Technická univerzita v Liberci

Hospodářská fakulta

Studijní program: 6209 Systémové inženýrství a informatika
Studijní obor: Manažerská informatika

Sdílení dat v heterogenních sítích

Sharing of data in heterogeneous networks

DP – MI – KIN – 2004 03

Bc. Pavel Hroza

Vedoucí práce: Ing. Petr Kretschmer, Katedra inženýrské informatiky

Odborný konzultant: Mgr. Jan Škoda, SPŠES a SOU ve Varnsdorfu

Počet stran 60, počet příloh 1

5. 1. 2004

Katedra informatiky **Školní rok 2003/2004**

ZADÁNÍ DIPLOMOVÉ PRÁCE

pro : Pavel Hroza

Studijní program :
Systémové inženýrství a informatika (6209T)

Studijní obor č. M 6209
Manažerská informatika

Vedoucí katedry Vám ve smyslu zákona č. 1111/1998 Sb. o vysokých školách a navazujících předpisů určuje tuto diplomovou práci :

Název tématu:

Sdílení dat v heterogenních sítích

Zásady pro vypracování :

1. Autentizace, autorizace, sdílení dat a služeb v sítích OS Windows.
2. Sdílení dat v heterogenních sítích.
3. Ekonomický přínos heterogenních sítí pro firmu.

Rozsah diplomové práce: 50-60
(do rozsahu nejsou započítány úvodní listy, přehled literatury a přílohy)

Doporučená literatura :
Eckstein, Collier-Brown, Kelly,: Using Samba, O'Reilly & Associates, 1999
Garfinkel, Spafford: Practical UNIX & Internet Security, O'Reilly & Associates, 1996
Satrapa, P., Randus, J.: Linux – Internet server, Neokortex, 1996
Linux – dokumentaèní projekt, Computer Press, 1998

Vedoucí diplomové práce: Ing. Petr Kretschmer

Odborný konzultant: Mgr. Jan Škoda

Termín odevzdání diplomové práce: 5.1.2004

Prof. Ing. Jan Ehleman, CSc.
vedoucí katedry

Prof. Ing. Jiří Kraft, CSc.
děkan Hospodářské fakulty

V Liberci dne 31.3.2003

Prohlášení

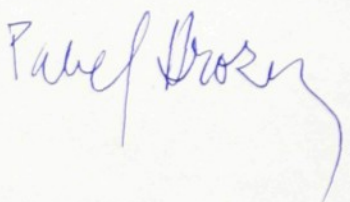
Prohlašuji, že jsem diplomovou práci vypracoval samostatně s použitím uvedené literatury pod vedením vedoucího a konzultanta. Byl jsem seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 o právu autorském, zejména § 60 (školní dílo) a § 35 (o nevýdělečném použití díla k vnitřní potřebě školy).

Beru na vědomí, že TUL má právo na uzavření licenční smlouvy o užití mé práce a prohlašuji, že souhlasím s případným užitím mé práce (prodej, zapůjčení apod.).

Jsem si vědom toho, že užít své diplomové práce či poskytnout licenci k jejímu užití mohu jen se souhlasem TUL, která má právo ode mne požadovat přiměřený příspěvek na úhradu nákladů, vynaložených univerzitou na vytvoření díla (až do jejich skutečné výše).

Po pěti letech si mohu tuto práci vyžádat v Univerzitní knihovně TU v Liberci, kde je uložena, a tím výše uvedená omezení vůči mé osobě končí.

V Liberci dne 5. 1. 2004



Poděkování

Rád bych touto cestou poděkoval vedoucímu své diplomové práce Ing. Petru Kretschmerovi za jeho ochotu a rady při konzultacích a kolegům Mgr. Janu Škodovi a Petru Rybníčkovi za jejich vstřícný přístup a pomoc při vypracování této práce. Také děkuji svým rodičům a Bc. Ivaně Škodové za jejich podněty při zpracování diplomové práce.

Resumé

Diplomová práce se zabývá implementací serverového operačního systému pro počítačovou síť malé organizace. Těžištěm práce je nalezení vhodných alternativ volně šiřitelného programového vybavení k programovému vybavení od firmy Microsoft a nahrazení homogenní sítě, ve které je dodavatelem serverových i klientských operačních systémů jeden výrobce, a velké množství používaných komunikačních protokolů je proprietárních nebo nekompatibilních se standardem, sítí heterogenní, ve které jsou využívány pouze otevřené protokoly a volně šiřitelné programové vybavení na straně serveru. V heterogenní síti jsou využívány otevřené standardy a proto je možná spolupráce systémů od mnoha výrobců. Jako příklad volně šiřitelného operačního systému je vybrán operační systém Linux. Důraz je kladen na technické srovnání vlastností programů pro oba operační systémy a popis možností konfigurace. V závěru práce je provedeno srovnání ekonomické výhodnosti obou řešení.

Diploma thesis deals with implementation of server operating system in computer network of small sized company. The work is focused to finding alternatives of Open Source software to software developed by Microsoft. The main goal is to replace homogeneous network, where both operating systems – workstation and server – is developed by one company, therefore most of the communication protocols is proprietary or incompatible with standards, by heterogeneous network, where only open, well documented protocols are used. Because of using open standards many programs from different developers and different platforms can easily cooperate. Operating system Linux has been chosen as an examle of Open Source operating system. Diploma thesis describes technical issues of implementig Linux and basic configurational steps. In the last part of the work there is financial comparison of implementation of Microsoft operating system and Open Source operating system.

Obsah

Seznam tabulek

Seznam zkratek a symbolů

ACL	Access Control List, systém přístupových práv, také jejich konkrétní nastavení
ASP	Active Server Pages, platforma pro provoz dynamických WWW stránek, také Application Service Provider, poskytovatel outsourcingu služeb
BDC	Backup Domain Controller, záložní řadič domény
CIFS	Common Internet File System, novější verze protokolu SMB, od Windows 2000
DHCP	Dynamic host configuration protocol
DNS	Domain Name Service, služba převodu jmen
FTP	File Transfer Protocol
GPL	General Public License, licence upravující podmínky použití volného software
IIS	Internet Information Server, produkt Microsoftu
ISA	Internet Security and Acceleration Server, produkt Microsoftu
ISP	Internet Service Provider, poskytovatel služeb Internetu, poskytovatel připojení
LAN	Local Area Network, lokální síť
MS	Microsoft
NAT	Network Address Translation, překlad síťových adres
PDC	Primary Domain Controller, primární řadič domény
RAM	Random Access Memory, operační paměť
RFC	Request For Comment, sada standardů
RSA	šifrovací algoritmus
SMB	Server Message Block, protokol využívaný ve Windows sítích
SQL	Structured Query Language, dotazovací jazyk
SSL	Secure Socket Layer, šifrování přenosu dat
TLS	Transport Layer Security, šifrování přenosu dat
TCP/IP	Transmission Control Protocol/Internet Protocol, síťový protokol
TP	Twisted Pair, kroucená dvoulinka
UPS	Uninterruptable Power Supply, nepřerušitelný zdroj napájení
VPN	Virtual Private Network, virtuální privátní síť
WINS	Windows Internet Name Service, jmenný server Windows
WWW	World Wide Web

1 Úvod

V dnešním turbulentním prostředí je již téměř vyžadováno použití výpočetní techniky. Počítače jsou všude kolem nás, organizace, která nepotřebuje ke své činnosti výpočetní techniku je již spíše výjimkou než pravidlem.

S rostoucím významem počítačů pro výkon a fungování organizace roste i význam sdílení dat mezi těmito počítači. Pokud se v organizaci vyskytuje více než jeden počítač, bude zřejmě vyžadováno, aby počítače mohly mezi sebou nějak komunikovat – vzniká počítačová síť. Lokální počítačové sítě jsou propojovány dohromady, připojovány do struktury sítě Internet a uživatelé mohou sdílet svá data s dalšími uživateli po celém světě. Stále více činností je možné provádět prostřednictvím počítačů. V loňském roce byla uzákoněna možnost podat daňové přiznání v elektronické podobě prostřednictvím sítě Internet a podobných možností bude jistě přibývat. Mnoho úřadů má svou *e-podatelnu*, kde je možné podávat formuláře elektronickou poštou.

Počítačová síť se však neskládá jen z pracovních stanic, skládá se zejména z prvků, které jsou běžnému uživateli skryté. Jedná se o různé servery, směrovače, vysílače, přijímače a podobně. Význam těchto prvků pro fungování počítačové sítě je kritický. Při výpadku pracovní stanice nemá přístup k počítačové síti uživatel této stanice, při výpadku směrovače jsou odříznuti všichni uživatelé za tímto směrovačem. Pokud hlavní server přestane poskytovat určitou službu, může dojít k rozpadu celé počítačové sítě, což může mít pro organizaci dalekosáhlé následky a může vyústit ve výrazné finanční ztráty.

Server je počítač, který poskytuje určité služby klientům – pracovním stanicím. Může jít například o sdílení místa na disku (*souborový server*), přístup k síťovým tiskárnám (*tiskový server*), různé služby, související se síťovou infrastrukturou (*DHCP server*, *DNS server*, *WWW server*). Serverem bývá nazýván i program, který danou službu realizuje (např. WWW server *Apache*). Použití jednoho termínu pro dva rozdílné pojmy může být matoucí, ale terminologie je tímto způsobem již zažitá. Server jako onen počítač poskytující služby je zpravidla realizován jako osobní počítač (s patřičnou konfigurací hardware) s operačním systémem, v němž běží servery jednotlivých služeb. Operačních systémů pro servery je celá řada. V zásadě se dnes ale situace rozdělila na dva hlavní proudy – operační systém firmy Microsoft (platforma Windows[1]) a unixové operační systémy (Linux, FreeBSD, OpenBSD a podobně).

1.1 Řešení firmy Microsoft

Firma Microsoft těží z velké penetrace jejích operačních systémů na pracovní stanice (výrazná majorita – až 80 %) a z dobré integrace jejích serverových a desktopových operačních sys-

[1] V dalším textu budu pod pojem *Windows* shrnovat všechny operační systémy na platformě Wintel – jak klientské (Windows 95, 98, Me, 2000 WS, XP Home), tak serverové (Windows NT, 2000, XP). Důvodem je zjednodušení terminologie.

témů. Dalšími pozitivy platformy Windows je přívětivé uživatelské rozhraní, které umožňuje konfigurovat stanice i servery pomocí myši a grafického rozhraní.

Na druhou stranu má toto řešení několik nevýhod. Jednou z hlavních nevýhod je uzavřenost kódu. Firma Microsoft si své intelektuální vlastnictví (zdrojový kód Windows) pečlivě střeží a jejich produkty jsou „černé skříňky", do kterých není vidět. Microsoft do svých produktů implementuje velké množství proprietárních protokolů (uzavřených, jejich definice nejsou zveřejňovány) a standardní, již funkční protokoly, si upravuje podle svého. Výsledkem je, že produkty Windows (serverové i klientské programy) se velice dobře integrují samy mezi sebou, ale integrace s produkty třetích firem je poměrně náročná.

Další nevýhodou je, že produkty Microsoftu jsou určeny pro jednoduchou správu. Jednoduché problémy pokrývají poměrně dobře, v případě komplexnějších požadavků již je zpravidla nutné přikoupit další programový balík, nebo tyto požadavky nejsou vzhledem k nižší flexibilitě systému řešitelné.

1.2 Operační systému unixového typu

V posledních několika letech prožívají boom volně šiřitelné operační systémy unixového typu. V zásadě se jedná o dva systémy. Prvním z nich je Linux, což je operační systém vyvíjený pod licencí GPL lidmi z celého světa. Vznikl v roce 1991 a v dnešní době se jedná o plnohodntotný operační systém s velkým množstvím aplikací a instalací. Existuje velké množství programátorů, který vyvíjejí jak jádro, tak i další aplikace. Linux je velmi dobře použitelný na pozici síťového serveru vzhledem ke své dobré podpoře sítí TCP/IP a aplikačních protokolů. Jeho síťový subsystém je velmi sofistikovaný, je implementována většina funkcí komerčních systémů a mnoho nových. Navíc zdrojový kód systému je volně přístupný a je možné jej v souladu s licenčními podmínkami upravovat a dále šířit. Tedy principiálně není složité přidávat nové vlastnosti. Výhodou volně přístupného zdrojového kódu je možnost jeho inspekce, čímž je zjednodušeno hledání bezpečnostních a jiných chyb.

S popularitou Linuxu se svezly i jiné volně šiřitelné operační systému, založené na BSD Unixu – FreeBSD, OpenBSD a další. Tyto systémy jsou vyvíjeny pod podobnou licencí, pouze okruh vývojářů a uživatelů systému je menší. Proto v systému nejsou implementovány všechny vlastnosti, které jsou vestavěny v Linuxu, na druhou stranu se uvádí, že implementace – zejména síťového subsystému – je robustnější a stabilnější, než v Linuxu. Valná většina aplikačního programového vybavení (servery služeb), která je dostupná pro Linux, je dostupná i pro BSD systémy a obráceně.

Unixové systémy mají oproti Windows velkou výhodu v tom, že je možné je lehce upravit pro své potřeby. Systém je z hlediska API velmi dobře popsán a většina programového vybavení je dostupná ve formě zdrojových kódů. Proto je možné při tvorbě nové funkce vycházet z existujícího kódu a tento upravovat pro své potřeby. Vynikající je podpora skriptovacích jazyků (Perl, Bash, Tcl a další), které je možné používat pro různé konverze dat, ovládání či

zjednodušení administrace. Konfigurace systému ze zpravidla provádí formou editace textového souboru, proto je jednoduché i zálohování konfigurace (na rozdíl od Windows, jejichž konfigurace je zpravidla „utopena" kdesi v registrech).

Porovnání cen a nákladů jednotlivých řešení (Microsoft a jiné varianty) není jednoduché, neboť kromě pořizovacích nákladů vstupují do hry i TCO (*Total cost of ownership*), jejichž výše je málokdy přesně vyčíslitelná.

1.3 Heterogenní sítě

Vzhledem k nesporným výhodám unixových operačních systémů oproti systému Windows je možné pozorovat narůstající trend přechodu od homogenních sítí, kde klienti – pracovní stanice – i servery využívají operační systém rodiny Windows, k sítím heterogenním. V heterogenních sítích jsou na pracovních stanicích využívány operační systémy Windows i jiné systémy a na serverech jsou zpravidla využívány jiné operační systémy, než Windows. Účelem heterogenní sítě je sdílení dat nezávisle na operačním systému pracovní stanice nebo serveru. K tomu, aby tyto počítač mohly spolu komunikovat, je nutné, aby byl implementován standard, pomocí kterého budou komunikovat. Tento standard musí být dodržován všemi počítači v heterogenní síti.

1.3.1 Konkrétní heterogenní síť

Pro účely této diplomové práce uvažuji hypotetickou běžnou počítačovou síť běžné organizace. Na příkladu této sítě popíši rozdíly mezi homogenní sítí, založenou na serverech s operačním systémem Windows a heterogenní sítí, kde veškeré serverové služby zabezpečují počítače s operačním systémem Linux. Linux byl vybrán jako v současné době nejrozšířenější alternativa k operačnímu systému Windows a také proto, že bude zajímavé porovnat náklady na komerční systém (Windows) a volně šiřitelný operační systém (Linux).

V síti se nachází jeden server, který plní následující funkce:

1. Autentizace a autorizace uživatelů (je používán bezpečnostní model, ve kterém se každý uživatel musí přihlásit, aby mohl využívat síťových prostředků)
2. Souborový server – sdílené místo na discích serveru, domácí adresáře uživatelů
3. Tiskový server – k serveru je připojena sdílená tiskárna, kterou používají uživatelé sítě
4. DHCP server – přidělování IP adres jednotlivým pracovním stanicím
5. router a firewall – server připojuje lokální síť k Internetu, funguje jako směrovač pro lokální síť a zároveň jako firewall, chránící lokální síť před útokem z vnější sítě.
6. DNS server – pro doménu organizace

7. Server elektronické pošty (*mail server*) – SMTP pro příjem a odesílání pošty z lokální sítě, protokoly POP3 a IMAP pro příchozí poštu

8. WWW server – pro WWW stránky organizace

Pro účely této práce předpokládám, že organizace je připojena k Internetu pevnou linkou, má vlastní doménu druhé úrovně a služby WWW, DNS, e-mail poskytuje prostřednictvím svého serveru.

V lokální síti organizace se nachází řádově desítky pracovních stanic s operačním systémem Windows (eventuálně některé stanice s jinými operačními systémy – pro účely této práce vcelku nepodstatné). Uživatelé na těchto pracovních stanicích provozují následující činnosti (nevyjmenované činnosti jsou nepodstatné z hlediska fungování serveru):

1. Práce v kancelářském balíku MS Office

2. Elektronická pošta

3. Přístup na WWW stránky

Účelem této diplomové práce je porovnat implementace operačních systémů Windows a Linux na síťový server s důrazem na konfiguraci řešení, založeného na operačním systému Linux. Budou srovnány výhody a nevýhody jednotlivých řešení a v závěru bude porovnána i finanční náročnost implementace jednotlivých systémů.

2 Souborový server a tiskový server

Prvním a nejdůležitějším úkolem serveru je funkce souborového serveru pro pracovní stanice Windows. Existence souborového serveru má mnoho pozitiv. Mezi ty nejdůležitější patří

- Jednoduché zálohování dokumentů – všechny jsou uloženy na jednom místě
- Dokumenty jsou přístupné z jakéhokoliv počítače, který má oprávnění k dokumentu přistupovat
- Sdílení souborů mezi uživateli – všichni uživatelé mohou přistupovat ke stejným dokumentům

V sítích založených na Windows je pro funkci souborového serveru využíván komunikační protokol SMB (*Server Message Block*).

