

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ  
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ  
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY  
DEPARTMENT OF INFORMATION SYSTEMS

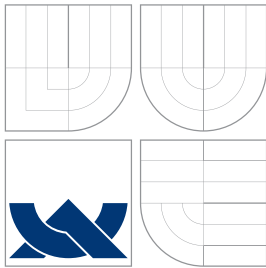
POKROČILÉ NASAZENÍ OS XBSD V SÍTI PRO  
STŘEDNÍ ŠKOLU

DIPLOMOVÁ PRÁCE  
MASTER'S THESIS

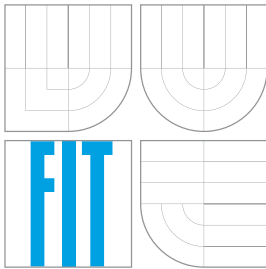
AUTOR PRÁCE  
AUTHOR

Bc. MARTIN ZADINA

BRNO 2007



**VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ**  
BRNO UNIVERSITY OF TECHNOLOGY



**FAKULTA INFORMAČNÍCH TECHNOLOGIÍ**  
**ÚSTAV INFORMAČNÍCH SYSTÉMŮ**

FACULTY OF INFORMATION TECHNOLOGY  
DEPARTMENT OF INFORMATION SYSTEMS

# **POKROČILÉ NASAZENÍ OS XBSD V SÍTI PRO STŘEDNÍ ŠKOLU**

USING ADVANCED XBSD BASED SERVERS FOR HIGH SCHOOL

**DIPLOMOVÁ PRÁCE**

MASTER'S THESIS

**AUTOR PRÁCE**

AUTHOR

**Bc. MARTIN ZADINA**

**VEDOUCÍ PRÁCE**

SUPERVISOR

**Ing. TOMÁŠ KAŠPÁREK**

BRNO 2007

## Vysoké učení technické v Brně - Fakulta informačních technologií

Centrum výpočetní techniky

Akademický rok 2006/2007

# Zadání diplomové práce

Řešitel: **Zadina Martin, Bc.**

Obor: Počítačové systémy a sítě

Téma: **Pokročilé nasazení OS xBSD v síti pro střední školu**

Kategorie: Operační systémy

Pokyny:

1. Seznamte se s rodinou operačních systémů BSD (FreeBSD, NetBSD, OpenBSD)
2. Vyberte vhodnou variantu a navrhnete a implementujte s jeho pomocí následující řešení.
3. Nainstalujte systém Samba jako primární řadič domény - s cílem nahradit stávající systém Windows 2000
4. Aktualizujte požadavky na připojení daných lokalit vzájemně a k ISP a proveďte potřebné modifikace připojení na HW i SW úrovni.
5. Navrhnete a implementujte systém pro zjednodušení instalace jednotlivých stanic na učebnách za předpokladu využití stejné HW konfigurace u všech počítačů na jedné učebně.
6. Závěrem shrňte potřebné úkoly pro další provoz vámi navrženého systému (zálohování, bezpečností aktualizace atd.)
7. Pokuste se objasnit, čím byla instalace v prostředí střední školy typická, které části vaší práce jsou pro daný typ nasazení opakovaně použitelné.

Literatura:

- FreeBSD ([www.freebsd.org](http://www.freebsd.org))
- NetBSD ([www.netbsd.org](http://www.netbsd.org))
- OpenBSD ([www.openbsd.org](http://www.openbsd.org))

Při obhajobě semestrální části diplomového projektu je požadováno:

- Body 1. až 3.

Podrobné závazné pokyny pro vypracování diplomové práce naleznete na adrese <http://www.fit.vutbr.cz/info/szz/>

Technická zpráva diplomové práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap, které byly vyřešeny v rámci ročníkového a semestrálního projektu (30 až 40% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním paměťovém médiu (disketa, CD-ROM), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Kašpárek Tomáš, Ing.,** CVT FIT VUT

Datum zadání: 28. února 2006

Datum odevzdání: 22. května 2007

Vysoké učení technické v Brně  
Fakulta informačních technologií  
Ústav inform. L.S. systémů  
602 00 Brno, Božetěchova 2



---

doc. Ing. Jaroslav Zendulka, CSc.  
vedoucí ústavu

## **Licenční smlouva**

Licenční smlouva je uložena v archivu Fakulty informačních technologií Vysokého učení technického v Brně.

## Abstrakt

Práce se zabývá nasazením software Samba na server s operačním systémem z rodiny BSD do role primárního řadiče domény v počítačové síti střední školy se stanicemi s operačním systémem Microsoft Windows. Po představení software Samba je podrobněji rozebrána problematika sítí Windows založených na protokolu SMB. Následně jsou uvedeny potřebné kroky konfigurace software Samba, nastavení diskových sdílení, vytváření uživatelských účtů a přidání klientské stanice do důvěryhodného vztahu s řadičem domény. Dále je popsána problematika síťového tisku v prostředí Windows, tiskových serverů a řešení problematiky pomocí klasických tiskových služeb systému FreeBSD a tiskového systému CUPS. V další části je zmíněna problematika hromadné instalace stanic se stejnou hardwarovou konfigurací v prostředí školních učeben. Závěrem jsou shrnuty úkony potřebné pro další provoz systému.

## Klíčová slova

FreeBSD, Samba, primární řadič domény, SMB, CIFS, NetBIOS, WINS, doména Windows, CUPS, LPD, síťový tisk, tiskový server, záloha oddílů NTFS, klonování disků, SystemRescueCD, Partimage, NFS

## Abstract

This work is about setting up Samba software on server with operating system from BSD family to primary domain controller role in the high school computer network environment with Microsoft Windows stations. After introduction to Samba software there is examined problem of Windows network based on SMB protocol. There are described steps that are necessary to setup Samba software, disk sharing services, creation of user accounts and adding client stations to domain trust. At the next there is described problematic of network printing in the Windows environment, print servers and the solution with classical printing support in FreeBSD and CUPS printing support. In the next part there is described mass installation procedure of Windows stations with same hardware configuration. At the finish, there are noticed some tasks that are necessary for next operation of installed system.

## Keywords

FreeBSD, Samba, primary domain controller, SMB, CIFS, NetBIOS, WINS, Windows domain, CUPS, LPD, network printing, print server, NTFS partition backup, disk cloning, SystemRescueCD, Partimage, NFS

## Citace

Martin Zadina: Pokročilé nasazení OS xBSD v síti pro střední školu, diplomová práce, Brno, FIT VUT v Brně, 2007

# Pokročilé nasazení OS xBSD v síti pro střední školu

## Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana Ing. Tomáše Kašpárka. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....

Martin Zadina  
13. května 2007

## Poděkování

Rád bych na tomto místě poděkoval panu Ing. Tomášovi Kašpárkovi za odbornou pomoc při řešení této práce a školám Gymnázium Otokara Březiny a Střední odborná škola v Telči, u nichž byla práce realizována.

© Martin Zadina, 2007.

*Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.*

# Obsah

<b>1</b>	<b>Úvod</b>	<b>3</b>
<b>2</b>	<b>Samba jako primární řadič domény</b>	<b>5</b>
2.1	Úvod	5
2.2	Poskytované služby	5
2.3	Historie	6
2.4	Seznámení s protokolem SMB	6
2.4.1	NetBIOS	6
2.4.2	Jmenné služby	7
2.4.3	Datagramy a relace	9
2.5	Rozšíření SMB firmy Microsoft	9
2.5.1	Pracovní skupiny Windows	9
2.5.2	Domény Windows NT	11
2.6	Možné role Samba 3 serveru	13
2.7	Popis balíku Samba 3	14
2.8	Instalace FreeBSD serveru	15
2.9	Instalace Samby na FreeBSD server	15
2.9.1	Konfigurace role primárního řadiče domény	15
2.9.2	Spuštění Samba serveru	17
2.9.3	Přihlašovací skripty	18
2.9.4	Uživatelské účty	18
2.9.5	Přidání stanice do domény	20
<b>3</b>	<b>Tiskové služby</b>	<b>21</b>
3.1	Úvod	21
3.2	Zpracování tiskových úloh Samba serverem	21
3.2.1	Požadavky kladené na tiskový podsystém	22
3.3	Klasická podpora tisku	23
3.3.1	Klasický tiskový podsystém ve FreeBSD	23
3.3.2	Nastavení tiskových sdílení v Sambě	26
3.4	Ovladače tiskáren	28
3.4.1	Úvod	28
3.4.2	Způsoby instalace ovladačů na klientské stanice	28
3.4.3	Nahrání ovladačů na server pomocí průvodce přidáním tiskárny	29
3.5	Tiskový systém CUPS	35
3.5.1	Podpora CUPS v Sambě	35
3.5.2	Tiskový server zpracovávající pouze RAW data	35
3.5.3	Pokročilý tisk s použitím ovladačů PostScript	36

3.5.4	Závěr	40
<b>4</b>	<b>Aktualizace propojení lokalit</b>	<b>42</b>
<b>5</b>	<b>Instalace stanic na učebnách</b>	<b>44</b>
5.1	Úvod	44
5.2	Norton Ghost	45
5.2.1	Kopírování disků po síti	45
5.2.2	Vypalování obrazů	46
5.2.3	Ukládání obrazů do souborů	46
5.2.4	Výhody a nevýhody použití Norton Ghost 2002	46
5.3	Alternativa založená na volně šiřitelném software	46
5.3.1	System	46
5.3.2	SystemRescueCD	47
5.3.3	Možnosti uložení diskového oddílu NTFS	47
5.3.4	Obnova obrazu na nový disk	51
5.3.5	Ukládání obrazů na server pomocí NFS	51
5.3.6	Vlastní verze SystemRescueCD	53
5.4	Závěr	54
<b>6</b>	<b>Další provoz systému</b>	<b>55</b>
6.1	Softwarové zrcadlení disků	55
6.1.1	Zrcadlení systémového disku	56
<b>7</b>	<b>Závěr</b>	<b>57</b>
<b>A</b>	<b>Konfigurační soubory</b>	<b>60</b>
A.1	Konfigurační soubor tiskového podsystému – printcap	60
A.2	Konfigurační soubor Samby smb.conf	60
A.3	Přihlašovací skript WinXP.bat	62
A.4	Skript autorun.sh	62
A.5	Skript user_add.sh	63
<b>B</b>	<b>Popis parametrů</b>	<b>64</b>
B.1	Přehled důležitých parametrů souboru smb.conf pro tiskové služby	64
B.1.1	Parametry speciální sekce [global]	64
B.1.2	Nastavení sekce [printers]	65
B.1.3	Parametry pro libovolnou sekci [tiskove_sdileni]	65



# Kapitola 1

## Úvod

Práce se zabývá problematikou sítí založených na protokolu SMB/CIFS a dále řeší instalaci serveru s operačním systémem z rodiny BSD a softwarového balíku Samba jako primárního řadiče domény se stanicemi Windows za účelem náhrady existujícího serveru s operačním systémem Microsoft Windows 2000 Server.

Práce je realizována na školní síti Gymnázia Otokara Březiny a Střední odborné školy v Telči. Server bude sloužit jako primární řadič domény části sítě gymnázia, s přibližně sedmi desítkami počítačů, s možností rozšíření pro část sítě odborné školy v případě, že se řešení osvědčí a vyřeší se vysokorychlostní propojení lokalit.

Stručný přehled kapitol:

**Kapitola 2** představuje software Samba, pojednává o problematice sítí Windows založených na protokolu SMB a řeší vlastní instalaci Samba serveru a uvedení do provozu

**Kapitola 3** pojednává o problematice síťového tisku v operačních systémech Windows, komunikaci mezi klienty Windows se serverem Samba při odesílání tiskové úlohy a komunikaci Samba serveru s tiskárnami pomocí tiskového podsystému operačního systému, na kterém Samba běží

**Kapitola 4** se zabývá problematikou propojení nezávislých budov školy a v návaznosti na bakalářskou práci pojednává o úkonech, které bylo potřeba provést během provozu v rámci změny přenosové technologie

**Kapitola 5** řeší problematiku hromadné instalace mnoha počítačů se stejnou hardwarovou konfigurací ve školní učebně a ukazuje nástroje a postupy k provedení tohoto úkonu

**Kapitola 6** shrnuje kroky nutné pro další provoz nainstalovaného systému a představuje možnost zvýšení odolnosti serveru proti poruše disku pomocí softwarového zrcadlení disků

O historii a vlastnostech jednotlivých nejrozšířenějších variant rodiny operačních systémů BSD bylo pojednáno v předcházející bakalářské práci autora [8]. Pro řešení zde byla vybrána varianta FreeBSD. Jelikož se provoz řešení navrženém v bakalářské práci a serverů s tímto operačním systémem autorovi osvědčil, byla vybrána stejná varianta i pro řešení dále popisované problematiky serveru se softwarem Samba v roli primárního řadiče domény Windows.

Diplomová práce navazuje na Semestrální projekt, ve kterém byla řešena problematika sítí Windows založených na protokolu SMB, popsán softwarový balík Samba, konfigurace a uvedení Samba serveru do provozu. Tato problematika je obsažena v kapitole 2.

## Kapitola 2

# Samba jako primární řadič domény

### 2.1 Úvod

Samba je rozsáhlý komplexní projekt. Tým vyvíjející Sambu tvoří přibližně tři desítky lidí rozprostřených po celém světě. Tým zahrnuje vědce, inženýry, programátory, studenty a další lidi se společným zájmem.

Členové týmu byli vtaženi do vzájemné spolupráce s cílem vývoje prostředku pro transparentní spolupráci a odstranění bariér mezi světy operačního systému Microsoft Windows a ostatními systémy.

Samba poskytuje služby sdílení souborů a tiskáren. Tyto služby mohou být hostovány na libovolném systému podporujícím protokol TCP/IP. Původními vývojovými platformami byly operační systémy UNIX a Linux. Dnes je možné využití na širokém spektru operačních systémů.

Projekt neobsahuje jenom samotné základní služby, ale také balík nástrojů pro zjednodušení správy, snadnou migraci a další nástroje pro zajištění interoperability s prostředím Microsoft Windows.

### 2.2 Poskytované služby

Samba je balík aplikací, který používá ke komunikaci protokol SMB. Operační systémy Microsoft Windows používají tento protokol pro komunikaci po síti typu klient – server k zajištění operací sdílení souborů a tiskáren. Samba běžící na systému s operačním systémem typu Unix umožňuje, díky podpoře stejného síťového protokolu, vystupovat na síti jako jiný Microsoft Windows systém z perspektivy klienta s Microsoft Windows.

Server Samba může poskytovat tyto základní služby:

- sdílení jednoho nebo více adresářových stromů;
- sdílení tiskáren;
- asistenci klientům při prohlížení sítě;
- autentizaci klientů při přístupu ke sdílenému prostředku;
- řízení domény se stanicemi Microsoft Windows;
- asistenci při převodu jmen systému Windows Internet Name Service (WINS).

Balík aplikací Samba také obsahuje klientskou aplikaci umožňující přístup k souborům a tiskárnám sdíleným jinými systémy na síti.

## 2.3 Historie

Otcem Samby je Andrew Tridgell. Projekt se zrodil v roce 1991, kdy Andrew pracoval se softwarovým balíkem firmy Digital Equipment Corporation (DEC) zvaným Pathworks určeným k propojení počítačů DEC VAX s počítači jiných společností. Andrew vytvořil aplikaci, která sloužila jako souborový server a podporovala protokol obsažený v balíku Pathworks. Tento protokol se později stal základem protokolu SMB (Server Message Block). Po několika letech Andrew svoji aplikaci rozšířil a začal ji distribuovat na Internetu pod názvem „SMB server“. Toto jméno nechtěl ale zachovat, protože náleželo již produktu jiné společnosti. Proto zkusil následující příkaz systému Unix:

```
# grep -i '^s.*m.*b' /usr/dict/words
```

Výsledkem příkazu byla slova:

```
salmonberry
samba
sawtimber
scramble
```

Takto vzniklo jméno „Samba“.

Samba je distribuována jako Open Source Software podle licence GNU General Public Licence (GPL). Od svého počátku byl vývoj Samby částečně sponzorován ANU (Australian National University), kde Andrew Tridgell studoval a získal titul Ph.D. Od té doby byli vývojáři Samby sponzorováni mnoha dalšími organizacemi včetně LinuxCare, VA Linux Systems, Hewlett-Packard a IBM. Aktivity kolem Samby jsou tak podporovány komerčními i nekomerčními organizacemi.

V roce 1996 přispěla materiálně i firma Microsoft zveřejněním definic protokolu SMB. Protokol CIFS (Common Internet File System) je pouze jiné jméno dalších verzí protokolu SMB, které je používáno v produktech Microsoft Windows, takže tato dvě jména jsou zaměnitelná. V dalším textu bude preferováno označení SMB.

## 2.4 Seznámení s protokolem SMB

V sítích založených na protokolu SMB existuje několik vlastností a odlišností v porovnání se sítěmi založenými pouze na TCP/IP a jmenném systému DNS.

### 2.4.1 NetBIOS

NetBIOS (Network Basic Input/Output System) je jednoduché aplikační programové rozhraní (API) pro práci v síti, představené firmou IBM v roce 1984. Rozhraní poskytuje základní myšlenku komunikace aplikací mezi různými počítači v síti a sdílení dat.

Rozhraní NetBIOS vyžaduje pro přenos požadavků po síti transportní protokol. Na konci roku 1985 byl vytvořen firmou IBM protokol, který byl sloučen s rozhraním NetBIOS a jmenoval se NetBEUI (NetBIOS Extended User Interface). Tento protokol byl navržen pro malé LAN sítě, kde každý počítač byl identifikován jedinečným názvem do délky 15

znaků. Malou síť LAN byla myšlena síť s méně než 255 uzly v síti. Tato hodnota byla již v roce 1985 považována za praktické omezení.

Ačkoliv se protokol NetBEUI stal u síťových aplikací velmi rozšířený, protokoly pro rozrůstající se prostředí Internetu se staly TCP/IP a UDP/IP. Implementace rozhraní NetBIOS nad těmito protokoly se stala brzo nutností.

V roce 1987 sdružení IETF (Internet Engineering Task Force) publikovalo dvojici standardizačních dokumentů RFC 1001 a RFC 1002, které popisují, jak by mělo rozhraní NetBIOS pracovat v síti založené na protokolech TCP a UDP. Informace obsažené v těchto dokumentech byly použity ve všech dnes dostupných implementacích, včetně těch, které jsou použity u systémů Microsoft Windows a v Sambě.

