. Následně jsou data odeslána z portu TCP/20 serveru na klientem zvolený port TCP/1023< svého PC.

[1] Nepovinné je pouze u IPv4. Nová generace – IPv6, zahrnuje zabezpečení ve vlastním základu.
[2] Je-li použit *tunelový mód* v IP Sec.

Tento režim lze využít i v případě, že uživatelské PC je skryto za NAT a toto NAT zařízení podporuje aktivní režim komunikace. Princip řešení je nahrazení příkazového řetězce nesoucí informaci o portu a IP adrese klientského PC pro server, IP adresou brány NAT a nového portu zvoleného bránou. Tato změna může změnit velikost celého paketu, proto musí být ošetřena i režijní pole závisející na délce paketu. Při použití SSL/TLS je tento způsob nefunkční.

Server FTP lze skrýt za bránu s NAT, ze které bude na jeho vnitřní IP směrován řídící port. Pro přihlášení budeme užívat veřejnou IP adresu brány na straně serveru.

Obr. 4 *Zahájení komunikace v „aktivním režimu“*

Pasivní režim

Je častěji se vyskytující situace v Internetu. Uživatelé jsou skryti za bránou s NAT a není možné směrovat všem PC uvnitř sítě rozsahy portů. Brána nepodporuje editování paketů viz aktivní režim (u levnějších zařízení), ať už z důvodu bezpečnosti, tak i zneužití. V této situaci nezbývá nic jiného, než aby řídící spojení a datové spojení otevíral klient a vytvořil tak funkční kanál. Server postupně vystavuje data v nastaveném rozsahu portů TCP/1023< a v řídícím spojení oznámí klientovi na kterém portu si jakou část dat může vyzvednout.

1.2.2 SMB (Server Message Block)

SMB protokol slouží pro sdílení souborů, tiskáren, pojmenovaných rour[3], sériových portů a dokonce poštovních slotů. Protokol má za sebou poměrně dlouhý vývoj od první technické reference z roku 1984. První výrazné nasazení bylo v programu Microsoft Lan Manager r. 1987 a později v OS/2 Lan Server od IBM.

Snahou bylo tento protokol prosadit jako jeden ze standardu Internetu. SMB je protokol aplikační vrstvy, který byl vyvinut nad relační vrstvou NetBIOS pro přenos po TCP/IP nebo NetBEUI. Tím je zajištěna nezávislost na nižších vrstvách, proto lze přenášet SMB pomocí protokolů IPX/SPX, NetBEUI nebo TCP/IP. Ve Windows Vista a Windows Server 2008 je implementována novější verze SMB 2.0

[3] V systému UNIX jsou tyto roury využívány k předávání dat mezi nesouvisejícími programy – procesy.

NetBIOS počítá jak se spojovaným, tak s nespojovaným provozem a umožňuje vysílání datagramů typu unicast, multicast i broadcast.

NetBIOS nepracuje vůbec s adresami uzlů ze síťové vrstvy, namísto toho využívá logických jmen (řetězec až 16 znaků), které si mohou jednotlivé nódy libovolně volit a registrovat. Na jednom adaptéru smí být zaregistrováno nejvýše logických 254 jmen.

- *stanice, která si hodlá přiřadit určité jméno, informuje broadcastem ostatní stanice sítě*
- *pokud tyto nepošlou v určeném časovém limitu negativní odpověď (požadované jméno již vlastní), může stanice prohlásit logické jméno za své.*

Mimo jmen jednoznačných, které může být v daném okamžiku přiřazeno pouze jediné stanici, pracuje NetBIOS také se jmény skupinovými. Skupinové jméno může být přiřazeno více stanicím a používá se pro vysílání typu multicast.

Z principu registrace jmen, který zahrnuje všesměrové vysílání, je zřejmé, že: - ve větších sítích LAN mohou nastat problémy se zahlcování sítě broadcasty - NetBIOS není možné bez přidaných řešení použít v sítích WAN z důvodu filtrování broadcastů routery.
Proto bylo v RFC 1001 a RFC 1002 definován provoz NetBIOS přes TCP/IP který používá point-to-point komunikaci se jmenným serverem (WINS nebo Dynamic DNS). Jména se registrují a vyhledávají u jmenného serveru a ten i brání jejich duplicitě.[4]

Zabezpečení SMB

SMB umožňuje dvě metody zabezpečení ke sdíleným prostředkům:

- K jednotlivým úrovním sdílených prostředků vyžaduje heslo;[4]
- uživatel se nejprve přihlásí loginem/heslem přes autentizační NT formulář a na základě úspěšného přihlášení je relaci přidělen identifikátor, kterým se prokazuje v následujících požadavcích. Server si tento identifikátor spojuje s oprávněním použitého uživatelského účtu.

U obou způsobů přenos přihlašovacích údajů probíhá v šifrované podobě.

[4] Zejména generace Windows 9x. Novější systémi využívají 2. způsob.

1.3 ELEKTRONICKÝ POŠTOVNÍ SYSTÉM (E-MAIL)

Před zprovozněním takového systému, zahrnující odesílání, přijímání elektronické pošty, je nutné mít potřebné znalosti. Ty je potřeba aplikovat a vytvořit tak uživatelům pošty jednoduché a funkční zázemí, které bude umožňovat přístup do jejich schránek.

První „e-mail“ vznikl ve formě, kdy si uživatelé jediné stanice zanechávali zprávy ve složce uživatele, pro kterého byla zpráva určena. Ten si ji po přihlášení přečetl. První mailový systém pracující na takovém principu byl pravděpodobně MAILBOX, využívaný v Massachusetts Institute of Technology po roce 1965. V této době neexistovaly sítě, které známe dnes. Počítače byly drahé, proto se hojně využívalo terminálů, jako takový „vzdálený ovladač“.

Situace se obrátila v nabývajícím počtu informačních technologií. Ceny výpočetní techniky klesaly. Počítače se vzájemně začaly propojovat do počítačových sítí. Vznikla otázka, jakým způsobem vytvořit sjednocené pravidlo, které by identifikovalo příjemce pošty. Ihned od počátku se uvažovalo, že k jednotlivým počítačům přistupuje vícero uživatelů. Standardizace tvaru adresy, kterou dnes užíváme[5], byla uskutečněna díky Ray Tomlinson, který je často označován za vynálezce pošty.

Systém elektronické pošty udělal velký poprask v tehdejší největší sítí, kterou byla americká militaristická síť ARPNET, efektivně pozvedl její smysl. Využití této sítě tvořilo později přibližně ze 75 % elektronická pošta, která se stala terčem výzkumu.

Do dnešní doby existovalo několik modelů takového systému, které byly vytvořeny různými společnostmi pro vlastní nasazení, ale celosvětově se uchytil pouze jeden, který známe dnes.

Celý mechanismus si můžeme dekomponovat na dva celky a to na „doručování“ a „výběr“ pošty. Každý celek je specifikován způsobem komunikace a používanými protokoly.

1.3.1 Doručování elektronické pošty

Vyhrazenými místy pro odesílání elektronické pošty slouží servery, na kterých běží program MTA (Mail Transport Agent). Jeho úkol je předávat zprávy do cílových systému s rozdílem, že místo poštovního směrovacího čísla nese adresa doménové jméno nebo IP adresou cílového místa. Smyslem MTA je i vytvoření takové politiky nastavení filtrů mezi servery, které slouží jako jedna z prevencí proti rozesílání SPAM. MTA jsou budovány v rámci domény (např. podniku, pobočky, organizace, atd.)

Součástí serveru zajišťující chod MTA je zpravidla MDA (Mail delivery agent) popřípadě prostředek, který zprávu vyhodnocenou MTA, určenou pro jeho doménu předá MDA. Prostředekem komunikace mezi servery MTA slouží protokol SMTP.

[5] *<jméno>@<doména>*

MX záznam

MX (Mail Exchange) záznam je specializovaný záznam adresy poštovního serveru v doméně. Záznam je uložený na DN serveru. Může být vytvořen pouze pod záštitou registrované domény, která může obsahovat několik takových záznamů. Obsahuje-li doména více MX záznamů, jsou rozlišeny podle určené priority.

Za normálních okolností se pošta bude směřovat na server, jehož záznam obsahuje nejmenší číslo priority. Nebude-li server funkční nebo dosažitelný, bude se pokoušet zdrojový systém o doručení na následující MX záznam. Jestliže ani server, na kterého ukazuje poslední MX záznam, nebude funkční, zdrojový systém bude zacházet se zprávou podle vlastních definovaných pravidel.[6]

Příjemné je, že pomocí MX záznamu může být pošta uschována v odlišné doméně, než které je zpráva adresována. Tento záznam není nezbytný pro provoz poštovního serveru. Lze užít i A záznam, ale v takovém případě pravá část emailové adresy musí obsahovat adresu poštovního MTA serveru. Nepříjemné je, pokud používáme takový server pro odchozí poštu, cílové MTA ji nemusí přijmout, zjistí-li že tento server nevlastní MX záznam.[7]

SMTP (Simple Mail Transport Protocol)

Tento protokol byl původně definován RFC 821/822 (r.1982) a nahrazen RFC 2821(r.2001). Často je rozšiřován dle RFC 1869. Samotný protokol předpokládá, že na jeho bezchybný přenos při komunikaci dohlíží nižší (transportní) protokol. V TCP/IP sítích tuto roli zastává spolehlivý spojově orientovaný protokol TCP. V něm je vyhrazen port č.25 určený pro komunikaci tohoto aplikačního protokolu.

Samotné doporučení definuje formát a syntaxe textové zprávy, která je schopna přenášet pouze text ASCII o maximální celkové velikosti 64kB. Samozřejmě toto omezení bylo z velké míry nedostačující, proto bylo vytvořeno rozšíření, jež definuje série RFC 2045, RFC2046, RFC 2049, RCF 1652 aj., které tvoří rodinu známou pod označením MIME. Tento standard rozšiřuje tělo zprávy na několik typů, z nichž má každý své podtypy. Jestliže zpráva přesáhne limitovanou velikost, je rozdělená do více bloků, které tuto velikost splňují. Rozšíření MIME umožňuje v těle zprávy přenášet text, který neobsahuje pouze znaky ASCII a různé přílohy (video, obrázky a jiné soubory).