2.1 Základy sítí Windows

Aby pracovní počítač mohl pracovat v síti Windows, musí být v této síti zaveden. Existují dvě základní schémata sítě Windows:

1. Pracovní skupiny (*Workgroup*)
2. Domény (*Domain*)

2.1.1 Pracovní skupiny

V případě **pracovní skupiny** neexistuje žádný vyhrazený server. Všechny počítače, které patří do jedné pracovní skupiny (skupin může být velké množství, například *Učtárna*, *Personální*, *Výroba* a podobně) jsou si rovny (*peer to peer*). Každý počítač může obsahovat určité zdroje (sdílené disky, tiskárny a podobně) a tyto zdroje poskytuje ostatním počítačům v pracovní skupině. Tyto zdroje se v anglické terminologii nazývají *share*.

Každý počítač v pracovní skupině je na stejné úrovni s ostatními počítači[2], neexistuje centrální počítač, na kterém by byly udržovány uživatelské účty a podobně.

Pojetí přístupových práv v pracovních skupinách je velmi jednoduché. Každému sdílenému prostředku je možné přidělit oprávnění (*čtení*, *zápis*) a využití tohoto oprávnění podmínit heslem. Ke každému sdílenému prostředku tedy mohou (nemusejí) existovat dvě hesla – jedno pro čtení, druhé pro zápis. Bezpečnostní rizika tohoto řešení jsou očividná: každý uživatel, který potřebuje právo zápisu k určenému sdílenému prostředku, musí znát heslo. Pokud je třeba jednomu uživateli toto právo odejmout, musí správce změnit heslo a všem ostatním uživatelům (kromě uživatele, který už nemá mít přístup) sdělit nové heslo.

[2]Není to tak úplně pravda, další úlohy počítače, jako například *browser*, zmíním později

Tento přístup má výhodu v tom, že neexistuje centrální prvek sítě, který by mohl selhat a tím vyřadit celou síť z provozu. Nevýhody jsou:

1. Žádná úroveň bezpečnosti (každý, kdo zná heslo, má právo)
2. Žádná možnost autentizace
3. Chaos ve sdílených prostředcích (každý může nastavovat podle svého, neexistuje kontrola)
4. Při větším počtu stanic není zvládnutelné

Pracovní skupiny jsou jako politika sdílení dat použitelné pouze v nejmenších sítích, o velikosti pouze jednotek počítačů. Zřejmě se dost dobře nedá mluvit o bezpečnosti tohoto řešení, do sítí, ve kterých je důležitá bezpečnost dat, se toto schéma naprosto nehodí. Je vhodné maximálně do domácí sítě, ve které je třeba například sdílet adresář mezi všemi počítači.

2.1.2 Domény

Druhým schématem sítě Windows jsou takzvané *domény*. Toto schéma je založeno z hlediska autentizace a autorizace na architektuře klient-server. To znamená, že v síti je jeden (nebo více) autentizačních serverů (v terminologii firmy Microsoft *Primary Domain Controller – PDC* a *Backup Domain Controller – BDC*. Na primárním řadiči domény je uložena databáze uživatelů a jejich hesel, sekundární řadič (řadiče) domény tuto databázi s primárním serverem synchronizují (jejich kopie je pouze pro čtení,m není možné do ní dělat jakékoliv změny – ty je možné dělat pouze na primárním řadiči. Sekundární řadiče slouží jako záloha pro případ výpadku primárního řadiče. Každý uživatel sítě musí mít přiřazeno své uživatelské jméno a heslo a musí být do sítě přihlášen. Při přihlašování proběhne výměna informací s autentizačním serverem – ověření uživatelského jména a hesla. Pokud je uživatel úspěšně ověřen, je autentizačním serverem potvrzeno přihlášení do sítě a uživatel může využívat sdílené zdroje.

Požaduje-li uživatel přístup ke sdílenému prostředku, počítač, na kterém jsou tyto prostředky zpřístupněny (nemusí se jednat o server, může to být kterýkoliv počítač v síti) ověří, zda je žádající uživatel v pořádku přihlášen. V případě, že ano, je mu po ověření přístupových práv umožněno využívat služeb sdíleného zdroje. Ověření je možné provést bez toho, aby bylo nutné kontaktovat autentizační server, při přihlášení do domény je vygenerován *přístupový token*, který potvrzuje úspěšné přihlášení do domény.

Při přidělování práv v doméně je využíváno systému ACL (*Access Control List*). To znamená, že každému sdílenému zdroji je možné přiřadit seznam uživatelů nebo uživatelských skupin a každému jednotlivci nebo skupině specifikovat jeho práva. Práva jsou různá podle

povahy sdíleného prostředku (adresář, tiskárna). V případě sdíleného adresáře se jedná o následující práva (vzhledem k tomu, že v každé verzi Windows dochází k změně množiny dostupných práv, platí tento seznam pro Windows 2000 - anglickou mutaci):

- Full control
- Modify
- Read & execute
- Read
- Write
- List folder contents (pouze pro adresáře)

Tato množina oprávnění není konečná, existují ještě rozšířená oprávnění, která umožňují přístupová práva upravit přesněji (například povolit nebo zakázat mazání souborů). Každé oprávnění lze buď povolit nebo potlačit (*Allow*, *Deny*). Každému uživateli nebo skupině uživatelů je možno přidělit jakoukoliv kombinaci těchto práv.

Výhody domény oproti pracovní skupině jsou zřejmé:

1. Centrální autentizační server, udržující údaje o uživatelích
2. Každý uživatel je identifikován
3. Přístupová práva je možné velmi přesně specifikovat

Na druhou stranu mají domény i své nevýhody:

1. Při výpadku PDC vyřazení celé sítě (lze řešit pomocí BDC - zálohy)
2. Nutný serverový operační systém (Windows NT Server, Windows 2000 Server)
3. Nutnost vyhradit jeden počítač pro funkci dedfikovaného serveru (není vhodné používat server jako pracovní stanici)
4. Náročnější administrace

Pro malé sítě bude zřejmě největší nevýhodou nutnost použití vyhrazeného serveru se serverovým operačním systémem. Mezi serverové systémy, které je možné použít jako řadiče domény, patří níže vyjmenované operační systémy firmy Microsoft.

Operační systémy, které mohou plnit funkci PDC (primární řadič domény):

- Windows NT 4.0 Server
- Windows 2000 Server (a vyšší – Advanced Server a Datacenter Server)
- Windows 2003 Server (a vyšší)

Windows XP ve verzi *Professional* neumějí službu řadiče domény poskytovat, umějí se pouze připojit do domény jako klienti. Systém Windows XP ve verzi *Home* není možné do domény ani připojit, může využívat pouze schématu pracovních skupin.

2.2 Sdílení

Jak již bylo uvedeno sítě Windows jsou založeny na *sdílených prostředcích*. Sdíleným prostředkem může být adresář nebo tiskárna, obecně nějaká služba. Každý počítač poskytuje určité sdílené prostředky, v počítačových sítích je žádoucí centralizace uložení dat, proto se dá předpokládat, že převážná většina sdílených prostředků bude poskytována serverem.

2.2.1 Adresář

Sdílený adresář je propagován okolním pracovním stanicím, které se k tomuto adresáři mohou připojit a využívat soubory, uložené v tomto adresáři. V případě, že je využito schéma domén, je možné přidělovat přístupová oprávnění buď celému adresáři, nebo jednotlivým souborům v adresáři. Pak mohou uživatelé přistupovat pouze k souborům, k nimž mají přidělena přístupová práva.

2.2.2 Tiskárna

Sdíleným prostředkem může být i tiskárna. V tom případě je možné, aby uživatelé jednotlivých pracovních stanic využívaly jedné společné tiskárny na serveru. Z hlediska přístupových práv je tiskárna obdobným prostředkem jako adresář. Je možné nastavovat přístupová práva jednotlivých uživatelů k tiskárnám (opět v případě využití Windows domén) a omezit využití některých tiskáren jen určitým uživatelům.

Technicky je možné využít samostatných tiskových serverů, což jsou malé krabičky, které se připojí do počítačové sítě a k nim se připojí tiskárna (například systém *JetDirect* firmy *Hewlett-Packard*), není pak třeba mít tiskárnu připojenou přímo k serveru, tiskovým serverem je pak ona krabička. Výkonné tiskárny pro pracovní skupiny mívají někdy tuto krabičku vestavěnou jako standardní příslušenství.

3 Programový balík Samba

Pro zajištění funkce *souborového* a *tiskového* serveru existuje pro operační systémy Unixového typu balík, nazvaný *Samba*. Tento program vyvinul Andrew Tridgell pod licencí GPL, což znamená, že je možné tento program volně používat bez jakýchkoliv poplatků (blíže k licenci GPL viz *http://www.fsf.org* a *http://www.gnu.org*. Program je vyvíjen kontinuálně od roku 1991 a neustále jsou do něj implementovány nové funkce. Domovská stránka programu je *http://www.samba.org*.

Program *Samba* umožňuje serverům s operačním systémem unixového typu pracovat jako servery v sítích Windows. V současné době (verze 2.2.8a, před několika týdny byla uvolněna nová verze 3.0) může program Samba plnit následující funkce:

1. Souborový server – několik bezpečnostních modelů
2. Tiskový server
3. Doménový řadič – funkce PDC
4. WINS server

Program *Samba* je možné použít buď jako samostatný server do sítě Windows (jediný server v síti), nebo je možné tento server integrovat do existující sítě Windows, ve které už servery Windows jsou. Bez větších problémů spolupracuje i se servery s operačním systémem firmy Microsoft.

Program *Samba* pouze emuluje služby serverů Windows tak, aby klienti mohli tyto služby bez problémů využívat. Vzhledem k tomu, že se jedná pouze o emulaci, není možné implementovat všechny vlastnosti, které poskytují souborové a tiskové servery s operačním systémem Microsoft. Základní funkce pro bezproblémový chod souborového a tiskového serveru a pro spolupráci serverů mezi sebou jsou ovšem plně funkční. Menší problémy nastávají v případě použití primárního a záložního řadiče domény, tyto problémy by však měla řešit v současnosti vyvíjená verze 3.0. Server, který provozuje program *Samba*, nebude nikdy dokonale emulovat funkci serveru s operačním systémem Windows. Je to z toho důvodu, že operační systém Unix a operační systém Windows jsou diametrálně odlišné, používají například zcela jinou reprezentaci přístupových práv (operační systém Windows využívá systém ACL, zatímco Unix využívá systém `rwxrwxrwx`). Navíc specifikaci protokolu *SMB/CIFS*, který je používán pro komunikaci, firma Microsoft zveřejnila jen částečně a proto je nutné některé jeho části (zejména se jedná o části, které popisují komunikaci mezi servery a synchronizaci doménových dat) získávat pomocí jiných metod (zejména reverzním inženýrstvím).

3.1 Základní konfigurace programu

Konfigurace je prováděna (jako ostatně u většiny programů v operačních systémech unixového typu) editací textového souboru. V případě Samby se jedná o soubor `smb.conf`. Tento soubor

se dělí na několik sekcí. Hlavní sekce se jmenuje `[global]`. V této sekci jsou nastaveny všechny volby, které ovlivňují chod celého serveru.

Základní volbou je nastavení jména domény nebo pracovní skupiny, ve které bude server umístěn v síti Windows (ve složce *Okolní počítače*). Toho docílíme direktivou `workgroup`. Poté je možné nastavit i textový řetězec, který bude uveden u jména serveru – může nějak popisovat server v případě, že by jeho jméno nebylo dostatečně popisné (položka `server string`). Jméno serveru (uvádí se také v *Okolních počítačích* si server konfiguruje automaticky, ale je možné jej ručně změnit (volba `netbios name`). Protože jsme v Čechách, kterým bylo do vínku dáno několik kódování diakritiky, nastavíme správný převod mezi MS-DOS kódováním (*codepage 852*) a normou Unixu (*ISO8859-2*).

```
[global]
    workgroup = WORKGROUP
    server string = Hlavni server
    client code page = 852
    character set = ISO8859-2
```

Nyní je třeba se rozhodnout, který bezpečnostní model bude použit. *Samba* podporuje celkem čtyři modely:

1. zabezpečení na úrovni sdílení (*share*)
2. zabezpečení na úrovni uživatelů (*user*) – tento model je používán standardně
3. zabezpečení na úrovni serveru (*server*)
4. zabezpečení na úrovni domény (*domain*)

Nejjednodušším je zabezpečení na úrovni sdílení (*share*), které by mělo být podobné pracovním skupinám ve Windows. Mělo by být podobné, ale vzhledem k rozdílné reprezentaci přístupových práv v Unixu a ve Windows pracuje toto nastavení trochu jinak. V systému Windows má každé takové sdílení přiděleno jedno nebo dvě hesla. Není zde žádné omezení v tom, kdo se může k prostředku připojit, jakémukoliv uživateli stačí pouze znalost hesla. V operačním systému Linux (obecně jakémkoliv operačním systému na bázi Unixu) není možné zadat specifické heslo pouze pro jedno sdílení, proto funguje tento bezpečnostní model trochu jinak. Každý uživatel, který se autorizuje heslem, které server Samba přijme (souhlasí dvojice *uživatelské jméno – heslo*), bude mít k danému sdílení přístup. Je očividné, že to je velmi naivní bezpečnostní model, použitelný maximálně v domácí síti s maximální důvěrou.

Zabezpečení na úrovni uživatelů (*user*) je již výrazně bezpečnější. Každý uživatel se musí autorizovat svým jménem a heslem a po úspěšné autorizaci bude mít přístup determinován svými uživatelskými právy. Tento model je používán standardně.

Model *server* je využit v případě, že server Samba je napojován do stávající struktury. Server od uživatele přijme kombinaci *jméno + heslo*, ale tuto kombinaci nebude ověřovat sám, ale předá ji k ověření na jiný server (který je uveden v nastavení – položka `password server`).

Model *domain* je použit v případě, že Samba server je členem domény. To znamená, že existuje primární řadič domény (nezáleží na tom, je-li to Windows Server nebo Samba). Server potom ověřuje všechny požadavky na doménovém řadiči.

Nejčastějším nastavením bude zřejmě u malých sítí s jedním serverem (o kterou se jedná v této práci) model *user*. Bezpečnostní model se nastavuje pomocí direktivy `security` v sekci `[global]`.

V sítích Windows jednotlivé stanice oznamují sdílené prostředky, které nabízejí. V rámci segmentu existuje vždy takzvaný *browser*, což je počítač, na kterém jsou všechna tato oznámení přiímána a který vytváří kompletní seznam pro příslušný segment. Na funkci *browser* jsou čas od času v segmrntu iniciovány *volby* a počítač, který plní funkci *browser* se dynamicky mění. Je vhodné, aby funkci browser plnil server Samba, je tedy nutné jej nastavit, aby vždy ve volbách „zvítězil". Vítěz voleb se určuje z mnoha parametrů, například i z verze operačního systému, proto by se mohlo stát, že Windows 2000 na pracovní stanici ve volbách zvítězí a funkci *browser* serveru Samba odebere. V případě seznamu sdílených prostředků není velký problém, že *browser* je jiný počítač, ale tato funkce ovlivňuje i autentifikaci uživatelů. Mohlo by se tedy stát, že uživatelé by se pokoušeli přihlašovat k počítači, na němž nemají vytvořen účet.

Tímto nastavením v sekci `[global]` donutíme server Samba, aby vždy zvítězil ve volbách:

```
local master = yes
os level = 255
preferred master = yes
```

Toto nastavení je velmi agresivní, ale zajistí serveru Samba vždy vítězství ve volbách. Mohlo by však v některých případech zapříčinit částečné zpomalení sítě a problémy s tvorbou seznamů sdílených prostředků. Mohlo by totiž dojít k soustavnému souboji mezi několika servery o vítězství ve volbách, neustále by byly vyhlašovány nové volby. Volba `local master` znamená, že Samba se má vždy účastnit voleb pro lokální segment (existuje ještě volba `domain master`, která totéž znamená pro celou doménu), `os level` nastavuje prioritu Samby ve volbách (vždy vítězí počítač s nejvyšší prioritou, 255 je maximální) a `preferred master` znamená, že vždy, když Samba není *browserem*, má vyvolat volby.

3.2 Sdílené adresáře

Každý sdílený adresář má v souboru `smb.conf` svou sekci. Sekce jsou nazvány jménem sdílení v hranaté závorce, například `[smlouvy]`. Speciální postavení má sekce `[homes]`. Pokud se tato

sekce nachází v konfiguračním souboru, bude každému uživateli vytvořen sdílený adresář. Tento adresář bude nazván jeho uživatelským jménem a pod tímto jménem bude přístupný.

Typické nastavení sdíleného adresáře (v tomto případě adresář `smlouvy`) je následující:

```
[smlouvy]
    comment = Soubory se zakaznickymi smlouvami
    path = /mnt/datadisk/smlouvy
    public = no
    writeable = yes
    browseable = yes
    write list = @prodej
```

Komentář adresáře `smlouvy` je *Soubory se zakaznickymi smlouvami*, tento komentář se objeví vedle názvu sdíleného adresáře při zobrazení podrobností nebo vlastností. Na disku je adresář umístěn v na cestě uvedené v položce `path`. Položka `public` nastavuje, že do adresáře je přístup pouze v případě předchozí úspěšné autentifikace (pro přístup je nutné být k serveru přihlášen). Má-li sdílení nastavenu vlastnost `writeable`, budou moci oprávnění uživatelé do adresáře zapisovat. Položka `browseable` povoluje zobrazení adresáře v seznamu sdílených položek. Položka `write list` nastavuje uživatele oprávněné k zápisu do adresáře, je-li název uvozen znakem `@`, jedná se o skupinu uživatelů a právo zápisu má každý uživatel v této skupině.

Adresář `homes` je speciální, není nutné nastavovat cestu k tomuto adresáři a i některé jiné položky jsou zbytečné. Plně postačující nastavení domácího adresáře je následující:

```
[homes]
comment = Domaci adresar
writeable = Yes
browseable = Yes
```

Přístupová práva je možné měnit pomocí grafických dialogů na pracovních stanicích s operačním systémem Windows, založených na jádru NT (Windows NT, Windows 2000). K povolení této funkčnosti slouží parametr `nt acl support`, který je standardně nastaven na hodnotu `yes` (není tedy nutné jej jakkoliv měnit). Operační systém Linux (respektive obecně většina Unixů) používá jiný způsob reprezentace přístupových práv než Windows a proto bude dialog konfigurace přístupových práv fungovat mírně odlišně. Například nebude možné vzhledem k rozdílům prezentace přístupových práv definovat přístupová práva pro konkrétní uživatele.