Standard, který dokumenty definují, se stal známým pod názvem NetBIOS over TCP/IP (zkráceně NBT). Standard NBT definuje trojici síťových služeb:

- jmenné služby
- dvě komunikační služby
  - datagramy
  - relace

Jmenné služby řeší problém převodu jména na adresu. Umožňují každému počítači registrovat si na síti unikátní jméno, které je možné převést na IP adresu, podobně jako u systému DNS používaném na Internetu.

Datagramové a relační služby jsou sekundárními komunikačními protokoly použitými pro přenos dat mezi jednotlivými počítači využívajícími rozhraní NetBIOS v síti.

#### 2.4.2 Jmenné služby

V sítích založených na rozhraní NetBIOS si musí každý počítač po připojení do sítě zaregistrovat jedinečné jméno, pomocí kterého bude adresovatelný. Proces se nazývá *registrace jména* a pro vyloučení možnosti dvou počítačů používajících stejné jméno se používají následující dva mechanismy:

- Každý počítač v síti oznámí svojí IP adresu, pokud zaslechne broadcast se svým jménem NetBIOS. Počítač registrující si jméno se nejdříve pomocí broadcastu dotáže na toto jméno a smí ho použít pouze pokud se mu nedostane odezvy.
- Pro sledování informací o registrovaných jménech v síti se použije jmenový server NetBIOS (NBNS – NetBIOS Name Server).

Se zmíněnými mechanismy registrace jména souvisí i způsob převodu jména NetBIOS na IP adresu. Pro rozlišení jména je použito buď jmenového serveru NetBIOS nebo broadcastu.

Výhodou použití jmenového serveru je nižší komunikační režie v síti, protože komunikace při dotazech na převod jména probíhá od klienta k serveru (point-to-point) a síť není při každém požadavku na převod jména zaplavována broadcastem. Další výhodou je možnost funkčnosti převodu jmen i v sítích rozdělených pomocí routerů do menších podsítí, u kterých broadcastový provoz přes routery neprojde.

## Typy uzlů

V sítích NetBIOS je potřeba specifikovat, jakým způsobem bude každý klient v síti provádět registraci a převod jmen. V závislosti na použité strategii registrace a převodu jmen má každý počítač v síti NBT přidělen jeden typ uzlu. Uzel může být typu *b*, *p*, *m* nebo *h*. Typy a význam uzlů je uveden v tabulce 2.1.

typ uzlu	popis
uzel b (b-node)	používá k registraci a převodu jmen pouze broadcast
uzel p (p-node)	používá pouze komunikaci typu point-to-point
uzel m (m-node), mixed	používá broadcast pro registraci, pokud je úspěšná, je uvědoměn jmenný server NetBIOS o výsledku; pro převod jmen používá též broadcast, v případě neúspěchu je použit jmenný server NetBIOS
uzel h (h-node), hybrid	používá jmenný server NetBIOS pro registraci a převod jmen; pokud je jmenný server nedostupný, použije broadcast

Tabulka 2.1: Typy uzlů v sítích NetBIOS

U klientů s operačním systémem Microsoft Windows je obvykle nastaven uzel typu *h*. Uzly typu *b*, *p* a *m* jsou součástí dokumentů RFC 1001/1002. Uzel typu *h* byl uveden později firmou Microsoft.

Typ použitého uzlu je možné nastavit u stanic také pomocí parametru protokolu DHCP, pokud je použit pro síťovou konfiguraci stanic.

## Jméno

Jména použitá u rozhraní NetBIOS se liší od jmen známých ze systému DNS. NetBIOS používá plochý jmenný prostor – není zde možná žádná hierarchie známá ze systému DNS. Jména NetBIOS se skládají z řetězce, který může být maximálně 15 znaků dlouhý a může se skládat pouze ze standardních alfanumerických znaků (a-z, A-Z, 0-9) a následujících znaků:

! @ # \$ % ^ & ( ) - ' { } . ~

Ačkoliv je povoleno i využití znaku tečka, není použití tohoto znaku doporučeno kvůli koexistenci stejných jmen v systému DNS, kde má tečka zvláštní význam oddělovače v hierarchii doménových jmen.

Ve skutečnosti má jméno vždy 15 znaků. Pokud je název kratší, než 15 znaků, je doplněn na velikost 15-ti znaků mezerami.

## Typy prostředků

Kromě samotného jména sděluje každý počítač také informace o službách, které poskytuje. Typ služby (prostředku), které počítač nabízí, je určen pomocí 16. bytu, který je přidán ke jménu. Pokud počítač nabízí více různých typů prostředků, provádí násobnou registraci jména pro každý prostředek s odlišným 16. bytem. Typy prostředků rozhraní NetBIOS jsou uvedeny v tabulce 2.2.

V systémech Windows je možné informace o jménech a poskytovaných prostředcích zjistit pomocí nástroje *nbtstat*.

prostředek	hex. hodnota bytu
Služba pracovní stanice (Standard Workstation Service)	00
Služba doručování zpráv (Messenger Service)	03
Server vzdáleného přístupu (RAS Server Service)	06
Hlavní prohlížeč domény (Domain Master Browser Service)	1B
Jméno hlavního prohlížeče (Master Browser Name)	1D
Služby NetDDE	1F
Souborový server vč. tiskového serveru	20
Klient služby vzdáleného přístupu (RAS Client Service)	21
Agent monitorování sítě (Network Monitor Agent)	BE
Nástroj monitorování sítě (Network Monitor Utility)	BF

Tabulka 2.2: Typy prostředků rozhraní NetBIOS

## Skupiny

Protokol SMB využívá koncept skupin, do kterých se stanice mohou registrovat. Stanice na síti mohou být rozděleny do jednotlivých skupin například dle oddělení organizace. Každá skupina může obsahovat jiné sdílené souborové servery, tiskárny a další služby.

### 2.4.3 Datagramy a relace

Protokol NetBIOS nad TCP/IP poskytuje kromě jmenných služeb datagramové a relační komunikační služby, které poskytují propojení mezi dvěma počítači.

Datagramová služba neustavuje spojení mezi počítači. Datové pakety jsou odesílány z jednoho počítače na druhý bez ohledu na pořadí ve kterém jsou přijaty u příjemce, pokud k příjemci dorazí. Využití datagramů vyžaduje menší režii, než v případě ustavování relace a proto se využívají k rychlému odesílání jednoduchých datových bloků na cílový počítač. Datagramy mohou být použity i pro všesměrové vysílání (broadcast). Transportním protokolem datagramů je protokol UDP.

Relační služba je složitější. Před komunikací je potřeba ustanovit spojení. Zato je zaručeno doručení dat ve správném pořadí a znovuodeslání v případě chyby. Komunikace je možná pouze mezi dvěma počítači. Tento typ spojení je využíván nejčastěji u služeb diskových sdílení a sdílení tiskáren. Transportním protokolem relační služby je TCP.

Komunikace pomocí datagramové a relační služby se skládá se základních primitiv uvedených v tabulkách 2.3 a 2.4.

## 2.5 Rozšíření SMB firmy Microsoft

Firma Microsoft přidala do sítí založených na SMB protokolu v operačním systému Windows několik rozšíření – *pracovní skupiny Windows* (Windows Workgroups) a *domény Windows*.

### 2.5.1 Pracovní skupiny Windows

Jsou velmi podobné již zmíněným skupinám SMB s dalšími vlastnostmi.

primitivum	popis
Poslat datagram (Send Datagram)	zašle datagram počítači nebo skupině počítačů
Poslat všesměrový datagram (Send Broadcast Datagram)	pošle všesměrový datagram všem počítačům čekajícím ve stavu „Přijmout všesměrový datagram“
Přijmout datagram (Receive Datagram)	čeká na přijetí datagramu od počítače
Přijmout všesměrový datagram (Receive Broadcast Datagram)	čeká na přijetí všesměrového datagramu

Tabulka 2.3: Primitiva datagramové služby

primitivum	popis
Volat (Call)	iniciuje spojení s počítačem, který naslouchá pod daným jménem
Poslouchat (Listen)	čeká na spojení
Zavěsit (Hang-up)	ukončí spojení
Poslat (Send)	odešle data účastníkovi spojení
Přijmout (Receive)	přijme data od účastníka spojení
Stav relace (Session Status)	získá informace o stavu požadované relace

Tabulka 2.4: Primitiva relační služby

### Prohlížení (browsing)

Prohlížení je proces hledání ostatních počítačů a sdílených prostředků v sítích Windows. Prohlížení dává možnost klientovi prohlížet počítače a jimi nabízené služby pomocí grafického uživatelského rozhraní a snadno, pomocí klikání myší, procházet síťové okolí (Místa v síti). Dříve, než existovalo prohlížení, uživatel musel znát jméno sdíleného prostředku a počítače a manuálně zadat adresu ve formátu UNC (Universal Naming Convention) do aplikace přistupující ke sdílenému prostředku.

Příklad: přístup ke sdílenému prostředku *folder* na serveru *srv* pomocí UNC:

`\\srv\folder`

V sítích SMB můžeme rozlišit dva typy prohlížení:

- prohlížení seznamu počítačů se sdílenými prostředky;
- prohlížení sdílených prostředků konkrétního počítače.

V každé podsíti pracovní skupiny nebo domény Windows má jeden počítač zodpovědnost za udržování seznamu dostupných počítačů. Tento počítač se nazývá *místní hlavní prohlížeč* (local master browser) a seznam, který udržuje *prohlížeč seznam* (browse list). Cílem je redukce síťového provozu, kde by se každá stanice musela periodicky dotazovat na všechny počítače v síti a udržovat si vlastní seznam. Místo toho se pouze dotáže místního hlavního prohlížeče. Každý počítač v pracovní skupině Windows je povinen oznámit svoji přítomnost místnímu hlavnímu prohlížeči ihned poté, co si zaregistruje svoje jméno NetBIOS.



Pro prohlížení prostředků na konkrétním počítači se k němu musí uživatel připojit přímo, tyto informace nemohou být získány z prohlízacího seznamu. Po připojení je odeslán seznam nabízených prostředků.

Pro zvýšení spolehlivosti prohlízacích seznamů jsou dynamicky voleny, dle počtu počítačů v pracovní skupině nebo doméně, záložní prohlížeče.

Jelikož mechanismus volby hlavních a záložních prohlížečů je v sítích Windows automatický a prohlížečem se může stát teoreticky libovolná stanice, musí existovat způsob, jak určit v libovolném okamžiku stanice, které budou tuto funkci vykonávat. Tento proces se nazývá volba prohlížeče (election).

V průběhu procesu volby prohlížeče, každý počítač odesílá o sobě pomocí všesměrových datagramů informace obsahující:

- verzi protokolu volby prohlížeče;
- verzi operačního systému;
- dobu připojení k síti;
- jméno.

Na základě těchto informací je vybrána stanice s nejlepšími předpoklady pro plnění funkce prohlížeče.

Problémem tohoto automatického procesu je bezpečnost, protože libovolná stanice se může připojit do sítě, vyhrát při volbě prohlížeče a případně libovolně manipulovat s prohlízacím seznamem.

### 2.5.2 Domény Windows NT

Domény Windows NT uvedl Microsoft se systémem Windows NT 3.51. Domény Windows NT jsou vlastně zmíněnými pracovními skupinami Windows. Hlavním rozdílem je přítomnost serveru, který zastává v síti roli řadiče domény. V sítích založených pouze na pracovních skupinách nejsou rozděleny role a neexistuje centrální prvek, který by řídil přístup k jednotlivým prostředkům. Tyto sítě jsou založeny na principu *peer-to-peer*, kde jednotlivé stanice mohou nabízet služby ostatním bez centrálního řízení. Tento model může být vhodný pro malé skupiny uživatelů, ale ve větších sítích začne být limitujícím faktorem. V pracovních skupinách musí být ke sdíleným prostředkům na každé stanici nastaveno zvlášť heslo, což vede na obtížnou spravovatelnost ve větších síťových prostředích, pro uživatele nutnost pamatovat si více hesel k jednotlivým prostředkům a v případě potřeby též obtížnou hromadnou změnu hesel.

Mezi hlavní výhody bezpečnostního modelu založeném na doménách Windows patří centrální správa uživatelů, možnost vytvářet skupiny, hromadně přidělovat a odebírat oprávnění ke sdíleným prostředkům v rámci celé domény. V dobře navrženém prostředí je možné využít jednotného přihlášení ke všem potřebným síťovým prostředkům – SSO (Single Sign On).

### Řadiče domény

Základní funkcí řadiče domény je udržování doménové databáze s informacemi o uživateli a skupinách a vykonávání dalších přidružených služeb. Řadič domény je zodpovědný za centrální řízení bezpečnosti, včetně autentizace, procesu přidělování přístupu k jednotlivým

prostředkům domény. Uživatelé jsou typicky autentizováni dle uživatelského jména a hesla. Služba zodpovídající za databázi na doménovém řadiči se nazývá *Security Account Manager* (SAM).

Bezpečnostní model domény Windows NT je založen na bezpečnostních identifikátorech (SIDs – Security IDentifiers) a na seznamech pro řízení přístupu (ACL – Access Control Lists). Bezpečnostní identifikátory slouží k reprezentaci objektů v doméně, například uživatelé, skupiny, počítače, procesy. Seznamy pro řízení přístupu jsou využity při přístupu ke sdíleným prostředkům a určují oprávnění při nakládání s prostředkem, například čtení, zápis.

## Typy doménových řadičů

Řadiče domény Windows lze rozdělit na:

- primární řadič domény (PDC – primary domain controller);
- záložní řadič domény (BDC – backup domain controller).

Primární řadič je v doméně jediný. Pro zajištění redundance a vyšší spolehlivosti může být nakonfigurován jeden nebo více záložních řadičů domény, které převzou funkci primárního řadiče v případě, kdy se stane primární řadič nedostupným. Záložní řadiče domény musí provádět v relativně krátkých časových okamžicích synchronizaci databáze s primárním řadičem. Záložní řadiče navíc obsahují kopii databáze pouze pro čtení, takže případné aktualizace se vždy provádí přímo na primárním řadiči. Při přístupu k doméně může být uživatel autentizován libovolně primárním nebo některým ze záložních řadičů. Záložní řadiče jsou při vyřizování požadavků o autentizaci preferovány kvůli distribuci zátěže primárního řadiče.

## Proces autentizace v doméně

Poté, co uživatel zadá při pokusu o přihlášení k doméně uživatelské jméno a heslo, je mezi klientským počítačem a řadičem domény spuštěn proces ověření uživatelského jména a hesla pomocí zabezpečeného protokolu založeném na principu *výzva – odpověď* (challenge – response). V případě úspěšného ověření odešle server klientovi bezpečnostní identifikátor (SID). Na základě tohoto identifikátoru klient následně vytvoří bezpečnostní přístupový token (SAT – Security Access Token). Tento token je platný pouze pro systém, ze kterého klient provedl autentizaci a obsahuje zakódované informace o uživateli, včetně uživatelského jména, skupiny a oprávnění v doméně. V tomto okamžiku je uživatel přihlášen k doméně.

Pokud se uživatel pokusí o přístup ke sdílenému prostředku uvnitř domény, opět je se systémem poskytujícím prostředek a klientem započata zabezpečená výměna autentizačních informací pomocí protokolu výzva – odpověď. Zároveň server nabízející prostředek kontaktuje řadič domény a provede kontrolu správnosti informací zaslanych klientem. Pokud řadič domény vyhodnotí informace jako správné, pošle serveru, který nabízí prostředek bezpečnostní identifikátor (SID), který ho použije pro vytvoření vlastního bezpečnostního tokenu (SAT) pro klienta, na základě kterého je klientovi povolen přístup ke sdílenému prostředku. V tomto okamžiku je klient autentizován pro přístup ke sdílenému prostředku. Server použije SID klienta ke zjištění, jaká má klient k požadovanému prostředku oprávnění porovnáním se záznamy v seznamu přístupových práv (ACL).

## Služba WINS

Služba WINS (Windows Internet Name Service) je implementací jmenného serveru NetBIOS od firmy Microsoft. Služba WINS dědí většinu vlastností charakteristických pro rozhraní NetBIOS a jmenný server NetBIOS. Prostor jmen je plochý bez možnosti tvorby hierarchie. Způsob registrace jmen je dynamický – po připojení klienta k síti klient kontaktuje WINS server a registruje informace o sobě (jméno, skupinu, adresu, nabízené prostředky). WINS server udržuje informace o klientovi, dokud je klient periodicky obnovuje. WINS server není omezen pouze jednou doménou nebo pracovní skupinou na jediné podsíti – může udržovat registrace pro více pracovních skupin a domén na více podsítích.

Více WINS serverů může být nakonfigurováno, aby mezi sebou prováděly synchronizace. Různé části sítě tak mohou být nastaveny k využívání různých WINS serverů. Snaha jednotlivých WINS serverů o výměnu aktuálních informací o klientech může být v rozlehlejších síťovém prostředí neefektivní, proto je lepší použít koncept pouze jednoho autoritativního serveru WINS, který udržuje registrace od všech stanic v síti, nezávisle na pracovních skupinách a doménách. Tento autoritativní (primární) WINS server může být doplněn sekundárními WINS servery, které jsou synchronizovány s primárním serverem a mohou převzít funkci v případě výpadku primárního serveru.