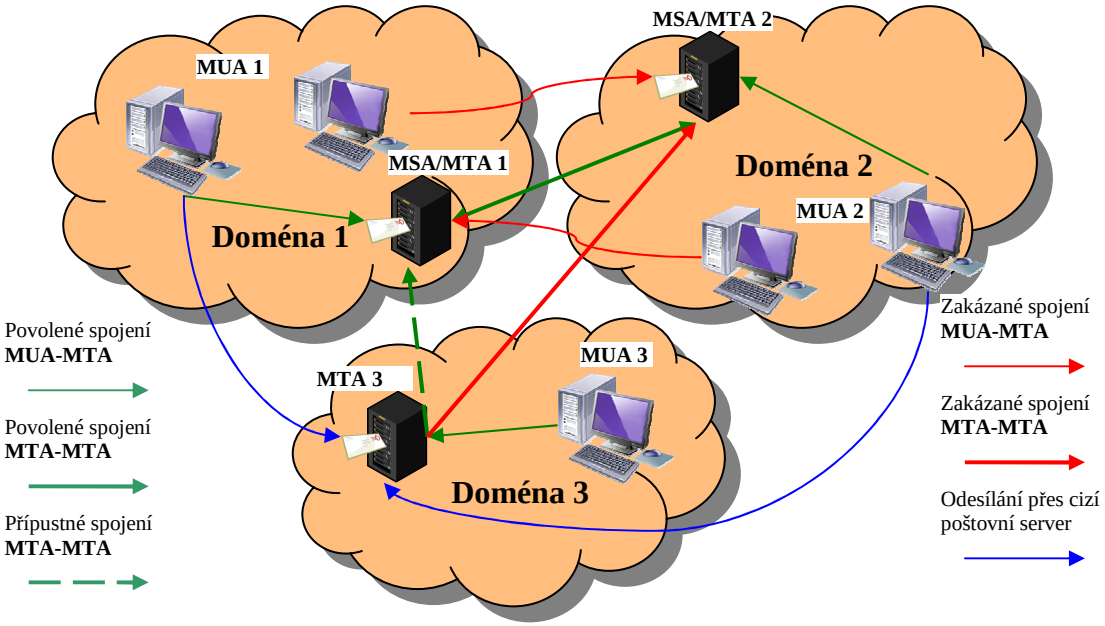
Tato expanze je umožněna nejen rozšiřujícími zprávami MIME, ale i jeho kódováním. K zajištění bezproblémové průchodnosti MIME pracujícím s osmi bity je nutné převod do 7 bitů, se kterými pracuje SMTP nebo použití rozšířeného ESMTP, který umožňuje přenos po 8 bitech. Na výběru se dohodnou komunikující strany na základě výměny informací.

[6] Např. pokusí se o nové odeslání po časovém intervalu nebo je oznámena nedoručitelnost a zpráva je zahozena.
[7] Účelem je zabránění nevyžádané pošty, která je často odesílána viry z nezabezpečených stanic s A záznamy.

SMTP užívají pro přenos zpráv následující druhy programů :

1) MTA (Mail Transport Agent) je program, který je spuštěn na „SMTP serverech“ a stará se předávání mezi MTA a doručování zpráv do cílových systémů MDA.
2) MUA (Mail User Agent) je program který se stará o vytvoření a předání zprávy k MSA.
3) MSA (Mail Submission Agent) slouží jako prostředník pro filtraci mezi MUA a MTA. Není klíčovou součástí. Bez jeho přítomnosti MUA předává zprávy přímo MTA.

MSA zachovává určitou robustnost celého elektronického poštovního systému. Většina „SMTP serverů“ nedovoluje přeposlat zprávu cizích MUA nebo MTA, respektive uživatelům nepatřící do jejich domény nebo uživatelům (serverům), kteří se k těmto serverům pokouší připojit bez platných identifikačních údajů.



Obr. 5. *Ilustrace případů vzájemné konfigurace MUA,MSA/MTA.*

Na Obr. 5 jsou znázorněny možnosti odesílání pošty. MUA1 může bez problémů odesílat poštu na MSA/MTA 1. Může využít i MTA 3 domény 3, nezakazuje-li toto spojení doména1. MTA 3 nemá nastavena žádná vstupní pravidla, ale od takového „open--relaying“ serveru mohou/nemusí přijmout poštu další nebo cílové MTA. V současnosti jsou „open-relaying“ servery nežádoucí a mohou být zanesení v tzv. „Blacklists” jiných MTA.

S určitým problémem se můžeme setkat, jestliže využíváme vlastní MUA (Outlook, Thunderbird…) a ISP dovoluje odeslání přes vlastní MTA s použitým MSA a osobní autentizací. Tento problém se ze zkušenosti vyskytuje zřídka. Jestliže vlastníme pouze jedinou autentizaci a nechceme její heslo svěřovat jiné osobě za účelem odeslání pošty, lze v takovém případě vytvořit místní MTA server, který pomocí „relaying“ přesměrovává zprávy na dostupný MTA. Spojení je autorizováno výše zmíněným účtem, který je zanesen na tomto MTA zcela transparentně vzhledem k uživatelům. Zároveň pro uži-

vatele využívající tento MTA lze definovat lokální pravidla. Dále můžeme vytvořit zcela nezávislý MTA, který ale mohou cizí MTA považovat za nedůvěryhodný, jestliže bude umožňovat rozvoj SPAM.

Splnění hierarchické struktury serverů blokuje do jisté míry zdroje nežádoucích emailů a šíření virů pomocí nich. Nežádoucí službou MTA je zmíněný „open-relaying“, který dovoluje komukoliv na internetu využít jeho poštovních služeb a odesílat přes něj poštu. Takový server se zanedlouho dostane do databáze „Blacklist”, ve kterém jsou uloženy adresy serverů, domén, z nichž dochází k odesílaní SPAM.

Zabezpečit odchozí poštu lze pomocí SSL a STARTTLS za předpokladu použití rozšířeného ESMTP a podpory klientského programu. Server rozpozná odchozí protokol (SMTP, ESMTP) na základě pozdravu klienta při navazování spojení:

- SMTP – „HELO“
- ESMTP – „EHLO“

Na základě zvolenému zabezpečení probíhá spojení standardně na tyto porty:

- SSL – TCP/465
- STARTTLS/TLS – TCP/25

Přenos probíhá formou dialogu mezi odesílatelem a příjemcem pomocí příkazů SMTP. Jestliže MTA dostane zprávu s příjemci na obálce ve tvaru *jmeno@domena*, kontroluje nejprve pravou[8] stranu. Zjistí-li, že se ho tato zpráva netýká, vyžádá si z doménového serveru MX záznamy cílových domén, které definují adresu poštovního serveru s MTA v jednotlivých doménách.[9] Následně přepošle na zjištěnou adresu držené zprávy s patřičnou obálkou. Zjistí-li cílový poštovní server, že zpráva je určená pro něj, předá ji programu MDA, který aplikuje nastavená pravidla (filtrování nevyžádané pošty, antivirová kontrola aj.) a umístí zprávu do příslušné schránky příjemce[10].

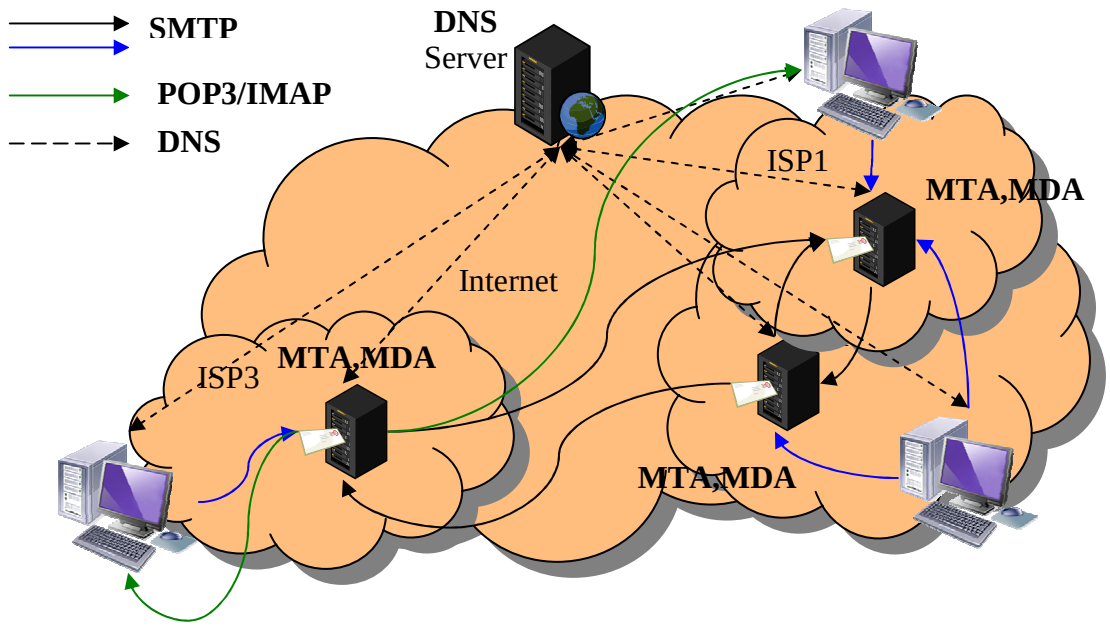
Obálka

Důležitou součástí zprávy tvoří tzv. obálka, kterou zpravidla vytváří MTA. Ta je nezbytnou součástí komunikace mezi MTA. Obálka obsahuje adresu odesílatele, adresu příjemce nebo příjemců. Je předřazená hlavičce a může plnit několik funkcí. Nejčastější funkcí je duplikace celé zprávy. Tyto kopie se opatří jednotlivými obálkami nesoucí adresu nebo skupinu adres příjemců jednotlivých směrů. Tímto se zabrání zahlcení sítě potulnou poštou postupným odebíráním příjemců z obálky, pro které už byla kopie odeslána jiným směrem. V hlavičce vlastní zprávy tito příjemci zůstanou z informativního charakteru.

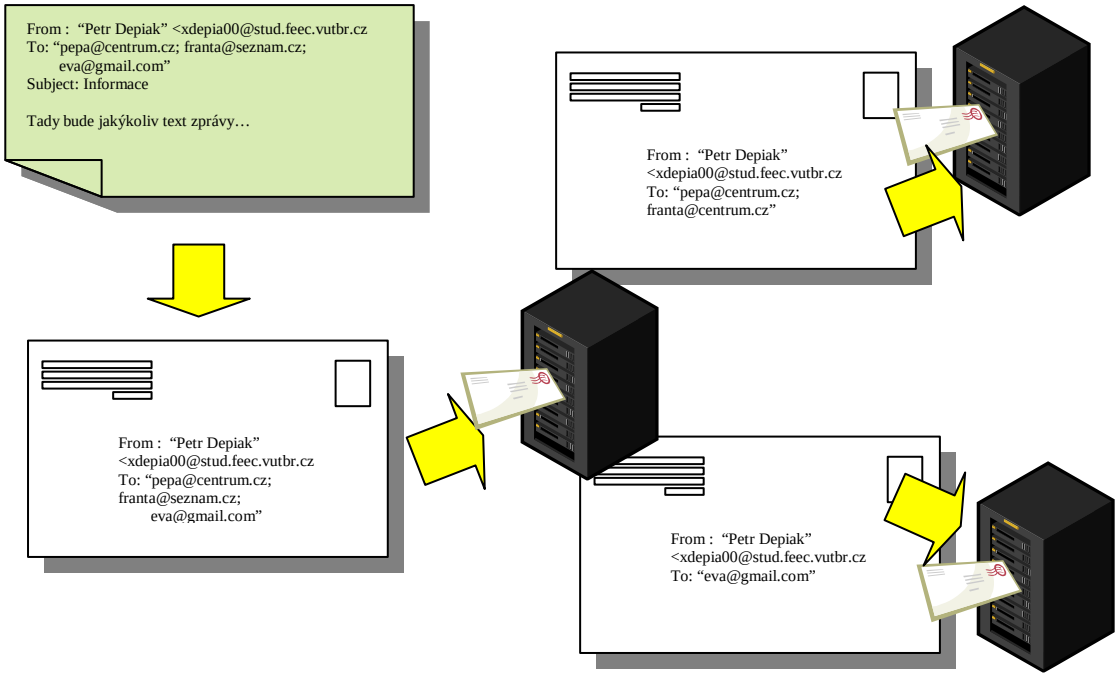
Např. jedna zpráva je určena do dvou různých cílových systémů, které ilustruje Obr. 7. Pokud by nebyla doplněna obálkou, šířila by se z každého uzlu zpětně na všechny adresy nebo by se museli postupně odebírat příjemci z hlavičky.