3.3 Sdílené tiskárny

Samba může pracovat i jako tiskový server. V tomto případě je však nutné, aby tiskárny, které má Samba poskytovat klientům, byly nainstalované v operačním systému Linux – Samba využívá tiskárny v operačním systému a pro klienty představuje jakousi mezivrstvu, která „převádí" požadavky Windows na tiskové úlohy Linuxu (ve skutečnosti nejde o převod formátů, na pracovních stanicích, které mají mít přístup k tiskárnám v Sambě, musí být nainstalovány ovladače příslušných tiskáren, Samba pouze zjistí, že se jedná o tisk z Windows a holá data předá přes tiskovou frontu Linuxu přímo tiskárně).

Každou tiskárnu je třeba nakonfigurovat, aby ji Samba mohla nabízet. Nejjednodušším způsobem konfigurace je doplnění těchto řádků do souboru `smb.conf` (sekce `[global]`):

```
printcap name = /etc/printcap
load printers = True
printing = bsd
[printers]
path = /tmp
printable = Yes
browseable = No
```

První řádek, definuje, ve kterém souboru se nachází konfigurace tiskáren pro Linux. Většinou je to právě soubor, uvedený v ukázce. Samozřejmě je nutné předem tiskárny do tohoto souboru nadefinovat (to však většinou moderní distribuce zařídí uživatelsky příjemným způsobem). Druhý řádek instruuje Sambu, aby tiskárny z tohoto souboru nahrála a použila. Třetí řádek definuje, který systém správy tiskové fronty je na tomto systému používán (existuje několik navzájem nekompatibilních systémů – např. `bsd`, `lprng`, `cups`). Dále musí být nadefinována sekce `[printers]`. Potom budou do konfigurace Samby automaticky nahrány tiskárny, nakonfigurované v operačním systému. Položka `browseable` popisuje pouze nastavení pro fiktivní tiskárnu `printers`, neříká nic o zobrazení vlastních tiskáren v seznamu zdrojů.

Je možné použít i pokročilejší nastavení, tiskárny definovat ručně, konfigurovat seznamy uživatelů nebo skupin, které mají k tiskárnám přístup a tím omezit přístupová práva. Konfigurace se provádí podobným způsobem, jako v případě sdílených adresářů, tiskárně se založí nová sdílená sekce, do které se uloží příslušná nastavení.

3.4 Správa uživatelů

Každý uživatel, který chce využívat služeb souborového nebo tiskového serveru, musí mít vytvořen účet v systému. Nejprve je nutné vytvořit účet v Linuxu (například příkazem `adduser`), poté je ještě nutné vytvořit uživateli účet v systému *Samba*. k tomu slouží příkaz `smbpasswd` nebo níže popsané grafické rozhraní.

3.5 Grafický konfigurátor

Novější verze programu *Samba* obsahují grafický konfigurační program *SWAT – Samba Web Administration Tool*. Ten je (po instalaci) dostupný na adrese *http://adresa_serveru:901* a umožňuje všechny konfigurační zásahy provádět pomocí grafického rozhraní s nápovědou. Konfigurace programu *Samba* je s tímto nástrojem mnohem snažší.

Pokud uživatelské rozhraní nefunguje, je nutné jej nastavit. V souboru `/etc/services` musí být uveden řádek

```
swat            901/tcp          # samba web configuration tool
```

a v souboru `/etc/inetd.conf` následující řádek (nebo podobný, závisí na přesné konfiguraci, například na použití přídavných bezpečnostních programů):

```
swat            stream  tcp     nowait.400 root /usr/sbin/swat  swat
```

Po restartu procesu `inetd` by měl konfigurační nástroj fungovat.

3.6 Server WINS

Jednou z funkcí programu *Samba* je server WINS. WINS (*Windows Internet Name Service*) je obdoba DNS, která funguje pro služby sítě Windows. Každý počítač, který nabízí nějaké sdílené prostředky, ohlašuje serveru WINS své jméno a nabízené prostředky. Všechny počítače v síti znají adresu WINS serveru (dozvědí se jí pomocí služby DHCP, která bude popsána dále) a sdílené prostředky na serveru využívají. Bez serveru WINS sice operační systémy Windows umějí oznamovat své sdílené prostředky svým sousedům v počítačové síti, ale toto oznamování funguje pouze v rámci jednoho segmentu. Server WINS je možnost, jak propagovat sdílené prostředky v rámci celé sítě.

Server Samba může pracovat buď jako klient služby WINS (v tom případě někde na síti existuje jiný server WINS – buď s operačním systémem Windows, nebo jiná Samba), nebo jako server služby WINS. Nastavení serveru Samba jako klienta služby WINS na jiném počítači je jednoduché. Postačí jeden řádek v souboru `smb.conf` (v sekci `[global]`):

```
wins server = 192.168.1.1
```

Tímto řádkem serveru Samba oznámíme, že má využívat WINS serveru na této adrese, na tomto serveru registrovat své služby. Nastavení serveru Samba jako serveru WINS je také velmi jednoduché. Opět jej vyřeší jeden řádek v konfiguračním souboru (v sekci `[global]`):

```
wins support = yes
```

Je nutné poznamenat dvě důležité věci:

1. Každý počítač v síti musí mít nastavenu adresu WINS serveru, počtače, které adresu nastavenu mít nebudou, nebudou oznamovat své zdroje a nebudou umět využívat zdroje ostatních počítačů

2. V síti může být pouze jeden WINS server

WINS server je velice vhodné v lokální síti spustit, předejde se tím problémům s „neviditelností" některých sdílení.

3.7 Samba jako primární řadič domény

V případě, že společnost využívá server Samba jako hlavní server a na pracovních stanicích využívá operační systém, který je možné integrovat do bezpečnostního modelu *domain*, může server Samba nakonfigurovat jako primární řadič domény. Domény mají některé výhody, například existenci centrálního místa autorizace uživatelů, vyšší bezpečnost, možnost konfigurace sdílených prostředků i na lokálních stanicích, možnost použití cestovních profilů. Cestovní profily umožňují nakonfigurovat každému uživateli stejné prostředí nezávisle na pracovní stanici, ze které se do domény přihlásil.

Každý uživatel sítě, aby se mohl přihlásit, musí mít vytvořen účet na primárním řadiči domény, stejně tak každý počítač, který je členem domény. Účet je možné vytvořit v operačním systému pomocí programu `adduser`, účet počítače se od účtu uživatele liší pouze tak, že na konci uživatelského jména (které je názvem počítače) musí být znak `$`. Poté je možné přidat účet příkazem `smbpasswd` i do programu Samba. Druhou možností – podle dokumentace vhodnější – je zakládání účtů počítačů při jejich prvním přihlášení pomocí přihlašovacích skriptů. Toho dosáhneme zápisem podobné konstrukce[3] do sekce `[global]`:

```
add user script = /usr/sbin/useradd -d /dev/null -g 100 -s /bin/false -M %u
```

Tímto parametrem Sambě nastavíme, že pro přidání uživatele (respektive počítače) má spustit příkaz `useradd` s uvedenými parametry.

Základními nastaveními pro provoz Samby jako PDC jsou v následující ukázce.[4] Konfigurace musí splňovat určité předpoklady:

1. Bezpečnostní model *user*

2. Samba musí být *local browser* i *domain browser* a musí vždy vyhrát volby

[3]Bohužel volba příkazů, které budou přiloženy v distribuci je plně na správci distribuce. Proto může někdy dojít k situaci, že dvě distribuce obsahují různé verze jednoho programu a přepínače, které v jedné verzi fungují, v druhé nefungují. Proto se parametry v každé distribuci mohou lišit. Tento příkaz platí pro distribuci RedHat ve verzi 6.2

[4]Převzata z [1] a mírně upravena

3. Musí existovat sdílený adresář s názvem `[netlogon]`

4. Každý uživatel musí mít založen účet (jak o operačním systému Linux, tak i programu Samba)

5. Musí existovat pouze jeden PDC v dané doméně

Možná konfigurace je tedy následující (součástí ukázky je komentář, který je uvozen středníky):

```
[global]
        ;název domény
    workgroup = SPOLECNOST
    encrypt passwords = yes
        ;Samba musí být local browser i domain browser
    domain master = yes
    local master = yes
    preferred master = yes
    os level = 255
    security = user
        ;Samba bude přijímat požadavky o přihlášení do domény
    domain logons = yes
```

Pro použití cestovních profilů je třeba nadefinovat jejich umístění a název přihlašovacího skriptu, `%L` je nahrazeno jménem Samba serveru, `%u` uživatelským jménem, `profiles` je název sdíleného adresáře, kde budou uloženy uživatelské profily (pro Windows NT, 2000). Dále je nastaven přihlašovací skript, který bude spuštěn při přihlášení uživatele do domény (`logon.bat`), je umístěn v adresáři sdíleném jako `[netlogon]`. Položka `logon drive` je název jednotky, na kterou bude namapován domácí adresář. Položka `logon home` definuje místo pro uložení cestovního profilu pro Windows 95, 98 a Me (cestovní profily pro tyto Windows se liší od cestovních profilů pro Windows NT a 2000).

```
    logon path = \\%L\profiles\%u\%m
    logon script = logon.bat
    logon drive = H:
    logon home = \\%L\%u\.win_profile\%m
    domain admin group = root administrator
add user script = /usr/sbin/useradd -d /dev/null -g 100 -s /bin/false -M %u
```

Nyní následují nastavení sdílených adresářů, které jsou nutné pro funkci Samby jako PDC. Jedná se o sdílení `[netlogon]`, které vyžadují klienti v průběhu přihlášení, sdílení

[profiles], kam jsou ukládány cestovní profily pro Windows NT a 2000 a sdílení [homes], kde jsou domácí adresáře (a kam ukládají cestovní profily Windws 95, 98 a Me).

```
[netlogon]
    path = /usr/local/samba/lib/netlogon
    writeable = no
    browseable = no

[profiles]
    path = /home/samba_profiles
    browseable = no
    writeable = yes
    create mask = 0600
    directory mask = 0700

[homes]
    read only = no
    browsable = no
    guest ok = no
```

Volba `guest ok` určuje, zda je možné využívat sdílení i bez znalosti hesla, volby nazvané `create mask` a `directory mask` určují přístupová práva pro nově vzniklé soubory nebo adresáře (v tomto případě v adresáři s cestovními profily). Čísla 600 (pro soubory), eventuálně 700 (pro adresáře) znamenají plný přístup pro vlastníka (uživatele, o jehož profil se jedná) a žádný přístup pro ostatní.

4 Služba DHCP

Služby souborového a tiskového serveru (a související služby, jako WINS a podobně) nejsou jedinými službami, které musí server v síti plnit. Jednou z velice důležitých služeb, je služba DHCP, sloužící pro přidělování IP adres. Tato služba je nezbytná pro zdárný chod sítě, bez funkčního přidělování IP adres by počítačová síť buď nefungovala vůbec, nebo by fungovala velice polovičatě[5].

4.1 Proč DHCP

Služba DHCP (*Dynamic Host Configuration Protocol* – definována v RFC 2131, 2132, navazuje na RFC 951) je určena ke konfiguraci síťových rozhraní klienských stanic. Pomocí DHCP jsou nastavovány IP adresy jednotlivých stanic, adresy jmenných serverů, serverů WINS a klienti jsou informování o základní struktuře sítě. Služba není pro chod sítě nezbytně nutná, v tom případě je však nutné tyto informace nastavovat na každé stanici ručně, což při větším počtu stanic není příliš pohodlné ani systematické. Výhodou využití DHCP je to, že všechny konfigurační informace jsou udržovány centrálně na jednom místě. Pro úplnost zmíním ještě třetí možnost: nevyužívat ani statické konfigurace (ruční), ani služby DHCP. V tom případě jsou stanice Windows schopny jakési částečné „samokonfigurace", svou IP adresu si náhodně zvolí z intervalu 169.254.0.0 – 169.254.255.255. Nemohou si ovšem správně zvolit další parametry sítě, jako jsou adresy jmenných serverů nebo adresa brány. Proto se jedná o nouzové řešení, které zpravidla není dostačující.

Služba DHCP funguje na jednoduchém principu: stanice v průběhu bootovacího procesu vyšle požadavek na konfoguraci, tento požadavek zachytí DHCP server a podle údajů ve své databázi odpoví s konkrétní konfigurací. Stanice přijme tuto odpověď a na jejím základě provede konfiguraci svého síťového rozhraní. Server služby DHCP musí být umístěn na každém segmentu sítě, protože požadavky na konfiguraci (respektive zprávy *broadcast*) není povoleno přenášet za hranici segmentu (v RFC 2131 je definován způsob, jak toto omezení obejít v souladu se standardy).

4.2 Konfigurace DHCP

Server s operačním systémem Linux může pochopitelně pracovat i jako server DHCP. Předpokladem je správná konfigurace. Tato konfigurace je zpravidla umístěna v konfiguračním souboru `/etc/dhcpd.conf` (pro funkci serveru služby DHCP existuje několik volně šiřitelných balíků, tentoi popis bude určen pro balík ISC-DHCP, který je standardní součástí většiny distribucí). Konfigurační soubor se dělí na nekolik částí, na část globální (platí pro všechny) a části specifické pro jednotlivé segmenty nebo klienty. Je velmi důležité dodržovat správnou

[5]Technicky vzato by tato služba měla být zprovozněna v síti jako první, proto její zařazení až za služby souborového a tiskového serveru je nesprávné, ale vzhledem k zaměření této práce je to lepší

syntaxi konfiguračního souboru, v opačném případě může běh serveru skončit s chybou – klienti by pak nedostávali konfigurační informace a přikročili by k „automatické samokonfiguraci".

Direktivy uvedené v globální sekci platí pro všechny stanice, které získají svou konfiguraci z tohoto serveru. Každá direktiva je ukončena *středníkem*. Nejdůležitějšími globálními direktivami jsou:

```
option domain-name "mojefirma.cz";
option domain-name-servers 192.168.1.1, ns.mojefirma.cz;
option netbios-name-servers 192.168.1.1;
max-lease-time 7200;
default-lease-time 600;
```

Parametr `domain-name` nastavuje jméno domény, ve které se stanice nachází, v parametru `domain-name-servers` jsou uvedeny jmenné serveru pro tuto doménu (služba DNS, viz. následující kapitola). Pokud se nachází u direktivy více položek, oddělují se čárkou. Direktiva `netbios-name-servers` nastavuje adresu serveru WINS (pro stanice Windows).

Direktivy `default-lease-time` a `max-lease-time` nastavují dobu, po kterou je konfigurace stanice platná (v sekundách). Po této době musí stanice požádat server o obnovení konfigurace. O obnovení konfigurace požádá po *default* sekundách a v případě, že v požadavku o obnovení konfigurace stanice uvede nějaký „vlastní návrh doby platnosti", bude tento návrh přijat v případě, že je nižší než `max-lease-time`. V tomto návrhu může být také uvedena IP adresa, jakou by si stanice „přála" – v případě, že tuto adresu již má a žádá o prodloužení doby platnosti.