## 2.6 Možné role Samba 3 serveru

Tabulka 2.5 souhrnně ukazuje role, které Samba v aktuální třetí verzi může zastávat. Některé role jsou omezené hlavně z důvodu nedostupnosti dokumentace k některým proprietárním protokolům firmy Microsoft, na které musí vývojový tým Samby aplikovat zpětné inženýrství. Souhrnně lze říci, že Samba obvykle nemůže, právě díky použití proprietárních protokolů, pracovat v záložních rolích serverů Windows a také plně nepodporuje systém Active Directory.

role	může zastávat?
Souborový server	Ano
Tiskový server	Ano
Microsoft Dfs server	Ano
Primární řadič domény	Ano
Záložní řadič domény	Ne
Řadič domény Active Directory	Ne
Autentizace klientů Windows 95/98/Me	Ano
Autentizace klientů Windows NT/2000/XP	Ano
Místní hlavní prohlížeč	Ano
Místní záložní prohlížeč	Ano
Doménový hlavní prohlížeč	Ano
Primární WINS server	Ano
Sekundární WINS server	Ne

Tabulka 2.5: Role podporované Samba serverem

## 2.7 Popis balíku Samba 3

Samba se skládá z několika programů. Základem Samby jsou tři síťové démony, doplněné sadou nástrojů pro příkazovou řádku. V následujícím textu budou tyto aplikace stručně popsány:

**smbd** – tento démon je zodpovědný za sdílení prostředků mezi serverem Samba a klienty. Poskytuje souborové a tiskové služby, služby prohlížení, obsluhuje veškerou komunikaci mezi Samba serverem a klienty, je zodpovědný za autentizaci uživatelů, uzamykání prostředků a sdílení dat s využitím protokolu SMB

**nmbd** – je jednoduchým jmenným serverem, který poskytuje funkcionalitu jmenného serveru WINS, udržuje prohlížecké seznamy a účastní se soutěžení o funkci prohlížeče

**winbindd** – démon potřebný, pokud je Samba v roli člena domény. Umožňuje serveru Samba provádět autorizaci klientů, přistupujících ke sdíleným prostředkům, vůči serveru Windows NT/2000

**findsmb** – program prohledávající lokální síť a zjišťující přítomnost klientů odpovídajících na protokol SMB

**make\_smbcodepage, make\_unicodemap** – programy pro práci s kódovými sadami

**net** – program pro vzdálenou administraci SMB serverů

**nmblookup** – program pro převod jména NetBIOS na IP adresu

**pdbedit** – program pro správu účtů v SAM databázi

**rpcclient** – program pro vzdálené volání procedury na klientech Windows

**smbcacls** – program pro zjištění nebo nastavení oprávnění (ACL) na souborových systémech Windows NT

**smbclient** – klient pro připojení ke sdílení SMB

**smbcontrol** – administrativní nástroj k posílání zpráv démonům smbd a nmbd

**smbgroupedit** – příkaz použitelný k definici mapování mezi skupinami Windows NT a Unix

**smbmnt, smbmount** – programy pro připojení vzdáleného SMB souborového systému

**smbpasswd** – program pro administraci účtů a změnu hesel

**smbsh** – nástroj pracující jako shell umožňující přístup Unixovým programům k vzdálenému SMB souborovému systému

**smbspool** – program umožňující zasílat soubory vzdáleným tiskárnám pomocí SMB

**smbstatus** – program zobrazující aktivní spojení ke sdíleným prostředkům serveru

**smbtar** – program pro zálohování dat na sdíleních SMB

**smbumount** – program k odpojení souborového systému připojeného pomocí smbmount

**testparm** – program pro kontrolu konfiguračního souboru Samby

**testprns** – program pro otestování správného rozpoznání tiskáren démonem smbd

**wbinfo** – nástroj použitelný pro dotazování winbindd démona

## 2.8 Instalace FreeBSD serveru

Instalace operačního systému FreeBSD byla podrobně zmíněna v kapitole 3.4.6 bakalářské práce [8].

## 2.9 Instalace Samby na FreeBSD server

Nejjednodušším způsobem instalace balíku Samba na server s operačním systémem FreeBSD je využití kolekce portů. Kolekce portů je umístěna v adresáři `/usr/ports`. Pokud tomu tak není, je potřeba ze stránek FreeBSD kolekci stáhnout a rozbalit ji:

```
# cd /usr
# fetch ftp://ftp.cz.freebsd.org/pub/FreeBSD/ports/ports/ports.tar.gz
# tar -xz -f ports.tar.gz
```

Po rozbalení kolekce je možné začít instalaci:

```
# cd /usr/ports/net/samba3
# make install
```

Po skončení procesu kompilace a instalace je balík Samba připraven k použití.

### 2.9.1 Konfigurace role primárního řadiče domény

Jádrem konfigurace celé Samby je jediný konfigurační soubor `smb.conf`, který se nachází v adresáři `/usr/local/etc`. Soubor může být dle typu konfigurace velmi rozsáhlý a složitý. V následujícím textu bude ukázána konfigurace potřebná pro roli primárního řadiče domény v síti střední školy. Konfigurační soubor je dělen do sekcí, které začínají názvem sdíleného prostředku uvedeného v hranatých závorkách a je následován konfiguračními parametry pro daný prostředek. Speciální sekcí je sekce `[global]`, ve které jsou nastaveny parametry ovlivňující chování celého serveru.

Níže uvedený konfigurační soubor ukazuje v sekci `[global]` nastavení Samba serveru jako primárního řadiče pro doménu s názvem GYMN. Jméno serveru je PROLIANT. Server je zároveň konfigurován jako WINS server. Domovský adresář uživatele je automaticky po přihlášení připojen jako disk `H`. Další sekce obsahují nastavení pro jednotlivá sdílení poskytovaná serverem. Pro doménová přihlášení jsou dále důležitá skrytá systémová sdílení `[homes]` obsahující nastavení pro domovské adresáře uživatelů, `[netlogon]` obsahující skripty spouštěné u klienta, výchozí profil, případně další systémové soubory a `[profiles]` obsahující nastavení a cesty pro ukládání cestovních profilů uživatelů.

Kromě těchto základních sdílených prostředků jsou nakonfigurována sdílení `[public]` a `[software]`, která jsou pomocí přihlašovacího skriptu připojena uživatelům jako síťové disky.

Okomentovaný soubor `smb.conf` se všemi potřebnými nastaveními:

```

[global]                                ;globální sekce
workgroup = GYMN                        ;název domény
netbios name = PROLIANT                 ;NetBIOS jméno serveru
passdb backend = tdbsam                 ;použitá databáze pro autentizaci
wins support = Yes                      ;zapnut WINS server
logon script = %a.bat                   ;jméno skriptu spuštěného při přihlášení
logon path = \\%L\profiles\%U\%a       ;cesta k cestovnímu profilu
logon drive = H:                        ;písmeno jednotky na kterou se připojí dom. adr.
domain logons = Yes                     ;zapnutí role PDC
os level = 34                           ;Samba bude hlavním místním prohlížečem
[homes]                                  ;nastavení pro domovské adresáře
comment = Home Directories
read only = No                           ;sdílení i pro zápis
browseable = No                          ;nezveřejňuje se v prohlížečích seznamech
create mask = 711                        ;maska pro vytváření nových souborů
directory mask = 711                    ;maska pro vytváření nových adresářů
map archive = Yes                        ;mapování atributu archivovat zapnuto
map hidden = Yes                         ;mapování atributu skrytý zapnuto
map system = Yes                         ;mapování atributu systémový zapnuto
[netlogon]                                ;systémové sdílení
comment = Network Logon Service
path = /samba/netlogon                  ;umístění na Samba serveru
public = no                              ;není povolen anonymní přístup
writeable = No                           ;není povolen zápis
browsable = No                           ;nezveřejňuje se v prohlížečích seznamech
map archive = Yes                        ;zapnuto mapování atributů
map hidden = Yes
map system = Yes
[profiles]                                ;sdílení pro ukládání profilů systému Windows
comment = Profile Share
path = /samba/profiles                  ;umístění na Samba serveru
writable = Yes                           ;povolen zápis
browsable = No                           ;nezveřejňuje se v prohlížečích seznamech
create mask = 711
directory mask = 711
map archive = Yes
map hidden = Yes
map system = Yes
;uživatelská sdílení
[public]
comment = Pro sdílení souboru
path = /samba/data/shares/public
writable = Yes
oplocks = No                             ;vypnutí oportunistických zámek souborů
level2 oplocks = No
[software]
comment = Software
path = /samba/data/shares/software

```

```
writable = Yes
oplocks = No
level2 oplocks = No
```

Konfigurační soubor je možné otestovat na syntaktickou správnost pomocí nástroje *testparm* spuštěného bez parametrů.

Adresáře uvedené v *path*, nad kterými jsou konfigurována sdílení, musí být na serveru ručně vytvořeny (příkaz *mkdir*) a také musí být nastavena správná oprávnění pro čtení, případně zápis (příkaz *chmod*).

Podadresáře sdílení [*profiles*] jsou pro jednotlivé uživatele vytvářeny automaticky při prvním přihlášení uživatele a inicializaci uživatelského profilu.

Z konfiguračního souboru je patrné, že obsahuje také proměnné uvozené znakem *%*. Samba umožňuje v konfiguračním souboru použití kolem dvaceti různých proměnných. Úplný seznam lze nalézt v manuálové stránce konfiguračního souboru *smb.conf*. Význam použitých proměnných je uveden v tabulce 2.6.

proměnná	význam
%a	verze operačního systému klienta – např. WinNT, WinXP, Win2k
%L	NetBIOS jméno serveru
%U	uživatelské jméno uživatele použité při relaci se serverem

Tabulka 2.6: Význam proměnných použitých v konfiguračním souboru

Proměnné *%a* je použito u parametru *logon script* k odlišení operačního systému, kvůli možné nekompatibilitě některých příkazů mezi různými verzemi operačního systému Windows.

Podobným způsobem bylo ošetřeno i uložení cestovních profilů, kde se opět ukázala problematická kompatibilita mezi různými verzemi operačního systému Windows (např. u systémů Windows NT a XP).

Dalším nastavením, které stojí za zmínění je mapování atributů. U souborových systémů používaných v operačních systémech Microsoft DOS a Windows existuje možnost nastavit atributy *archivovat*, *skrytý* a *systémový*. Jelikož k těmto atributům neexistuje v Unixu ekvivalent, nabízí Samba řešení jak tyto atributy pro klienty Windows zachovat – mapováním na bity příznaku spustitelnosti souboru v systému Unix. Bohužel tímto způsobem vznikají nesmyslně nastavené příznaky spustitelnosti v systému Unix, ale zachování atributů pro klienty Windows může být důležitější. Pokud je jediným způsobem přístupu klientů k serveru sdílení SMB, nemusí tento vedlejší efekt vadit vůbec.

Co se týče nastavení chování oportunistických zámků pomocí parametrů *oplocks* a *level2 oplocks*, byly vypnuty kvůli problémům s některým softwarem instalovaným později na vytvořená sdílení, který měl následně problémy s uzamykáním a odemykáním souborů. Oportunistické zámkové by měly, pokud jsou povoleny, zvýšit rychlost přístupu k souborům na Samba serveru, protože umožňují klientům intenzivní ukládání dat do lokální mezipaměti.

## 2.9.2 Spuštění Samba serveru

Po provedení konfigurace můžeme spustit služby Samba serveru a otestovat výsledek. V operačním systému FreeBSD je potřeba, pokud byl Samba server instalován zmíněným způsobem pomocí systému portů, spuštění Samba serveru nejdříve povolit. Povolení provedeme v konfiguračním souboru */etc/rc.conf* přidáním řádku

```
samba_enable="YES"
```

Poté je Samba server automaticky spuštěn při startu operačního systému. Konfigurační soubor `rc.conf` obsahuje informace o službách, které mají být spuštěny při startu systému. Tyto služby nejsou spuštěny přímo, ale pomocí dalších skriptů, které jsou pro programy doinstalovávány do operačního systému pomocí kolekce portů umístěny v adresáři `/usr/local/etc/rc.d`. Soubor `rc.conf` je místem pro jednotné povolení/zakázání instalovaných služeb a nastavení parametrů operačního systému.

Manuálně můžeme Samba server ovládat během běhu systému pomocí skriptu:

```
/usr/local/etc/rc.d/samba start|stop|restart
```

Informace o činnosti démonů jsou zaznamenávány do logovacích souborů `log.smbd` a `log.nmbd` umístěných v adresáři `/var/log/samba`.

### 2.9.3 Přihlašovací skripty

Přihlašovací skript je automaticky spuštěn na počítači klienta při procesu přihlašování ke stanici. Jméno a cesta k přihlašovacímu skriptu je uvedena v sekci `[global]` a nastavena parametrem `logon script`. Skript s daným jménem a případně cestou musí být umístěn v systémovém sdílení `[netlogon]`. Jelikož se jedná o skript (dávku) spouštěnou v klientském prostředí Windows, je potřeba při vytváření souboru dbát na správný formát – tj. řádky ukončené dvojicí znaků CR LF.

Následující obsah skriptu ukazuje mapování síťových disků po přihlášení uživatele. Síťová sdílení `[public]` a `[software]` jsou připojena jako síťové disky *P* a *S*:

```
net use p: \\proliant\public
net use s: \\proliant\software
```

### 2.9.4 Uživatelské účty

Uživatelé, kteří přistupují k serveru pomocí Samby, musí mít vytvořen uživatelský účet. Jelikož standardní databáze v systémech Unix není kompatibilní s databází, která uchovává informace o uživateli Samby, musí uživatel existovat v obou databázích. Musí být vytvořen účet v systému, na kterém Samba běží (kvůli identifikátoru uživatele, použitému u vlastnictví a oprávnění). Tento účet může být následně přidán do databáze Samby.

Zároveň tak vznikají dvě databáze šifrovaných hesel, které jsou problematicky synchronizovatelné. V případě, že uživatel přistupuje k serveru pouze přes sdílení nabízená Samba serverem, není tento problém třeba řešit. Pokud je potřeba obojí přístup uživatele (například SSH a Samba) a přihlášení pomocí jednotného hesla, je možné využít autentizačních modulů a provádět autentizaci proti Samba serveru.

V konkrétní popisované instalaci takovýto přístup požadován nebyl. Uživatelé přistupují k serveru pouze pomocí Samby a vzdálené přihlášení přes SSH bylo běžným uživatelům zakázáno.

Přidání konkrétního uživatele s uživatelským jménem *novak* může být učiněno následovně:

Přidání uživatele do systému:

```
proliant# adduser
Username: novak
Full name: Novak Pavel
```



```
Enter password: *****
Enter password again: *****
```

Přidání uživatele do Samby:

```
proliant# smbpasswd -a novak
New SMB password: *****
Retype new SMB password: *****
Added user novak.
```

Nyní je uživatel vytvořen a může se přihlásit do domény.

Pro hromadné vytváření uživatelských účtů ve FreeBSD je vhodnější použití programů umožňujících dávkové zpracování, například *chpass* nebo *pw*. Skript umožňující vytvoření uživatelského účtu a následně jeho přidání do Samby je uveden v příloze [A.5](#)

Hned z počátku je také vhodné přidat do databáze Samby uživatele *root*, bude později potřeba při přidávání stanic do domény.

### Důvěryhodné účty stanic

Důvěryhodný účet stanice je použit k autentizaci klientské stanice vůči řadiči domény. Autentizace klientské stanice je využito z bezpečnostních důvodů, aby se nemohla jiná stanice, která použije stejné jméno NetBIOS, podílet na bezpečnostních operacích domény a získat tak přístup k doménovým účtům a skupinám.

Důvěryhodné účty stanic jsou vytvářeny obdobným způsobem, jako běžné uživatelské účty, tzn. účet je nejprve vytvořen v systému, na kterém Samba běží a poté přidán do Samby. Účet musí být v okamžiku, kdy chceme stanici přidat do domény, vytvořen.

Pro účty stanic byla zavedena konvence – jejich uživatelské jméno je tvořeno jménem NetBIOS stanice přidávané do domény následované znakem \$.

Přidání účtu stanice může vypadat následovně:

Přidání do systému:

```
proliant# chpass -a \  
'jmeno_stanice$:*:101:100::0:0:Ucet stanice:/dev/null:/sbin/nologin'
```

Přidání do Samby:

```
proliant# smbpasswd -a -m jmeno_stanice
```

Přidání uživatelského účtu pomocí *chpass* má výhodu spíše pro dávkové zpracování. Je potřeba správně nastavit UID a GID. Zato je možné vše nastavit v jednom příkazu, narozdíl od interaktivního zadávání informací pomocí příkazu *adduser*.

### Autentizační databáze Samby

Samba používá samostatnou databázi pro ukládání informací o uživatelských jménech a dalších informací potřebných pro funkcionalitu doménového řadiče.

Typ použité databáze je nastaven opět v konfiguračním souboru *smb.conf* v sekci `[global]` pomocí parametru *passdb backend*. V tomto případě byla použita databáze *tdb-sam*. Uložení dat v *tdb* (trivial database) nevyžaduje žádnou další konfiguraci a databáze je obhospodářována plně v režii Samba serveru. Databáze není doporučena pro rozlehlá

síťová prostředí, kde je požadována škálovatelnost a implementace záložních řadičů domény, protože replikace a synchronizace tdb může být problematická. V prostředích s jedním serverem je však databáze tdb velmi dobře použitelná.

Pro rozlehlá síťová prostředí je jednoznačně doporučeno používat pro ukládání informací některý z LDAP serverů (například implementaci OpenLDAP).

Z důvodů kompatibility jsou podporována i nešifrovaná hesla od klientů, která jsou následně porovnávána vůči Unixové databázi hesel. Toto nastavení není doporučeno jednak kvůli nutnosti speciální konfigurace klientů (vypnutí šifrování hesel), ale hlavně nešifrovaný přenos hesel po síti není bezpečný.

Dalším, již zastaralým způsobem, je uložení hesel spolu s dalšími informacemi v souboru *smbpasswd*, jako ASCII text se šifrovanými hesly. Tento způsob není efektivní jednak kvůli nutnosti sekvenčního procházení souboru a také neumožňuje uložit všechny informace potřebné v novějších verzích Samba serveru.

### 2.9.5 Přidání stanice do domény

Jak již bylo zmíněno, pro přidání stanice do domény, tedy k vytvoření důvěryhodného vztahu s primárním řadičem domény, je potřeba vytvořit na Samba serveru účet stanice.

Samotné přidání je nutné provést na klientské stanici Windows následovně:

V nabídce *Start* vybereme *Nastavení* a otevřeme okno *Ovládací panely*. Zde poklepáním na ikonu *Systém* otevřeme dialogové okno a vybereme kartu *Název počítače*. Klikneme na tlačítko *Změnit* a otevře se další okno. Z pracovní skupiny přepneme kliknutím na doménu a vyplníme název domény, jejímž má být stanice členem. Po potvrzení jsme dotázáni na jméno a heslo uživatele s oprávněním přidávat stanice do domény. Zadáme jméno a heslo uživatele root a potvrdíme. Pokud bylo vše správně nakonfigurováno, objeví se uvítací hláška oznamující úspěšné připojení k doméně. Poté je potřeba provést restart systému, po němž je stanice připravena na doménová přihlášení uživatelů.

Vstoupení do důvěryhodného vztahu s doménou je možné u operačních systémů Windows NT, 2000 a XP Professional. V operačním systému Windows XP Home je podpora doménových přihlášení odebrána. U systémů Windows 95/98/Me je sice možnost přihlašování do domény, ale ve skutečnosti tyto systémy nemohou být pravými členy domény, protože nepodporují důvěryhodné účty a nemohou vstoupit do důvěryhodného vztahu s doménou.