[8] Doménovou adresu
[9] Neexistuje-li MX záznam, doménová adresa se bere jako A záznam, na kterou se pokouší o doručení.
[10] Příjemce je určen na levé straně od „@“.

Obálka nás může informovat i o nedoručitelnosti na příjemcovu adresu. Toto hlášení se vrátí na adresu odesílatele.



Obr. 6 *Protokoly v jednotlivých částí systému elektronické pošty*



Obr. 7 *Princip použití obálek v elektronické poště*

1.3.2 Výběr elektronické pošty

Předchozí text byl věnován principům doručování elektronické pošty, proto se tato kapitola bude věnovat metodám a možnostem jejího výběru. Málo který uživatel má zřízený poštovní server ze svého počítače, ale většina využívá ať už podnikový, školní nebo veřejné poštovní servery v určité doméně, respektive servery s MDA programy.

Zatímco pro doručování pošty mohlo existovat více alternativ odchozích směrů závislé na nastavení MSA, MTA a nastavení sítě ISP v případě použití explicitního MUA, kdy bylo možné poštu odeslat na různé servery. Příchozí pošta dané domény se shromažďuje pouze v jediném systému (serveru nebo clusteru), na kterém jsou zpravidla udržovány zálohy a další opatření proti havárii a poškození dat. K tomuto místu, ať jsme na kterémkoliv místě s přístupem na internet se připojujeme.

Pokud poštovní systém podporuje grafické rozhraní, neboli existuje aplikační server s webovým rozhraním, prostřednictvím kterého přistupujeme do databáze MDA, můžeme si poštu prohlížet přímo v tomto prostředí. Samozřejmě ji lze přenést do našeho MUA a prohlížet si poštu v něm. Každá možnost má své pro i proti. Např. je hloupost poštu stahovat do veřejného PC, kde by se muselo provádět neustále nastavení MUA, ke kterému uživatel nemusí mít potřebná oprávnění. Zde je vhodnější využít grafické rozhraní poštovního systému, u kterého se staráme pouze o zadaní loginu a hesla. Naopak je výhodnější stahovat poštu do osobního PC, kdy z důvodu pomalého připojení ztrácíme čas vykreslováním grafického rozhraní poštovního systému. S tímto souvisí i protokoly pro komunikaci mezi MUA a MDA.

POP3 (Post Office Protocol 3)

POP3 protokol byl vytvořen k účelu navázání spojení mezi MUA a poštovní schránkou, respektive MDA programem. Definuje jej dokument RFC 1939. Protokol naváže spojení ke schránce s MDA na portu TCP/110 a na základě identifikace je uživateli poskytnut obsah v ní uložených zpráv, které se zkopírují do MUA. Ve schránce se původní zprávy zpravidla smažou. Říkáme, že pracujeme v režimu „off-line“, protože zprávy jsou nejprve stáhnuty a po té je nezávisle zpracovány.

Protokol nejdříve podporoval pouze nezabezpečený přenos přihlašovacích údajů. Nyní lze doplnit protokol POP3 o následující autentizační protokoly a využít tak několika metod pro zabezpečení přihlášení podle rozšíření RFC 2449:

1. APOP – šifruje pouze heslo hashovací funkcí MD5, ale nezabrání proti opětovnému zneužití hashovaného řetězce dle RFC 2195; nešifruje data;
2. SASL – soustava zabezpečovacích mechanismů vzdálené identifikace a zabezpečeného datového přenosu dle RFC 2222;
3. SSL/TLS – zabezpečovací vrstva viz str.14. Takto zabezpečený přístup zajišťuje většina provozovatelů na odlišném portu. Např. *gmail* na portu TCP/995.

IMAP (Internet Message Access Protocol)

V současnosti se dostává na výslunní právě tento protokol. Konkrétně je využívána verze IMAP4rev1 definována RFC 3501. Komunikace probíhá přes TCP obdobně jako u POP3, ale na portu TCP/143.

Protokol je navržen pro účel pracovat se zprávami přímo na serveru. Tedy říkáme v „online“ režimu. IMAP umožňuje současnou práci několika uživatelů v jediné schránce, mezi kterými udržuje synchronizaci a okamžitě detekuje změny provedené připojenými

uživateli. Těchto výhod je využito převážně při komunikaci v podnikatelské oblasti, kdy v takovém případě je POP3 těžko myslitelný. IMAP podporuje připojení sdílených složek uživatelů a veřejných složek, které mohou být několika typů (složka, kontakty apod.). Např. ve firemní poště lze využívat společnou databázi kontaktů, pro kterou pomocí protokolu LDAP lze definovat oprávnění jednotlivým uživatelům. Stejně tak každý uživatel může zvolit určitou složku, kterou bude sdílet jinému uživateli, skupině nebo třeba všem uživatelům stejné domény. Variabilita je závislá na konkrétním programu MDA.

V případě, pracuje-li s jedinou schránkou víc než jeden uživatel a počítá se s hojným užíváním schránky, je vhodnější využívat k připojení jednoúčelovou GUI aplikaci, než webové rozhraní. Např. většina MUA (MS Outlook, Mozilla Thunderbird, atd.). Webové rozhraní naopak v případě špatného naprogramování, může nešikovným obnovováním značně vytěžovat aplikační server i síť nebo provedené změny jinými uživateli nemusí být postřehnutelné. Obecně platí, GUI klient je na komunikaci méně náročný.

Příjemnou vlastností přístupu přes IMAP je možnost separování jednotlivých formátů zpráv uložených v MIME. U staršího POP3 máme možnost pouze stahovat nebo nestahovat novou zprávu, ale už nelze zvolit, jestli chceme stáhnout jen text zprávy bez příloh, případně jen zvolený formát příloh (zvuk, video, obrázky…). IMAP tuto funkci svým klientům umožňuje.

Součástí protokolu je mechanismus pro přihlášení, který předává přihlašovací údaje v šifrované podobě. Ačkoliv spuštění tohoto mechanismu musí odsouhlasit předem obě strany (server i klient), jinak přihlášení probíhá otevřeným textem. Pro zabezpečené spojení se využívá SSL vrstva. Spojení následně probíhá standardně na port TCP/993.

1.4 WWW (WORLD WIDE WEB)

WWW značí systém elektronických dokumentů spojený hypertextovými odkazy v síti Internet. Tyto dokumenty byly zprvu tvořeny jako prostý text, ve kterém byly umístěny specifické značky, podle kterých prohlížecí program vygeneroval výslednou podobu. Nyní nejsou tyto dokumenty omezeny pouze textem. Mohou interpretovat obrázky, zvuk atd., jako součást elektronické prezentace.

Jako komunikační prostředek mezi dotazy na hypertextové odkazy a odpověďmi byl vytvořen aplikační protokol HTTP, který může pracovat nad jakýmkoliv spojově orientovaným protokolem nižší vrstvy. Protože nejrozšířenější jsou TCP/IP sítě, je v této síti přenášen v protokolu TCP. Servery nejčastěji naslouchají dotazům na portu č. 80, který je k tomu vyhrazen.

Při vytváření dotazů se využívá koncepce adresového URI (Uniform Resource Identifier) schématu. Definuje celou řadu dotazů pro různé služby. Je to nejvyšší možná adresace, jež obsahem podle schématu definuje použitý protokol, adresu, parametry dotazu pro cílový server. Ve spojení s internetovými stránkami se častěji vyskytuje označení

URL (Uniform Resource Locator), což je v podstatě synonymum k URI.[11] Je to zejména oblíbené veřejné označení.

1.4.1 Protokol HTTP (Hypertext Transfer Protocol)

Jak již bylo řečeno dříve, ke komunikaci mezi klientem a serverem slouží protokol HTTP. Je to bezestavový protokol, pomocí něhož je dáváno serveru najevo, co je od něj požadováno. Server na dotaz reaguje zasláním odpovědi v hlavičce odpovědí a žádaná data. Součástí hlavičky protokolu je URL adresa. K hlavičce mohou být přidány další parametry, které určují formu přenosu informace HTTP. Hlavičku si lze představit obdobně, jako u protokolu SMTP, ale HTTP přenáší v hlavičkách více informací. Proto lze tyto informace rozdělit podle účelu do skupin hlaviček:

1. **Obecné hlavičky** – nesou obecné informace; např.:
2. **Dotazové hlavičky** – určují parametry dotazu:
3. **Hlavičky odpovědí** – reakce serveru:
4. **Hlavičky těla** – nese údaje o těle zprávy:

1.4.2 HTTPS

Je alternativou protokolu HTTP, který zajišťuje bezpečnost přenášených dat. Hlavní rozdíl mezi HTTP a HTTPS je použití zabezpečovací vrstvy SSL/TLS. Ve většině případů servery čekající na spojení naslouchají na portu TCP/443[12]. Pro splnění podmínky takové komunikace musí server vlastnit certifikát, kterým prokazuje svoji důvěryhodnost a na jeho základě jsou generovány šifrovací klíče.

1.4.3 HTTP server

Jestliže je nutné nabízet nějakou službu, je k tomu potřeba uzpůsobený program. Takový program označujeme jako server[13]. Dnes již existuje mnoho programů, kterými lze poskytovat potřebné WWW dokumenty.

V zásadě lze u těchto serverů rozdělit sběr informací pro interpretaci dat dvěma schématy:

- **Statické** – server nemusí vykonávat žádné složité procesy, jen odešle předem připravený dokument uživateli. Jedná se o kód a data dokumentu, která se k uživateli přenáší celá. Nejčastěji se pro formátování dokumentu užívá značkovací jazyk HTML/XHTML, který je doplněn stylizovacím jazykem CSS. Součástí obsahu kódu mohou být i skriptovací jazyky (např. JavaScript). [14]

[11] V textu budou URI a URL vzájemně záměnná.
[12] Doporučené výchozí nastavení z RFC 2018.
[13] „Serverem“ se označuje program hostující službu nebo hardware, který je vyhrazen pro běh těchto aplikací.
[14] Tyto jazyky se provádějí přímo v prohlížeči uživatele, který musí obsahovat nutné knihovny k jejich provádění.

Pomocí podpory MIME může protokol HTTP přenášet jakákoliv data dokumentu k uživateli (obrázky, video,zvukové soubory…).

- **Dynamické** – server poskytuje dynamicky se měnící data na základě požadavků. Data jsou nejprve sestavena na serveru z potřebných zdrojů, které jsou dotazovány. Sestavený dokument je zaslán uživateli v konečné podobě dokumentu. Stejně jako v předchozím se pro reprezentaci užívají značkovací, stylizovací a skriptovací jazyky. Aby HTTP server mohl zpracovávat dynamické dokumenty, musí mít implementovány potřebné knihovny použitého interpretačního jazyka (PHP, ASP.NET, PERL…). Například chceme-li interpretovat dynamické dokumenty napsány v PHP, server musí tomuto kódu rozumět, aby ze zdrojových textů byl schopen vygenerovat HTML dokument. Takové jazyky se spojují s různými relačními databázovými systémy. Jejich obsahem jsou různá data (převážně textového původu).

  Takové spojení systémů přináší řadu výhod, protože lze dekomponovat práci s vlastními daty databáze, logickou a vizuální strukturalizací, která interpretuje zdrojová data dokumentu.