Dále je třeba definovat pro každé síťové rozhraní (tedy pro *každý* segment, který je k serveru připojen) sekci, která je společná pro všechny počítače na segmentu:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.100 192.168.1.200;
option broadcast-address 192.168.1.255;
option routers 192.168.1.1;
}
```

Zde je nutné zejména dodržet správnou syntaxi. Záhlaví položky nás informuje, pro jakou podsíť s jakou maskou je následující záznam určen. Ve složených závorkách je potom uveden vlastní záznam. Položka `range` definuje spodní a horní rozsah IP adres, který bude klientům přiřazován *dynamicky*. V případě, že požadavek přijde na server z tohoto segmentu a klientská stanice nebude zavedena v databázi, bude jí přidělena IP adresa z tohoto rozsahu. Položka `broadcast-address` nastavuje adresu všesměrového vysílání pro daný segment a konečně položka `routers` informuje o bráně pro příslušný segment. Pokud by tato položka nebyla

definována, počítače na tomto segmentu by nebyli informováníо tom, kterému počítači předávat pakety směřující mimo lokální segment (to znamená, že by mohly komunikovat pouze v rámci tohoto segmentu).

V další části souboru mohou být potom uloženy konfigurační informace pro jednotlivé stanice. Tyto informace tam být nemusejí v případě, že je definována direktiva `range` v segmentové části, potom každý počítač dostane adresu z intervalu, uvedeného v této direktivě. Konfigurace pro jednotlivý počítač může mít následující tvar:

```
host stanice-01 {
hardware ethernet 01:02:03:04:05:06;
fixed-address 192.168.1.201;
}
```

Je definováno jméno počítače, jeho MAC adresa (položka `hardware ethernet`) a jeho IP adresa (položka `fixed-address`). Existuje-li v síti DNS server s údaji o počítačích v interní síti, je možné získávat IP adresu z DNS, je však třeba počítat s jistým zpožděním kvůli vyřizování dotazu.

Po každé změně v konfiguraci je třeba proces, který zajišťuje služby serveru DHCP, restartovat.

4.3 Hledání závad v konfiguraci

Hledání závad v konfiguraci DHCP je poměrně jednoduché. Pokud je v konfiguraci nějaká závada, chová se program poměrně přímočaře. Postup hledání závady může být následující:

1. V případě, že klienti získávají alespoň nějakou konfiguraci, znamená to, že server funguje a nějak odpovídá. V operačním systému Windows existují dva diagnostické nástroje použitelné pro diagnostiku DHCP. Jedná se o příkazy `ipconfig` a `winipcfg` (tento pouze ve Windows 98). Z informací, které poskytne příkaz `ipconfig /all` (nebo položka *Podrobnosti* v příkazu `winipcfg`), je možné zjistit, jaké informace a od jakého serveru klient obdržel. Poté je možné v konfiguračním souboru provést patřičné úpravy.

2. Pokud klient neobdrží žádnou informaci a konfiguraci si „vymyslí“ (jeho IP adresa je z rozsahu 169.254.0.0 – 169.254.255.255), znamená to, že nedošlo k výměně informací mezi serverem a klientem. Je třeba zjistit, zda server běží (zda na serveru běží proces `dhcpd`).

3. Běží-li server DHCP (proces `dhcpd` existuje), může být chyba v síťové infrastruktuře, kabeláži, nebo nevhodně nastavených bezpečnostních pravidlech (jsou blokovány požadavky nebo odpovědi). Z protokolů serveru (zpravidla v adresáři `/var/log`, např souboru `messages`) je možné zjistit, zda požadavek k serveru dorazil a co s ním server provedl.

4. Pokud server DHCP neběží (proces `dhcpd` neexistuje), je chyba v konfiguraci. S pomocí protokolových souborů a výpisů při ručním spuštění je možné zjistit, na jaké direktivě konfiguračního souboru server zhavaroval. Nejčastěji se jedná o zapomenuté středníky, chybné párování složených závorek a překlepy. Velmi častou chybou je také chybějící definice pro některé síťové rozhraní.

5 Služba DNS

Další službou, kterou mohl zajišťovat server Windows, je služba DNS (*Domain Name Service*). Pro fungování interní sítě není zcela nezbytná, ačkoliv v komplexnějších prostředích je nutná. Je ovšem zcela nutná ve chvíli, kdy je společnost připojena k Internetu a prostřednictvím svého serveru poskytuje jakékoliv služby. V modelové situaci, kterou popisuje tato práce, společnost vystavuje na svém serveru WWW stránky, FTP strom a odesílá a přijímá poštu. Proto je DNS server nezbytný.

Společnost má svou doménu druhé úrovně v doméně první úrovně `.cz`. Na serveru (původně s OS Windows, nyní s OS Linux) je provozován primární nameserver organizace, sekundární nameserver (pro úspěšnou registraci domény druhé úrovně jsou vyžadovány dva funkční, nezávislé nameservery) poskytuje organizaci například poskytovatel pevné linky (pro účely této práce je vcelku nepodstatné, kdo poskytuje službu sekundárního nameserveru, stačí vědět jeho IP adresu pro správné nastavení replikace zóny). V operačním systému Windows je vestavěn jednoduchý DNS server, který postačuje pro základní funkci systému DNS. Je ovšem problematické jej nastavit pokročilejším způsobem.

Pod operačním systémem Linux existuje několik programů, které mohou plnit funkci serveru DNS. Jedním z klasických je program *bind*. Je tak klasický, že v některých konfiguračních direktivách operačního systému je výraz `bind` synonymem pro DNS. Tento program je využíván jako server DNS ve velké části Internetu, včetně kořenových serverů.

5.1 Základní konfigurace

Základním konfiguračním souborem programu *bind* je soubor `named.conf`. V tomto souboru jsou popsána základní nastavení serveru. Pro začátek bude stačit, aby server vyřizoval požadavky na převod jmen na IP adresy pro počítače v lokální síti. Nameserver bude tedy zatím pracovat jako takzvaný *caching-only*. To znamená, že pouze přebírá požadavky od klientů, tyto požadavky za ně vyřídí, vrátí výsledek a zároveň si výsledek zapamatuje pro případ, že by další klient položil stejný dotaz. Klienti již vědí, kterého serveru se mají dotazovat (dozvěděli se to pomocí DHCP). Aby server DNS mohl vyřizovat požadavky, musí vědět o ostatních serverech DNS – alespoň o některých. Služba DNS je založena na decentralizovaném, hierarchickém systému, kde v každé doméně je určen DNS server, který je pro danou doménu *autoritativní*. Autoritativní server je takový server, který je zodpovědný za informace o doméně, udržuje databázi domény (takzvanou *zónu*) a vyřizuje požadavky na převod jmen z dané domény. Bližší princip hierarchického uspořádání služby DNS je popsán v literatuře, uvedené na konci této práce.

Aby server mohl vyřizovat požadavky svých klientů, musí vědět, kde se nacházejí další servery DNS. Do konfigurace se tedy uvádějí takzvané *root servery*, kořenové servery DNS, které obsahují odkazy na servery domén nejvyšší úrovně. Tyto servery jsou velice důležité,

při jejich výpadku by se Internet rozpadl na jednotlivé domény nejvyšší úrovně. V současné době je jich 13 a jejich seznam je uveden v konfiguračním souboru, který se většinou jmenuje `named.ca` nebo `root.hint`.

Základní konfigurace programu *bind* bude tedy v konfiguračním souboru `named.conf` popsána následujícími direktivami:

```
options {
        directory "/var/named";
};

zone "." IN {
        type hint;
        file "named.ca";
};
```

Konfigurační soubory zón jsou uloženy v adresáři `/var/named` (direktiva `directory`) a je nadefinována jediná zóna – kořenová (značí znak „tečka"), která je uložena v souboru `named.ca`. Typ `hint` říká, že nameserver se má pro tuto zónu chovat jako *caching-only*. Je nutné přesně dodržet syntaxi souboru, jinak program *bind* při startu zhavaruje.

Nyní je třeba nadefinovat jednotlivé zóny – každá zóna popisuje nastavení jedné domény. První dvě zóny, které je třeba nadefinovat, jsou zóny pro převod jména `localhost` na adresu `127.0.0.1` (tato adresa definuje na *každém* počítači ten příslušný lokální počítač). Dvě zóny – jedna je pro dopředný převod (jméno na IP adresu) a jedna pro reverzní (zpětný převod – IP adresa na jméno). Do souboru `named.conf` se dodají další dvě definice:

```
zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};
```

Zpravidla tyto dvě definice jsou již součástí distribuce programu *bind*, stejně tak oba soubory (`localhost.zone` i `named.local` – jména se mohou lišit). Klauzule `allow-update`

definuje, ze kterých počítačů je možné přijímat dynamické aktualizace zóny (možné použít v případě, že jiný počítač aktualizuje zónu – například DHCP server). Zde je nadefinováno, že dynamické aktualizace nebudou přijímány z žádného počítače (logicky, zóny pro `localhost` se nemění).

5.2 Konfigurace DNS serveru pro doménu druhé úrovně

DNS server v organizaci slouží jako nameserver pro vlastní doménu druhé úrovně. Proto je nutné tuto doménu na serveru nakonfigurovat. Nejprve je nutné připravit si konfigurační soubory jednotlivých zón (zóny budou dvě – jedna pro dopředný převod, ta je nezbytná, druhá pro zpětný převod – ta sice není nezbytná, ale je doporučeno, aby byla definována). V tomto hypotetickém případě budu předpokládat, že firma si zaregistruje doménu *organizace.cz* a veřejná IP adresa jejího serveru je 111.112.113.114 (jméno domény i IP adresa jsou zcela fiktivní).

Nyní je tedy potřeba připravit dva zónové soubory. Prvním bude zónový soubor pro dopředný převod. Název tohoto souboru bude například `organizace.cz.db`. Soubor musí nejprve obsahovat hlavičku, která shrnuje nejdůležitější informace o doméně[6]. Jedná se o takzvaný *SOA* záznam (*Start Of Authority*).

```
$TTL    86400
$ORIGIN organizace.cz.
@        1D IN SOA       server.organizace.cz. webmaster.organizace.cz. (
                                    2003111101      ; serial
                                    3H              ; refresh
                                    15M             ; retry
                                    1W              ; expiry
                                    1D )            ; minimum

@                       1D IN NS        server
server                  1D IN A         111.112.113.114
```

Toto záhlaví musí být přítomno v každém zónovém souboru. Do položky `$ORIGIN` se uvede jméno domény, pro kterou je tento zónový soubor vytvořen (důležitá je tečka na konci). Položka `server.organizace.cz.` říká, že primárním name serverem pro tuto doménu je počítač `server.organizace.cz` Položka `webmaster.organizace.cz.` oznamuje e-mailovou adresu osoby, která je zodpovědná za nastavení DNS serveru (zde *webmaster@organizace.cz*, zavináč se nahrazuje tečkou, tečka za `cz` je důležitá). Důležitým číslem je položka `Serial`, která popisuje *verzi* souboru. Po každé změně souboru musí být zvýšena. Další čtyři údaje definují časové konstanty související s chodem serveru.

[6]Technicky vzato je rozdíl mezi *doménou* a *zónou*, ale domnívám se, že výklad není na této úrovni podstatný

Záznam typu NS definuje, který počítač je autoritativním nameserverem domény – v tomto případě je to počítač server.organizace.cz (protože název počítače nekončí tečkou, bude k němu připojen název domény, který je definován v položce $ORIGIN – to je ona důležitá tečka). Záznam typu A již definuje vlastní přiřazení jména a IP adresy (počítač server.organizace.cz má IP adresu 111.112.113.114).

Každá platná doména druhé úrovně však musí mít dva nezávislé nameservery. Proto je nutné nadefinovat v zónovém souboru další nameserver. Zpravidla dělá sekundární nameserver buď poskytovatel připojení k Internetu. Další častou metodou je dohoda dvou organizací, že si budou navzájem poskytovat službu sekundárního nameserveru. V tomto hypotetickém případě tedy předpokládejme, že se organizace dohodla s jinou organizací a navzájem si poskytují tuto službu. Druhá organizace vlastní doménu spolecnost.cz, nameserver má jméno ns.spolecnost.cz a IP adresu 100.101.102.103. Do zónového souboru se doplní informace o dalším nameserveru pro doménu:

```
@                       1D IN NS        ns.spolecnost.cz.
```

Základní nastavení zóny je připraveno, nyní se vytvoří v zóně záznamy pro WWW server organizace (počítač www.organizace.cz), a FTP server organizace (ftp.organizace.cz) a základní DNS nastavení pro příjem elektronické pošty (v DNS databázi musí být řečeno, který počítač přijímá poštu pro tuto doménu). Všechny tyto počítače budou ve skutečnosti jeden jediný počítač (server.organizace.cz), ale lépe ty vypadá, pokud se připojujeme k počítači www.organizace.cz než k počítači server.organizace.cz. Je tedy nutné nastavit takzvané *aliasy*. Ty se tvoří klíčovým slovem CNAME.

```
@  1D IN MX 10     server
www              1D IN CNAME     server
ftp              1D IN CNAME     server
```

První záznam definuje, že pošta pro doménu organizace.cz bude předávána počítači server.organizace.cz, hodnota 10 nastavuje prioritu v případě většího počtu serverů pro příjem pošty.

Tímto je tedy hotová základní konfigurace dopředné zóny, nyní by měl být nastaven ještě zpětný převod (převod z IP adresy na jméno). Vzhledem k tomu, že organizace má pouze jednu veřejnou IP adresu, není nutné zpětný převod (tedy vlastně převod z IP adresy 111.112.113.114 na jméno server.organizace.cz konfigurovat na tomto serveru, konfiguraci již na svém serveru provedl poskytovatel připojení (adresa 111.112.113.114 spadá do jeho adresového prostoru). V další podkapitole jen pro úplnost uvedu jednoduchou konfiguraci zpětného převodu.

Aby byl dopředný převod funkční, je třeba jej nakonfigurovat ještě v hlavním konfiguračním souboru `named.conf`. Do tohoto souboru je třeba přidat sekci pro tuto zónu:

```
zone "organizace.cz" IN {
        type master;
        file "organizace.cz.db";
        allow-update { none; };
allow-transfer {100.101.102.103;};
};
```

Zápis znamená následující: tento server je primárním serverem domény `organizace.cz` (typ `master`), jejíž konfigurace je uložena v souboru `organizace.cz.db`, žádny počítač nesmí dynamicky aktualizovat nastavení a počítač 100.101.102.103 (záložní server, který pro nás zprostředkovává jiná společnost) si může stahovat celý soubor zóny. Toto nastavení je nadbytečné, neboť na vyšší úrovni to žádnému počítači nebylo zakázáno, ale z bezpečnostních důvodů bývá doporučeno povolit přenos celé zóny pouze sekundárnímu serveru.

Ještě chybí jedno nastavení. Na oplátku poskytuje tato organizace jiné společnosti službu sekundárního serveru. To je také třeba programu *bind* oznámit. Docílíme toho následující konfigurací:

```
zone "spolecnost.cz" IN {
        type slave;
        file "spolecnost.cz.bk";
masters { 100.101.102.103; };
};
```

Zápis znamená: tento server je sekundárním serverem pro doménu `spolecnost.cz` (typ `slave`), konfigurace je uložena v soubrou `spolecnost.cz.bk`. Je potřeba si uvědomit, jak pracuje sekundární server. Na tomto serveru se záznamy needitují, server si je stahuje průběžně z primárnho serveru vždy, když zjistí, že se změnila verze dat na primárním serveru (důležité číslo `Serial`). Do souboru `spolecnost.cz.bk` si tedy zálohu ukládá server *sám*, aby byl urychlen jeho start. Položka `masters` říká, ze kterého serveru si má sekundární server stahovat platné údaje (tedy je to adresa primárního serveru druhé společnosti).

Pro správnou funkci je samozřejmě nutné mít uvedené oba servery jako nameservery u národního registrátora, ale vzhledem k tomu, že síť už předtím fungovala s operačním systémem Windows na serveru, dá se předpokládat, že registrace byla správně provedena.

5.3 Další konfigurace

Základní konfigurace DNS serveru je hotová. V této podobě by DNS server mohl bez problémů fungovat jako primární DNS server domény `organizace.cz`. Konfioguraci je však možné ještě vylepšit. Některá vylepšení tedy zmíním v této kapitole.

5.3.1 Zóna pro interní síť

V organizaci pro jednoduchost není využívána služba DNS pro lokální síť. To znamená, že jednotlivé počítače nemají přidělené jmenné názvy, využívají pro tento převod pouze službu WINS. Tato služba je ale omezena pouze na systémy, které využívají protokol SMB/CIFS. Pokud by organizace chtěla (například pro zvýšení průhlednost lokální sítě) implementovat DNS i pro počítače v interní síti, je to možné. Každý počítač by měl pak přiřazenou v DNS jednoznačnou jmennou adresu (například `uctarna.organizace.cz`, `sklad.organizace.cz`).

Konfigurace je jednoduchá. Každému počítači se přidá do souboru `organizace.cz.db` jeden `A` záznam a pro interní síť se založí reverzní zóna. Do souboru `organizace.cz.db` se přidají následující řádky:

```
uctarna                    1D IN A         192.168.1.100
sklad   1D IN A   192.168.1.101
```

Nyní je třeba založit reverzní zónu. Tato zóna mapuje převod z IP adresy na jméno. Pro vytváření reverzních zón se využívá fiktivní doména `in-addr.arpa`. To znamená, že síť číslo 192.168.1.0 (maska 255.255.255.0) je reprezentována doménou `1.168.192.in-addr.arpa`. Do souboru s názvem například `192.168.1.db` se vloží následující informace:

```
$TTL    86400
@       IN      SOA     server.organizace.cz webmaster.organizace.cz.  (
                                        2003112101 ; Serial
                                        28800      ; Refresh
                                        14400      ; Retry
                                        3600000    ; Expire
                                        86400 )    ; Minimum
@               IN      NS      server.organizace.cz.