Vstoupením stanice do důvěryhodného vztahu s doménou mohou uživatelé využívat výhod doménového bezpečnostního modelu – centrální autentizace vůči Samba serveru, řízení přístupu, centrálního přidělování a odebrání oprávnění k prostředkům domény, které může vést na jednotné přihlášení uživatele ke všem potřebným síťovým prostředkům – SSO (Single Sign On).

## Kapitola 3

# Tiskové služby

### 3.1 Úvod

Sdílení tiskáren v síti patří, spolu se sdílením souborů, k základním službám, které může Samba server pomocí protokolu SMB poskytovat. Se službami sdílení tiskáren a souborů je v interakci přímo uživatel. V základním principu jsou si tyto dvě služby velice podobné, protože u sdílení souborů i tiskáren jsou přenášeny po síti soubory. Zatímco soubor přenesený na server u služby sdílení souborů je trvale uložen na diskové médium, soubor tiskové služby je uložen dočasně do fronty tiskových úloh tiskárny a po dokončení tiskové úlohy tiskárnou odstraněn.

Zpracování tiskové úlohy má svá specifika i na straně klienta. Před odesláním tiskového souboru na server musí být data zpracována do formátu srozumitelného pro tiskárnu nebo tiskový podsystém serveru. Formáty dat pro tiskárny a konfigurační nastavení posílaná tiskárně (například kvalita tisku, více stránek na list, oboustranný tisk a další specifická nastavení závislá na možnostech konkrétního modelu tiskárny) se mohou lišit modelem tiskárny i jednotlivými výrobci. V prostředí Windows řeší tato specifika tiskáren ovladače, které po instalaci zpřístupní instalovaný model tiskárny v nabídkách pro tisk, včetně nabídek pro nastavení možností tisku, a obstarají správný formát dat tiskové úlohy. Tiskárny mohou používat i standardní jazyk pro popis dokumentů pro tisk – PostScript. Podpora tohoto jazyka nebývá samozřejmostí, zvláště u levnějších typů tiskáren.

Problematika tiskových sdílení na Samba serveru, přípravy a zpracování tiskových úloh, komunikace Samba serveru se vzdálenými tiskárnami, ovladačů tiskáren a jejich instalace na stanice Windows, automatického přidání do seznamu tiskáren každého uživatele a přípravy síťových tiskáren k okamžitému použití bez nutnosti interakce ze strany uživatele, bude obsahem dalších kapitol.

### 3.2 Zpracování tiskových úloh Samba serverem

Tiskové služby mohou běžet na serveru Samba nebo na samostatném tiskovém serveru. Podpora tiskových služeb v Sambě je vždy závislá na instalovaném tiskovém podsystému v systému, na kterém Samba běží. Samba pouze přebírá tiskový soubor pomocí protokolu SMB od klienta a předává ho ke zpracování tiskovému podsystému. Samba neprovádí na datech tiskového souboru žádné zpracování ani filtraci. Samba sehrává u tiskových služeb pouze roli prostředníka. Zpřístupňuje tisková sdílení pomocí protokolu SMB a předává tiskové úlohy přijaté od klientů ke zpracování tiskovému podsystému voláním příslušného

příkazu.

Zpracování tiskové úlohy je složeno z několika kroků:

1. Otevření spojení k tiskovému sdílení a autentizace klienta.
2. Přenos tiskového souboru po síti.
3. Odpojení klienta od sdílení.
4. Uložení souboru do fronty tiskových úloh na serveru.
5. Volání příkazu tiskového podsystému.
6. Přenos souboru do tiskového zařízení.
7. Odstranění souboru z fronty tiskových úloh serveru.

Kroky 1 – 3 jsou součástí komunikace klienta se Samba serverem pomocí protokolu SMB. Po uložení souboru do tiskové fronty tiskárny musí další úkony obstarat služby tiskového podsystému běžícího na Samba serveru. Samba implementuje podporu pro interakci s několika tiskovými službami systému Unix. K podporovaným patří klasické tiskové systémy stylu UNIX BSD a System V a novější tiskový systém CUPS (Common Unix Printing System).

### 3.2.1 Požadavky kladené na tiskový podsystém

V síti střední školy byly zjištěny následující požadavky na síťový tisk:

- celkem tři tiskárny umístěné ve dvou počítačových učebnách – 2x černobílé laserové HP, 1x barevná laserová Epson;
- tiskárny HP připojeny do sítě pomocí harwarových tiskových serverů;
- tiskárna Epson připojena ke stanici Windows;
- tisk možný z libovolného PC;
- funkcionality účtování a řízení přístupu není vyžadována (přístup pod dohledem vyučujícího).

Pro řešení problematiky tiskových služeb byl na základě požadavků kladených na tiskový systém vybrán klasický tiskový systém typu BSD. Tento tiskový systém je integrován již v základní instalaci operačního systému FreeBSD a plně vyhovuje požadavkům řešené sítě.

Pokud jsou kladené na tiskové služby větší nároky a jsou požadovány například služby centrálního účtování, sledování jednotlivých tiskových stran a různých statistických dat, je doporučeno použít tiskový systém CUPS, kde je tato funkcionality lépe podporována.

## 3.3 Klasická podpora tisku

### 3.3.1 Klasický tiskový podsystém ve FreeBSD

Standardním tiskovým podsystémem v operačním systému FreeBSD je *Berkeley line printer spooling system* známý též jako LPD.

LPD obstarává vše potřebné pro provedení tisku. Je zodpovědný za:

- řízení přístupu k připojeným tiskárnám a k tiskárnám připojeným k jiným hostitelským počítačům na síti;
- umožňuje uživatelům odeslání tiskové úlohy na tiskárnu;
- obstarává mechanismus pro nekonfliktní sdílení tiskáren a tiskové fronty;
- obstarává komunikaci se samotnými tiskárnami přes různá rozhraní (sériové, paralelní, USB, síť...);
- může spouštět speciální filtry nad přijatými tiskovými úlohami;
- může sbírat informace o využití tiskáren.

Konfigurace tiskového podsystému LPD je umístěna v souboru `/etc/printcap`. Tento konfigurační soubor je načítán při každém použití LPD, takže případně provedené změny vstupují v platnost téměř ihned.

Před provedením editace souboru `/etc/printcap` je potřeba provést přípravu adresářů, do nichž se budou ukládat příchozí tiskové úlohy pro jednotlivé tiskárny. Obvyklým umístěním je adresář `/var/spool/lpd`. Adresář je potřeba vytvořit:

```
mkdir /var/spool/lpd
```

Je vhodné dále vytvářet podadresáře s identickým pojmenováním jako je jméno tiskárny:

```
mkdir /var/spool/lpd/jmeno-tiskarny
```

Pro ochranu adresářů s tiskovými úlohami před nežádoucím přístupem je vhodné nastavit na jednotlivých podadresářích tiskáren následující oprávnění:

```
chown daemon:daemon /var/spool/lpd/jmeno-tiskarny
chmod 770 /var/spool/lpd/jmeno-tiskarny
```

Nyní je potřeba zeditovat soubor `/etc/printcap` a doplnit potřebné informace o tiskárnách. Konfigurace pro jednu tiskárnu s názvem `laserjet` připojenou lokálně pomocí paralelního portu by mohla vypadat následovně:

```
laserjet|lp:\
    :sh:sd=/var/spool/lpd/laserjet:\
    :lp=/dev/lpt0:
```

Znakem „|“ jsou oddělena alternativní pojmenování tiskárny, kterých může být několik. Název `lp` má navíc speciální význam, protože specifikuje výchozí tiskárnu. Parametr `sh` potlačuje tisk hlavičkové stránky tiskové úlohy, `sd` určuje umístění adresáře s frontou tiskových úloh a `lp` jméno zařízení pro tiskový výstup.

## Spuštění LPD

Po vytvoření konfigurace v konfiguračním souboru `/etc/printcap` můžeme provést spuštění démona LPD. Spuštění démona je potřeba povolit v konfiguračním souboru `/etc/rc.conf` přidáním řádku:

```
lpd_enable="YES"
```

Po příštím startu systému dojde k automatickému startu démona. Bez restartu systému je možné démona spustit zadáním příkazu:

```
# lpd
```

Nyní je tiskový systém LPD připraven k použití.

## Tisk pomocí hardwarových tiskových serverů

Jelikož požadavky na umístění síťových tiskáren mohou být (a obvykle jsou) značně odlišné od umístění samotného serveru, nebývá tisk pomocí lokálních portů (LPT, COM, USB...) dobře použitelný. Řešením může být připojení tiskárny k libovolnému jinému počítači v síti a přeposílání tiskových úloh. V případě počítače s Unixovým systémem může být pro splnění této úlohy použito opět LPD nastaveného pro komunikaci po síti přes TCP/IP. Stejně tak je možné využít tiskárnu připojenou v síti k počítači s operačním systémem Windows použitím skriptu `smbprint` jakožto filtru volaného pomocí LPD.

Nevýhody tohoto řešení jsou především v nutnosti zapnutého počítače, ke kterému je tiskárna připojena a jeho nezaručené dostupnosti, pokud je použit zároveň jako stanice pro běžné uživatele.

Lepším řešením je použití hardwarových tiskových serverů – zařízení, která se připojí k tiskárně a k počítačové síti a samostatně zprostředkovávají přístup k tiskárně přes síť. Cena těchto zařízení není vysoká, mohou poskytovat různou funkcionalitu a různé typy a počet portů pro připojení tiskáren. Některé typy tiskáren nabízejí tiskový server již v základní výbavě, jiné mohou disponovat rozšiřujícími pozicemi pro dokoupení modulu tiskového serveru jako příslušenství. Hardwarový tiskový server může být bez problémů zapnutý spolu s tiskárnou stále.

Nastavení hardwarového tiskového serveru je možné obvykle pomocí webového rozhraní a/nebo speciální aplikace od výrobce. Konkrétní postup konfigurace je závislý na výrobci daného zařízení.

Pro komunikaci s LPD je potřeba znát následující údaje:

- nastavenou IP adresu zařízení (potřeba správně nastavit dle síťového prostředí);
- názvy tiskových portů, které zařízení poskytuje.

Konkrétní nastavení v souboru `/etc/printcap` může pro tiskárnu `ljivt` vypadat následovně:

```
ljivt:\
:lp=:\
:rm=ljivt:\
:rp=L1:\
:lf=/var/spool/lpd/ljivt.log:\
:sd=/var/spool/lpd/ljivt:
```

Parametr `lp` zde nemá nastavenou hodnotu, `rm` určuje název nebo IP adresu vzdáleného tiskového serveru, `rp` vzdálený tiskový port poskytovaný zařízením, `lf` umístění logovacího souboru tiskárny a `sd` umístění adresáře s tiskovou frontou. Kompletní konfigurační soubor použitý v prostředí školy je uveden v dodatku [A.1](#)

### Tisk na vzdálené tiskárně připojené ke stanici s operačním systémem Windows

Ačkoliv pořízení hardwarového tiskového serveru může být lepší volba, může být požadováno využití tiskárny připojené ke stanici Windows jako síťové tiskárny. Za tímto účelem je možné použít skript `smbprint`, který je možné po instalaci Samby nalézt v adresáři `/usr/local/share/examples/samba/printing`. Skript je vhodné zkopírovat do jiného umístění. Následně se použije jako vstupní filtr, určený parametrem `if`, při konfiguraci tiskárny v souboru `/etc/printcap`:

```
ljivtcolor:\
:lp=/dev/null:\
:lf=/var/spool/lpd/ljivtcolor.log:\
:sd=/var/spool/lpd/ljivtcolor:\
:sh:\
:if=/usr/local/samba/bin/smbprint:
```

Skript `smbprint` obstará při provádění tiskové úlohy připojení se k počítači s Windows pomocí protokolu SMB a odeslání tiskové úlohy.

U tiskárny je potřeba na stanici Windows provést sdílení. Na sdílení může být aplikováno oprávnění a vytvořen pro tisk speciální uživatel, který jediný bude mít oprávnění na sdílené tiskárně síťově tisknout a pomocí kterého se bude tiskový podsystém k tiskárně připojovat. Následně je potřeba tyto informace dodat skriptu `smbprint`. Ve výchozím nastavení očekává konfigurační soubor s názvem `.config` v adresáři určeném parametrem `sd` v souboru `printcap` u dané tiskárny. Skript `smbprint` očekává v souboru `.config` následující parametry:

```
server
service
password
username (volitelně)
IP (volitelně)
debug (volitelně)
debugsmb (volitelně)
debugfile (volitelně)
```

Konkrétní příklad souboru `.config`:

```
#název stanice
server="ivt_10"
#název tiskového sdílení
service="ljivtcolor"
#uživatel, pod kterým se skript připojí ke sdílení
username="printuser"
#heslo
password="passwd"
```

Další informace lze nalézt v samotném souboru se skriptem `smbprint`, který je hojně komentován.

### 3.3.2 Nastavení tiskových sdílení v Sambě

Konfigurace tiskových sdílení je velmi podobná konfiguraci souborových sdílení a stejně jako v případě souborových sdílení je provedena jednotně v souboru `smb.conf`. K dispozici jsou opět globální parametry, které mohou být uvedeny pouze v sekci `[global]` a parametry nastavitelné pro každé jednotlivé sdílení, které mohou být uvedeny jednak v sekcích `[global]` a `[printers]`, ve kterých specifikují výchozí hodnoty parametrů pro všechna sdílení, ale také u samotných jednotlivých sdílení (v tomto případě mají přednost před globálně nastavenými). Tisková sdílení mají v porovnání se souborovými navíc některé specifické parametry.

Příklad jednoduché konfigurace:

```
[global]
printing = bsd
load printers = yes
[printers]
path = /var/spool/samba
printable = yes
writable = no
[ljivt]
comment = "Tiskarna u ucebne IVT"
path = /var/spool/samba/ljivt
printable = yes
```

Popis důležitých parametrů specifických pro tisková sdílení je uveden v příloze [B.1](#) a kompletní soubor `smb.conf` v příloze [A.2](#).

#### Sekce `[printers]`

Sekce `[printers]` je speciální sekci, podobně jako sekce `[global]`. Pokud je tato sekce uvedena v souboru `smb.conf`, je klientům zveřejněn seznam tiskáren uvedený v souboru `/etc/printcap` a jsou zpřístupněna tisková sdílení. Parametry specifikované v této sekci jsou aplikovány na všechna tisková sdílení jako výchozí hodnoty. V případě potřeby je možné pro konkrétní tiskárny vytvořit vlastní nastavení vytvořením dalších sekcí s názvem tiskárny v souboru `smb.conf`.

#### Sekce `[jméno_tiskárny]`

Pokud je v souboru `smb.conf` nalezena speciální sekce pojmenovaná stejně jako tiskárna, a navíc obsahuje parametr `printable = YES`, Samba zpracuje tuto sekci jako specifické tiskové sdílení. Je potřeba dát si pozor při pojmenovávání tiskových sdílení, aby nebyly v konfliktu s existujícím souborovým sdílením nebo názvem uživatelského účtu existujícího uživatele. Při požadavku klienta na sdílení jsou nejdříve vyhodnocována souborová sdílení a v případě konfliktu by byl uživatel připojen k souborovému sdílení, místo k požadovanému tiskovému.



## Tiskové příkazy

V každé sekci, která definuje tiskárnu, nebo ve společné sekci `[printers]`, mohou být uvedeny parametry, které určují, jaké příkazy tiskového podsystému jsou volány Sambou nad souborem přijatým od klienta a uloženým do adresáře tiskové fronty. Tyto příkazy obvykle není nutné pro správnou komunikaci Samby s tiskovým podsystémem měnit, protože jsou nastaveny automaticky podle zvoleného tiskového podsystému parametrem `printing`.

Mohou však nastat situace, ve kterých je možnost změny volaného příkazu užitečná. Například při hledání chyb, pokud tiskový podsystém nefunguje správně. V takovém případě je možné jako tiskový příkaz volat například skript, který zaznamená ladící informace o tiskové úloze pro následnou analýzu problému.

Možnost volby tiskových příkazů nemusí být užitečná jenom v případě hledání chyb. Může být použita pro vytváření vlastních tiskových skriptů, které kromě samotného tisku vykonávají další úkony.

Pokud je použito místo klasického tiskového systému tiskového systému CUPS a Samba je zkompilována s podporou CUPS, jsou veškeré tiskové příkazy specifikované v souboru `smb.conf` ignorovány, protože Samba pro komunikaci s CUPS používá přímo aplikační rozhraní knihoven CUPS. Tabulka 3.1 zobrazuje výchozí hodnoty tiskových příkazů pro hodnotu parametru `printing=bsd`.

úloha	parametr v smb.conf	výchozí příkaz
zahájení tisku	<code>print command</code>	<code>lpr -r -P\%p \%s</code>
výpis úloh tiskové fronty	<code>lpq command</code>	<code>lpq -P\%p</code>
odstranění úlohy z tiskové fronty	<code>lprm command</code>	<code>lprm -P\%p \%j</code>
pozastavení tiskové úlohy	<code>lppause command</code>	<code>lp -i \%p-\%j -H hold</code>
obnovení tiskové úlohy	<code>lpresume command</code>	<code>lp -i \%p-\%j -H resume</code>

Tabulka 3.1: Výchozí hodnoty tiskových příkazů

Příkazy jsou volány s příslušnými parametry. Znak „%“ uvozuje makro, které je při volání příkazu nahrazeno skutečnou hodnotou. V tabulce 3.2 je uveden seznam nejdůležitějších maker použitelných při volání tiskových příkazů.

makro	význam
<code>\%s</code> , <code>\%f</code>	cesta k tiskovému souboru uloženému do adresáře tiskové fronty
<code>\%p</code>	název tiskárny
<code>\%J</code>	jméno tiskové úlohy přijaté od klienta
<code>\%c</code>	počet vytisknutých stran tiskové úlohy (pokud je známo)
<code>\%z</code>	velikost tiskové úlohy ve frontě (v bytech)

Tabulka 3.2: Makra použitelná při volání tiskových příkazů

Tiskový příkaz musí obsahovat alespoň jeden výskyt makra `%s` nebo `%f`. Výskyt `%p` je volitelný. Pokud není specifikován, je použito výchozí tiskárny.

Tiskové příkazy mohou být specifikovány v sekci `[global]`. V takovém případě jsou použity jako výchozí pro každé tiskové sdílení, které neobsahuje vlastní specifikaci.

Příklad vlastního tiskového příkazu uvedeného v souboru `smb.conf`:

```
print command = echo Printing \%s >> /tmp/print.log; lpr -P \%p \%s; rm \%s
```

Tiskové příkazy jsou předány přímo Unixovému shellu. Uvedený příklad zaznamená jméno souboru tiskové úlohy do souboru `/tmp/print.log`, zavolá příkaz tiskového pod-systému a nakonec soubor tiskové úlohy smaže.