  Výhoda relační databáze je možnost umístění na zcela odlišné místo (např. jiný hardware), než je provozován HTTP server. Nebo lze využít jedinou databázi pro více aplikačních serverů, v našem případě pro několik HTTP serverů.

Velice rozšířené programy HTTP serverů zastupují Apache nyní od Apache Software Foundation a Internet Information Services od Microsoft. Podle průzkumu [2] z března 2008 zastupuje Apache 50 % z celkového množství HTTP serverů. Microsoft zastupuje 35 % a 15 % tvoří servery jiných firem.

HTTP Apache Server

V dnešní době Apache převládá mezi webovými servery na Internetu. Jeho předností je podpora řady operačních systémů (Unix, Novell NetWare, Windows, Mac Os, Solaris, Free BSD a Linux) a bezplatnost produktu. Existuje velký sortiment modulů, které díky jeho architektuře mohou být implementovány. Např. moduly pro Perl, Python, PHP a další. Lze přidávat i autentizační moduly. Apache umožňuje zabezpečenou komunikaci přes SSL. Umí filtrovat přístupy podle zadaných parametrů (doména, IP…).

Díky funkci Virtual host, je možné provozovat jeden server Apache pro několik webových aplikací. Toho zejména ocení poskytovatelé internetového „hostingu”.

Nastavení lze provádět přímo přes konfigurační soubory nebo pomocí volně šiřitelných grafických rozhraní. Další předností Apache je podpora dynamických stránek, které se zpracovávají na straně serveru.[1]

1.4.4 Databázové servery

MySQL

Databázový systém MySQL je distribuován i jako nekomerční produkt. MySQL je kompletně napsaná v jazyce C. Nejčastěji se vyskytuje ve spojeni s webovým serverem Apache. Jako ovládací prvek pro interpretaci nebo ukládání dat do databáze se používají CGI skripty psané v jazyce PERL nebo PHP. Tyto jazyky potřebují pro práci s databázemi mít nainstalované DBI (DataBase Interface), jež obsahuje sadu funkcí pro práci s použitým typem databáze.

Do databázových systémů často ukládáme důležitá data, proto je nutné dělat pravidelné zálohy. Dalším předpokladem pro využití databáze je stabilní platforma např. Linux nebo serverové edice Windows. Běžné je použití diskových polí pro zvýšení přístupové rychlosti a zabezpečení proti ztrátě dat.[1]

Oracle

Oracle je relační databáze pracující na principu PL/SQL dotazů nebo v prostředí .NET. Komerční verze jsou tvořeny pro střední a rozsáhlé sítě s řadou pokročilých funkcí a rozsáhlými administračními nástroji. Podporuje velký sortiment operačních systémů.

Před vydáním omezené verze *Express Edition,* která nabízí obdobné možnosti jako MySQL, tvůrčí společnost neměla žádné zastoupení mezi nekomerčními databázemi. Stejně jako k MySQL lze i k Oracle přistupovat pomocí různých programovacích a interpretačních jazyků. Výhodou Oracle je efektivita transakčních operací s minimem vzájemného blokování, protože blokace probíhá na úrovni řádků.

1.4.5 Interpreti dynamických dokumentů

PHP

PHP je intepretační skriptovací jazyk navržen pro vývoj internetových aplikací. Jeho funkce není závislá pouze na HTTP serverech a prohlížečích. Programy, v něm napsané, lze provozovat jako samostatnou GUI aplikaci nebo spouštět jejich skripty pomocí příkazové řádky.[15] Vlastní kód PHP lze jednoduše vložit mezi značky „<?php“ a „?>“ v HTML jazyce, proto je velmi oblíbený k tvorbě dynamických www dokumentů. Pomocí předem definovaných funkcí lze jednoduše aplikaci připojit k relační databázi MySQL, Oracle nebo jiné. Použití a koncepce je jednodušší než u většiny konkurenčních jazyků. Od verze PHP3 je tento jazyk schopen objektového programování. Soubory potřebné k funkci aplikací v PHP kódu lze volně stáhnout na Internetu. Aktuální řada je PHP 5.

[15] Za předpokladu implementovaného PHP interpretu.

Perl

Perl je interpretační programovací jazyk, který se využívá zejména pro www a v oblasti zpracování souborů. Jeho působnost je ale daleko větší. I přesto, že je relativně jednoduchý na naučení, je možné pomocí něho psát velmi složité a velmi rozsáhlé aplikace, podporující práci s grafickým uživatelským rozhraním, práci s databází, síťovou komunikaci... Název Perl je zkratka z anglického „Practical Extraction and Reporting Language "

Původně byl Perl napsán na Unix platformu, ale dnes již běží i na jiných systémech (Windows, Atari, MS DOS, Novell,...).[5]

ASP.NET

ASP.NET je profesionální technologie pro tvorbu webových aplikací z dílny Microsoft. Je součástí nadstavby operačního systému, kterou je *.NET Framework*, pomocí něhož se aplikace spojují s databázemi, grafikou, práci se soubory a dalšími systémovými objekty.

Výhodou technologie ASP.NET není omezení na jediný programovací jazyk. *.NET Framework* počítá s použitím programovacích jazyků, které byly určeny zejména pro objektové programování „okenních" aplikací. Programátor může pracovat v jazycích jako je Visual Basic.NET, C#.NET, ale v Perl či Pascalu. Multijazyčnost je umožněna pomocí kompilace na řízený kód MSIL. Ten je následně zpracováván prostředím *Common Language Runtime* obsaženého v *.NET Framework.*

Nevýhodou ASP.NET je zatím poměrně malá podpora oproti PHP u hostingových služeb. ASP.NET je odkázaná na IIS serverových platforem Windows.

1.5 Síť Novell

Společnost Novell je od počátku prvních počítačových sítí nedílnou součástí vývoje síťových operačních systémů Novell NetWare a jejich programového vybavení. Zpočátku využíval osobité metody a vlastní řešení protokolů, které vycházely z předešlého vývoje Xeroxu. Konkrétně se jednalo o protokoly IDP a SPP, které vyvinul Xerox. Novell tyto protokoly upravil a označil je jako IPX a SPX. Tyto protokoly byly vyvinuty pro lokální sítě a pro jejich neuniverzálnost byly nahrazeny rodinou protokolů TCP/IP. Ovšem principielně jsou IPX/SPX tvořeny pro LAN a nelze jim upřít v těchto sítích vyšší efektivitu ve srovnání s TCP/IP. Je to dáno tím, že hlavička paketů obsahuje méně režijních dat.

1.5.1 Cíl Novellu

Novell věnoval řadu svých prostředků pro vývoj volně-šířitelných klientských programů, díky nimž je možné připojit do sítě Novell, stanice s většinou OS.

Společnost Novell zajistila pro provoz sítí Novell nasazení vlastních produktů. K většinovému využití služeb je nezbytné provozovat alespoň jeden server Novellu. Služby,

které Novell poskytuje závisí na jejich programovém vybavení a doplňcích. Ačkoliv migruje svoje komponenty na platformu Suse Linux, stávají se tyto prostředky komerční.

Nezbytnou součástí sítě tvoří databáze udržující informace o všech jednotlivých objektech (servery, uživatelé, aplikace atd.). V průběhu vývoje systémů NetWare prošla vývojem i tato databáze. Nejdříve nesla označení „Bindery“. V novějších verzích od NetWare 4.0 byla tato služba inovována a označena jako „eDirectory“. Je dostupná, jako součást Novellovských serverových systémů, i samostatně pro velký sortiment jiných OS. Mezi nabízené OS patří i Windows 2000/2003.

1.5.2 Novell a Windows Server 2003

Běžně jsou provozovány pracovní stanice s OS Windows v síti Novell, která obsahuje server s OS NetWare. Často také doplňují síť Novell servery s jinými OS, opatřující některé služby. Problém nastává, je-li vedle sítě Novell provozována síť Microsoft. Ačkoliv je nelogické, proč by měl být problém s propojením klientských stanic s OS Windows a serverem s OS Windows Server. Vysvětlení je následující – jestliže je provozována síť Novell, klientské stanice mají instalovány příslušný software pro komunikaci se sítí, který omezuje možnosti přihlášení pouze do sítě typu Novell. Dále je u těchto stanic omezené oprávnění konfigurace. Microsoft a Novell řeší dohody o vzájemné spolupráci důležitého programového vybavení mezi jejich platformy. Nicméně neustále není možné poskytovat kompletní služby sítě Novell pouze na platformách Microsoft.

Možné částečné řešení je využití služby eDirectory, kterou zprovozníme na platformě Windows 2003 Server. Pomocí ní zajistíme proceduru přihlášení přizpůsobených pracovních stanic pro síť Novell do námi vytvořené sítě.

Využité jsou užitečné vlastnosti eDirectory, která disponuje správou přihlašovacích skriptu. Ačkoli jazyk pro tyto skripty je uzpůsoben pro nástroje Novellu, které díky absenci novellovkého serveru postrádáme, můžeme jej využít pro spouštění programů a příkazů ve Windows. Tohoto předpokladu využijeme pro mapování síťových disků na pracovní stanice se systémy Windows.

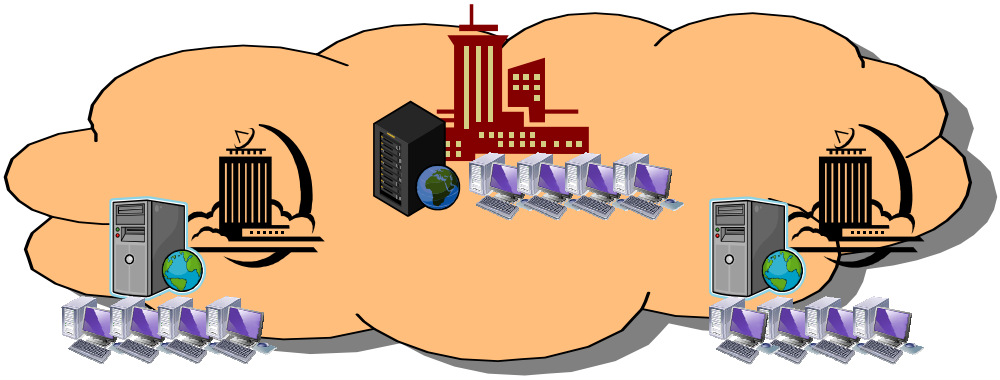
1.5.3 eDirectory

Služba eDirectory je objektově orientovaná databáze, v niž všechny objekty jsou uspořádány do určité hierarchické struktury – stromu. Účelem této databáze je určit vztahy mezi jednotlivými objekty. Tyto objekty představují jednotlivé „komponenty“ sítě Novell, kterými mohou být uživatele, skupiny, služby, datová úložiště, síťové řadiče, logické struktury atp.

eDirectory ke každému takovému objektu obsahuje sadu pravidel (atributů), které popisují chování vzhledem k ostatním objektům. Protože může obsahovat řadu objektů, které by musely být samostatně popsány, je koncipována do hierarchické struktury.

V takové struktuře pak stačí změnit pravidla nadřazeného prvku a změny se projeví i v podřízených objektech. Administrace se rapidně zjednodušuje a centralizuje.

Významnou koncepcí eDirectory je promyšlená možnost replikace. Můžeme tvrdit, že eDirectory není uložena na jediném místě, ale může volně plout na celé síti a zpracování jejich požadavku může vykonávat současně několik serverů. Např. budeme-li mít firmu s hlavním sídlem a 2 pobočkami viz Obr. 8, čítající statisíce objektů.