1       IN      PTR     uctarna.organizace.cz.
2       IN      PTR     sklad.organizace.cz.
```

Dále je nutné zónu nadefinovat v `named.conf`. Do souboru `named.conf` se přidá následující sekce:

```
zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "192.168.1.db";
        allow-update { none; };
};
```

5.3.2 Pohledy

Nyní tedy funguje DNS i v rámci interní sítě. Poslední problém, který zbývá, je pomíchání záznamů pro interní síť a vnější síť v jedné zóně. V interní síti se používají vyhrazené IP adresy z rozsahu, který je podle RFC 1597 vyhražen pro lokální sítě. Není tedy v pořádku, že v případě, že když se klient z internetu zeptá na IP adresu počítače `uctarna`, že dostane jako odpověď adresu 192.168.1.100 (z privátního rozsahu). Pro řešení tohoto problému existuje několik možností, všechny jsou ovšem poněkud *neobvyklé*. Naštěstí program *bind* od verze 9 podporuje takzvané pohledy (*views*). To znamená, že může vracet rozdílné odpovědi podle toho, odkud přišel dotaz. Soubor `named.conf` se upraví následujícím způsobem:

```
view "internal" {
      match-clients { 192.168.0.0/16; };
zone "organizace.cz" IN {
         type master;
        file "organizace.cz.interni";
         allow-update { none; };
};
zone "1.168.192.in-addr.arpa" IN {
         type master;
        file "192.168.1.db";
        allow-update { none; };
};
};

view "external" {
      match-clients { any; };
zone "organizace.cz" IN {
         type master;
        file "organizace.cz.externi";
        allow-update { none; };
```

```
allow-transfer {100.101.102.103;};
};

};
```

Po vytvoření souborů `organizace.cz.interni` (zónový soubor pro interní klienty – kompletní) a `organizace.cz.externi` (pro externí dotazy, pouze veřejné položky) bude vše tak, jak má být v ideálním světě.

6 Informační služby

Každá společnost, která má vlastní server v Internetu, jej má v první řadě proto, aby pomocí něj mohla zveřejňovat informace. Zřejmě nejpoužívanější informační službou je služba WWW (*World Wide Web*). Ve světě MS Windows existuje mnoho programů pro tuto službu, ale nejčastěji je využíván (zejména u menších sítí, které nevyužijí drahá *enterprise* řešení) *Internet Information Server* (IIS), který je standardně dodáván jako součást serverových operačních systémů firmy Microsoft. Další službou, která je často používaná pro distribuci souborů, je služba FTP – zejména anonymní FTP. Sice v posledních letech je vytlačována univerzálnějším WWW, přesto se jedná o klasiku, která by neměla být opomenuta. Ve Windows poskytuje IIS i službu FTP.

V dnešní době převažuje odklon od statických WWW stránek směrem k dynamicky generovaným WWW stránkám. To znamená, že stránky nejsou napevno uloženy někde na pevném disku a při požadavku na otevření této stránky jsou poslány ke klientovi, ale stránka je vygenerována na základě chodu nějakého programu jako jeho výstup. Typickým příkladem je například *elektronický obchod*. To je aplikace, která by zřejmě nešla realizovat pomocí statických WWW stránek tak, aby byl zachován komfort pro uživatele. Proto existuje mnoho jazyků pro tvorbu dynamických WWW stránek.

Ve světě Windows se jedná zejména o

- Javascript – jazyk takzvaně *client-side* (zpracovávaný na klientovi)
- Java – *client-side* i *server-side* (*servlets*)
- ASP – aplikační platforma pro jazyky jako *Visual Basic* a podobně
- Perl – převzat z Unixu díky své popularitě

Dynamické WWW stránky nejčastěji získávají informace z databází. Ve světě Windows existuje mnoho databázových systémů, namátkou je možné zmínit například

- Microsoft SQL Server
- Oracle
- Sybase Adaptive Server
- Informix

Z velké části se jedná o komerční produkty (a vcelku nákladné), které se nedodávají v základní instalaci Windows (výjimkou je pouze Microsoft SQL Server, který je dodáván v Microsoft Small Business Serveru).

Existuje velké množství funkcí, které mohou nabízet WWW servery, mnoho z nich nabídne standardní server, dodávaný společně s Windows. Ale protože účelem této práce je navrhnout postup přechodu hlavního serveru z Windows na Linux, je třeba najít Unixové náhrady Windows produktů.

6.1 Služba WWW

Nejznámějším WWW serverem pro operační systémy rodiny Unix je server *Apache* (domácí stránka *http://www.apache.org*, existuje i ve verzi pro Win32). Jedná se o velmi pokročilý a velmi rozšířený WWW server (podle informací NetCraft Survey z října 2002 má tržní podíl asi 65 %, IIS má podíl 25 %). Mezi nejdůležitější vlastnosti *Apache* patří:

- modularita – je možné přidávat nové vlastnosti ve formě modulů,
- kontrola přístupu – omezování přístupu k WWW stránkám na základě definovaných pravidel,
- šifrování – podpora protokolů SSL a TLS pro přenos dat šifrovaným kanálem,
- výkon a škálovatelnost,
- *load balancing* – rozvažování výkonu mezi několik serverů,
- podpora *virtuálních serverů*

Nejedná se však pouze o server, WWW server je jen jednou částí rozsáhlého projektu společnosti *Apache Software Foundation*. Mezi další projekty, které jsou vyvíjeny společně s Apache a přinášejí jednoduchou integraci nebo spolupráci s *Apache*, patří například:

- *Tomcat* – oficiální implementace Java sevrletů a Java Server Pages,
- *JAMES* – Java Apache Mail Enterprise Server,
- *Lucene* – výkoné vyhledávací jádro pro vyhledávání v textových souborech,
- *JetSpeed* – Web portál v Javě, s modulárním API pro spojení různých datových zdrojů
- a další

Pro tento WWW server existuje mnoho jazyků pro tvorbu dynamických WWW stránek. Jen namátkou je možné zmínit:

- *Perl* – velmi populární jazyk, umožňuje silné manipulace s texty, přístup k databázím, využití obrovského množství modulů, které byly vyvinuty v tomto jazyce (viz. *http://www.cpan.org*). Plně integrován do *Apache*,

- *PHP* – silný jazyk pro tvorbu dynamických stránek, připojení k databázím, viz. dále,
- *Python* – objektově orientovaný jazyk,
- *TCL* – jednoduchý, rozšiřitelný skriptovací jazyk,
- *ASP* – existují komerční řešení pro provoz ASP aplikací na serveru *Apache* v operačních systémech Unix,
- *.Net* – s rozšiřujícím modulem je možné provozovat ASP.Net aplikace,
- a v neposlední řadě samozřejmě Java

6.1.1 PHP

Jedním z velice oblíbených jazyků pro tvorbu dynamických stránek je jazyk *PHP* (domácí stránka *http://www.php.net*). Jazyk je vyvíjen již několik let a z původního jednoduchého nástroje se vyvinul do podoby komplexního, flexibilního a rozšiřitelného jazyka. Jedná se o interpretovaný jazyk, existují však i komerční kompilátory. Jde o takzvaný *HTML Embedded* jazyk, to znamená, že programové konstrukce se vkládají přímo do kódu HTML stránky. Mezi nejdůležitější vlastnosti jazyka patří:

- jednoduchá syntaxe jazyka,
- modularita, mnoho rozšiřujících modulů,
- výborná podpora mnoha databází,
- podpora XML,
- podpora LDAP,
- podpora aplikačních protokolů HTTP, FTP, SNMP, SMTP, IMAP, POP3, NNTP,
- podpora formátů PDF, dynamické generování obrázků
- a další

6.1.2 Databáze

Pro operační systém Linux existuje mnoho databázových produktů. Od produktů, uvolněných pod licencí GPL, až po porty databází komerčních firem jako Oracle, Sybase nebo IBM. S většinou z těchto databází umí jazyk PHP komunikovat. Nabídka databázových produktů pro Linux je opravdu velice široká.

Namátkou je možné zmínit následujících několik příkladů volně šiřitelných i komerčních databází pro Linux:

- *MySQL* – velmi rychlá databáze, často používaná pro jednodušší WWW projekty. Není vybavena takovou funkčností, jako jiné databáze, například nepodporuje vnořené selecty, transakce podporuje pouze nejnovější řada a podobně. Vyniká rychlostí a dobrou podporou češtiny, včetně například správného třídění znaku `ch`. Je uvolněna pod licencí, která umožňuje za splnění určitých podmínek použití zdarma.
- *PostgreSQL* – výkonná databáze s velkou funkčností. Má implementovánu značnou část normy SQL92 (SQL2) a dokonce část SQL3. Je vhodnější pro složitější projekty, podporuje transakce, triggery, vložené procedury. Je uvolněna pod licencí GPL.
- *Firebird* – nástupce Interbase dirmy Borland,
- *Oracle, Sybase, IBM DB2* – komerční databáze.

V malých organizacích a pro účely tvorby dynamických WWW stránek se nejčastěji využívají *MySQL* a *PostgreSQL*.

6.1.3 Konfigurace Apache

V této modelové situaci bude *Apache* sloužit jako WWW server organizace, pro dynamické stránky bude využíván jazyk PHP a jako databáze bude použit program *MySQL* (použití *MySQL* pro interní potřebu firmy spadá pod povolená užití, pro která není třeba zakoupit licenci). Je tedy třeba nakonfigurovat server *Apache* pro spolupráci těchto tří programů.

Konfigurační soubor *Apache* se většinou nachází v adresáři `/etc/apache` a jmenuje se `httpd.conf`. V tomto adresáři se nachází více souborů, ve starších verzích emphApache byla konfogurace rozprostřena do několika souborů, ale již několik let je uložena pouze v souboru `httpd.conf`. Tento soubor již jakousi základní konfiguraci obsahuje, uvedu zde tedy jen několik nejdůležitějších nastavení.

```
ServerType standalone
```

Je možné zvolit dva základní módy provozu serveru. Mód `standalone` znamená, že *Apache* je spuštěn při startu a běží po celou dobu chodu počítače (nezávisle na tom, zda k němu někdo přistupuje nebo ne). Druhým módem je `inetd`, který znamená, že *Apache* je spouštěn pouze ve chvíli, kdy přijde požadavek, v ostatních chvílich není v paměti přítomen. Mohlo by se zdát, že mód `inetd` je lepší, ale není tomu tak. *Apache* vyžaduje při spuštění určitý čas, takže pokud bude spouštěn pouze při příchodu dotazu, dojde ke zpoždění při vyřízení dotazu. Takže tento mód se hodí pouze na server, kde není vyžadována rychlá odezva a dochází pouze k několika přístupům denně. V opačném případě není možné tento mód doporučit.

```
DocumentRoot "/var/www/wwwroot"
```

Jedno z nejdůležitějších nastavení – popisuje, ve kterém adresáři je uložen WWW strom serveru, tedy vlastní WWW stránky.

```
User nobody
Group nobody
ServerAdmin webmaster@organizace.cz
ServerName www.organizace.cz
```

Další nastavení říkají, s právy jakého uživatele má WWW server pracovat. Většinou se *Apache* startuje s právy uživatele `root`, což je nutnost, pokud má pracovat na standardním portu 80, ale tato práva nepředává svým potomkům, kteří vyřizují dotazy. Tito potomci by měli běžet s právy uživatele, který má v systému minimální oprávnění. Tentop uživatel se většinou jmenuje `nobody`. Je to důležité proto, že v programu *Apache* může být chyba, kterou by mohl útočník využít k získání práv uživatele `root`. Takto získá práva uživatele `nobody` (tedy téměř žádná práva). Položka `ServerAdmin` oznamuje, kdo je správcem tohoto WWW serveru. Adresa je vypsána do odpovědi v případě, že server vyprodukuje nějaké chybové hlášení, a klient poté ví, koho má kontaktovat pro odstranění problému. `ServerName` je použito ve chvíli, kdy se má server hlásit jiným jménem, než je jeho primární jméno (tedy jméno, které má nastavené v konfiguraci sítě a které na něj ukazuje v DNS). Je to případ tohoto serveru, který se jmenuje `server.organizace.cz`, ale měl by se hlásit jako `www.organizace.cz`.

Následují nastavení portů a adres, pomocí kterých bude server dostupný. WWW server je většinou očekáván na portu 80, za určitých okolností je možné použít i jiný port (pak je ale třeba počítat s tím, že klientům bude nutné spolu s adresou serveru sdělit i port). Direktivy `BindAddress` a `Listen` jsou potřeba až při pokročilejších nastaveních, kdy má server poslouchat na více portech nebo jen na určitých IP adresách, proto jsou nyní zakomentované (předřazením znaku `#`). V případě potřeby pokročilejší konfigurace je vše podrobně popsáno v manuálu serveru *Apache*.

```
Port 80
#BindAddress *
#Listen 8080
#Listen 111.112.113.114:81
```

Zajímavým parametrem je `DirectoryIndex`. V případě, že klient bude požadovat nikoliv stránku (například `http://www.organizace.cz/prodej.html`), ale adresář bez určení jména souboru (`http://www.organizace.cz/prodej/`), zjistí *Apache*, zda se v adresáři nenachází soubor `index.php` nebo `index.html`. Pokud ano, zobrazí jej, pokud ne, provede akci, která

je závislá na dalších nastaveních. Nastavení je „obaleno“ v podmínce, která jej aplikuje pouze v případě, že je nainstalován příslušný modul (`mod_dir.c`) – viz. dále.

```
<IfModule mod_dir.c>
    DirectoryIndex index.php index.html
</IfModule>
```

Silnou stránkou *Apache* je kontrola přístupu a omezení oprávnění. Oprávnění je možné definovat na úrověň jednotlivých adresářů nebo souborů. Následující kousek konfigurace je vypůjčen ze standardní instalace serveru a nastavuje pro hlavní adresář počítače (nikoliv hlavní adresář WWW stromu) poměrně restriktivní politiku. Umožňuje pouze následovat symbolické odkazy a neumožňuje upravit oprávnění pomocí souborů `.htaccess`. Soubor `.htaccess` se používá k úpravě oprávnění na bázi jednotlivých adresářů. Konfigurace uložená v tomto souboru je platná pouze pro adresář, ve kterém je tento soubor umístěn. Parametr `AllowOverride` říká, která nastavení mohou být v tomto souboru změněna oproti nastavení v konfiguračním souboru `httpd.conf`. `None` znamená, že žádná.

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>
```

Níže jsou nastavení pro adresář, ve kterém je uložen hlavní strom WWW serveru (opět použita snandardní nastavení). Volba `Indexes` povoluje vygenerování seznamu souborů v adresáři v případě, že neexistuje soubor definovaný v `DirectoryIndex` a klient zadal adresu adresáře. Volba `MultiViews` je použitelná pro výběr nejvhodnějšího souboru na základě preferencí klienta, které byly předány v dotazu (může se jednat například o jazykovou verzi stránky). Položky `Order`,`Allow` a `Deny` nastavují přístupová práva podle IP adresy nebo jména počítače (domény) klienta.

```
<Directory "/var/www/wwwroot">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

Podobnou direktivou jako `Directory` je i direktiva `Location`. Používá se stejným způsobem, má stejnou syntaxi, rozdíl je v tom, že `Directory` je uváděn z hlavního adresáře, zatímco `Location` z adresáře `DocumentRoot`. Direktiva `Files` platí ne na adresáře, ale na soubory.

Další volby ovlivňují výkon WWW serveru. Jejich správné nastavení může výrazně ovlivnit počet obsloužených požadavků za časovou jednotku. Server *Apache* spouští při startu několik potomků. Každý potomek obsluhuje v jednu chvíli jednoho klienta. V případě, že se právě nepřipojil žádný klient, je potomek nevytížený a čeká (pokud jich je spuštěných více, přebyteční jsou ukončeni). Volba `StartServers` nastavuje počet potomků spuštěných při startu serveru, `MaxClients` maximální počet současně spuštěných potomků – pokud bude v jednom okamžiku klientů víc než je hodnota `MaxClients` budou nadbyteční klienti odmítnuti, spojení se nezdaří. `MinSpareServers` a `MaxSpareServers` určují minimální a maximální počet spuštěných nevyužitých klientů. Server *Apache* se bude snažit udržovat počet nevytížených potomků v tomto intervalu. Hodnota `MaxRequestsPerChild` určuje, kolik klientů jeden potomek postupně obslouží, než dojde k jeho ukončení a spuštění nové kopie potomka. Tato hodnota má význam v případě, že by se v serveru vyskytovala nějaká chyba alokace paměti, díky které by postupně ropstla paměť obsazená jedním potomkem. Hodnota 0 znamená „neomezeně".

```
MinSpareServers 5
MaxSpareServers 10
StartServers 5
MaxClients 150
MaxRequestsPerChild 0
```

Tyto hodnoty jsou velmi důležité, jejich volba zásadně ovlivňuje výkon serveru:

- Příliš nízko položená hodnota `MaxClients` může u zatížených serverů způsobit odmítání spojení přespočetným klientům
- Příliš vysoko položená hodnota `MaxClients` může vyčerpat paměť a zpomalit server odkládáním do odkládacího prostoru (*swap*), v krajním případě může dojít k havárii vlivem nedostatku paměti – to ovšem znamená, že hardware serveru je vzhledem k zátěži poddimenzovaný
- Nízká hodnota `MinSpareServers` a `MaxSpareServers` zdržuje vyřizování požadavků při příchodu většího počtu požadavků najednou – musí se startovat noví potomci, kteří již mohli být nachystaní v paměti
- Vysoká hodnota `MinSpareServers` a `MaxSpareServers` zabírá místo v paměti nepotřebnými nevyužitými potomky

Je třeba říci, že neexistují *univerzální* hodnoty. Správné hodnoty nastavení se vždy odvíjejí od konkrétního zatížení konkrétního serveru. Jiné hodnoty budou pro server malé sítě a jiné pro velký server ISP. Pro málo zatížené servery jsou uvedené hodnoty zřejmě postačující.

Každý uživatel, který má na serveru založen účet (například pro příjem pošty – viz kapitola o elektronické poště), může mít i své domácí stránky. Tyto stránky uloží do svého domácího adresáře, do podadresáře, jehož jméno je uvedeno v direktivě `UserDir`. Tyto stránky pak budou přístupné na adrese `http://www.organizace.cz/~jmeno_uzivatele/` (například `http://www.organizace.cz/~hroza/`). Je nutné mít správně nastavená práva do domácího adresáře a práva tohoto adresáře, aby *Apache* mohl k těmto souborům přistupovat (přinejmenším právo `x` pro uživatele `nobody` – respektive *others* – v domácím adresáři a `rx` v adresáři `public_html`). Direktiva je opět obalena podmínkou, která ji aplikuje pouze v případě, že je zaveden příslušný modul – ne vždy je žádoucí, aby všichni uživatelé mohli volně publikovat své stránky na firemním serveru.

```
<IfModule mod_userdir.c>
    UserDir public_html
</IfModule>
```

Již jsem se zmínil o souboru `.htaccess`. Direktiva `AccessFileName` definuje název souboru, který bude použit pro nastavení v adresáři, dále je vhodné pomocí `Files` omezit přístup k tomuto souboru (může obsahovat neveřejné informace) prostřednictvím WWW serveru. Regulární výraz `"^\.ht"` je platný i pro soubor `.htpasswd` do kterého se ukládají hesla pro HTTP autentifikaci.