## 3.4 Ovladače tiskáren

### 3.4.1 Úvod

V dřívějších verzích Samby byla podpora tisku omezena na tisková volání protokolu LanMan. Stejný protokol používají pro poskytování tiskových sdílení stanice s operačním systémem Windows 9x/Me. Uvedením Samby verze 2.2.0 byla zahájena podpora tisku pomocí stejných mechanismů, které používají operační systémy typu Windows NT. V těchto systémech je podpora tisku implementována pomocí vzdáleného volání procedury (MS-RPC - *Microsoft Remote Procedure Call*). MS-RPC využívá pro tisk pojmenovaných rour (*named pipes*).

Oproti původní podpoře implementované pomocí protokolu LanMan nabízí tisk pomocí MS-RPC následující možnosti:

- podporu pro stažení ovladačů tiskárny ze serveru na vyžádání;
- nahrání ovladačů nové tiskárny na server pomocí průvodce přidáním tiskárny, který je k dispozici v NT verzích operačního systému Windows;
- podporu oprávnění (ACL – *Access Control Lists*) stylu NT aplikovaných na tisková sdílení;
- vylepšenou manipulaci s tiskovými frontami pomocí interní databáze TDB (*trivial database*) Samby, uchovávající informace o tiskových úlohách čekajících v tiskových frontách.

### 3.4.2 Způsoby instalace ovladačů na klientské stanice

Při instalaci ovladačů pro tiskárny poskytované tiskovým sdílením Samba serveru na klientské stanice jsou možné dva přístupy:

- ruční přidání tiskárny a instalace ovladačů na každé klientské stanici, která chce tiskárnu využívat;
- automatické stažení ovladačů ze serveru a instalace ovladačů tiskáren při jejich prvním použití.

Preferována je druhá možnost, protože nabízí snadnou instalaci tiskárny a centrální distribuci ovladačů klientům pomocí Samba serveru.

Pro uložení ovladačů existuje na serveru speciální skryté systémové sdílení, podobné například systémovým sdílením `[netlogon]`, pro uložení přihlašovacích skriptů a ostatních souborů souvisejících s přihlašováním uživatelů a `[profiles]` sloužící pro uložení uživatelských profilů. Sdílení pro uložení ovladačů má název `[print$]` a musí být definováno v souboru `smb.conf` podobně jako ostatní sdílení.

Aby si klienti Windows mohli ovladače stáhnout, je potřeba do vytvořeného speciálního sdílení `[print$]` ovladače tiskáren připravit a uložit. Ovladače nemohou být jednoduše do připraveného sdílení pouze zkopírovány. Použití některého z následujících postupů je nutné,

aby si Samba vytvořila správné záznamy ve svých interních databázových strukturách a mohly být poskytnuty správné ovladače pro jednotlivá tisková sdílení. Postupů uložení ovladačů do tohoto sdílení a následně jejich provázání s konkrétním tiskovým sdílením je několik:

- nahrání ovladačů pomocí grafického uživatelského rozhraní z klienta Windows pomocí průvodce přidáním nové tiskárny;
- použití příkazové řádky na stanici Unix a nástrojů `smbclient` a `rpcclient`;
- využití nástroje `lmprints`;
- použití nástroje `cupsaddsmb` (při použití tiskového systému CUPS).

Samba tyto ovladače uložené na serveru žádným způsobem při své činnosti nevyužívá (jedná se o binární soubory systému Windows). Ovladače jsou pouze poskytnuty pro stažení a jsou kompletně prováděny na straně klienta Windows, který pomocí tiskového sdílení odesílá hotový tiskový soubor, který je výstupem zpracování daného ovladače tiskárny.

U tiskového serveru založeném na operačním systému Windows NT existuje navíc další možnost zpracování tiskové úlohy. Ovladače mohou být spuštěny na serveru samotném a server poskytuje klientovi pouze určité informace o tiskárně pro zobrazení konkrétních tiskových dialogů.

Zpracování tiskových úloh na serveru využívá také tiskový systém CUPS popsany v kapitole 3.5

Dále bude popsán první postup instalace ovladačů na server z uvedeného seznamu – nahrání ovladačů na server pomocí průvodce přidáním tiskárny z klientské stanice Windows.

### 3.4.3 Nahrání ovladačů na server pomocí průvodce přidáním tiskárny

Předpokladem následujících úkonů je existující systémové sdílení `[print$]`. Pro jeho vytvoření je potřeba nejdříve vytvořit na Samba serveru potřebný adresář:

```
mkdir /usr/local/samba/drivers
```

a do souboru `smb.conf` přidat následující řádky:

```
[print$]
comment = Printer Driver Download Area
path = /usr/local/samba/drivers
browseable = yes
guest ok = yes
read only = yes
write list = @ntadmin, root
```

#### Struktura tiskového sdílení

Uspořádání adresářů s souborů ve sdílení `[print$]` bylo navrženo s ohledem na možnost existence klientů s různými operačními systémy a platformami. Tato struktura je pevně daná. Proto je potřeba před samotným nahráním vytvořit adresáře pro platformy, pro které hodláme ovladače poskytovat:

```
[print$]--+
|--W32X86      # ovladače pro Windows NT x86
|--WIN40       # ovladače pro Windows 95/98
|--W32ALPHA    # ovladače pro Windows NT Alpha_AXP
|--W32MIPS     # ovladače pro Windows NT R4000
|--W32PPC      # ovladače pro Windows NT PowerPC
```

Pro platformu Windows NT/2000/XP vytvoříme podadresář:

```
mkdir /usr/local/samba/drivers/W32X86
```

Nahrání ovladačů na server je potřeba provést buď pod uživatelským účtem s uid=0 (root) nebo může ovladače nahrát uživatelský účet, který je uveden v souboru `smb.conf` v seznamu parametru `printer admin`. Tento účet musí mít zároveň oprávnění zapisovat do sdílení `[print$]` v systému Unix.

### Instalace ovladačů ze stanice Windows

Tiskárny zpřístupněné pomocí tiskových sdílení Samba serveru lze zobrazit na stanici s Windows XP v *Místech v síti* nalezením a prohlížením serveru Samba a otevřením sdílených tiskáren. Po nalezení tiskárny, pro kterou chceme na server instalovat ovladače, ji vybereme kliknutím pravým tlačítkem myši a vybereme „*Vlastnosti*“. Jelikož se nyní pokoušíme o zobrazení vlastností tiskárny, která nemá doposud přiřazený ovladač, je vráceno chybové hlášení: „*Vlastnosti zařízení nemohou být zobrazeny. Ovladač pro vybranou tiskárnu není nainstalován. Chcete nyní nainstalovat ovladač?*“

Pozor. V tomto chybovém dialogu místo (logického) kliknutí na „*Ano*“ je potřeba kliknout na „*Ne*“. Poté je zobrazeno okno s vlastnostmi tiskárny. Nyní je možné provést instalaci požadovaných ovladačů buď vybráním ovladače ze seznamu instalovaných ovladačů (ve výchozím stavu prázdný) nebo vybrat instalaci nového ovladače tiskárny, která spustí průvodce přidáním tiskárny.

Jakmile je průvodce spuštěn, je způsob instalace stejný jako při instalaci jakékoliv jiné (místní) tiskárny. Po instalaci ovladačů je možné provést nastavení některých dalších parametrů tiskového sdílení jako oprávnění tiskárny (ACL) a nastavení výchozích parametrů tiskárny.

### Inicializace ovladačů

Velice důležitým okamžikem pro dokončení kompletní přípravy ovladačů tiskáren na Samba serveru je instalace ovladačů ze serveru na první klientskou stanici. Poté, co je instalace u prvního klienta dokončena, jsou ovladače inicializovány, vytvořeny potřebné záznamy ve vnitřních databázi Samby a nadále při instalaci ovladačů u dalších klientů nevyžadují již žádnou další pozornost.

Z první stanice, na kterou se provádí instalace ovladačů, je potřeba se k tiskovému sdílení připojit jako uživatel s uid=0 (root) nebo pomocí účtu s oprávněním administrace tiskáren. Z konzole Windows je možné připojit se ke sdílení s ovladači zadáním následujícího příkazu:

```
net use \\SAMBA-SERVER\print$ /user:root
```

V případě, že již ke sdílení existuje připojení pod jiným uživatelským jménem, je vypsáno chybové hlášení. Bohužel ve Windows není snadné řídit připojení ke sdílením a neexistuje snadný způsob provedení odhlášení od již připojeného sdílení. Ve verzích Windows vycházejících z Windows NT je možné odpojit se od všech sdílení restartováním služby *Workstation*. Nejjednodušším řešením může být restart stanice a přihlášení se pod uživatelským účtem s potřebným oprávněním.

Postup instalace ovladačů je potřeba provést v následujících krocích:

- najít pomocí prohlížení síťového okolí server Samba, otevřít složku se sdílenými tiskárnami;
- na tiskárnu, kterou hodláme instalovat, kliknout pravým tlačítkem myši a vybrat „*Nainstalovat tiskárnu*“.

Po proběhnutí instalace by se měla nově nainstalovaná tiskárna objevit ve složce lokálních tiskáren (*start* → *nastavení* → *ovládací panely* → *tiskárny a faxy*).

Obvykle je po instalaci tiskárny nabídnuta možnost vytisknutí zkušební stránky. Můžeme s nabídkou k vytištění souhlasit, ale s největší pravděpodobností nám bude vráceno chybové hlášení, že nelze zkušební stránku vytisknout. Důvodem je stále chybějící prvotní inicializace ovladačů a chybějící informace tiskového ovladače na Samba serveru.

Proto, aby byly ovladače použitelné, musí být k dispozici následující informace:

- nastavení zařízení vygenerované ovladačem tiskárny (například velikost papíru, orientace, nastavení duplexní jednotky);
- množina dalších interních dat ovladače nutných pro správnou funkčnost ovladače.

V případě, že nejsou tyto informace správně inicializovány, pokus o tisk může generovat množství chybových hlášení a špatný tiskový výstup. Samba si ukládá informace do interních databázových souborů (konkrétně *ntprinters.tdb*, *ntdrivers.tdb*, *printing.tdb*, *ntforms.tdb*).

Správnou inicializaci je možné provést pouze provedením kódu ovladače. Jelikož se jedná o spustitelné soubory systému Windows, je potřeba provést inicializaci z klientského počítače s operačním systémem Windows. Protože Samba nemůže spustit kód ovladačů pro Windows, jsou výchozí hodnoty v databázových strukturách inicializovány hodnotou *NULL*.

Nejjednodušším způsobem vygenerování správných hodnot pro inicializaci ovladače je otevření vlastností dané síťové tiskárny na klientském počítači a například změna orientace stránky ze stojato naležato a zpět. Vždy je potřeba provést uložení změn mezi jednotlivými změnami. Tento úkon vede na provedení dostatečného množství kódu ovladače a na Samba serveru jsou inicializovány v interní databázi všechny potřebné hodnoty.

V tomto okamžiku je také správný čas pro nastavení všech požadovaných výchozích hodnot nastavení tiskárny, neboť provedená nastavení dostanou všichni budoucí klienti, kteří se připojí k tiskárně, jako výchozí.

Nyní by měl tisk probíhat dle očekávání.

Další možností, jak provést inicializaci ovladače je parametr souboru *smb.conf* uvedený u tiskového sdílení s názvem *default devmode*. Některé ovladače fungují s tímto nastavením dobře, jiné mohou mít problémy. Proto je vždy nejlepší použít popsanou metodu provedení inicializace pomocí provedení ovladače u klienta.

## Instalace ovladačů u klientů Windows

Instalace inicializovaných ovladačů na další klientské stanice je obdobná jako prvotní instalace s těmito rozdíly:

- tiskárna může být připojena pod libovolným uživatelem;
- po připojení tiskárny (tedy po jejím přidání mezi lokální tiskárny uživatele) je možné tuto tiskárnu ihned použít pro tisk.

Jediný problém který zde vyvstává je, že u uživatele, který poprvé instaluje danou tiskárnu na dané pracovní stanici, dojde ke stažení ovladačů ze serveru na lokální disk. Uživatel který tuto operaci provádí nemusí mít speciální oprávnění na serveru (nepotřebuje oprávnění správce tiskáren ani uživatele root), ale musí mít dostatečná oprávnění na pracovní stanici. Jakýkoliv další uživatel, připojující se s síťové tiskárně na dané pracovní stanici, již speciální oprávnění na serveru ani stanici nepotřebuje.

S tímto je potřeba počítat v prostředích, ve kterých mají uživatelé Windows na stanicích omezená oprávnění zápisu a lokální instalace softwaru a je potřeba při přidávání nové tiskárny zajistit tuto prvotní instalaci ovladačů pod privilegovaným uživatelem systému Windows.

## Správný postup pro nastavení výchozích vlastností tisku

Postup nastavení výchozích vlastností tisku byl již popsán v kapitole věnované inicializaci ovladačů. Nyní bude popsáno, jak toto výchozí nastavení tisku v budoucnu změnit. Sice se jedná o relativně jednoduchý úkon, problém ovšem spočívá v tom, že je možné změnu nastavení tiskárny provést více způsoby a k nastavení se dostat provedením různých kroků. Ačkoliv pak nabídky vypadají stejně, pouze při provedení správného postupu jsou nové hodnoty uloženy.

Výchozím předpokladem pro uložení nového výchozího nastavení tiskárny na server je opět provedení následujících úkonů pod uživatelským účtem s oprávněním správce tiskáren nebo uživatele s uid=0 (root).

Zde je potřeba zmínit, že toto nastavení se projeví pouze pro uživatele, kteří se připojují k síťové tiskárně poprvé. Proto je vhodné nastavit všechny potřebné hodnoty správně již při inicializaci tiskového ovladače. Důvodem tohoto chování je, že operační systém Windows 2000/XP umožňuje každému uživateli uložit si vlastní nastavení tiskárny do svého vlastního uživatelského profilu, jakmile si tiskárnu poprvé připojí. Změny výchozích hodnot se tedy projeví pouze u uživatelů nově se připojujících k tiskovému sdílení.

Existují tři hlavní postupy, jak se dostat ke stejnému dialogovému oknu nastavení tiskárny. Přesto pouze u jednoho postupu je docíleno trvalého uložení nových hodnot:

Postup 1 – chybný:

- otevřeme složku s tiskárnami;
- klikneme na tiskárnu pravým tlačítkem a vybereme z kontextové nabídky „*Předvolby tisku*“;
- objeví se dialog s nastavením tiskárny.

Postup 2 – chybný:

- otevřeme složku s tiskárnami;
- klikneme na tiskárnu pravým tlačítkem a vybereme z kontextové nabídky „*Vlastnosti*“;
- klikneme na záložku „*Obecné*“;
- klikneme na tlačítko „*Předvolby tisku*“;
- objeví se dialog s nastavením tiskárny.

Postup 3 – správný:

- zopakujeme kroky 1 – 3 postupu 2;
- klikneme na záložku „*Upřesnit*“;
- klikneme na tlačítko „*Výchozí vlastnosti...*“;
- objeví se dialog s nastavením tiskárny;
- klikneme na tlačítko „*Upřesnit*“ na nově otevřeném dialogu.

Ačkoliv výsledkem všech uvedených postupů bylo stejné dialogové okno, pouze změny provedené pomocí postupu 3 jsou uloženy jako výchozí nastavení zpět na server.

### **Podpora tiskových portů v Sambě**

Servery Windows založené na NT asociují s každou tiskárnou tiskový port. Tiskové porty jsou obvykle označovány LPT1:, COM1:, FILE: apod. Samba musí podporovat porty asociované s tiskárnami kvůli klientům Windows také. Samba sama o sobě tiskové porty k provedení tisku nepotřebuje, ale klienti Windows informaci o dostupných tiskových portech vyžadují. V případě neexistence tiskového portu je klientem Windows vráceno chybové hlášení. Proto ve výchozím nastavení Samba nabízí klientům port s názvem „*Samba printer port*“. Význam tohoto portu je pouze v poskytnutí „podvržené“ informace klientům Windows o existujícím portu.

Samba interně nepodporuje funkcionalitu mnoha tiskových portů přiřazených jedné tiskárně s účelem rozdělování zátěže jedné logické tiskárny na více fyzických nebo více fyzických tiskáren pod jednou logickou s účelem zálohy proti výpadku.

Pokud je z jakéhokoliv důvodu potřeba, aby bylo s jednou tiskárnou asociováno v Sambě více tiskových portů, je možné specifikovat v souboru `smb.conf` parametr `enumports command`, který může být využit k definování externího programu, který vygeneruje seznam tiskových portů pro danou tiskárnu.

### **Automatická lokální instalace tiskárny bez nutnosti interakce uživatele**

Cílem automatické instalace tiskárny je příprava tiskárny bez nutnosti uživatelské lokální instalace tiskárny. Je využito možnosti provést lokální instalaci tiskárny pomocí příkazové řádky systému Windows a možnosti spuštění skriptů při doménovém přihlašování uživatele ke stanici Windows.

Následující postup funguje pouze pod operačními systémy Windows 2000 a XP. Nefunguje pod Windows NT. Pro provedení požadovaných nastavení tiskáren z příkazové řádky je použito volání funkcí knihovny `printui.dll`. Následující příkaz vypíše ve vyskakovacím okně nápovědu pro použití jednotlivých přepínačů pro příkazovou řádku:

```
rundll32 printui.dll,PrintUIEntry /?
```

Příklad použitelný v přihlašovacím skriptu:

```
rundll32 printui.dll,PrintUIEntry /dn /n "\\sambaserver\hplj-ivt" /q  
rundll32 printui.dll,PrintUIEntry /in /n "\\sambaserver\hplj-ivt"  
rundll32 printui.dll,PrintUIEntry /y /n "\\sambaserver\hplj-ivt"
```

Popis parametrů:

/dn – smaže síťové připojení k tiskárně  
/q – quiet – nejsou zobrazena žádná hlášení („tichý režim“)  
/n – jméno tiskárny  
/in – přidání síťového připojení k tiskárně  
/y – nastavení tiskárny jako výchozí

Řádek 1 uvedeného příkladu smaže síťovou tiskárnu `hplj-ivt`, pokud byla dříve přidána do místních tiskáren uživatele. Přepínač `q` potlačí případná chybová hlášení.

Řádek 2 přidá znovu do lokálních tiskáren uživatele tiskárnu `hplj-ivt`. Případné změny provedené ve výchozí konfiguraci ovladače tiskárny jsou staženy na klientskou stanici.