Obr. 8 *Příklad podnikové sítě s eDirectory.*

Replikace kompletní databáze na všechny řadiče by byla náročná a zbytečná. Proto je možné ji rozdělit na úseky, se kterými pracují jednotlivé servery. Tzn. databáze v hlavní budově bude obsahovat jen nezbytné objekty, které jsou nejčastěji užívány místními objekty. To samé bude i u pobočkových budov. V případě potřeby objektu jedné časti, který vyžaduje informace mezi ním a objektem v jiné části sítě, se řadiče vzájemně dotazují na potřebné informace. Zrovna tak je možné připojení na jakýkoliv řadič samostatně, má-li k tomu cizí objekt oprávnění.

2 PRAKTICKÉ ŘEŠENÍ

2.1 Volba platformy Windows

Vlastnosti a vhodnost použití jednotlivých platforem byly rozebírány v [1], proto je v následujícím textu uvedeno shrnutí zamýšlených platforem Windows.

2.1.1 Shrnutí platforem Windows

Windows NT

Windows NT jsou nyní zastaralým OS. Jejich stabilita nebyla nikdy na konkurenci schopné úrovni tehdejších serverových systémů. Zejména jejich programová výbava byla chudá a bylo nutné platit za její rozšíření. Citlivé místo OS je zranitelnost jeho MBR, jehož poškození způsobí nevratný pád OS. Windows NT neumožňují centralizovanou správu připojených stanic a schází podpora výrobce.

Windows 2000

Poměrně povedený systém oproti jeho předchůdci. Stabilita systému je na dobré úrovni. Byla implementována technologie *Active Directory* pro centralizovanou správu sítě. Existuje mnoho variant tohoto OS:

- Windows 2000 Professional – určená pro osobní počítače;
- Windows 2000 Server – základní serverová edice, která podporuje veškeré potřebné funkce sítí LAN;
- Windows 2000 Advanced Server – vhodný pro nasazení do rozsáhlých sítí, protože umožňuje vyvažování zátěže mezi několika servery a podporuje jejich spojování do clusterů;
- Windows 2000 Datacentr Server – koncipován pro práci s datovými toky na pokročilém hardware.

V současnosti se postupně tento OS opouští, protože ze strany výrobce ustává podpora.

Windows XP

Windows XP jsou orientovány na osobní počítače, notebooky a mediální centra jako multimediální a zábavný OS. V sítích, kde je potřebná hierarchická struktura jsou nasazovány jako klientské stanice se serverovými OS Windows 2000, Windows 2003 nebo po rozšíření o klientský software do sítě Novell.

Windows Server 2003

V dnešní době představují nejrozšířenější serverovou platformu na bázi Windows. Představují mnoho variací zaměřené dle typu poskytovaných služeb:

- Windows 2003 Small Business Server – systém je omezen na použití jediného serveru na doménu. Obsahuje Microsoft Exchange Server;
- Windows Server 2003 Web Edition – je degradovaná verze Windows 2003 určená pro hostování webových aplikací. Při sdílení souborů je omezena na 10 současných spojení. OS nelze použít jako doménový řadič;
- Windows Server 2003 Home Edition – určený ke správě domácí sítě o max. počtu 10 PC;
- Windows Server 2003 Standard Edition – OS je orientován do malých a středně velkých sítí. Zahrnuje celé zázemí služeb pro tyto sítě.
- Windows Server 2003 Enterprise Edition – jsou rozšířením Standard Edition. Orientují se na střední a velké sítě. Podporují pokročilý hardware a umožňují spojování serverů do clusterů;
- Windows Server 2003 Datacenter Edition – nadále rozšiřují Enterprise Edition. Jsou určeny pro nasazení na specificky přísně testovaný hardware. Tento OS je koncipován pro vysokou spolehlivost a bezpečnost.
- Windows Server 2003 Storage Server – jednoúčelový OS pro poskytování souborových služeb. Integruje se do sítí SAN.

Windows Server 2008

Windows 2008 byly na trhu uvedeny 27. 2. 2008 dle [6], proto v této práci jejich nasazení nebylo zvažováno.[16]

2.1.2 Zvolená platforma

Volba platformy *Windows Server 2003 Enterprise Edition R2* probíhala na základě studovaných materiálů ze semestrálního projektu [1] a vlastních zkušeností. Přispěla k tomu možnost využití bezplatné školní licence, kterou nabízí program MSDN Academic Alliance.

2.2 Realizace FTP serveru

V systému Microsoft Windows Enterprise Server 2003 R2 je na výběr využití implicitního FTP serveru, který je součástí služby IIS 6.0 nebo explicitního výběru z řady komerčních i nekomerčních programů.

Z požadavků na tento server (tzn. veřejný) je vhodný a postačující implicitní FTP server. Poskytuje celistvou a nativní správu v rámci OS. Aby nebyla odepřena možnost zabezpečeného přihlášení sdílených souborů pomocí SMB, není vhodné k těmto souborům nebo složkám, kde toto zabezpečení je vyžadováno, připojovat FTP server. Z důvodu přehlednosti bude vhodné poskytovaná veřejná data přesunout do složky, ke

[16] Od 1.5.2008 je k dispozici licence programu MSDN AA.

kterým je nastaveno oprávnění anonymního přístupu pro serverovou aplikaci FTP (v IIS) a nejlépe kterou si IIS automaticky vytvoří.[17]

Integrovaná služba FTP v IIS nepodporuje šifrování SSL/TLS, proto případný privátní přístup bude sloužit pouze jako logické oddělení a zabezpečení proti nechtěnému poškození dat. K bezpečnému přihlášení je vhodnější využít sdílení systému Windows pomocí protokolu SMB, jež využívá zabezpečného autentizačního mechanismu Windows.

2.2.1 Oprávnění

Služba FTP umožňuje provozovat současně více serverů na odlišných portech nebo síťových kartách v PC. Obsahuje i běžnou funkci virtuálních adresářů, do kterých jednoduše mapujeme soubory nebo adresáře. Na tyto adresáře je aplikováno souborové uživatelské oprávnění zapsané v NTFS a přistupovat k nim může pouze :

1) uživatel, který se pomocí svého účtu (login/heslo), založeného na serveru v systému Windows, přihlásí na FTP server a jeho účet je oprávněn přistoupit k dané složce;
2) uživatel přihlášený anonymně („anonymous“). Anonymnímu účtu je standardně přiřazen systémový účet (IUSR_*<název PC>*), na který se vztahují systémová oprávnění v dané složce nebo souboru, ke kterému je přistupováno. Tomuto účtu lze přiřadit jakýkoliv účet nacházející se na serveru, na který se budou aplikovat pravidla přístupu.

První zmíněný případ se nedoporučuje z důvodu otevřeného přenosu hesla uživatelského účtu. Proto se využívá 2. možnost, u které odhalení nevadí

Službou FTP v IIS lze při sdílení stanovit ke konkrétní složce masku oprávnění „read“ a „write“. Tato maska funguje na změny oprávnění k nižší úrovni. Nelze povolit zápis, jestliže použitý účet toto oprávnění nemá.

2.2.2 Instalace

FTP server není dostupný po čerstvé instalaci systému, proto se musí dodatečně instalovat následujícím způsobem :

- ✓ *Start->Control Panel->Add or Remove Programs;*
- ✓ v položce *Add/Remove Windows Components* se pomocí *Details* ve skupině *Application Server->Internet information Services(IIS)* zobrazí několik nabízených komponent systému, mezi nimiž se vyskytuje *File Transfer Protocol (FTP) Service.*[18]

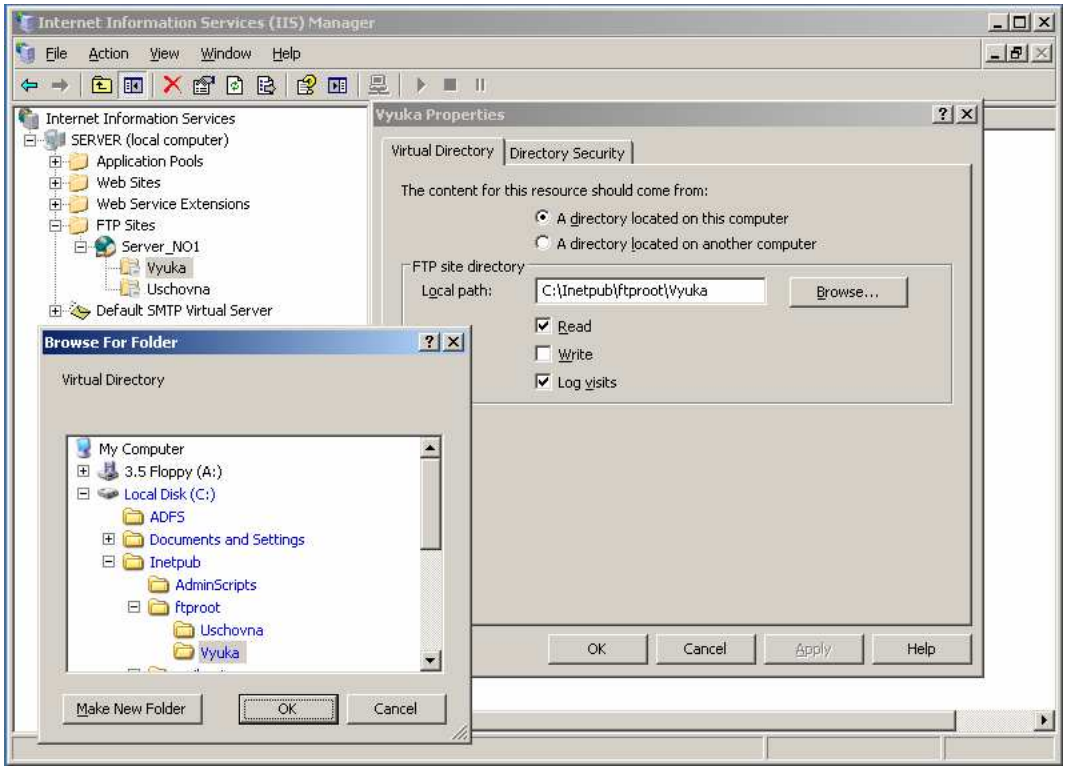
2.2.3 Konfigurace

K možnostem nastavení se lze dostat způsobem:[19]

[17] C:\Inetpub\ftproot\
[18] Instalace vyžaduje instalační CD1.
[19] V praxi existuje několik možnosti, které vedou ke společnému cíly.

✓ *Start->Administrative Tools->Internet Information Service(IIS) Manager.*

Po otevření konzole se nabídne správa instalovaných služeb IIS viz Obr. 9



Obr. 9 *Ukázka definování pravidel virtuálních složek v IIS*

✓ Ve vlastnostech „*Server_NO1*“[20] je nastaven řídící port a síťová karta, na které bude služba naslouchat, způsob přihlášení, upozorňovací zprávy aj.

✓ V konfiguraci je zvoleno nastavení *Allow anonymus connection*, které povoluje použití anonymního účtu a zároveň je nastaveno *Allow only anonymus connection*, které zakazuje použití jiného než anonymního účtu. Použití uživatelských účtů by mohlo způsobit odhalení hesel a způsobit jejich zneužití např. v jiných službách.

U sdílených složek se stálým obsahem je vhodné omezit oprávnění uživatelských účtů, které k nim mohou přistupovat a měnit jejich obsah např. z terminálové služby.