```
AccessFileName .htaccess
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
</Files>
```

6.1.4 Moduly

Již několikrát byly zmíněny moduly. Modul je samostatná jednotka, která rozšiřuje funkčnost serveru *Apache*. Některé konfigurační direktivy uvedené výše závisí na zavedení příslušných modulů. Ve standardní instalaci serveru *Apache* je dodáno několik desítek modulů a existují další moduly od jiných dodavatelů. Moduly se zavádějí pomocí direktiv `AddModule` a `LoadModule` v závislosti na tom, v jaké formě je modul dodáván.

Pro zprovoznění PHP se serverem *Apache* je třeba do konfiguračního souboru přidat následující sekci:

```
LoadModule php4_module libexec/libphp4.so
AddModule mod_php4.c
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
```

První dva řádky přidávají modul pro PHP do konfigurace, třetí řádek říká, že soubory s příponou `.php` jsou PHP skripty (nastavuje MIME typ)a čtvrtý řádek, který není nutný (často je dokonce nežádoucí), umožňuje u souborů s příponou `.phps` zobrazit formátovaný výpis programu. Dále je nutné správně nastavit PHP (soubor `php.ini`) a *MySQL*. Tím se však již nebudu zabývat.

6.1.5 Virtuální servery

Server *Apache* podporuje takzvané *virtuální servery*. To znamená, že na jednom fyzickém počítači je umístěno několik různých serverů s různými názvy. Například pokud má organizace více poboček a chce pro každou z nich mít „jiný" server, může mít virtuální servery `http://liberec.organizace.cz` a `http://jablonec.organizace.cz`, ačkoliv oba jsou fyzicky umístěny na jednom serveru. Obě doménová jména musí pochopitelně v DNS směřovat na `www.organizace.cz` (stačí záznam `CNAME`).

Soubor `httpd.conf` obsahuje mnoho dalších voleb, ale není účelem tohoto textu popsat je všechny. Součástí každé instalace *Apache* je vyčerpávající manuál ve formátu HTML a ten je možné použít pro další konfiguraci.

6.2 Služba FTP

V minulosti měla služba FTP značný význam, pomocí FTP se distribuovaly soubory, avšak v dnešní době bylo FTP ve značné míře nahrazeno uživatelsky přítulnějším WWW. Přesto si FTP servery stále udržují poměrně velkou popularitu. Přístup pomocí FTP se dá rozdělit na dvě základní skupiny:

1. přístup pro „řádné" uživatele – každý uživatel má své uživatelské jméno a heslo, kterým se přihlásí k serveru a na základě jeho identity a přístupových práv je mu umožněn zápis nebo čtení (nebo nic, nebo oboje). Často se používá například u *webhostingů*.

2. přístup pro anonymní uživatele – uživatel nemá na serveru, ke kterému se připojuje, účet a připojuje se s univerzální identitou `ftp` nebo `anonymous`. Jako heslo používá svou e-mailovou adresu. Tento systém se často používá pro distribuci software nebo jiných souborů, uživatelé mívají přístup pouze pro čtení, výjimečně existuje adresář pro zápis.

Programů, které mohou sloužit jako servery FTP je mnoho, namátkou je možné jmenovat *wu-ftpd* nebo *proftpd*. U každého z nich by se našlo mnoho odpůrců i zastánců, kteří by do krve přesvědčovali druhou skupinu, že právě oni mají pravdu. Oba programy se dodávají se základním konfiguračním souborem, jehož syntaxe je vcelku pochopitelná a nastavení je funkční ihned „vybalení z krabice". Zmíním zde tedy jen nejzákladnější možnosti nastavení (bez konkrétní syntaxe).

Zřejmě nejvíce nás bude zajímat anonymní přístup, který je možno použít pro distribuci souborů.

V obou výše zmíněných programech je mozné nastavit:

- soubor, jehož obsah se zobrazí při přihlášení k FTP serveru (`welcome.msg`),
- soubor, jehož obsah se zobrazí při vstupu do adresáře (`.message`)
- počet anonymních klientů, kteří mohou být připojeni v jednom okamžiku
- server *wu-ftpd* může dokonce dělit přístupy do skupin podle času nebo IP adresy a jednotlivým skupinám povolovat různý počet současných připojení
- oprávnění k souborům v FTP stromu
- nastavení adresáře pro *upload* souborů
- virtuální FTP servery (stejná funkčnost jako u virtuálních WWW serverů

Někdy je žádoucí, aby anonymní uživatelé měli možnost přispívat svými soubory na FTP server. K tomu slouží adresář, který se většinou jmenuje `uploads` a do tohoto adresáře mohou uživatelé zapisovat soubory, které chtějí předat na FTP server. Tento adresář je však pouze pro zápis, čtení není uživatelům umožněno, je nežádoucí, aby jeden anonymní uživatel mohl na server cokoliv nakopírovat a druhý anonymní uživatel mohl tento soubor stáhnout. Server by se brzy stal distribučním centrem. Proto mohou uživatelé do adresáře `uploads` pouze zapisovat, číst může pouze správce serveru, který po inspekci může soubor přesunout do jiné – čitelné – části FTP stromu.

7 Elektronická pošta

Elektronická pošta je bezpochyby nejvyužívanější službou Internetu. Bude jistě využívána v každé společnosti, která je k Internetu připojena. Elektronická pošta je název služby, ale v podstatě se jedná o skupinu mnoha samostatných služeb, které mohou zahrnovat:

- odesílání a příjem elektronické pošty protokolem SMTP
- čtení elektronické pošty pomocí protokolů IMAP a POP3
- WWW klienta elektronické pošty
- další pokročilé schopnosti
  - antivirová ochrana před viry a makroviry v přílohách
  - ochrana před nevyžádanou poštou – spamem

V dnešní době se stále více využívají takzvaná *groupware* řešení. *Groupware* je programové vybavení, které umožňuje dvěma a více lidem navzájem komunikovat, kooperovat na společném díle a koordinovat své aktivity. Groupware zahrnuje následující činnosti:

- *Komunikace* – výměna zpráv, požadavků, instrukcí (elektronická pošta, videokonference, chat, instant messaging)
- *Kooperace* – práce nad společnými dokumenty (úložiště dokumentů a sledování přístupu k dokumentům)
- *Koordinace* – vzájemné sladění činností (plánování času, schůzek, přehled o úkolech, plánování zdrojů)

Tyto aplikace jednak usnadňují týmovou spolupráci díky snadnému přístupu ke společným informacím a výkonným komunikačním prostředkům, ale vedou také často k organizačním změnám. Podporují spolupráci lidí, kteří jsou geograficky rozptýleni, vedou ke zploštění hierarchické organizační struktury, k delegování pravomocí na pracovní týmy a zvyšují produktivitu práce těchto týmů.

Těchto balíků existuje velké množství, jmenovitě například z největších hráčů Microsoft Exchange Server a Lotus Notes. Z menších společností je velmi známou firma Kerio, která vyvinula Kerio Mail Server a další.

7.1 Microsoft Exchange Server

Pro operační systém Windows existuje několik poštovních balíků. Jako první je třeba jmenovat systém Microsoft Exchange, což není pouze poštovní server, ale kompletní *groupware* řešení.

Základní schopnosti *Microsoft Exchange Serveru* jsou tyto:

- odesílání a příjem elektronické pošty pomocí protokolu SMTP
- čtení elektronické pošty pomocí protokolů POP3 a IMAP
- WWW klient elektronické pošty – Outlook Web Access
- přístup z mobilních zařízení
- šifrování spojení
- kalendář
- adresáře kontaktů
- plánovač schůzek, úkolů, zdrojů
- úložiště dokumentů (veřejné složky) s přístupovými právy
- plná integrace do bezpečnostního modelu Windows
- možnost clusterování serverů pro velký výkon
- zálohování a replikace obsahu
- anti-spam funkce (autentizace před odesláním)
- antivirové rozhraní
- blokování příloh
- distribuční seznamy, konference
- grafické rozhraní pro konfiguraci a správu

Systém Microsoft Exchange Server je zřejmě nejrozšířenější mailový a groupware server na platformě Windows, díky tomu, že je dodáván jako součást balíku *Microsoft Small Business Server*. Je škálovatelný až do řádově tisíců uživatelských účtů.

7.2 Kerio Mail Server

Pro plnění funkce serveru elektronické pošty existují pro operační systém Windows i jiné produkty, za všechny je možné zmínit například *Kerio Mail Server*. Tento produkt existuje i pro operační systém Linux, kde je podporován výrobcem v distribuci RedHat. Mezi nejdůležitější vlastnosti patří:

- odesílání a příjem elektronické pošty pomocí protokolu SMTP

- čtení elektronické pošty pomocí protokolů POP3 a IMAP
- WWW klient elektronické pošty, WAP klient
- adresáře kontaktů
- šifrování spojení
- anti-spamové funkce (autentizace před odesláním)
- antivirová kontrola, blokování příloh
- e-mailové konference
- spolupráce s bezpečnostním modelem Windows
- zálohování pošty
- grafické rozhraní pro konfiguraci a správu

Jedná se o jednodušší řešení, než v případě výše zmíněného Microsoft Exchange Serveru, proto je tento server často nasazován v malých společnostech, které nechtějí investovat do Exchange, neboť nevyžadují plnou funkcionalitu Exchange. Výhodou je (i v případě Linuxového řešení) grafické rozhraní pro konfiguraci a správu – narozdíl od většiny Unixových programů, které se konfigurují editací textových souborů.

7.3 Produkty pro Linux

Kromě produktu Kerio Mail Server, který byl zmíněn v předchozí části, existuje pro operační systém Linux několik dalších groupware balíků. Většina z nich není komplexním řešením, jako v případě Exchange nebo Notes, které implementují vše dohromady (SMTP server, POP3 server, IMAP server, groupware funkce), ale jedná se o groupware nadstavbu, která vyžaduje určité programy již nainstalované. Jmenovitě se jedná o SMTP server, POP3 nebo IMAP server, které musí být nainstalovány nezávisle na groupware balíku, který společnost hodlá použít.

7.3.1 Servery pro elektronickou poštu

V první řadě je tedy nutné nainstalovat programy pro elektronickou poštu:

- server elektronické pošty – pro odesílání nebo příjem elektronické pošty
- POP3 server nebo IMAP server – pro přístup k poště z pracovních stanic
- WWW rozhraní elektronické pošty

Serverů elektronické pošty existuje velké množství, nejznámější univerzální balíky jsou *Sendmail*, *Postfix* a *Qmail*.

Balík *Qmail* byl velice oblíbený pro vysoký důraz, který kladl na bezpečnost, v současné době již však není dále vyvíjen. *Sendmail* je veterán podobně jako program *Bind*. Je velmi flexibilní a robustní, v minulosti se však vyznačoval velkým počtem bezpečnostních problémů (stejně jako program *Bind*). V nových verzích se bezpečnost výrazně zvýšila. Dalším problémem byla nepřehledná konfigurace, té je možné se vyhnout použitím předpřipravených konfiguračních „kousků", které jsou „lepeny" dohromady jednoduchým konfigurátorem. Sendmail se vyznačuje obrovskou konfigurovatelností, která umožňuje jeho nasazení v nejrůznějších prostředích.

Postfix je rychlý, jednoduše spravovatelný a bezpečný server elektronické pošty, který se snaží být co nejvíce funkčně srovnatelný s programem *Sendmail*. Má mnoho pokročilých vlastností, včetně filtrování, spolupráce s externími programy (anti-spam, antiviry a podobně). Rozhodnutí, který program použít záleží na každém správci. Každý server má své výhody a nevýhody, pro běžné použití jsou oba vcelku funkčně srovnatelné. Neexistuje univerzální odpověď na otázku, který z nich zvolit, na toto téma se pravidelně vedou vzrušené diskuze v mnoha diskusních listech.

7.3.2 POP3 a IMAP servery

Dalším nutným programovým vybavením je POP3 server a IMAP server. Tyto programy umožňují „stažení" příchozí pošty ze serveru na pracovní stanici uživatele. Protokol POP3 je starší a jednodušší, pouze stáhne poštu na pracovní stanici, kde si ji uživatel může přečíst. Novější protokol IMAP je sofistikovanější, umožňuje pracovat s poštou i na serveru, bez toho, aby všechnu poštu stahoval uživatel na pracovní stanici. Zprávy je možné mazat či přesouvat přímo na serveru, na pracovní stanici se do poštovního klienta zasílají jen potřebné informace – odesílatel, předmět, a pouze pokud chce uživatel zprávu přečíst, tak obsah zprávy.

Existuje velké množství POP3 a IMAP serverů, zpravidla se alespoň jeden nachází v distribuci. Liší se podporou jednotlivých serverů elektronické pošty (existují jiné servery pro *Qmail* a pro ostatní) a podporou různých protokolů (např APOP3 – šifrované POP3). Mezi nejznámější patří *Qpopper*, *cucipop*, *Cyrus-IMAP*, *Courier IMAP* a IMAP server z Washingtonské univerzity.

7.3.3 Antiviry, anti-spam

V dnešní době je výhodou, pokud server elektronické pošty podporuje inspekci obsahu zpráv. Jedná se konkrétně o dva dnes velice rozšířené problémy: viry a *spam*. Téměř každý týden se objeví nový virus a například makroviry pro klienta elektronické pošty Microsoft Outlook se často aktivují jen tím, že si uživatel zobrazí náhled zprávy. Nevyžádaná pošta je také velký problém, určitě již každému přišel některý z proslulých „nigerijských dopisů". Proto je vhodné

viry i spam detekovat co nejdříve a nedovolit, aby pronikly až na pracovní stanici uživatele (spam obtěžuje, viry se množí a mohou i ničit). Všechny zmíněné poštovní servery (*Sendmail*, *Postfix* i *Qmail*) podporují spolupráci s externími antivirovými programy a programy pro filtraci spamu.

Pro Linux existuje několik antivirových programů, použitelných na serveru elektronické pošty. Tyto programy oplývají funkcemi stejnými jako jejich protějšky pro Windows, obsahují jak serverovou, tak klientskou část. Antivirové programy pro poštovní server by měly mít přinejmenším následující vlastnosti:

- kontrola příchozí pošty (naprostá nutnost)
- kontrola odchozí pošty
- definice akcí při zjištěné infekci
  - oznámení o infekci
  - možnost smazání infikované zprávy
  - přesun zprávy do karantény a možnost manuální reakce správce
- častá aktualizace virových databází
- jednoduchá správa

Princip instalace antivirového programu na server elektronické pošty je poněkud netradiční. Většinou je nutné nainstalovat program, který umí spolupracovat s poštovním serverem a na tento program se poté napojí jako externí filtr antnivirový program (podobným způsobem často pracují i anti-spamové programy). Takovými programemy jsou například *AMaVis*, *MessageWall*, *Anomy Sanitizer*

Nejznámějšími antiviry pro Linux, které mohou plnit i funkci antivirové programu na poštovním serveru, jsou:

- *NOD32* – `http://www.eset.sk`
- *McAfee Antivirus* – `http://www.mcafee.com`
- *Sophos Antivirus* – `http://www.sophos.com`
- *ClamAV* – `http://www.clamav.org`, uvolněn pod licencí GNU/GPL
- *F-Prot* – `http://www.f-prot.com`
- *Panda Antivirus* – `http://www.pandasoftware.com`
- *RAV Antivirus* `http://www.rav.ro`, po akvizici firmy Microsoftem byl ukončen vývoj portu pro Linux

Další – v poslední době stále populárnější – funkcí je detekce a filtrace spamu. V tomto regionu ještě není objem nevyžádané pošty tak enormní jako například ve Spojených státech, kde připadá jedna nevyžádané zpráva na 3 až 5 regulerních, ale i zde se situace začíná pomalu zhoršovat. Jedním z nejlepších programů pro detekci a odstranění spamu je *SpamAssassin*. Tento program se vyznačuje implementací Bayesova filtru, který mu umožňuje učit se v průběhu činnosti z došlých zpráv. Po instalaci si začně budovat svou databázi a na základě zachycených zpráv upřesňuje rozpoznávací schopnosti.

7.3.4 WWW klienti