Řádek 3 nastaví přidanou tiskárnu jako výchozí tiskárnu pro tisk.

Tímto postupem je možné instalovat/odebírat tiskárny a měnit nastavení tiskáren připojených do profilů uživatelů dle potřeby. Samozřejmě je možné pro různé uživatele provést různé nastavení pomocí přidělení různých přihlašovacích skriptů různým uživatelům nebo skupinám uživatelů.

Jelikož neexistuje snadný způsob, jak testovat v přihlašovacím skriptu existenci nainstalované síťové tiskárny, nejjednodušším řešením je provést v přihlašovacím skriptu reinstalaci tiskárny při každém přihlášení uživatele. Tato procedura zabere maximálně jednotky vteřin, takže nepřináší zásadní zpomalení přihlašovacího procesu. Z provedení procesu reinstalace tiskárny při každém přihlášení plynou navíc následující výhody:

- je aktualizováno výchozí nastavení tiskárny u klienta dle nastavení na serveru;
- je jistota, že tiskárny budou nainstalovány u všech uživatelů (i nově vytvořených) přihlašujících se do domény Windows;
- tiskárny mohou být centrálně přidávány, odebírány a měněno jejich nastavení;
- není potřeba interakce ze strany uživatele – tiskárny jsou připraveny k použití.

Nevýhodou je pouze prodloužení přihlašovacího procesu o několik vteřin.

Kompletní přihlašovací skript je uveden v příloze [A.3](#)



## 3.5 Tiskový systém CUPS

CUPS bývá výchozím tiskovým systémem mnoha známých distribucí operačního systému Linux. CUPS nabízí mnoho možností, které tradiční systémy neposkytují. Z pohledu spolupráce se Samba serverem a zpracování tiskových úloh od klientů Windows nabízí zajímavé řešení problematiky ovladačů pro různé tiskárny, jednotného zpracování tiskových úloh na serveru, převody mezi různými formáty tiskových zařízení, možnost použití jednotného ovladače pro klienty Windows a převedení tiskové úlohy na formát specifický pro konkrétní model tiskárny na serveru. Tento přístup umožňuje funkcionalitu centrálního účtování, sledování vytištěných stran a podobné služby, které jsou při použití tradičního systému, který pouze přeposílá tiskárně tiskovou úlohu přijatou od klienta Windows v binárním formátu, obtížně realizovatelné.

CUPS je kompletním systémem pro správu tiskových úloh, který dodržuje standard Internet Printing Protocol, který je průmyslovým standardem IETF (Engineering Task Force) pro síťový tisk. Mnoho funkcí CUPS může být spravováno přes webový prohlížeč, čímž je poskytnut k tiskovému serveru přístup nezávislý na platformě. K dispozici jsou tradiční rozhraní příkazové řádky, ale také různé grafické nadstavby.

CUPS umožňuje vytváření tiskových zařízení typu RAW<sup>1</sup>, u kterých již nedochází k žádnému zpracování tiskového souboru, stejně jako tiskových zařízení, u kterých dochází ke zpracování tiskového souboru CUPS serverem dle požadavků tiskárny.

### 3.5.1 Podpora CUPS v Sambě

Pro spolupráci Samba serveru s CUPS musí být Samba server zkompileován s podporou pro knihovny CUPS. Při instalaci v systému FreeBSD pomocí kolekce portů stačí vybrat tuto volbu v nabídce zobrazené automaticky před kompilací Samby. Samba zkompileovaná s podporou pro CUPS používá aplikační rozhraní (API) systému CUPS pro načtení tiskáren, odesílání tiskových úloh apod.

Základní konfigurace v souboru `smb.conf` pro tisk pomocí CUPS může vypadat následovně:

```
[global]
load printers = yes
printing = cups
printcap name = cups
[printers]
comment = All Printers
path = /var/spool/samba
writable = no
printable = yes
printer admin = root, @ntadmins
```

### 3.5.2 Tiskový server zpracovávající pouze RAW data

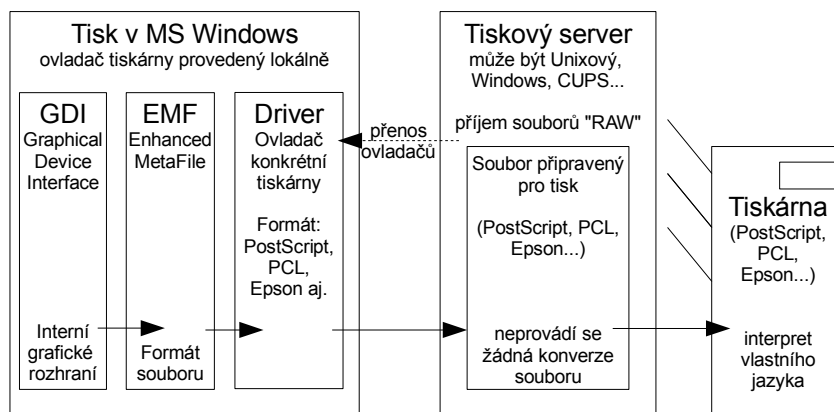
Tradiční Unixové tiskové systémy zprostředkovávající tiskové služby klientům Windows pomocí Samby zastávají pouze úlohu správy tiskových front a odesílání tiskových úloh na tiskárny. Tento přístup předpokládá, že klienti Windows připraví soubor s tiskovou úlohou

<sup>1</sup>„RAW“ je zde ve významu zařízení, u kterého nedochází ke zpracování dat – data jsou ponechána tak, jak byla přijata od jiného podsystému a pouze přeposlána dále

k odeslání na tiskárnu bez nutnosti jakéhokoliv dalšího zpracování. V tomto případě musí být na každém klientovi Windows nainstalován ovladač příslušného typu tiskárny.

Tiskový systém CUPS může být nakonfigurován stejným způsobem, jako tradiční tiskové systémy pro tisk, tedy jako prostředník pro přeposílání připravených tiskových souborů klientů.

Konfigurace systému CUPS pro RAW tisk je nejjednodušší konfigurací. Jsou však ztraceny další výhody z použití CUPS a stejnou funkcionalitu RAW tisku mohou zastat i tradiční tiskové systémy. Postup zpracování tiskové úlohy je zobrazen na obrázku 3.1.



Obrázek 3.1: Zpracování tiskové úlohy RAW

### 3.5.3 Pokročilý tisk s použitím ovladačů PostScript

Hlavními důvody pro chytřejší nastavení tiskového serveru mohou být:

- zpracování statistik tiskáren – počet vytištěných stran na jednotlivých tiskárnách, velikost tiskových úloh, zatížení tiskáren během pracovní doby, které skupiny uživatelů vytisknou kolik stránek apod.;
- tiskové kvóty – blokování tisku jednotlivých uživatelů po vyčerpání daného limitu za dané období;
- jednotné rozhraní pro komunikaci s tiskárnami.

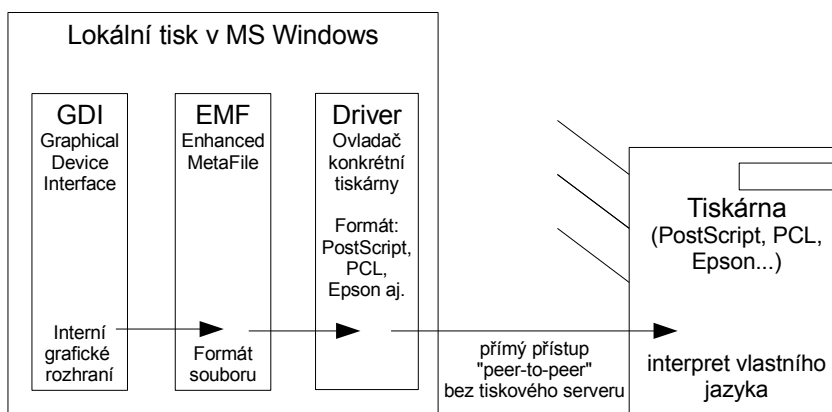
Těchto cílů nemůže být dosaženo s tiskovým serverem v konfiguraci RAW tisku. Dále bude popsána problematika zabývající se formátem tiskových úloh, jejich konverzí a konečně úpravě pro odeslání tiskárně pomocí CUPS.

#### Tiskové rozhraní Windows a Unix

Problémem zpracování tiskových úloh je neexistence společného standardu formátu tiskových souborů, který by byl akceptován všemi výrobci a jednotlivými typy tiskových zařízení. Ačkoliv PostScript (ochranná známka patří firmě Adobe) a PCL (ochranná známka Hewlett-Packard) se staly polooficiálními standardy a patří k nejčastěji využívaným jazykům pro popis tiskových stran (PDL – *page description language*), stále je mnoho výrobců, kteří používají své vlastní standardy.

## Ovladače Windows, GDI a EMF

V operačních systémech Microsoft Windows obstarávají konverzi souboru tiskové úlohy do formátu srozumitelného tiskárně ovladače dodávané výrobcem tiskárny. V operačních systémech Microsoft Windows je k dispozici vestavěné aplikační rozhraní (API) – rozhraní grafického zařízení GDI (*Graphical Device Interface*). Jádro GDI je použito jako společný základ pro všechny programy k vykreslování obrázků, fontů a dokumentů na obrazovku a tisk. Díky tomuto standardizovanému rozhraní mohou výrobci ovladačů tiskových zařízení stavět své ovladače na výstupu dat z GDI, která jsou použita jako vstupní data pro ovladač tiskárny. Zachování stejného vzhledu tištěných dat a dat zobrazených na obrazovce tak nečiní příliš velké problémy, protože grafická primitiva na obrazovce, stejně jako data pro tiskárnu pocházejí ze stejného zdroje. Výstupem GDI je často formát zvaný EMF – *Enhanced MetaFile*. Formát EMF je následně zpracován ovladačem tiskárny a převeden do formátu specifickém pro danou tiskárnu. Postup při lokálním tisku na stanici Windows je znázorněn na obrázku 3.2.



Obrázek 3.2: Lokální tisk na stanici Windows

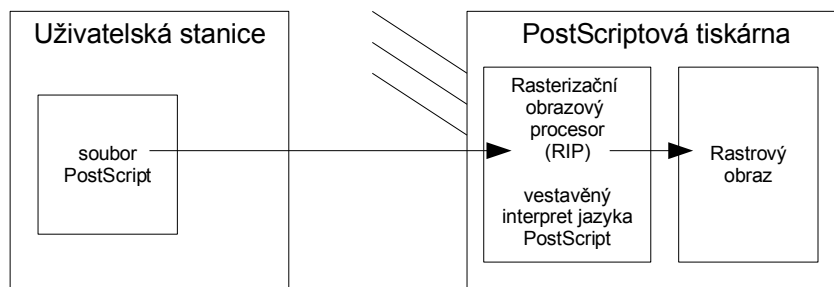
## Tisk v Unixu

V Unixových systémech není k dispozici vrstva srovnatelná s GDI. Každá aplikace je tak sama zodpovědná za vytvoření tiskového výstupu. Naštěstí většina aplikací používá rozhraní PostScript, které tak tvoří společný základ. Bohužel zachování stejného vzhledu na obrazovce i výstupu z tiskárny je zde mnohem složitější a interpretace dat na obrazovce a při odeslání na tiskárnu může být značně odlišná.

Tisk pod Unixovými systémy je relativně jednoduchý za předpokladu, že již máme k dispozici soubor ve formátu PostScript a tiskárnu s vestavěným interpretem jazyka PostScript a rasterizačním procesorem. Provedení tiskové úlohy potom spočívá v odeslání souboru ve formátu PostScript do tiskárny. Situaci znázorňuje obrázek 3.3.

## PostScript

Jazyk PostScript byl vytvořen firmou Adobe, ale jeho specifikace jsou veřejně publikované a dostupné. Jazyk se vyznačuje mocnými vyjadřovacími prostředky pro popis grafických objektů, jejich atributů a manipulaci s nimi. Díky otevřené specifikaci může kdokoliv vytvořit vlastní interpret tohoto jazyka. Jelikož většina zařízení s grafickým výstupem je



Obrázek 3.3: Lokální tisk souboru ve formátu PostScript na tiskárně s podporou PostScriptu

rastrového typu, instrukce jazyka PostScript musí být interpretovány rasterizační jednotkou (rasterizér). Výstupem rasterizéru jsou jednotlivé obrazové body (pixely) výsledného obrazu.

### Soubory s popisem tiskáren – PPD

Zatímco jazyk PostScript je ve své podstatě jazyk pro popis dokumentů (PDL) nezávislý na použitém zařízení, skutečná tisková zařízení se vždy vyznačují svými specifickými vlastnostmi.

K dispozici jsou tiskárny s různými možnostmi provedení tisku samotného a různými volitelnými nastaveními provedení tiskové úlohy. Například duplexní jednotka, možnost volby rozlišení, sytosti tisku, zásobníku papíru, tisku více stran na list apod. Tyto možnosti jsou závislé na konkrétním typu tiskárny a proto je potřeba dalšího prostředku pro řízení volitelných možností, které tiskárna podporuje. Z důvodu zohlednění všech těchto odlišností a možnosti budoucího rozšiřování, specifikovala společnost Adobe syntaxi a formát souborů pro popis tiskáren PPD (PostScript Printer Description).

Soubory PPD obsahují všechny tyto informace o základních a speciálních možnostech daného hardwaru. Pro každou položku je použito speciálního příkazu ve formátu řetězce, který je v případě potřeby odeslán do tiskárny.

Možnosti tiskového zařízení popsané v souboru PPD mohou být následně použity v grafickém uživatelském rozhraní pro vygenerování příslušných položek tiskového dialogu.

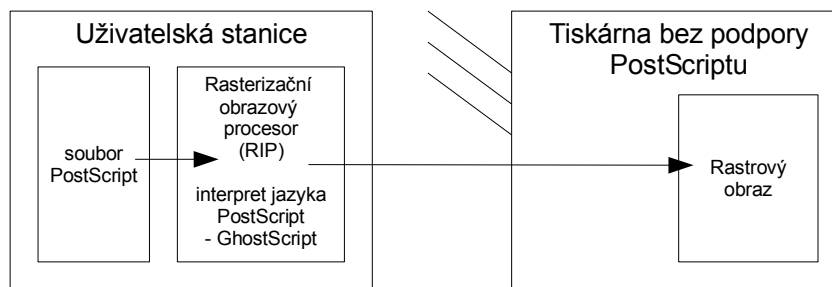
Soubory PPD nebyly obvykle v tradičních Unixových programech a tiskových systémech podporovány a uživatelé tak byli ochuzeni o případná nastavení a rozšířené možnosti tiskáren. Systém CUPS tuto problematiku řeší.

### Ghostscript

K dispozici je ovšem velké množství tiskáren, které jazyk PostScript interpretovat neumějí. Používají vlastní jazyk pro popis tiskových úloh, který je často proprietární. Zatímco výstupem většiny Unixových aplikací jsou soubory ve formátu PostScript a tyto tiskárny jazyku PostScript nerozumí, je potřeba provést konverzi tiskových souborů z formátu PostScript do formátu srozumitelného tiskárně.

Ghostscript je softwarovým interpretrem jazyka PostScript. Poskytuje softwarovou funkcionalitu rasterizačního procesoru s možností konverze do širokého spektra jiných formátů hardwarových zařízení, ale i softwarových. Ghostscript tak umožňuje tisk souborů ve formátu PostScript na zařízeních, která tento formát nepodporují. Tisk souboru

PostScript pomocí interpretru Ghostscript znázorňuje obrázek 3.4.



Obrázek 3.4: Lokální tisk souboru ve formátu PostScript na tiskárně bez podpory PostScriptu

## PPD a CUPS

Formát souborů PPD je standardizován a obvykle by neměl být problém využít soubory PPD poskytované výrobcem pro operační systém Windows v systému CUPS.

Tiskový systém CUPS využívá PPD soubory i pro popis tiskáren bez podpory jazyka PostScript. Tyto soubory nejsou obvykle k dispozici od výrobce zařízení.

Je tak využito jednotného rozhraní a konceptu pro popis vlastností tiskáren s podporou i bez podpory jazyka PostScript.

Při použití tiskového systému CUPS jako tiskového serveru pro klienty Windows je možné použít u klientů jako společný základ jednotného ovladače PostScript (doporučen ovladač „*CUPS PostScript driver for Windows*“) pro všechny typy tiskáren, který je doplněn PPD souborem pro konkrétní typ tiskárny, na jehož základě jsou vygenerovány nabídky pro vlastnosti konkrétní tiskárny.

Tato vlastnost umožňuje tiskovému systému CUPS:

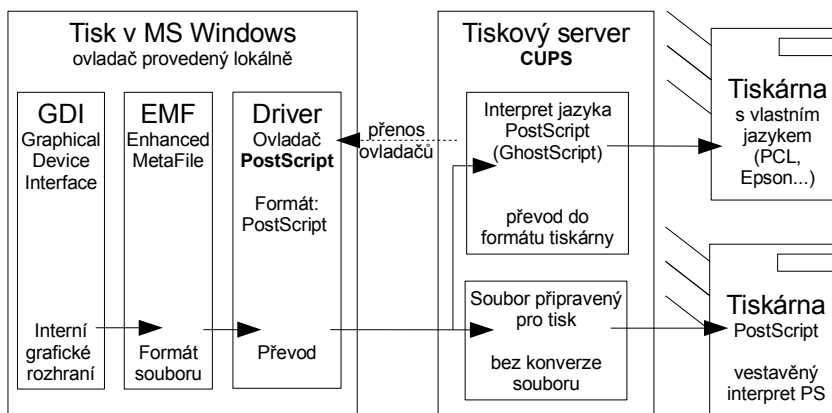
- vystupovat jednotným způsobem jako síťový PostScriptový rasterizační procesor;
- zastávat roli centrálního tiskového serveru s možností služeb účtování, získávání tiskových statistik apod. úlohy, které nejsou realizovatelné při pouhém přeposílání dat ve formátu RAW;
- možnost využívat jednotný PostScriptový ovladač u klientů pro mnoho různých tiskáren.

Jádro filtrovacího systému CUPS je založeno na software Ghostscript. Dále používá CUPS další vlastní filtry.