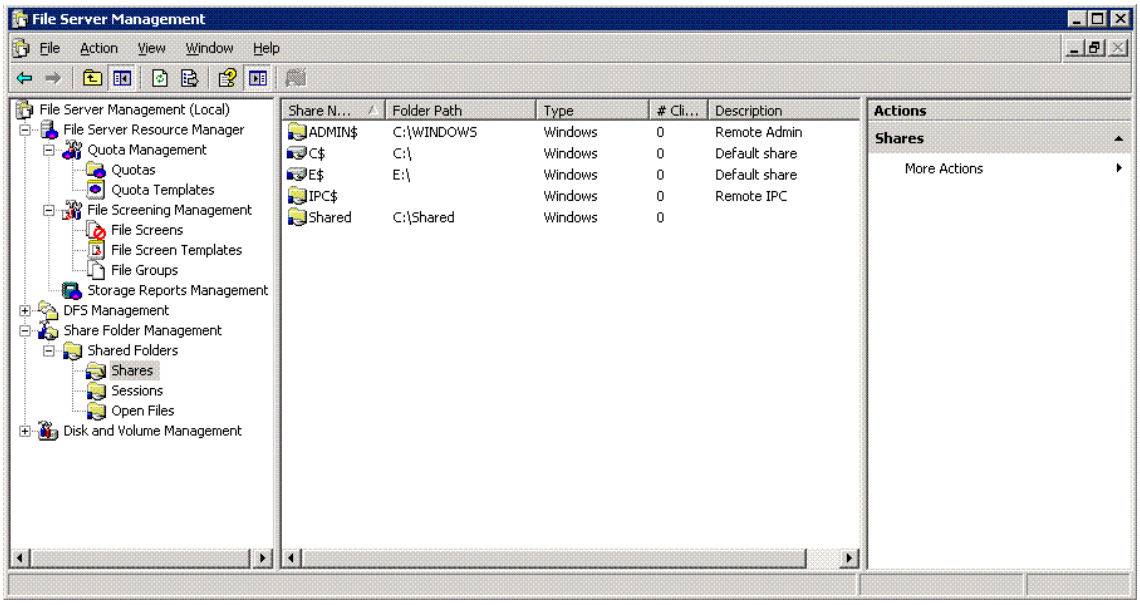
Bohužel implementovaná služba FTP postrádá možnost omezování rychlosti upload/download a systém kreditování. Tento nedostatek se projeví, je-li aktivních mnoho spojení na zahlcení sítě, nechceme-li omezovat počet aktivních spojení. Jestliže bude takový problém nutné vyřešit, aniž provedeme závažný zásah do nastavení FTP, aplikujeme explicitní filtr omezující šířku pásma pro zvolenou komunikaci.

[20] Vyjadřuje jméno serveru, které se na vytvořeném pracovním serveru může lišit.

2.3 Realizace File serveru

Součástí Windows Server 2003 je služba souborového serveru *File Server*, která zajišťuje jednoduché sdílení souborů. V edici Enterprise R2 je nástroj *File Server Ressource Manager*, který umožňuje dohled nad jednotlivými sdílenými soubory. Pomocí něj lze spravovat diskové kvóty a zaznamenávat události o přístupu v podobě záznamů.

Užitečnou funkcí souborového serveru je i *File Screening Management*, kterým lze vytvářet šablony pravidel, podle nichž lze filtrovat přístup vybraných typů souborů do zvolených sdílených složek.



Obr. 10 *Konsole pro správu souborového serveru*

Detailní popis funkcí souborového serveru a nástrojů určených pro jeho správu je nad rámec této bakalářské práce, proto budou obsaženy základní informace o postupu sdílení složky a nastavení jejího omezení v podobě diskové kvóty. Filtrace typů souborů nebude aplikována, protože na pracovní server nejsou v tomto bodě stanovaná žádná specifická kritéria.

2.3.1 Instalace

Role souborového serveru je přidána:

- ✓ *Start->Manager Your Server->Add or remove a role* ;
- ✓ nabídne se výběr několika služeb, mezi nimiž je zvolen *File Server.*[21]

2.3.2 Konfigurace

- ✓ Konsole pro správu souborového serveru je spuštěna: *Start->Administrative Tools->File Server Management ;*
- ✓ v rozbalené skupině *Share Folder Management-> Share Folders->Shares* vytvoříme novou sdílenou složku;

[21] Instalace vyžaduje CD2.

- ✓ ve spuštěném průvodci je do *Folder path* zadána cesta ke sdílené složce *c:\Shared*
- ✓ následující obrazovka určuje název složky v síti a její popis;
- ✓ dále jsou zvoleny oprávnění přístupu ke sdílené složce;
- ✓ pro sdílenou složku je nastavena kvóta ve skupině *File Server Ressource Manager-> Quota Management->Qutota Templates ;*
- ✓ jako šablona je aplikována limitní kvóta 2GB pomocí funkce *Create Quota from Template…*
- ✓ *v Quota path* je požadována cesta sdílené položky, na kterou se bude kvóta vztahovat.

2.4 Realizace poštovního serveru

2.4.1 SMTP server

Windows Server 2003 obsahují službu serveru odchozí pošty MTA jako součást IIS. Zvládá nejnutnější potřeby, dokonce lze provozovat zabezpečené spojení[22], nastavení filtrů velikosti zpráv a nastavení odchozích pravidel. Ovšem implementace IMAP není součástí služeb systému. Existují volně šířitelné komplexně řešené programy, které dokáží zastoupit celý poštovní systém. Bohužel to vše bez jakéhokoliv zabezpečení přihlašovacích údajů nebo podpory SSL/TLS. Stejně tak implicitní podpora POP3 schránek nenabízí zabezpečení spojení.

Instalace

Server pro odchozí poštu SMTP je stejně jako server FTP dodatečně instalován:

- ✓ *Start->Control Panel->Add or Remove Programs;*
- ✓ v položce *Add/Remove Windows Components* se pomocí *Details* ve skupině *Application Server->Internet information Services(IIS)* zobrazí několik nabízených komponent systému, mezi nimiž se vyskytuje *SMTP Service*.[23]

Konfigurace

Nastavení probíhá v konsole IIS, jejíž spuštění je popsáno na str. 34. Možnosti konfigurace jsou bohatší, než tomu bylo u služby FTP.

- ✓ V IIS se v postranním stromu nachází položka *Default SMTP Virtual Service-> ->Properties*;
- ✓ v objeveném okně lze zvolit IP adresu rozhraní na kterém bude služba pracovat;
- ✓ dále je zaškrtnuta kolonka *Limit numer of connection*s to – počet současných spojení.[24]

Důležitou roli hraje záložka *Access*, protože určuje veškerá pravidla pro příchozí spojení. Bohužel školní síť VUT doručuje zprávy na pracovní server pouze, je-li

[22] Pro zabezpečené spojení musí být správně nakonfigurovány všechny zúčastněné strany.
[23] Instalace vyžaduje CD1.
[24] V řešené práci je omezeno počet na 20 spojení.

povolen anonymní přístup bez další metody zabezpečení. Je-li na SMTP serveru aplikován certifikát, spojení ze strany školního serveru není akceptováno, protože certifikát je na poštovním serveru VUT odmítán.

Pro odesílání pošty mimo síť VUT musí pracovní server odesílat zprávy na nadřazený poštovní server VUT. Nastavení je provedeno:

- ✓ v záložce *Delivery* pod tlačítkem *Advanced…*
- ✓ do položky *Smart host* je nutné zapsat adresu nadřazeného serveru `fest.stud.feec.vutbr.cz` , na který jsou zprávy přeposílány;
- ✓ v záložce *Delivery* pod tlačítkem *Outbound Security…*lze vybrat způsob autentizace při odesílání zpráv na VUT server. Protože server leží uvnitř sítě, lze přistupovat pomocí anonymního přístupu a nastavit TLS šifrování pro odesílané zprávy.

Zprávy jsou směrovány na server VUT z důvodu výjimky blokace potřebné poštovní komunikace na hraničních firewallech VUT. Blokovaná je i komunikace ze vnějšku sítě na port TCP/25 pracovního serveru.

Pokud by se v jiných podmínkách zvažoval zabezpečený přístup k pracovnímu SMTP serveru, možné nastavení by mohlo vypadat takto: v *Authentication* nastaveno *Basic authentication*, které vyžaduje autentizaci některým lokálním účtem např. umístěným ke schránkám POP3 na tomto serveru. Samotná *Basic authentication*, jak název napovídá přenáší informace pouze jako otevřený text, proto by komunikace byla doplněna zabezpečovací vrstvou TLS/SSL, která vyžaduje službu certifikační autority.

Po implementaci certifikátu je možné využít šifrovaný přenos zpráv mezi pracovním serverem a zdrojovým MUA nebo MTA. Nepříjemné je, že MTA a MUA musí obsahovat kompatibilní zabezpečovací parametry pro navázání spojení.

2.4.2 POP3 server

Mimo SMTP služby obsahují Windows Server 2003 i službu POP3 schránek. MDA program je ochuzen o prvky, které ho omezují o detailní konfiguraci, SPAM filtry a možnosti zabezpečeného přenosu zpráv. Na druhou stranu je služba vhodná jako přechodné řešení.

Instalace

- ✓ *Start->Control Panel->Add or Remove Programs;*
- ✓ v položce *Add/Remove Windows Components* zaškrtněme *E-mail Services.*

Současně se instaluje i služba *SMTP Service*, pokud již není instalována.[25]

[25] SMTP je instalována z důvodu určení a předání zprávy do cílového MDA programu.

Konfigurace

- ✓ Konfigurační konsole je otevřena: *Start->Administrative Tools->POP3 Service;*
- ✓ v *Properties* jména serveru je vybrán port[26], na kterém server naslouchá příchozím spojení. V nastavení je určena cesta pro úschovu zpráv. Důležitá vlastnost je *Require Secure Password Authentification…*[27], která zajišťuje přenos hesla v šifrované podobě;
- ✓ založením domény *New Domain*, se určí doména, kterou bude tato služba obhospodařovat. Dojde i k zavedení stejné domény ve službě SMTP;[28]
- ✓ pro každou doménu se nyní pomocí *Add Mailbox* mohou vytvářet jednotlivé schránky. Na účty schránek se vztahují pravidla účtů systému Windows. V případě změny hesla učtu se změna vztahuje na veškeré služby s tímto účtem spojené.

2.4.3 Alternativní poštovní systém

Jako alternativní poštovní server lze využít např. volně-šířitelný program *hMail*. Jeho součástí je SMTP i POP3 server. Nicméně neposkytuje šifrovaný přenos dat.

Instalace

Potřebný instalační balík lze získat na WWW [19].

- ✓ Zvolena je cílová složka a rozsah plné instalace;
- ✓ v obrazovce *Select databáze server type* je vhodné využít později instalované databáze MySQL zvolením *Use external databáze server*;
- ✓ průvodce nabídne možnosti databáze ve kterých je vybráno *Vytvořit novou databázi serveru hMailServer* a následná volba *MySQL Server*;
- ✓ Adresa databázového serveru: `uc-126-2.utko.feec.vutbr.cz`
  Název databáze: `hmail` a Autentizace je zvolena na základě vytvořeného účtu v MySQL databázi;
- ✓ před dokončením je vyžadováno heslo, pomocí kterého bude povolen přístup administračnímu rozhraní.