Součástí balíku *Microsoft Exchange Server* je také WWW klient elektronické pošty. Ačkoliv se zdá, že WWW klient na serveru je věc zcela zbytečná, pro některé případy může být výhodný. Hlavní výhodou aplikací s WWW rozhraním je jejich platformní nezávislost na straně klienta. Klientovi postačuje jakýkoliv prohlížeč (*browser*) k tomu, aby mohl přistupovat ke své poště. Nezávisí na tom, kde se uživatel nachází (může pracovat střídavě na několika počítačích, může používat několik operačních systémů), prostě se vždy přihlásí ke svému účtu ve WWW rozhraní a může pracovat se svou poštou. WWW klienti jsou funkčně srovnatelní s klasickými klienty elektronické pošty, podporují

- odesílání elektronické pošty, přeposílání, odpovídání
- příjem elektronické pošty
- práci s přílohami
- adresáře (seznamy kontaktů) – například i globální a soukromé
- práci se složkami
- kontrolu pravopisu

Důležitou vlastností všech klientských nástrojů, které mají být používány běžnými uživateli, je grafické rozhraní. Jeho přehlednost, intuitivnost, jednoduchost používání, a hlavně lokalizace. Je pohodlnější pracovat s programem, který je lokalizován do českého jazyka. To bude pravděpodobně jedním z hlavních požadavků na WWW klienta elektronické pošty.

Většina klientů podporuje pro příjem pošty protokol IMAP, některé i protokol POP3. Jako příklad je možné uvést dva rozšířené klienty:

- *SquirrelMail* – program je napsán v jazyce PHP, pracuje s protokolem IMAP (neumí POP3) a je lokalizován do češtiny
- *IMP* – také napsán v jazyce PHP, pracuje s protokoly POP3 a IMAP (při práci pomocí protokolu POP3 je díky jednoduchosti protokolu omezena jeho funkčnost v manipulaci se složkami) a je také lokalizován do češtiny

Nutným předpokladem pro použití těchto klientů je funkční IMAP server. Některé balíky neobsahují pouze podporu elektronické pošty, přidávají další funkce, známé spíše z oblasti *groupware* systémů.

7.3.5 Groupware

Program *Microsoft Exchange Server* není jen obyčejným poštovním serverem, integruje v sobě i funkce pro týmovou spolupráci. Společnosti mohou požadovat podobnou funkcionalitu i po přechodu na operační systém Linux. Bohužel *Microsoft Exchange Server* nebyl zatím představen ve verzi funkční i v Linuxu :-), proto bude nutné vybírat z alternativních řešení. Pro operační systém Linux jich existuje několik. Dají se rozdělit v zásadě na dvě skupiny – na komerční balíky a balíky uvolněné pod některou „open source" licencí.

Mezi balíky z první skupiny je nutné v první řadě uvést kompletní groupwarové řešení firmy IBM (původně Lotus) *Lotus Notes/Domino*. Jedná se o kompletní balík, který svými funkcemi dokonce přesahuje schopnosti *Microsoft Exchange Serveru*. Je to ale řešení, které bude pro většinu malých a středních společností zbytečné robustní a nákladné. Existují však i další:

- *DeskNow Mail nad Collaborative Server* – kompletní groupware řešení, základní verze je zdarma (bez zdrojových kódů), za rozšířenou verzi s plnou funkčností se platí. Základní verze přidává do textu elektronické pošty poznámku o verzi.
- *OpenGroupware* – také existuje verze zdarma i komerční, záleží na předpokládaném využití.

V oblasti *Open Source* groupware produktů převažují systémy v jazyce PHP. Jejich vlastnosti se liší, každý program je zaměřen trochu jiným směrem, každý má své výhody a nevýhody. Z mnoha, které existují, je toto pouze výběr:

- *PHPgroupware* – `http://www.phpgroupware.org`, zřejmě nejznámější, nejkomplexnější balík
- *PHProjekt* – `http://www.phprojekt.com`
- *NullLogic Groupware* – `http://nullgroupware.sourceforge.org`
- *Sherpath* – `http://www.sherpath.org`
- *TUTOS* – `http://www.tutos.org`
- *TWIG* – `http://twig.screwdriver.net`

7.3.6 Závěr

Ve světě Unixu (a tedy i Linuxu) je preferováno použití malých, jednoúčelových programů, které spolupracují, před velkými, univerzálními, monolitickými programy typu „vše v jednom“. Z tohoto důvodu se konfigurace poštovního serveru sestává z konfigurace několika samostatných programů. Tento přístup má samozřejmě své výhody i nevýhody.

Výhodou je, že správce si může z velkého portfolia programů pro daný účel vybrat program, který nejlépe vyhoví jeho požadavkům a bude mu vyhovovat. Je možné kombinovat různé programy s různou funkčností. Nevýhodou je, že žádné dva systémy nebudou zcela stejné, a že pro dosažení plné funkčnosti a spolupráce je nutné konfigurovat několik samostatných programů.

S rostoucí oblibou Linuxu roste množství aplikací, které jsou na Linux portovány z jiných prostředí a mezi tyto aplikace patří i komplexní programové balíky „vše v jednom“ (typickým příkladem je Lotus Notes/Domino).

8 Zabezpečení sítě

V dnešní době je nutné, aby každý počítač, který je připojen k síti Internet, byl odpovídajícím způsobem zabezpečen. Internet je „divoká zóna", ve které se pohybuje obrovské množství lidí, přičemž někteří z nich využívají celosvětové sítě i k nekalým praktikám. Protože Internet je schopen propojit miliardy lidí z celého světa, je třeba být připraven na každou – i tu nejméně pravděpodobnou – situaci. Je tedy nutné počítač přiměřeně zabezpečit.

Existuje několik možných ohrožení:

- Počítač může být napaden s úmyslem odcizit data
- Počítač může být napaden s úmyslem zničit data
- Počítač může být donucen, aby odepřel službu, to znamená, že útočník nezíská data, nezíská je však ani nikdo jiný – včetně těch, kteří by je měli získat
- Počítač může být skrytě napaden a později využit jako základna pro další útok

V bezpečí nejsou ani domácí stanice, které se k Internetu připojují pouze na omezenou dobu. I v této omezené době je možné jejich počítač napadnout. Operační systémy Windows (zejména systémy pro pracovní stanice, jako Windows 95 nebo Windows98) jsou ve své standardní instalaci naprosto nezabezpečené a umožňují připojení k této stanici v podstatě komukoliv a odkudkoliv – včetně přístupu odkudsi z Internetu.

Každý operační systém má nějakou chybu. Mnoho těchto chyb je veřejně známých a existují programy, které těchto chyb využívají pro průnik do počítače – takzvané *exploity*. Mnohé z těchto chyb je možné zabezpečit tak, že útočníkovi nedáme šanci této chyby využít, například tak, že zakážeme přístup ke službě, která je postižena. Počítač, který není zabezpečen, je velice snadno napadnutelný. Naproti tomu počítač, který nemá chybu opravenu (například proto, že oprava neexistuje, nebo proto, že se nejedná o chybu, ale o „feature"), ale zablokoval přístup k chybě, je zabezpečen nepoměrně lépe.

Počítačová bezpečnost je velmi široký obor, který není možné popsat na několika stránkách. Proto tento přehled není ani v nejmenším vyčerpávající. Zabezpečení počítače je možné rozdělit na několik relativně samostatných skupin:

- Aktualizace systému – odstraňování nalezených chyb
- Výběr vhodných aplikací a jejich vhodná konfigurace
- Ochrana před neoprávněným přístupem – *firewall*
- Ochrana před útoky DOS (*Denial of Service* – odepření služby)
- Antivirová ochrana

Výčet není zdaleka kompletní, ale postačuje pro hrubou představu toho, co je třeba udělat pro zvýšení bezpečnosti počítače připojeného k Internetu.

8.1 Aktualizace systému

Aktualizace systému je velmi důležitá součást bezpečnostní politiky. JAk již bylo řečeno, každý operační systém (respektive každý program – podle Murphyho obsahuje chybu každý program delší než 100 řádků) obsahuje chyby. Tyto chyby jsou postupně odhalovány a opravovány. Většinou se jedná o jakýsi „souboj" v rychlosti mezi těmi, kteří chyby opravují a těmi, kteří chyby zneužívají. Je objevena chyba, na tuto chybu se rychle objeví *exploit*, po určité době se objeví aktualizace. Po nějaké době je objevena další chyba a tak dále.

Každá firma, která produkuje operační systémy, má vyvinutu metodiku pro aktualizaci systému. Důležité je:

- Jak rychle po objevení chyby je k dispozici oprava
- Jaké úsilí je třeba pro nalezení opravy
- Jak dlouho firma podporuje operační systém (například již skončila podpora operačního systému Windows 95, nové opravy pro tento systém již nejsou uvolňovány)
- Jaké úsilí je třeba pro instalaci opravy

Reakční doba na objevení nové chyby je velice důležitým parametrem. Velmi často dochází k objevení chyby týmem, který se specializuje na tvorbu *exploitů*. Tento tým tedy zároveň s objevením chyby vytvoří program, který chyby zneužívá pro průnik do systému. Dnes je na Internetu zcela běžné, že narušení počítačů se šíří lavinovitě (viz. například BugBear) a během několika hodin může zaplavit celý Internet. Proto je nutné reagovat na vzniklé nebezpeči rychle.

V minulosti firma Microsoft nevynikala rychlou reakcí na objevené chyby, její politika byla zaměřena na vydávání balíků mnoha oprav dohromady například jednou za půl roku (takzvaný *Service Pack*). Dnes je situace jiná, firma Microsoft vydává jak opravy jednotlivých chyb, tak i souhrnné *Service Packy*, které sdružují všechny opravy, které byly uvolněny samostatně v průběhu předchozích několika měsíců.

Jednotlivé distribuce operačního systému Linux mají také vypracovánu metodiku aktualizace systému. Reakční doba je individuální, zpravidla několik hodin až (maximálně) několik dní. Na bezpečnost je v Linuxu kladen velký důraz, proto je snahou výrobců jednotlivých distribucí, aby reakční doba byla co nejkratší.

Aby bylo možné opravu nainstalovat, musí správce systému vědět, že nějaká chyba a oprava na ni existuje. Proto výrobci operačních systémů zveřejňují seznam odhalených chyb a oprav například na WWW stránkách. Operační systém Windows má v sobě integrovánu

službu *Windows Update*, která kontroluje, zda neexistují na WWW serveru firmy Microsoft nové opravy a nabízí jejich stažení a instalaci. Správce tedy nemusí na Internetu složitě hledat popisy chyb a oprav, ale má vše připraveno. Podobný systém využívají i výrobci distribucí Linuxu. Na svých WWW stránkách zveřejňují nalezené chyby a jejich opravy. Součástí většiny distribucí je také systém pro stahování a instalaci jednotlivých oprav.

Velmi důležitým ukazatelem pro správce systému je, jak dlouho výrobci podporují svůj operační systém. Instalace serveru je činnost, která se neprovádí každého půl roku, jak firmy uvolňují nové verze svých operačních systémů, server prostě funguje s nainstalovanou verzí tak dlouho, dokud nainstalovaný systém splňuje požadavky. Navíc upgrade serveru není jednoduchá a bezproblémová záležitost. Měly by být tedy preferovány firmy, které podporují své operační systémy ještě minimálně několik měsíců po uvedení nové verze. Zde je třeba zmínit firmu RedHat, výrobce RedHat Linuxu, která pro neplatící zákazníky (zákazníky, kteří si nezakoupili produkt *RedHat Enterprise Server*, ale využili nabídku stažení zdarma z Internetu) ukončuje podporu zhruba půl roku po uvolnění. Pro účely malé firmy, která nechce platit téměř tisíc dolarů za licenci, proto bude diskutabilní, zda zvolit tuto distribuci.

Instalace opravy pro opravy zveřejněné přímo výrobcem je většinou jednoduchá. V operačním systému Windows dojde k instalaci automaticky po stažení systémem *Windows Update*. V operačním systému LInux výrobci připravují opravy tak, aby bylo možné opravu nainstalovat jednoduše balíčkovacím systémem, který jednotlivé distribuce podporují (*rpm*, *apt*,*dpkg*, *pkgtool*).

Je však třeba říci, že sebelepší systém aktualizace je dobrý pouze v případě, že je správcem správně využíván. Je smutnou skutečností, že mnoho systémů je napadnutelných i přesto, že na příslušnou chybu existuje již půl roku oprava, ale správce neaktualizuje svůj systém.

8.2 Výběr vhodných aplikací

Při zabezpečení systému je třeba dávat pozor i na firemní aplikace, které budou na serveru provozovány, zejména jedná-li se o aplikace napsané na zakázku. Není příliš platné mít skvěle zabezpečený server, na kterém poběží aplikace, vytvořená na zakázku pro konkrétní firmu, s fatální bezpečnostní chybou. Byla-li aplikace vyrobena na zakázku a jedná se například pouze o jednu instalaci aplikace, je pravděpodobné, že zpracoatelská firma se nebude příliš zabývat aktivním vyhledáváním chyb ve svém produktu a že chyba bude dřímat v aplikaci, dokud nebude objevena útočníkem. Proto je nutné pečlivě vybírat zpracovatelskou firmu a pečlivě zabezpečit, že aplikaci nemůže zneužít někdo nepovolaný.

8.3 Firewall

Jedním z bezpečnostních prvků, které by neměly chybět v žádném systému, připojeném k internetu, je *firewall*. *Firewall* je program, nebo zařízení, které sleduje síťový provoz a na základě daných pravidel povoluje nebo zakazuje přístup k prostředkům počítače. Nejčastějším

případem firewallu je firewall, který pracuje na čtvrté vrstvě TCP/IP a nazývá se *paketový* (paketová hráz, hradba...). Tento firewall filtruje provoz na základě informací v paketu (IP adresy odesílatele a příjemce, protokolu, portu odesílatele a příjemce, stav spojení a další nastavení vlastností paketu).

V operačním systému Windows 2000 a Windows XP je vestavěn jednoduchý (velmi jednoduchý) paketový firewall. Mnohem komplexnějším řešením je zakoupení produktu *Microsoft ISA Server*, který navíc k vlastnostem paketového firewallu přidává možnost využití *proxy caching* serveru.

Mezi nejdůležitější vlastnosti ISA serveru patří:[7]

- víceúrovňový firewall
- stavová filtrace
- široká podpora aplikačních protokolů
- integrovaná podpora VPN, NAT
- zvýšení zabezpečení systému
- integrovaná detekce narušení
- transparentnost pro všechny klienty
- rozšířená autentizace (pouze v sítích Windows)

Pro operační systém Linux existuje alternativa k ISA serveru. Nejedná se o jeden komplexní produkt, ale o kombinaci několika programů. Základním programem pro vytváření paketového firewallu je program *iptables* (respektive balík *Netfilter*).

Program *iptables* a balík *Netfilter* mají následující vlastnosti (v porovnání s ISA server):

- víceúrovňový firewall
- stavová filtrace
- integrovaná podpora NAT, VPN řešeno pomocí externích produktů
- zvýšení zabezpečení systému
- reporting narušení pravidel
- transparentnost pro všechny klienty
- modulární struktura

[7] Informace pocházejí z WWW stránek firmy Microsoft

- mnoho rozšiřujících modulů
- možnost velmi pokročilé konfigurace
- možnost konfigurace pro obranu před DOS

Základni rozhraní pro ovládání *iptables* je textové, provádí se pomocí příkazů `iptables`, `iptables-save`, `iptables-restore`. Existují uživatelské nástavby, nejrozšířenější jsou například *Shorewall* a *FWBuilder*, ty však nabízejí většinou jen omezenou (přesto bohatou) paletu funkcí. Pomocí textového rozhraní je možné ovládat všechny funkce programu *iptables*, včetně funkcí, které byly přidány díky modularitě systému (instalace těchto funkcí však často vyžaduje netriviální zásah do systému). Syntaxe příkazů je jednoduchá, navíc základní nastavení, které bude použitelné pro většinu společností, je poměrně jednoduché.

Pro ilustraci konfigurace je zde uvedeno jednoduché nastavení firewallu. Toto nastavení není vhodné do produkčního systému bez náležité analýzy a definice vlastních požadavků, je zde uvedeno pouze pro ilustraci. Pro konfiguraci reálného firewallu je nutné přesně definovat, jakým způsobem má firewall pracovat a připravit na míru vlastní sadu pravidel. NAstavení firewallu není činnost, která se dá provozovat bez rozmyslu,m jedná se o velmi důležité nastavení, které by bez náležité přípravy mohlo ponechat nebezpečné díry do systému.