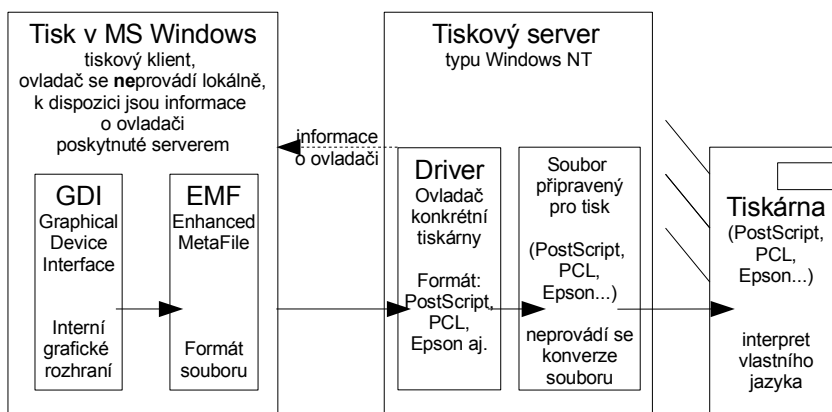
## Proces rasterizace

Systém CUPS zastává roli rasterizačního procesoru pro soubory ve formátu PostScript. V případě odesílání tiskového souboru na tiskárnu s podporou jazyka PostScript není potřeba provádět rasterizaci a převod, protože rasterizaci obstará rasterizační procesor vestavěný v tiskárně. Rasterizaci souboru ve formátu PostScript a další převod je potřeba

provést před odesláním na tiskárny bez podpory PostScriptu. Situaci znázorňuje obrázek 3.5. Pro srovnání a úplnost je na obrázku 3.6 uvedeno možné zpracování tiskové úlohy na serveru při použití tiskového serveru s operačním systémem Windows NT.



Obrázek 3.5: Zpracování tiskové úlohy pomocí CUPS



Obrázek 3.6: Zpracování tiskové úlohy na serveru Windows NT

Při rasterizaci souboru PostScript do bitmapy je postupováno ve dvou krocích následovně:

1. Pomocí Ghostscriptu je vygenerován generický rastrový formát *CUPS rastr*.
2. *CUPS rastr* je převeden do rastru specifického pro daný typ zařízení.

### 3.5.4 Závěr

Cílem kapitoly bylo nastítnit možnosti tiskového systému CUPS a možné výhody plynoucí z jeho použití v multiplatformním prostředí a jako tiskového systému pro klienty Windows.

Shrnutí vlastností CUPS:

- základním spojujícím prvkem pro tiskové úlohy je tiskový soubor ve formátu PostScript;
- vlastnosti tiskáren jsou popsány ve standardizovaných souborech PPD (*PostScript Printer Description*); soubory jsou využity i pro popis tiskáren bez podpory PostScriptu;
- CUPS využívá softwarový interpret jazyka PostScript – GhostScript;
- pro tiskárny, které nepodporují jazyk PostScript, poskytuje CUPS funkci rasterizačního procesoru (RIP) PostScriptových souborů a funkci převodního filtru do jazyka srozumitelného danému typu tiskárny;
- CUPS může být konfigurován i pro pouhé přeposílání již naformátovaných RAW dat od klientů;
- CUPS může přijímat data i v jiných formátech než PostScript a pomocí vstupních filtrů provádět konverze do formátu PostScript.

Další informace o tiskovém systému CUPS a jeho propojení se Samba serverem lze nalézt v [7] v kapitole 22.

## Kapitola 4

# Aktualizace propojení lokalit

Prostředí škol, na nichž byl projekt řešen se rozprostírá v nezávislých budovách jednoho města. Ke škole patří v současné době tři budovy. Jednu z budov tvoří ubytovací zařízení škol.

Problematika propojení dvou pracovišť školy byla řešena v rámci bakalářské práce autora [8], ve které byly popsány jednotlivé technologické možnosti a výsledná realizace propojení v době řešení. S ohledem na možnosti a propustnost byly zrealizovány dva nezávislé bezdrátové spoje pomocí technologie WiFi dle standardu 802.11b. Jeden spoj byl využit na propojení privátních sítí lokalit, druhý na přivedení přípojky k Internetu z jedné lokality do druhé. Toto řešení mělo velmi omezenou propustnost kolem 4-5 Mb/s na každý spoj (half-duplex) danou použitou technologií. Z pohledu připojení k Internetu jedné budovy školy by byla tato rychlost aktuálně ještě postačující, z pohledu propojení vnitřních sítí již nikoliv.

Jedním z řešení vedoucím ke zvýšení propusti by mohl být upgrade použité technologie. Pro pásmo 2,4 GHz jsou nyní k dispozici zařízení pracující dle standardu 802.11g, nabízející 4-5x vyšší propustnost, než v případě 802.11b. Zařízení pracující dle 802.11g nebyla v době realizace ještě běžně dostupná. Otázkou je, jestli by byl přínos upgrade skutečně takový, protože zároveň se zvyšováním dostupnosti této technologie mnohonásobně vzrostlo zarušení pásma 2,4 GHz v prostředí lokalit škol, ačkoliv budovy jsou vzdáleny od sebe pouze řádově stovky metrů.

Další možností by bylo použití technologie v pásmu 5 GHz. Použití tohoto rádiového pásma nebylo v době řešení propojení možné vůbec, povoleno bylo teprve později.

Propojení pomocí technologie v licencovaném pásmu nebo technologie pracující v pásmu 10 GHz nepřipadalo vzhledem k cenám a finančním možnostem v úvahu.

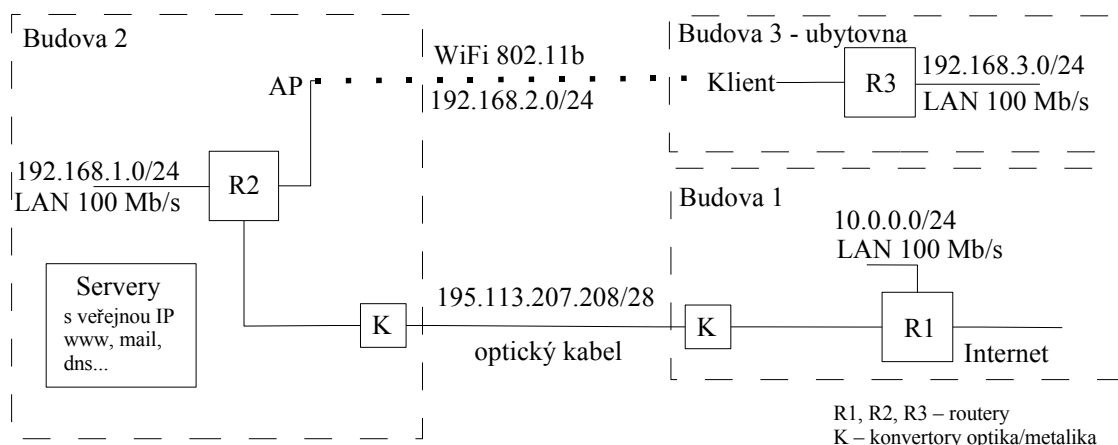
Nejlepším řešením z pohledu propustnosti a jejím možným navýšováním v budoucnu je pevné propojení pomocí optického kabelu. V rámci realizace městské metropolitní sítě se škole v rámci projektu takováto možnost naskytla. Od provozovatele metropolitní sítě byla pronajata optická trasa mezi budovami. Z pohledu technologie jsou obě zakončení optického kabelu vybavena aktivními síťovými prvky Signamax 065-7726S. Jedná se o síťové přepínače (switch) s managementem obsahující 24x 100 Mb/s porty a 2x 1 Gb/s porty s možností použití metalických portů (RJ 45) nebo optických modulů. Optická kabeláž mezi budovami je vedena přes jádro metropolitní sítě, kde je vyvedena do patch panelu. Přes jádro metropolitní sítě prochází bez aktivního prvku pouhým propojením v patch panelu. Jedná se tedy o přímé propojení.

Po zprovoznění optické linky byly učiněny následující úpravy:



- 2 routery na straně lokality s připojením k Internetu byly sloučeny a nahrazeny jedním;
- byly zrušena šifrovaná virtuální linka sloužící k zabezpečení provozu přes WiFi mezi routery škol a upraveny směrovací tabulky.

Výsledná situace po úpravách je znázorněna na obrázku 4.1.



Obrázek 4.1: Propojení lokalit školy

WiFi spoj použitý pro přivedení připojení k Internetu do druhé lokality byl odstra- ven, zařízení však bylo ponecháno nainstalované pro případ, že by došlo k dlouhodobějším problémům s optickým propojením.

Druhý spoj – pro propojení vnitřních sítí byl využit pro připojení ubytovny škol k In- ternetu. Z důvodu oddělení podsítě s počítači v budově od WiFi sítě byl v ubytovně nain- stalován router (na obrázku 4.1 znázorněn jako R3), který zároveň slouží jako vyrovnávací paměť pro DNS požadavky a webové stránky získávané pomocí protokolu HTTP, z důvodu maximální úspory malé šířky pásma bezdrátového spoje. Jako mezipaměť pro webové stránky byl použit software Squid a nakonfigurován jako transparentní proxy server. Po- stup pro vytvoření zabezpečeného spoje mezi lokalitami pomocí software OpenVPN přes bezdrátové spojení, konfigurace proxy serveru a DNS byl též popsán v bakalářské práci [8] v kapitolách 3 a 4.

## Kapitola 5

# Instalace stanic na učebnách

### 5.1 Úvod

V prostředí školních učeben je obvyklou situací zakoupení vybavení celé učebny naráz. Díky tomu může být obvykle zachována jednotná konfigurace hardwaru. Při instalaci učebny se tak nabízí otázka, jak využít této výhodné vlastnosti stejné konfigurace mnoha počítačů pro zjednodušení a urychlení mnoha stejných instalací tvořících operační systém samotný, používaný software a konfiguraci. Použitím vhodných nástrojů lze využít stejné kopie celého disku nebo diskových oddílů na všech počítačích.

Typické úkony, které je potřeba provést pro instalaci jednotlivé stanice jsou:

1. Rozdělení disku – v řešeném školním prostředí disk dělen vždy na dvě části – systémový oddíl s omezeným oprávněním zápisu a oddíl ponechaný uživatelům volně k dispozici pro případné dočasné odložení většího množství dat.
2. Instalace operačního systému.
3. Instalace programového vybavení.
4. Konfigurace výchozích vlastností softwaru, je-li potřeba.
5. Nastavení omezení zápisu na systémový oddíl.
6. Začlenění stanice do důvěryhodného vztahu s doménou.

Body 2 – 5 jsou přitom časově nejnáročnější a náchylné na chybu opomenutí některého úkonu. Za předpokladu stejné nebo velmi podobné hardwarové konfigurace lze body 1 – 5 nebo 2 – 5, podle použitého postupu, provést pouze jednou, na jediné stanici připravit vše podle požadavků a přenést na další stanice.

Přenesení kompletní instalace, tedy obsahu disku nebo diskového oddílu na další počítač, se často označuje jako *klonování*.

K provedení tohoto úkonu jsou k dispozici různé nástroje. Ve světě Unixových systémů může být tento úkon proveden pomocí standardních nástrojů pro zálohování a obnovu obsažených ve většině distribucí těchto systémů (například programy `dump/restore` a `tar`).

Ve světě operačního systému Windows, což je případ řešených učeben střední školy, je situace poněkud složitější, především kvůli použití proprietárního souborového systému

NTFS, který není, kvůli uzavřeným specifikacím, v jiných systémech zcela dobře a bezproblémově podporován. I v případě pokusů o podporu souborového systému NTFS v Unixu za pomoci ovladače převzatého z Windows nebo samostatnou reimplementací ovladače, je zde problém různé interpretace a využití souborových atributů a oprávnění v operačních systémech typu Unix a Windows.

Cestou pro vyřešení těchto komplikací může být použití specializovaných komerčních programů, určených pro účel zálohování/kopírování disků a diskových oddílů. K neznámějším a osvědčeným programům v této oblasti patří patrně *Norton Ghost* od firmy Symantec. Nyní dostupný ve verzi 10.0.

Je možné vydat se i cestou volně šířitelného softwaru. Na klonování diskových oddílů s Windows lze přes uvedené problémy přesto použít některé standardní nástroje systému Unix nebo specializovaného nástroje pro zálohování/obnovu diskových oddílů – *Partimage*.

## 5.2 Norton Ghost

V prostředí školní sítě byla poslední používanou verzí zakoupená verze 2002. Tento software nabízí více možností způsobů provedení zálohy diskových oddílů nebo celého disku. Z daných možností byly využívány následující:

- klonování diskových oddílů/disků po síti v režimu *master/slave*;
- vypalování obrazů na CD na stanici se zapisovací mechanikou;
- ukládání obrazů do souborů (lokálně, po síti).

První možnost byla využívána ke zkopírování disků celé učebny po finální instalaci první stanice, druhá a třetí pro zálohu obrazu disku této stanice pro jeho zachování pro případnou budoucí obnovu.

Postup použití nástroje Norton Ghost 2002 byl následující:

- instalace softwaru z dodávaného CD na stanici Windows;
- vytvoření bootovacích disket pro daný účel pomocí průvodce ve Windows – v případě požadované funkcionality sítě je potřeba vybrat/dodat ovladače síťové karty; výsledkem je bootovací disketa s operačním systémem DOS, po jejímž nabootování se spustí grafické uživatelské rozhraní programu.

### 5.2.1 Kopírování disků po síti

Postup kopírování disků po síti byl využíván následujícím způsobem:

- na dvou stanicích bylo nabootováno z vytvořené diskety – u cílové stanice pro kopírování obrazu vybrán režim *slave* a u zdrojové *master*;
- u *master* stanice vložena IP adresa zobrazená *slave* stanicí (získaná z DHCP serveru);
- na *master* stanici v nabídce vybráno kopírování *disk to disk* nebo *partition to disk*;
- po vybrání zdrojového/cílového oddílu nebo disku a po potvrzení spuštěn proces kopírování po síti.

Tímto způsobem byla, v případě kopírování celé učebny, zkopírována nejdříve první nainstalovaná zdrojová stanice. Po zkopírování této stanice byla použita nově nakopírovaná též jako zdrojová a spuštěno kopírování ze dvou na další dvě zároveň a dále obdobným postupem, až do nakopírování celé učebny.

Doba kopírování diskového oddílu o velikosti 17,58 GB s využitým místem 5,24 GB pomocí tohoto postupu byla 18 minut.

### 5.2.2 Vypalování obrazů

Norton Ghost 2002 umožňuje vytvoření bootovací diskety s podporou zápisu na CD. Bohužel toto použití se neukázalo být úplně stabilní a často skončilo havárií procesu vypalování. Jediný způsob, který se ukázal jako použitelný, bylo vypnutí komprese při vytváření obrazu a místo CD-R použití médií CD-RW (pravděpodobně kvůli různé maximální rychlosti zápisu).

### 5.2.3 Ukládání obrazů do souborů

Posledním používaným způsobem bylo ukládání obrazu disku nebo oddílu do souboru. Tato možnost byla použitelná za předpokladu, že existoval pro uložení obrazu diskový oddíl se souborovým systémem FAT. Uložení do souboru bylo možné použít na lokálním počítači (záloha na jiný oddíl nebo disk) i přes síť (na cílovém počítači existující oddíl FAT).

### 5.2.4 Výhody a nevýhody použití Norton Ghost 2002

K výhodám patří bezproblémová podpora NTFS, možnost kopírovat jak celé diskové oddíly, tak disky, obvykle bezproblémová automatická změna velikosti diskového oddílu v případě jiné velikosti cílového oddílu nebo disku a velikost jedné bootovací diskety.

Za jednu z nevýhod se dá označit nutnost zadávat licenční číslo při každém pokusu o kopírování obrazu, což je při kopírování většího množství počítačů již úkon nepřijemný a zdržující.

## 5.3 Alternativa založená na volně šiřitelném software

Cílem byla snaha o nalezení volně šiřitelné alternativy pro zálohování a obnovu diskových oddílů, možnosti proces obnovy maximálně zjednodušit pro obsluhu a využít jednotné centrální skladiště pro diskové obrazy pro jednotlivé učebny nebo série stejných počítačů umístěné na existujícím serveru s operačním systémem FreeBSD použitím standardních Unixových příkazů a služeb.

### 5.3.1 Systém

Prvním úkolem bylo nalézt vhodný operační systém spustitelný z vyměnitelného média – nejlépe disket nebo CD, protože mechaniky pro tato média jsou k dispozici na každém počítači učebny. Dalším použitelným médiem jsou také USB flash disky, pokud má základní deska podporu pro bootování z USB. Tato podmínka nebyla bohužel u starších PC splněna. Vzhledem ke kapacitě disket vyšlo jako řešení použití bootovacího CD s operačním systémem Linux, protože u tohoto systému lze nalézt velké množství tzv. *live* distribucí běžících z CD. Pro tento účel se jako vhodná, vzhledem k obsaženým nástrojům, ukázala distribuce *SystemRescueCD* určená pro požadovaný účel zálohování a obnovy.

### 5.3.2 SystemRescueCD

SystemRescueCD je distribuce běžící z bootovacího CD založená na Gentoo Linuxu.

Mezi nejdůležitější nástroje, které aktuální verze 0.3.5 obsahuje patří:

- **GParted** – program pro správu diskových oddílů pomocí grafického uživatelského rozhraní;
- **GNU Parted** – nástroj pro editaci diskových oddílů s ovládáním pomocí příkazové řádky;
- **Partimage** – nástroj pro zálohování/obnovu diskových oddílů;
- **Ntfs3g** – umožňuje připojení souborového systému NTFS pro plný přístup zápis/čtení;
- **Sfdisk** – zálohování a obnova tabulky rozdělení disků;
- **Test-disk** – nástroj pro kontrolu a obnovení smazaných diskových oddílů s podporou NTFS, FAT32, EXT2, EXT3, ReiserFS a dalších;
- nástroje pro různé souborové systémy – manipulace, formátování, změna velikosti;
- nástroje pro práci v síti – Samba, NFS, standardní nástroje ping, nslookup a další.

K dalším možnostem patří:

- snadná výroba vlastních verzí CD s možností přidání dalšího obsahu (vlastní skripty, programy ...);
- možnost výroby bootovacího DVD s využitím až 4,2 GB kapacity pro vlastní data (například obraz zálohy);
- instalace na USB flash disk.

### 5.3.3 Možnosti uložení diskového oddílu NTFS

Vzhledem k problémům s úplnou podporou souborového systému NTFS v Unixových systémech, jsou použitelné následující metody:

- použití přímého přístupu k diskovému oddílu a vytvoření obrazu oddílu pomocí standardních Unixových nástrojů;
- použití specializovaného nástroje Partimage pro zálohu a obnovu diskových oddílů.