Konfigurace

Server je konfigurován nástrojem *hMailServer Administrator* v instalované programové skupině, kterým lze konfigurovat více instancí hMail serveru.

- ✓ V průvodci je vytvořena doména *uc-127-2.utko.feec.vutbr.cz,* které lze přidat libovolné účty;
- ✓ nastavení přeposílání je přístupné v *Nastavení->Protokoly->SMTP*;

[26] Výchozí port POP3 je TCP/110
[27] *Vyžadovat zabezpečení hesla při autentizaci…*
[28] Při vlastním řešení byl použit A záznam vyhrazené stanice : uc-126-2.utko.feec.vutbr.cz

- ✓ v rozšířeném nastavení lze volit pravidla pro nevyžádanou poštu a rozsahy IP adres, na která budou aplikována pravidla.

Rozhraní je uživatelsky přívětivé a jednoduché. Konfigurace bude pro funkci v síti VUT obdobná jako konfigurace předchozích serverů, proto tato práce neobsahuje detailní postup.

2.5 Realizace HTTP serveru

Instalace potřebných nástrojů je kolikrát veliký oříšek. Cílem práce je najít nejvhodnější řešení pro zprovoznění všech nutných částí pro poskytování dynamických dokumentů. Použitá je nejaktuálnější verze Apache 2.2.8 s podporou SSL spojení. Do HTTP serveru jsou vloženy moduly PHP interpreta verze 5.2.5 a databázový server je tvořen MySQL 5[29], případně Oracle XE[30].

2.5.1 Instalace

K získání potřebných souborů je možné použít tyto WWW stránky :

- ✓ Apache 2.2.8 – [12]
- ✓ MySQL5 – [21][31]
- ✓ PHP 5.2.6 – [13]
- ✓ Oracle – [20][29]

Instalace Apache:

- ✓ Po přijetí licenční smlouvy je do kolonky *Network domain* vepsána doména `utko.feec.vutbr.cz`, jež zastřešuje pracovní server. Do názvu serveru *Server Name* je zadáno přidělené doménové jméno pracovního serveru `uc-126-2.utko.feec.vutbr.cz` a do adresy administrátora *Administrator's Email Address* je vložena adresa, která se případně zobrazí při poruše nebo při špatné konfiguraci serveru;
- ✓ způsob instalace je zvolen *Typical install* ;
- ✓ instalace je provedena do adresáře *c:\Program Files\Apache Group\Apache2.2* .

Instalace PHP:

- ✓ Zdrojový archiv je rozbalen do složky *c:\dev\php*

Instalace MySQL:

- ✓ Typ instalace je zvolen *Typical;*
- ✓ po nahrání souborů je pokračováno v konfiguraci *Configure the MySQL Server now;*

[29] MySQL Community Server; Windows Essentials (x86);
[30] Oracle Databáze 10g Express Edition;
[31] Stránka požaduje před stáhnutím vyplnění registračních údajů.

- ✓ vybrána je *Standard Configuration*, ve které je zaškrtnuto *Install As Windows Service, Lunch the MySQL Server automatically* a *Include Bin Directory in Windows PATH;*
- ✓ v následující obrazovce je vytvořen hlavní účet databáze s možností *Enable root access from remote machines;*
- ✓ v poslední obrazovce je zahájena instalace tlačítkem *Execute.*

Instalace Oracle:

Oracle Database 10g Express Edition je limitována použitím 1 CPU, 1GB RAM a maximální velikostí databáze 4GB.

- ✓ Při instalaci je určenena složka instalace a požaduje se zadaní administrátorského hesla pro správu databáze;
- ✓ Konfigurace je prováděna uživatelsky přívětivým webovým prostředím, které se spustí *Go To Database Home Page* z programové skupiny nabídky *Start ;*

Popis konfigurace je nad rámec této bakalářské práce. Podrobný přehled ovládaní a nastavení včetně tutoriálu lze naleznout v dokumentaci [9].

2.5.2 Konfigurace

Konfigurace je provedena, aby byla zajištěna funkce zpracování PHP skriptů a server podporoval i zabezpečené spojení.

Konfigurace Apache 2.2:

Nejprve je vhodné nastavit základní vlastnosti v souboru *Apache2.2\conf\httpd.conf*

- ✓ Parametr `DocumentRoot "C:/Inetpub/wwwroot"` určuje výchozí složku pro hledání dokumentů, do které jsou určena oprávnění mezi příkazy `<Directory />` a `</Directory>;`
- ✓ Apache 2.2 vyžaduje kromě předchozího nastavení zvlášť nastavení pro jednotlivé složky se kterými pracuje. Proto za předchozí `<Directory />` a `</Directory>` následují parametry, kterými si zajistíme přístup do dvou složek:

```
<Directory "C:/Inetpub/wwwroot">
Options Indexes FollowSymLinks
AllowOverride None
Order allow,deny
Allow from all
</Directory>
<Directory "C:/Inetpub/wwwsecureroot">
Options Indexes FollowSymLinks
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

Složka *wwwsecureroot* bude sloužit pro dokumenty, ke kterým bude nastavena později zabezpečená komunikace.

- ✓ Nalezneme řádek `DirectoryIndex` a doplníme referenční dokumenty `index.html index.htm index.php` ;
- ✓ pro aktivaci SSL je nutné uvolnit řádky `LoadModule ssl_module modules/mod_ssl.so` a `Include conf/extra/httpd-ssl.conf`
- ✓ pro zavedení modulů PHP jsou vloženy do souboru řádky:

```
php5_module "c:/dev/php/php5apache2_2.dll"

AddType application/x-httpd-php.php .
```

Nyní je konfigurováno vlastní SSL v souboru *Apache2.2\conf\extra\httpd-ssl.conf*

- ✓ Je nutné přepsat řádky:

```
DocumentRoot "C:/Inetpub/wwwsecureroot"
ServerName uc-126-2.utko.feec.vutbr.cz:443
```

- ✓ provedení nastavení pro zavedení certifikátu, který bude umístěn do složky *Apache2.2\conf\ssl* s názvy vlastního certifikátu *monster.cert* a jeho klíče *monster.key* je v následujících řádcích:

```
SSLCertificateFile "C:/Program Files/Apache Group/
/Apache2.2/conf/ssl/monster.cert"

SSLCertificateKeyFile "C:/Program Files/Apache Group/
/Apache2.2/conf/ssl/monster.key"
```

Vytvoření certifikátu

Certifikát je vytvořen pomocí OpenSSL, který lze získat na WWW [14]. instalován je běžným způsobem. Pro správnou funkci klíče je nutné přepsat soubor *OpenSSL\bin\openssl.cnf* souborem z následující WWW adresy [15].

- ✓ Po spuštění openssl.exe jsou zadávány tyto příkazy:

```
req -config openssl.cnf -new -out monster.csr -keyout
monster.pem ,
```

kde je zadáno heslo a jméno adresy, pro kterou bude certifikát určen;

```
rsa -in monster.pem -out monster.key

x509 -in monster.csr -out monster.cert -req -signkey
monster.key -days 365
```

- ✓ vytvořené soubory *monster.cert* a *monster.key* jsou překopírovány do složky *Apache2.2\conf\ssl* .

Konfigurace PHP

- ✓ Nejprve je nutné přidat do systémové proměnné Windows cestu k PHP: *Start->Control Panel->System->Advanced->Environment Variables;*
- ✓ do proměnné Path je pomocí *Edit* vložena cesta *C:/dev/php*

- ✓ překopírován je soubor *c:\dev\php\libmysql.dll* do *c:\Windows\System32* a soubor *c:\dev\php\php.ini-recommended* do *c:\Windows\php.ini*
- ✓ v nově vytvořeném souboru jsou uvolněny řádky :

```
extension=php_gd2.dll
extension=php_gettext.dll
extension=php_mysql.dll
extension=php_tidy.dll
extension=php_xmlrpc.dll
extension=php_xsl.dll
```

- ✓ následně je změněn řádek :

```
extension_dir = "c:/dev/php/ext"
```

Po předchozí konfiguraci je k dispozici HTTP server se zavedenými moduly PHP. Připravená je i databáze MySQL a Oracle, ke kterým mohou aplikace PHP přistupovat.

2.6 Realizace eDirectory

V této práci je služba eDirectory implementována pro zajištění přihlášení uživatelských PC VUT mimo síť VUT. Bohužel nelze implementovat technologii Active Directory, která zajišťuje obdobnou funkci jako eDirectory, ale je určena přímo pro stanice podřízené serverům Windows.
Nasazení Active Directory je znemožněno instalovanými klientskými programy sítě Novell na těchto stanicích. Realizovaná eDirectory bude poskytovat pouze velice omezené možnosti.

2.6.1 Instalace

Pro realizaci služby jsou využity tyto programy dostupné z WWW:

- ✓ eDirectory 8.8 SP2 v podobě iso souboru – [16];
- ✓ iManager 2.7 v podobě zip souboru – [17];
- ✓ Novell Klient 4.91 SP4 En – [18].

eDirectory

- ✓ Obraz CD je vložen do libovolného programu emulující CD mechaniku, který pracuje s *.iso* soubory;
- ✓ po volbě *Install…* jsou instalovány kryptografické nástroje NICI, po jejichž instalaci je nutné restartovat systém;
- ✓ následuje výběr umístění instalovaných komponent které jsou instalovány do *c:\Novell\NDS* ;
- ✓ typ instalace je zvolen pro vytvoření nového stromu *Create a new eDirectory tree* ;
- ✓ Po souhlasu s licenčními podmínky a zvolení jazyka je zadáno do *Tree Name:* `VUT-TESTING` a do *Server object kontext:* `VUT-MONSTER-NDS.BP` ;

- ✓ pro administraci je vytvořen účet včetně kontextu kam bude zahrnut: *Admin Name:*`Admin a` *Admin Kontext:*`O=BP` ;
- ✓ následující nastavení zůstane zachováno a začne vlastní instalace eDirectory;

iManager

Vytváří webové administrativní rozhraní pro eDirectory. Pomocí něj jsou na pracovní server vytvářeny uživatelské účty s možností psaní přihlašovacích skriptů.

- ✓ Instalace je spuštěna souborem *iManagerInstall.exe* v rozbaleném archivu;
- ✓ po výběru požadovaného jazyka a odsouhlasení licenční smlouvy se nabízí možnost volby potřebných komponentů. Pro instalaci potřebných nástrojů je ponechána výchozí volba;
- ✓ instalace je provedena do adresáře *c:\Novell* ;
- ✓ z internetové nabídky modulů je k instalaci vybrán *eDirectory88 Plugins* ;
- ✓ lokální výběr modulů je přeskočen;
- ✓ pro získání přístupu k eDirectory je nezbytné zadat do *Username:* `Admin.BP` a do *Treename:*`VUT-TESTING` ;

2.6.2 Konfigurace

Konfigurace eDirectory je provedena pomocí iManageru z webového rozhraní.

- ✓ Přihlašovací obrazovka je dostupná na adrese z: https://147.229.149.102:8443/nps/servlet/webacc?taskId=fw.Startup
- ✓ po přihlášení s administrátorským oprávněním[32] se vybídne obrazovka s rozsáhlými možnosti konfigurace;
- ✓ v položce *Users* lze vytvářet uživatelské účty, pod kterými je možné přihlášení ke službě eDirectory;
- ✓ pomocí *Modify User* je vybrán uživatel;
- ✓ po zobrazení nabídky modifikace lze v záložce *Generar->Login Script* zadávat parametry skriptu a pomocí nich spouštět i programy Windows, které budou využity při mapování jednotek sdílených složek pracovního serveru.

Připojení síťových jednotek pomocí skriptu

Pro automatické připojení sdílených složek jako síťové disky přihlášených stanic lze využit program *Net use*, který je součástí Windows. Bohužel omezení tohoto programu se mohou vyskytnout při použití účtu s oprávněním *Guest.*

Připojení sdílené složky *moje* na stanici *pocitac*, do které má uživatelské oprávnění účet *Pokus* s heslem *123*, jako síťový disk *x* by vypadalo následovně:

```
#net use x: \\pocitac\moje 123 /user:Pokus
```

Bližší dokumentaci k příkazu *net use* lze naleznout ve [10].

[32] účtem *admin.BP*.

2.7 Návrh HW konfigurace serveru

Návrh správné hardwarové konfigurace je důležitý předpoklad pro realizaci serverové stanice. Na výslednou konfiguraci mají hlavní vliv tyto faktory:

- velikost sítě – počet obsluhovaných stanic;
- technické vybavení sítě – architektura, šířka pásma apod.;
- typ a počet poskytovaných služeb, např.:
  - Souborový server;
  - HTTP server;
  - DNS;
  - DHCP, WINS;
  - Active Directory;
  - a jiné.
- předpokládaný způsob příchozích požadavků na serveru :
  - rovnoměrné;
  - skokové[33];
- druh provozu:
  - nepřetržitý;
  - částečný;

Návrhy konfigurací vycházejí ze současné nabídky trhu a v ceně jsou zvažovány komponenty typu: procesor, paměť, základní deska, grafická karta, skříň, zdroj, disk a mechaniky.

2.7.1 Malé sítě

V této práci jsou zvažovány malé sítě řadově spojení několika PC s využitím služeb, které jsou aplikovány na pracovním serveru. Přibližně se jedná o počet do 20 PC.
Pro takovou konfiguraci splňují podmínky:

- procesor – postačuje druhořadé kvality (Intel Celeron, AMD Sempron) od 1,6 GHz[34];
- paměť – low-end 1024 DDRII 800;
- základní deska – low-end s požadovanou paticí obsahující síťovou a grafickou kartu;
- pevný disk – zde je nutné zvažovat druh provozu a důležitost uschovávaných dat. Doporučeno je využití zrcadlení dat mezi více disků;
- napájecí zdroj – postačující je zdroj běžné kvality;
- přibližná cena 4 000,-.

[33] Např. registrace předmětů na VUT.
[34] Při současných cenách a nabídky trhu nemá smysl se zabývat horším hardwarem.

2.7.2 Střední sítě

Zvažován je rozsah přibližně 50 PC s častým přístupem k poskytovaným službám.

- Procesor – kvalitní procesor pro běžné PC s velkou vyrovnávací pamětí. Zejména modelové řady Intel Core 2 Duo, Core 2 Quad nebo AMD Athlon 64 X2 Dual-Core.
- paměť – alespoň 2GB kvalitní DDRII;
- základní deska – dle procesoru s kvalitním síťovým a diskovým řadičem;
- pevný disk – v provedení pro nepřetržitý provoz o velikosti podle požadavků. Data by měla být zajištěna minimálně jednou replikací;
- zdroj – kvalitní zdroj hlídaný záložní UPS;
- přibližná cena 15 000,-.

2.7.3 Vélké sítě

V této konfiguraci jsou zvažována kvalita služeb na profesionální úrovni :

- procesor – spolupráce několika specializovaných procesorů procesorů Intel Xeon;
- paměť – plně buffrované jakostní paměti s kapacitou od 16GB;
- základní deska – specializovaná základní deska pro více CPU;
- pevný disk – několik disků pro neustálí provoz v konfiguraci několika diskových skupin s rozprostřenými daty a násobně replikovány mezi těmito skupinami;
- přibližná cena začíná na hranici od 40 000,-.

3 ZÁVĚR

Na základě teoretického obsahu práce byl vytvořen pracovní server ze stolního PC, jehož hardwarová konfigurace obsahuje tyto základní prvky:

- Procesor: Intel Pentium 4 @ 2400 MHz s 512kB L2 Cache;
- Paměť : 2 x modul 256 MB DDR-SDRAM PC-2300;
- Základní deska: Asus P4B533-E ;
- Pevný disk: Seagate ST340016A (40GB).

Na této konfiguraci je instalován síťový operační systém MS Windows 2003 Server Enterprise Edition R2.

Tento OS tvoří základ pro poskytování souborových služeb využívající protokol FTP, který je nastaven pro anonymní přístup. Anonymní je z důvodu ochrany uživatelských účtů, jejiž hesla při pokusu o přístup na FTP server by mohla být odhalena. Součástí poskytování souborových služeb je souborový server, který poskytuje sdílená data pomocí protokolu SMB. Server poskytuje přístup ke sdíleným složkám na základě přiřazených oprávnění a hlídá pravidla překročení kapacity pomocí diskových kvót.

Na pracovním serveru je implementována služba poštovního serveru využívající prostředků Windows 2003 Server. Umožňuje přes něj odesílat poštu z nastaveného rozsahu adres sítě VUT. Služba aplikuje na příchozí spojení pravidla, které omezují velikost předávané zprávy a počet příjemců při hromadném odesílání. Zprávy odcházející mimo síť VUT jsou směrovány na poštovní server VUT. Na pracovním serveru mohou být vytvořeny schránky, do kterých lze doručovat zprávy z poštovního serveru VUT. Jako alternativní řešení programového vybavení pro poštovní služby je přiblížena instalace a konfigurace volně-šířitelného programu hMail.

Pro poskytování služeb WWW jsou implementovány programové prostředky umožňující prezentaci dynamických dokumentů. Zahrnují HTTP server Apache včetně modulů interpreta skriptovacího jazyka PHP. Server je doplněn o relační databázi MySQL5 a je poskytnuta i alternativa pro instalaci Oracle Express Edition. Do HTTP serveru je implementován certifikát, na základě něhož a několika SSL modulů poskytuje i zabezpečené spojení. HTTP server je nastaven pomocí virtuálního serveru Apache tak, aby přistupoval do jiné složky se zdrojovými soubory při zabezpečeném spojení.

Pracovní server poskytuje službu přihlášení stanic s klientskými programy sítě Novell pomocí lokálních účtů eDirectory na pracovním serveru. Na základě přiřazených přihlašovacích skriptu umožňuje stanicím s OS Windows připojovat síťové disky, které poskytuje služba souborového serveru.

V neposlední řadě je zmínka o tvorbě návrhu HW konfigurace serveru. Zahrnuje tři doporučené konfigurace podle velikosti obsluhované sítě.

LITERATURA

[1] DEPIAK, P. *Realizace víceúčelového serveru na bázi WINDOWS.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008. XY s. Vedoucí semestrální práce Ing. Václav Pfeifer.

[2] NETCRAFT :*Apríl 2008 Web Server Survey* [online].2008,14 .4 2008 [cit. 2008-5-29]. Dostupné z: <http://news.netcraft.com/archives/web_server_survey.html

[3] OBREMSKI, Neil C.. *Apache2 SSL on Windows* [online]. 2006 [cit. 2006-08-30]. Dostupný z WWW: <http://www.neilstuff.com/apache/apache2-ssl-windows.htm>.

[4] MALLAT. *Co je co v IT : NetBIOS* [online]. 2004 , 04.08.2004 [cit. 2008-05- 23]. Dostupný z WWW: <http://hps.mallat.cz/view.php?cisloclanku=2004080202>. ISSN 1214-4436.

[5] ADAMEC, L., et al. *Perl referenční příručka ke skriptovacímu jazyku : Charakteristika Perlu* [online]. 2007 [cit. 2008-05-26]. Dostupný z WWW: <http://perl.lukada.cz/charakteristika.html>.

[6] STRÁNSKÝ, V. *Deník redakce : Na trh byl uveden nový operační systém Windows Server 2008* [online]. 2008 [cit. 2008-05-26]. Dostupný z WWW: http://technet.idnes.cz/na-trh-byl-uveden-novy-operacni-system-windows-server-2008-pen-/tec_denik.asp?c=A080227_154702_tec_denik_kuz

[7] MALINA, P.: *Microsoft Windows Server 2003 : Hotová řešení* ,Computer Press, Brno 2006, ISBN 80-251-1096-6.

[8] *Http://interval.cz* [online]. 2003 , 7.4.2003 [cit. 2007-12-13]. Microsoft Windows Server 2003 ve výrobě. V češtině. Dostupný z WWW: <http://interval.cz/tiskove-zpravy/microsoft-windows-server-2003-ve-vyrobe/>. ISSN 1212-865.

[9] *Oracle Database 10g Express Edition Tutorial* [online]. 2006 , 1.3.2006 [cit. 2008-05-29]. Dostupný z WWW: <http://st-curriculum.oracle.com/tutorial/DBXETutorial/index.htm>.

[10] *Příkaz Net use* [online]. Microsoft, 2005 , 21.1.2005 [cit. 2008-05-29]. Dostupný z WWW: <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/cs/library/ServerHelp/dd619380-bb33-4d3a-b0b5-29c620600035.mspx?mfr=true>.

[11] VANĚK, J. *Síť a síťové prvky : Protokoly - IMAP protokol* [online]. 2007-2008 [cit. 2008-05-29]. Dostupný z WWW: <http://jirivanek.eu/protokoly-imap-protokol>.

Odkazy k souborům

[12] http://apache.mirror.superhosting.cz/httpd/binaries/win32/apache_2.2.8-win32- x86-openssl-0.9.8g.msi
[13] http://cz.php.net/distributions/php-5.2.6-Win32.zip
[14] http://www.slproweb.com/products/Win32OpenSSL.html
[15] http://www.neilstuff.com/apache/openssl.cnf
[16] http://download.novell.com/Download?buildid=7hvDT3VNzNw~
[17] http://download.novell.com/Download?buildid=7aBB5fT0yiw~
[18] http://download.novell.com/Download?buildid=SyZ1G2ti7wU~
[19] http://download.hmailserver.com/hMailServer-4.4.1-B273.exe
[20] http://www.oracle.com/technology/products/database/xe/index.html
[21] http://dev.mysql.com/get/Downloads/MySQL-5.0/mysql-essential-5.0.51b-win32.msi/from/pick>

SEZNAM ZKRATEK

CGI	Common Gateway Interface
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DN	Domain Name
DNS	Domain Name Server
FTP	File Transfer Protocol
GPL	General Public Licence
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HW	Hardware
IIS	Internet Information Service
IMAP	Internet Message Acess Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MBR	Master Boot Record
MDA	Mail Delivery Agent
MIME	Multipurpose Internet Mail Extensions
MS	Microsoft
MSIL	Microsoft Intermediate Language
MTA	Mail Transport Agent
MUA	Mail User Agent
NAT	Network Address Translation
NT	New Tchnology
OS	Operační Systém
PC	Personal Computer
PHP	Hypertext Preprocessor
PKI	Public Key Infrasctrucure
POP3	Post Office Protocol
R2	Release 2
RAM	Random Access Memory
RCF	Request For Comments
SAN	Storage Area Network
SMB	Server Message Block
SMTP	Simple Mail Transport Protocol
SP	Service Pack
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VUT	Vysoké učení technické
W2K	Windows 2000
WWW	World Wide Web
XHTML	Extensible HyperText Markup Language