```
iptables -A FORWARD -m state --state=INVALID -j DROP
iptables -A FORWARD -m state --state=ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state=NEW -i eth0 -j DROP
iptables -A INPUT -m state --state=ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p TCP --dport 80 -i eth0 -j ACCEPT
iptables -A INPUT -p TCP --dport 25 -i eth0 -j ACCEPT
iptables -A INPUT -p TCP --dport 53 -i eth0 -j ACCEPT
iptables -A INPUT -p UDP --dport 53 -i eth0 -j ACCEPT
iptables -A INPUT -p ICMP -i eth0 -j ACCEPT
iptables -A INPUT -m state --state=NEW -i eth0 -j DROP
```

Vzorová konfigurace předpokládá, že server je připojen do veřejné sítě Internet rozhraním (síťovou kartou), která je označena `eth0`. Toto označení v Linuxu znamená první síťová karta Ethernet. Parametr `-A` popisuje, na které pakety se vztahuje příslušné pravidlo. Řetězec `FORWARD` popisuje pakety, které daným počítačem pouze procházejí (například provoz z vnitřní sítě směrem do vnější sítě a obráceně), `INPUT` označuje pakety, určené přímo pro tento počítač. V sekci `FORWARD` je nastaven pouze stavový firewall, který blokuje (`DROP`) vadné pakety (`INVALID`), povoluje pakety, které patří k již navázaným spojením (`ESTABLISHED`, `RELATED`) a navazování nových spojení zakazuje z Internetu směrem do vnitřní sítě – v opačném směru není definována žádná politika, použije se tedy standardní `ACCEPT`. Pro spojení

přímo na server jsou povoleny pakety, které patří k již navázaným spojením, dále spojení na služby, které server poskytuje do Internetu (služba WWW – port 80/TCP, elektronická pošta – port 25/TCP, služba DNS – port 53/TCP a 53/UDP). Další nová spojení z Internetu jsou zakázána.

Je třeba poznamenat, že tato vzorová konfigurace byla vytvořena spíše pro názornost, než pro praxi. Není vhodné používat ji bez úprav, protože neřeší některé zásadní problémy. Například není žádným způsobem omezen přístup k serveru ze strany vnitřní sítě. Proto je třeba tuto ukázku chápat pouze jako příklad syntaxe programu `iptables` a východisko pro konfiguraci vlastního firewallu.

8.3.1 Rozšíření *iptables*

Obrovskou výhodou systému *iptables* (respektive *Netfilter*) je modularita. Díky dobře popsanému API je velice jednoduché přidávat k základnímu balíku další moduly, rozšiřující jeho funkčnost. Zajímavými moduly, které mohou být dobře použitelné, jsou například:

- `condition` – omezuje platnost pravidel na základě externích proměnných
- `connbytes` – omezení objemu dat v rámci jednoho spojení
- `connlimit`, `iplimit` – omezení maximálního počtu simultánních spojení
- `limit` – omezení maximálního počtu událostí za časovou jednotku, je možné použít proti DOS útokům
- `quota` – je možné omezit objem dat, který může být přenesen
- `recent` – umožňuje řadit počítače do skupin podle předchozího chování a uplatňovat pravidla na základě těchto skupin. Je možné použít pro detekci počítače, který se pokusil o neoprávněný přístup například k chráněnému portu a tomuto počítači poté nastavit speciální pravidla pro firewall.
- `string` – prohledává pakety na přítomnost textového řetězce
- `time` – omezení časového intervalu, ve kterém bude určité pravidlo platit

Tyto moduly jsou přímo součástí instalace *iptables*, mnoho dalších modulů je možné nalézt na Internetu od nezávislých vývojářů.

8.4 Aplikační proxy a proxy cache

Součástí ISA Serveru je také *proxy cache*. *Proxy cache* je vyrovnávací paměť, která schraňuje od klientů požadavky na WWW stránky (například), tyto požadavky za klienty vyřizuje a zároveň si ukládá stránky v sobě. V případě, že přijde znovu požadavek na stránku (respektive

na objekt, objekter může být HTML soubor, obrázek, jakýkoliv jiný soubor), která je již uložena, bude klientovi poskytnut objekt z vyrovnávací paměti a nebude navazováno spojení ke vzdálenému serveru. Celkovým výsledkem využití vyrovnávací paměti je urychlení přístupu k Internetu, zejména k často využívaným zdrojům. Dobře nastavená vyrovnávací paměť může v závislosti na běžném využití sítě ušetřit až 40 % přístupů (tím vlastně zrychlí linku).

I pro operační systém Linux existuje program pro plnění funkce vyrovnávací paměti. Jedná se o program *Squid* (*http://www.squid-cache.org*). Tento program má mnoho pokročilých vlastností, které jej povyšují nad obyčejnou vyrovnávací paměť, například:

- Spolupráce s externími programy (například externí autentizace)
- Možnost přesměrování na základě URL
- Mechanismus ACL pro omezování přístupu
- Omezování průtoku dat – je možné rezervovat pro jednotlivá oddělení určitou kapacitu linky
- Možnost hierarchické spolupráce několika serverů

9 Srovnání

Účelem této kapitoly je porovnat řešení serveru na bázi operačního systému Windows firmy Microsoft s řešením na bázi Linuxu. Pro účely výpočtu nákladů na pořízení systémů je třeba upřesnit popis společnosti, který byl nastíněn v úvodní kapitole na straně 13

Jedná se o společnost, ve které se nachází

- 1 server, plnící vyjmenované funkce
- 30 stanic propojených lokální sítí

Základní požadavky na funkci serveru jsou následující:

- souborový server
- tiskový server
- DHCP server
- DNS server
- WWW a FTP server
- server elektronické pošty
- firewall a vyrovnávací server

Cílovým stavem je definice pořizovacích nákladů, které může společnost očekávat, přičemž se rozhoduje mezi implementací operačního systému rodiny Windows (konkrétně *Microsoft Small Business Server*) a mezi operačním systémem Linux a příslušnými aplikacemi tak, jak byly popsány v předchozích kapitolách. Volba distribuce je vcelku irelevantní, rozdíly mezi distribucemi jsou důležité z technického, nikoliv z ekonomického hlediska. Výjimkou by mohla být distribuce SuSE, jejíž prodejní cena je v závislosti na verzi od cca 3 000 Kč do zhruba 30 000 Kč. Ale předpokládejme, že společnost si zvolila některou z distibucí, která je dodávána za cenu distribučních nákladů. V závěru bude provedeno krátké srovnání pro případ, že firma zvolí právě distribuci SuSE.

Při výpočtu nákladů budu vycházet z ceníku společnosti Autocont CZ, a.s., nebo z ceníků dodavatelů software. Ceny jsou bez DPH a platné ke dni 20. 12. 2003.

9.1 Pořizovací náklady na implementaci Windows

Vzhledem k současné nabídce produktů u distributorů budeme předpokládat, že společnost se rozhoduje mezi implementací *Microsoft Small Business Serveru* ve verzi 2003 a jakékoliv distribuce Linuxu. Jediné náklady, které je možné stanovit přesně, jsou náklady na pořízení programového vybavení. Náklady na instalaci, prvotní konfiguraci a provozní náklady není

možné stanovit bez detailní znalosti společnosti, jejích přesných a konkrétních požadavků. Dalšími nutnými náklady by byly poplatky servisní organizaci za instalaci a konfiguraci, je nutné znát přesnou hodinovou sazbu technika a časovou náročnost instalace. Oboje opět záleží na konkrétních požadavcích společnosti. Další možností samozřejmě je, že společnost provede instalaci a konfiguraci interně, v tomto případě je vyčíslení nákladů ještě složitější, je nutné vyčíslit hodinovou sazbu interního pracovníka a spočítat ztráty, které vzniknou tím, že pracovník se nemůže věnovat své práci a zabývá se instalací. Proto tyto náklady nebudu pro jednoduchost uvažovat a vyčíslím pouze náklady na pořízení potřebných licencí. Současně se *Small Business Serverem* bude pořizován antivirový program NOD32 pro systém Microsoft Exchange s aktualizací na 1 rok (nejbližší vyšší počet klientů je 50).

Rozpočet pro dosažení požadované funkčnosti je uveden v tabulce.

Windows SBS 2003 Standard + 5 CL	17 240 Kč
Windows SBS 2003 20 CL	55 673 Kč
Windows SBS 2003 5 CL	13 936 Kč
NOD32 pro MS Exchange, 50 CL, 1 rok	15 300 Kč
Celkem	**102 149 Kč**

Tabulka 1: Small Business Server 2003 Standard

K produktu *Microsoft Small Business Server* je nutné dokoupit ještě další klienské licence, základní balík obsahuje pouze 5 klientských licencí (5 současně připojených klientů). To tedy znamená, že za cenu 86 849 Kč dostane společnost licenci k provozování operačního systému na serveru a 30 klienstkých licencí. Ve společnosti se nachází 30 pracovních stanic, to tedy znamená, že v případě pořízení další stanice je nutné dokoupit další licence (nebo zařídit, aby k serveru přistupovalo dohromady maximálně 30 klientů). V případě, že by společnost vyžadovala (například pro chod své interní aplikace) databázový server, musí místo verze *Standard* zakoupit verzi *Premium*, která obsahuje SQL server (nebo zakoupit databázový server jiného výrobce). V tom případě se ovšem náklady změní (rozpočet pro verzi *Premium*):

Windows SBS 2003 Premium + 5 CL	42 988 Kč
Windows SBS 2003 20 CL	55 673 Kč
Windows SBS 2003 5 CL	13 936 Kč
NOD32 pro MS Exchange, 50 CL, 1 rok	15 300 Kč
Celkem	**127 897 Kč**

Tabulka 2: Small Business Server 2003 Premium

Ceny byly kalkulovány dle Autocont CZ, a.s. a Eset Software, spol.s r.o. (NOD32).

9.2 Pořizovací náklady na implementaci Linuxu

V případě implementace operačního systému Linux již není situace tak černobílá. V úvahu připadá několik scénářů. Pokusím se postupně vyčíslit některé z nich. Podotýkám, že vzhledem k nemožnosti vyčíslit další náklady se jedná pouze o pořizovací náklady. Skutečné náklady by byly navýšeny přinejmenším o srovnatelnou částku, jako v případě implementace Windows, pravděpodobně však o částku vyšší – vzhledem k náročnosti instalace a konfigurace, ať již časové nebo znalostní.

9.2.1 Řešení pouze pomocí volně šiřitelných programů

Náklady, které zde vstupují do hry, jsou náklady na pořízení distribuce Linuxu a náklady na antivirový systém. Náklady na pořízení distribuce Linuxu se pohybují řádově ve stokorunách.

Pořízení distribuce Linuxu	1 000 Kč
NOD32 pro Linux Mail Server, 50 CL, 1 rok	9 400 Kč
Celkem	**10 400 Kč**

Tabulka 3: Operační systém Linux

Při implementaci Linuxu nezáleží na počtu klientů, proto je cena za pořízení nezávislá na počtu připojených klientů. Počet klientů je důležitý v případě antivirového systému. Zde počet klientů znamená počet samostatných účtů elektronické pošty. Pro možnost srovnání byl zvolen stejný jako v případě implementace Windows. V porovnání s předchozí nabídkou je zřejmé, že z finančního hlediska je výhodnější implementace Linuxu v případě, že implementační náklady nepřesáhnou částku 91 749 Kč (respektive 117 497 Kč za verzi *Premium*).

9.2.2 Implementace Linuxu a Kerio Mail Server

V tomto případě se společnost rozhodla, že jako poštovní server nasadí Kerio Mail Server pro Linux. Pořizovací cena se tedy navýší o cenu poštovního serveru a jeho klientských licencí. Vzhledem ke změně verze antiviru se také změní způsob licencování antivirového programu.

Pořízení distribuce Linuxu	1 000 Kč
Kerio Mail Server 20 CL	12 500 Kč
Kerio Add-On +20 CL	2 900 Kč
NOD32 pro Kerio Mail Server, 20 CL, 1 rok	7200 Kč
NOD32 pro KMS Add-On +20 CL	3 600 Kč
Celkem	**27 200 Kč**

Tabulka 4: Operační systém Linux a Kerio Mail Server

Vidíme, že instalace tohoto scénáře se vyplatí v případě, že náklady na implementaci nepřesáhnou částku 74 949 Kč (respektive 100 697 Kč ve verzi *Premium*).

9.2.3 Implementace SuSE Linux Enterprise Server

V posledním scénáři se společnost rozhodne nainstalovat distribuci SuSE (konkrétně serverový systém SuSE Linux Enterprise Server). Tato verze distribuce SuSE je komerční distribuce, optimalizovaná přímo pro použití jako výkonný server. Součástí distribuce jou i grafické konfigurační nástroje, které konfiguraci značně zjednodušují. Firma SuSE má zastoupení v České republice, ceny budou kalkulovány z ceníku českého zastoupení.

SuSE Linux Enterprise Server 8	28 381 Kč
NOD32 pro Linux Mail Server, 50 CL, 1 rok	9 400 Kč
Celkem	**37 781 Kč**

Tabulka 5: SuSE Linux Enterprise Server 8

Rozdíl oproti implementaci Windows je 64 368 Kč (respektive 90 116 Kč). Je nutné podotknout, že zakoupením SuSE Linux Enterprise Server společnost získá kompexní serverový operační systém s vyspělými grafickými konfiguračními nástroji, pravidelnou aktualizací a technickou podporou.

10 Závěr

Přechodem od Windows k Linux se společnosti dostávají do rozmanitého světa volně šiřitelného software. Většina programového vybavení je uvolněna pod licencí GPL, což umožňuje jejich volné použití i pro komerční účely. Rozsah dostupných aplikací je velmi široký, jejich schopnosti jsou se schopnostni programů pro systém Microsoft Windows přinejmenším srovnatelné. Ovšem jako všechno má i toto řešení své výhody a nevýhody.

Jednou z výhod je nižší finanční náročnost na pořízení systému založeného na operačním systému Linux. Toto tvrzení však nemůže být bráno jako dogma, náklady na pořízení systému jsou jen částí celkových nákladů na provoz systému. TCO (*Total Cost of Ownership*) – čili celkové náklady na provoz systému v delším časovém úseku – mohou být v konečném důsledku srovnatelné s implementací řešení firmy Microsoft.

Největší výhodou je možnost využití širokého portfolia aplikací. Bude-li společnost využívat jedno kompletní řešení typu „vše v jednom" (například *Microsoft Small Business Server*, který obsahuje souborový a tiskový server, databázový server, WWW a FTP server, firewall a proxy server v jednom balení), je nucena používat programy, které byly složeny dohromady někým jiným. Jsou mezi nimi programy dobré, které firmě zcela vyhovují, i programy špatné, které jsou například příliš složité pro účely firmy, nebo nesplňují její požadavky. Zakoupení dalšího programu, který bude požadavky splňovat lépe, s sebou nese náklady na zakoupení nového programu a skryté náklady v podobě nevyužívání programu dodaného v balíku „vše v jednom".

Většina programů pro Linux (obecně to nejsou jen programy pro Linux, Linux je pouze jedna z mnoha portací) je velice kvalitních, mají za sebou dlouhý vývoj a jsou nasazovány jako centrální prvky sítě Internet (třebaže na jiném operačním systému unixového typu). Příkladem mohou být programy jako *Bind*, *Sendmail*, *Apache*, *Squid*.

Nevýhodou je horší integrace s produkty firmy Microsoft, které jsou majoritními produkty na pracovních stanicích. Firma Microsoft implementuje do svých programů proprietární protokoly, jejich specifikace nezveřejňuje, v případě implementace standardních protokolů velmi často provede jejich úpravu nebo rozšíření tak, že nejsou s původním standardem plně kompatibilní. Tyto úpravy samozřejmě zapracuje i do ostatních svých produktů, ale nezveřejní jejich podrobnosti. Proto je často obtížné propojit bezproblémově Windows a ostatní platformy.

Další nevýhodou může být i výše zmíněná výhoda rozmanitosti. Problémy, které jsou v operačním systému Windows řešeny jedním programovým balíkem, jsou ve světě Open Source řešeny vhodnou kombinací samostatných balíků, vyvinutých pro jednu každou konkrétní činnost. Každý program je však nutné spravovat samostatně, každý má jiný systém konfigurace a každý vyžaduje něco jiného. Proto jsou požadavky kladené na dobrého správce takového systému výrazně vyšší, musí mít znalosti všech programů, které jsou nainstalovány a využívány.

V některých oblastech výpočetní techniky si již Linux a Open Source vybojovaly své místo. Na poli serverů je Linux nasazován stále více, mnoho velkých balíků již bylo pro Linux portováno (například *Oracle*, *DB/2*) a pro firmy jako je Oracle nebo IBM je Linux podporovaným operačním systémem na stejné úrovni jako například Windows. Open Source programy jsou pilířem Internetu, jejich tržní podíl mnohdy převyšuje tržní podíl Microsoftu (server *Apache* 67 % trhu v prosinci 2003 – údaj dle Netcraft).

V oblasti desktopů, pracovních stanic, se Linux a Open Source prosazují váhavěji. Linux je stále ještě systém, jehož uživatelské rozhraní a integrace nemůže soupeřit s Windows. Existují sice projekty uživatelských rozhraní jako KDE a Gnome, ale množina aplikací ještě stále není tak široká, jako v případě Windows. Do nedávné doby například chyběl rozumně použitelný kancelářský balík. Poslední verze balíku OpenOffice již mohou být soupeřem kancelářským balíkům od Microsoftu, mají však svou pozici ztíženou velkou penetrací Microsoft Office mezi uživateli. Organizace, které léta používaly jeden kancelářský balík a mají tisíce dokumentů vytvořených v tomto balíku, budou pečlivě hodnotit výhody a nevýhody přechodu na nový kancelářský balík, který navíc není zcela kompatibilní (v datovém formátu) se stávajícím balíkem. Zde čeká Open Source ještě dlouhá cesta.

Přechod na Linux má smysl. Má smysl pro společnosti, které nejsou z nějakého důvodu (organizačního či technického) nuceny zůstat u systémů firmy Microsoft. Složitější konfigurace a přechodové bolesti v průběhu implementace budou vykoupeny vyšší flexibilitou systému, nabídkou kvalitních a výkonných programů a v neposlední řadě mnohem méně restriktivní licencí.

Seznam literatury

1. Eckstein, Collier-Brown, Kelly: *Using Samba*, O'Reilly & Associates, 1999
2. Garfinkel, Spafford: *Practical Unix & Internet Security*, O'Reilly & Associates, 1996
3. Dobda, Luboš: *Ochrana dat v informačních systémech*, 1.vyd, Grada, Praha 1998
4. Carda, A., Kunstová, R.: *Workflow, Řízení firemních procesů*, Grada Publishing, 2001
5. Satrapa, P., Randus, J.: *Linux - Internet Server*, Neokortex, 1996
6. Kol. autorů: *Linux - dokumentační projekt*, Computer Press, 1998

Přílohy

1. Seznam odkazů

Seznam odkazů

Operační systémy

`http://www.fsf.org`	*Free Software Foundation*
`http://www.gnu.org`	Projekt *GNU*
`http://www.linux.org`	Domácí stránka Linuxu
`http://www.linux.cz`	Česká domácí stránka Linuxu
`http://www.redhat.com`	Domácí stránka distribuce RedHat
`http://www.debian.org`	Domácí stránka distribuce Debian
`http://www.suse.de`	Domácí stránka distribuce SuSE
`http://www.slackware.com`	Domácí stránka distribuce Slackware
`http://www.microsoft.com`	Společnost Microsoft
`http://www.microsoft.cz`	Česká pobočka společnosti Microsoft

Servery služeb

`http://www.samba.org`	Server Samba
`http://www.isc.org/products/BIND/`	DNS server *Bind*
`http://www.isc.org/products/DHCP/`	DHCP server

WWW server a související

`http://www.apache.org`	Domácí stránka projektu *Apache*
`http://www.perl.org`	Programovací jazyk *Perl*
`http://www.cpan.org`	Rozšiřující moduly pro *Perl*
`http://www.php.net`	Interpret jazyka *PHP*
`http://www.mysql.com`	Databáze *MySQL*
`http://www.postgresql.org`	Databáze *PostgreSQL* – licence GPL

Servery elektronické pošty, antiviry, anti-spam

`http://www.sendmail.com`	Server *Sendmail*
`http://www.postfix.org`	Server *Postfix*
`http://www.kerio.cz`	Společnost *Kerio*
`http://www.eset.sk`	Slovenský antivirus *NOD32*
`http://www.mcafee.com`	McAfee – výrobce software, antivir
`http://www.sophos.com`	Sophos Antivirus
`http://clamav.elektrapro.com`	GPL antivirus *ClamAV*
`http://www.f-prot.com`	Antivirus *F-Prot*
`http://www.pandasoftware.com`	Panda Antivirus

`http://www.amavis.org`	*AMaViS*
`http://mailtools.anomy.net`	*Anomy Sanitizer*
`http://www.messagewall.org`	*MessageWall*
`http://www.spamassassin.org`	*Spam Assassin* – detekce spamu

WWW klienti elektronické pošty a groupware

`http://www.squirrelmail.org`	WWW klient *SquirrelMail*
`http://www.horde.org/imp/`	WWW klient *IMP*
`http://www.lotus.com`	Groupware *Lotus Notes/Domino*
`http://www.desknow.com`	*DeskNow* groupware, zdarma i komerční
`http://www.opengroupware.org`	*OpenGroupware*, zdarma i komerční
`http://www.phpgroupware.org`	*PHPgroupware*, GPL groupware
`http://www.phprojekt.com`	*PHProjekt*, GPL groupware
`http://nullgroupware.sourceforge.org`	*NullLogic Groupware*, GPL groupware
`http://www.sherpath.org`	*Sherpath*, GPL groupware
`http://www.tutos.org`	*TUTOS*, GPL groupware
`http://twig.screwdriver.net`	*TWIG*, GPL groupware

Bezpečnost

`http://www.netfilter.org`	Projekt *Netfilter*, součástí jsou *iptables*
`http://www.squid-cache.org`	Vyrovnávací paměť *Squid*

Dokumentace a zpravodajství

`http://www.root.cz`	Zpravodajský server o Linuxu
`http://www.abclinuxu.cz`	Zpravodajský server o Linuxu
`http://docs.linux.cz`	Dokumentační server o Linuxu
`http://www.linuxlinks.cz`	Odkazy na linuxové programy
`http://www.netcraft.com`	Statistiky Internetu

Všechny odkazy jsou platné ke dni 1. 1. 2004.