#### Použití přímého přístupu k disku

U tohoto postupu je využito možnosti přístupu k celému disku nebo diskovému oddílu v Unixu pomocí standardních nástrojů.

Zadáním příkazu

```
# fdisk -l
```

si můžeme nechat vypsat seznam diskových oddílů a zařízení, pod kterými jsou k dispozici:

```
Disk /dev/hda: 20.0 GB, 20003880960 bytes
255 heads, 63 sectors/track, 2432 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Zařízení Boot      Start          End          Blocks      Id System
/dev/hda1  *              1            1220        9799618+    7  HPFS/NTFS
Partition 1 does not end on cylinder boundary.
/dev/hda2              1221          2367        9213277+    83  Linux
/dev/hda3              2368          2432         522112+     82  Linux swap / Solaris
```

Na uvedeném výpisu vidíme, že NTFS oddíl s Windows je k dispozici pomocí zařízení /dev/hda1. Obraz tohoto oddílu můžeme vytvořit zadáním:

```
cat /dev/hda1 > hda1image
```

Tento příkaz vytvoří kompletní binární kopii diskového oddílu hda1 do souboru hda1image. Program cat začne číst obsah oddílu zpřístupněný pomocí souboru zařízení /dev/hda1 a vypisovat na standardní výstup, který je pomocí znaku > přeměřován do souboru hda1image.

Nevýhodou je stejná velikost vytvořeného souboru jako zálohovaného oddílu, bez ohledu na využití místo v tomto oddílu. Bude-li mít například diskový oddíl velikost 10 GB a obsazeno na něm bude pouze 5 GB a zbytek bude volné místo, velikost obrazu bude 10 GB, bude tedy zkopírován i s volným místem.

Možného zlepšení v místě zabraném obrazem lze dosáhnout použitím komprese:

```
cat /dev/hda1 | gzip -c > hda1image.gz
```

Problémem použití této komprese je, že oddíl může obsahovat různá data v místech „prázdného“ místa, jakožto pozůstatek po dřívější smazaných souborech. Možnou další optimalizací je příprava oddílu již před instalací operačního systému vyplněním oddílu nulami:

```
cat /dev/zero > /dev/hda1
```

Poté provedení instalace systému a vytvoření obrazu:

```
cat /dev/hda1 | gzip -c > hda1image.gz
```

Nyní, jelikož v místech prázdného místa bude obsahovat disk převážně stejná data – nuly, která budou podstatně lépe komprimovatelná, než data mající náhodný charakter, by měl obraz zabírat podstatně méně místa.

Nevýhody obrazu vytvořeného tímto postupem jsou:

- při obnově musí mít cílový oddíl naprosto přesně stejnou velikost, na což je potřeba dát si při rozdělování disků dalších stanic pozor;
- delší doba obnovy, protože se zapisuje i prázdné místo.

Obnovu vytvořeného obrazu provedeme následovně:

```
cat hda1image > /dev/hda1
```

resp. při použití komprese:

```
gzcat hda1image > /dev/hda1
```

Tuto metodu lze použít i obecněji – pro zálohování nejen diskového oddílu, ale celého disku:

```
cat /dev/hda > hdaimage
```

Výhodou je skutečně kompletní obraz disku a to včetně případného rozdělení na různé diskové oddíly i s více operačními systémy.

Tímto postupem (s použitím komprese a přípravy disku) byl vytvořen obraz disku o velikosti 40 GB se zabraným místem 5,24 GB. Obraz měl velikost 2841 MB a doba obnovy oddílu byla změřena 25 minut a 5 vteřin při čtení obrazu ze sítě pomocí NFS.

Disk, na který se takovýto obraz kopíruje, musí být stejně velký nebo větší než zdrojový. V případě že by byl menší, nastanou problémy s oddílem přesahujícím fyzickou velikost disku. Při zkopírování na větší disk se přebývající velikost projeví v editoru diskových oddílů jako volné místo, které je k dispozici na konci disku a které je možné alokovat změnou velikosti posledního oddílu nebo vytvořením nového oddílu.

V učebnách je tohoto postupu používáno při kompletní obnově systému po havárii a výměně disku, protože nový disk je, vzhledem k růstu kapacity disků, vždy větší než původní (původní disky mají 40 GB) a zbylé místo na konci disku je ponecháno jako nevyužitá (není vzhledem k vyžití disku potřeba).

## Partimage

Partimage je specializovaný nástroj pro zálohování a obnovu diskových oddílů. Obrazy vytvářené tímto nástrojem mohou být automaticky komprimovány pomocí kompresních programů `gzip` a `bzip2` a rozdělovány do více souborů (o velikosti cílového média – například CD/DVD). Další vlastností je možnost ukládání obrazů přes síť pomocí vlastního serveru `partimaged`.

Hlavní výhodou nástroje Partimage je kopírování pouze využitých datových bloků z diskového oddílu. Prázdné datové bloky nejsou zapisovány do obrazu, což má značný vliv na rychlost a také velikost obrazu.

Podporované souborové systémy v aktuální verzi 0.6.5 jsou uvedeny v tabulce 5.1.

jméno	popis	podpora
ext2/ext3	standardní souborový systém v Linuxu	stabilní
Reiser 3	souborový systém s žurnálem	stabilní
FAT16/32	používaný v OS DOS a Windows	stabilní
HPFS	souborový systém používaný v IBS OS/2	stabilní
JFS	s žurnálem od IBM, používaný na AIXu	stabilní
XFS	s žurnálem od SGI, používaný na IRIXu	stabilní
UFS	Unixový souborový systém	beta verze
HFS	souborový systém MacOS	beta verze
NTFS	Windows NT, 2000 a XP	experimentální

Tabulka 5.1: Podporované souborové systémy v programu Partimage

Podpora NTFS je v experimentálním stavu. Na NTFS oddíl jsou kladeny následující omezení, aby bylo možné provedení zálohy:

- diskový oddíl NTFS nesmí být příliš fragmentován;
- soubory nesmí používat kompresi poskytovanou souborovým systémem NTFS.

V případě, že se obraz podaří vytvořit bez chybového hlášení, neměl by být problém ho obnovit. V případě chyby je možné zkusit provést defragmentaci disku a vypnout kompresi, je-li použita.

Ačkoliv je podpora souborového systému NTFS označena jako experimentální, při dlouhodobém používání při ukládání/obnově oddílů ve školním prostředí nebyly pozorovány žádné problémy s uložením nebo obnovou oddílů.

Ovládání programu Partimage je možné pomocí příkazové řádky (vhodné pro využití pomocí skriptů) nebo pomocí interaktivního textového uživatelského rozhraní, které je spuštěno v případě volání programu Partimage bez parametrů. Seznam parametrů příkazové řádky lze získat zadáním:

```
partimage --help
```

Ovládání interaktivní verze je jednoduché. Po spuštění je zobrazena obrazovka s dostupnými oddíly na lokálních discích.

Po vybrání požadovaného oddílu je možné vybrat jednu ze třech akcí:

- uložení obrazu oddílu do souboru obrazu;
- obnova oddílu ze souboru obrazu;
- obnova hlavního spouštěcího záznamu disku (MBR) ze souboru obrazu.

Dále je požadováno zadání jména souboru obrazu k vytvoření/obnově a případně je možné zadat adresu `partimaged` serveru, je-li použit. Stisknutím klávesy F5 je zobrazena další obrazovka. V případě obnovy oddílu je obnova po potvrzení spuštěna, v případě ukládání je k dispozici obrazovka s dalšími nastaveními:

- úroveň komprese (žádná, gzip, bzip2);
- akce provedená po dokončení (čekat, restartovat, vypnout systém, ukončit program);
- chování při rozdělování obrazů do více souborů (automatické, dělení na zadanou velikost);
- další nastavení (kontrola oddílu, zadání popisku oddílu před vytvořením, chování v případě existence cílového souboru).

Po započetí procesu vytváření zálohy nebo obnovy je zobrazena obrazovka s informacemi o průběhu úlohy (počet zkopírovaných dat, čas, procentuální průběh apod.)

Doba obnovy diskového oddílu o velikosti 17,58 GB s využitým místem 5,24 GB, čtením obrazu ze sítě přes NFS a s použitím komprese gzip, byla změřena 9 minut a 57 vteřin.



### 5.3.4 Obnova obrazu na nový disk

Pomocí nástroje Partimage je možné učinit pouze zálohu/obnovu jednotlivých existujících diskových oddílů. Bylo odzkoušeno, že Partimage si dobře poradí se změnou velikosti oddílu, pokud je nový cílový při obnově větší. Neporadí si se zmenšením oddílu, i když zálohovaný oddíl nebyl plně obsazen.

Při obnově obrazu diskového oddílu vytvořeného pomocí Partimage na nový disk, je potřeba na tomto disku nejdříve vytvořit diskové oddíly a dle potřeby na diskových oddílech vytvořit souborový systém. Toho se nepodařilo používanou verzí SystemRescueCD 0.2.19 uspokojivě dosáhnout. CD sice obsahuje program *Qtparted* pro manipulaci s diskovými oddíly (spouštěný pomocí `run_qtparted`), nicméně většina pokusů o vytváření/manipulaci s diskovými oddíly se souborovým systémem NTFS skončila havárií souborového systému nebo celého rozdělení disku, čímž byl tento nástroj nepoužitelný. Řešením bylo použít osvědčeného komerčního programu *Partition Magic* (firma Symantec), bootovací CD Windows nebo pro prvotní obnovu po výměně disku použít metodu přímého přístupu k disku popsanou v kapitole 5.3.3.

Ve verzích SystemRescueCD následujících používané verzi 0.2.19 tj. 0.3.0 vydané 20. 12. 2006, byl program *Qtparted* nahrazen programem *GParted* a přidáno grafické uživatelské rozhraní *X.Org* a správce oken *WindowMaker*. Po vydání verze 0.3.0 následovalo v celkem rychlém sledu ještě několik nových verzí, poslední 0.3.5 z 19. 3. 2007. Program *GParted* byl otestován a po prvních experimentech vypadá jako dobře použitelný i pro manipulaci s oddíly NTFS (během experimentů nedošlo k problémům s poškozením souborového systému). Do verze SystemRescueCD 0.3.x byl také začleněn ovladač *Ntfs3g*, který umožňuje připojení NTFS oddílu v Unixových systémech pro čtení i zápis. Jeho první verze označená jako stabilní byla uvolněna 28. 3. 2007. Poslední verze je z 16. 4. 2007. Operace nastavení oprávnění a vlastnictví však nejsou stále plně podporovány. Experimenty s možností zálohování přímo na úrovni souborů pomocí standardních Unixových nástrojů již nebyly učiněny.

Ve verzích SystemRescueCD 0.3.x se též vyskytl problém s podporou integrovaných gigabitových síťových karet u nově zakoupených PC, které ve verzi 0.2.19 fungují.

### 5.3.5 Ukládání obrazů na server pomocí NFS

NFS – *Network File System* je protokol, který umožňuje připojení vzdálených adresářových stromů do lokální adresářové struktury pomocí sítě. Jedná se o standardní protokol používaný v Unixových systémech. SystemRescueCD má kromě NFS podporu i pro připojování adresářových stromů pomocí protokolu SMB (obsahuje Samba klienta).

Na serveru s operačním systémem FreeBSD bylo potřeba provést následující úpravy. Vytvořit adresář pro ukládání obrazů a nastavit oprávnění pro umožnění čtení a zápisu:

```
# mkdir /samba/data/images
# chmod 777 /samba/data/images
```

Dále je potřeba zeditovat soubor `/etc/exports`, ve kterém jsou definovány adresáře přístupné pomocí NFS a přidat následující řádek:

```
/samba/data/images -network 192.168.1.0 -mask 255.255.255.0
```

Uvedený řádek znamená, že je vyexportován adresář `/samba/data/images`, který je přístupný pro klienty z podsítě 192.168.1.0 se síťovou maskou 255.255.255.0. Nyní

můžeme provést přípravu pro spuštění NFS serveru přidáním následujících řádků do souboru `/etc/rc.conf`:

```
rpcbind_enable="YES"
nfs_server_enable="YES"
mountd_flags="-r"
```

Ke spuštění NFS serveru dojde po provedení uvedené konfigurace při příštím startu operačního systému nebo je možné provést spuštění ručně bez restartu zadáním:

```
# rpcbind
# nfsd -u -t -n 4
# mountd -r
```

Pokud konfigurace a spuštění proběhly bez chyb, máme NFS server připravený. Nyní můžeme na stanici, kterou budeme zálohovat, nabootovat SystemRescueCD. Po naběhnutí se můžeme pokusit připojit k adresáři na serveru.

Nejdříve je potřeba vytvořit nový adresář, do kterého budeme adresář ze serveru připojovat:

```
# mkdir /mnt/image
```

Adresář je potřeba vytvořit, ačkoliv by se mohlo zdát rozumné provést připojení přímo pod `/mnt`. Po naběhnutí SystemRescueCD je však vypsáno varování, že pokus o připojení přímo pod `/mnt` vede k zamrznutí systému a vytvoření podadresáře je tedy nutné.

Před samotným pokusem o připojení je potřeba spustit ještě službu `portmap`:

```
# portmap
```

Nyní již můžeme připojit adresář ze serveru zadáním:

```
# mount -o nolock proliant:/samba/data/images /mnt/image
```

`Proliant` je jméno serveru a parametr `-o nolock` znamená, že nebude použito uzamykání pomocí služby `lockd` (na serveru není spuštěna podpora pro zamykání a uzamykání by selhalo).

Zda je svazek připojen se můžeme přesvědčit zadáním příkazu `mount` bez parametrů.

Nyní můžeme použít některou z popsaných metod vytváření/obnovy obrazu s tím rozdílem, že jako cíle/zdroje budeme používat soubory umístěné v `/mnt/image`.

### Zabezpečení vyexportovaného adresáře

Dle uvedeného postupu byl vytvořen na serveru adresář přístupný pomocí NFS z libovolného počítače z podsítě `192.168.1.0/24` a nastaveno oprávnění na plný přístup pro čtení/zápis. Zabezpečení na základě identifikátoru uživatele UID zde není příliš účinné, protože nabootování z CD, případně z vlastního počítače na síti, s přístupem k uživatelskému účtu `root`, není problém vytvořit si uživatele s potřebným UID. Vyexportovaný adresář tak zůstává chráněný pouze nevědomostí o jeho existenci. Jelikož proces zálohování a obnovy není tak často prováděným úkonem a vytváření samotného obrazu je ještě méně časté než jeho obnova, je možné učinit několik opatření.

Obrazy nainstalovaných školních stanic v daném prostředí neobsahují žádná kritická a atraktivní data, takže může stačit po vytvoření obrazů změnit na serveru oprávnění adresáře a souborů pouze pro čtení, jakožto ochranu před neoprávněným nebo nechtěným smazáním obrazů. Dále je možné export adresáře povolit pouze na dobu obnovy/zálohování. Záleží na konkrétním prostředí a požadavcích na zabezpečení dat obrazů.

### 5.3.6 Vlastní verze SystemRescueCD

Důvody k vytvoření vlastní verze SystemRescueCD mohou být:

- přidání vlastních nástrojů (programů, skriptů) na CD;
- přidání zálohy diskového oddílu a vypálení spolu se SystemRescueCD přímo na CD nebo DVD.

V prostředí školy bylo důvodem k výrobě vlastního CD automatické provedení následujících kroků po bootu CD:

- spuštění potřebných služeb a připojení adresáře přes NFS;
- spuštění skriptu umístěného na NFS serveru.

Tím je umožněno použitím jednoho CD dělat v budoucnu změny pouze ve skriptu na serveru a automaticky spustit požadované úlohy ihned po startu CD nebo vytvořit pro obsluhu nabídku s jednotlivými možnostmi obnovy.

#### Autorun skripty

SystemRescueCD má od verze 0.2.6 přidánu podporu *autorun* skriptů, což jsou skripty, které se spustí automaticky po spuštění systému. Autorun skripty jsou ve výchozím nastavení umístěny v kořenovém adresáři CD. Pokud je použit jeden samostatný skript, jeho jméno je *autorun*. Může se zde nacházet i více skriptů, které musí být pak pojmenované *autorun0*, *autorun1*,... V tomto případě může být spuštění jednotlivých skriptů ovlivněno ještě před započítím bootování systému z CD přidáním parametru *autoruns=* na řádce s výzvou *boot*: například:

```
fb800 autoruns=2,3,4
```

začne bootovat s obrazem jádra *fb800* a spustí po bootu skripty *autorun2*, *autorun3*, *autorun4*.

Autorun skripty mohou být spuštěny i z jiného umístění, například z diskety:

```
fb800 ar_source=/dev/fd0
```

Pro automatickou přípravu připojení k NFS serveru a spuštění skriptu umístěného na serveru byl vytvořen následující skript se jménem *autorun* a přidán na CD:

```
#!/bin/bash
mkdir /mnt/image
portmap
mount -o nolock proliant:/samba/data/images /mnt/image
/mnt/image/scripts/autorun.sh
exit 0
```

Skript *autorun.sh* umístěný na serveru je uveden v příloze [A.4](#).

## Postup vytvoření vlastní verze SystemRescueCD

Postup se skládá z následujících kroků:

1. Nabootování z CD.
2. Vytvoření adresáře pro připojení pracovního oddílu:  
`# mkdir /mnt/custom`
3. Připojení pracovního diskového oddílu s volným místem například:  
`# mount /dev/hda1 /mnt/custom`
4. Extrahování souborů z obrazu `sysresccd.dat`, který se používá při bootu z CD:  
`# /usr/sbin/sysresccd-custom extract`  
Soubory extrahované z obrazu jsou extrahovány do adresáře  
`/mnt/custom/customcd/files/`
5. Úprava extrahovaných souborů, pokud je potřeba.
6. Vytvoření nového obrazu – přečtení souborů z `/mnt/custom/customcd/files/` a vytvoření nového obrazu v `/mnt/custom/customcd/isoroot/sysrcd.dat`:  
`# /usr/sbin/sysresccd-custom squashfs`
7. Přidání souborů do ISO obrazu CD (pokud je potřeba)  
v našem případě nakopírování `autorun` skriptu s výše uvedeným obsahem:  
`# cp autorun /mnt/custom/customcd/isoroot`  
`# chmod 755 /mnt/custom/customcd/isoroot/autorun`
8. Nastavení klávesnice (u originálního CD je při bootování zobrazena výzva s výběrem):  
`# /usr/sbin/sysresccd-custom setkmap us`
9. Editace parametrů bootování (volitelně) – provádí se editací souboru  
`/mnt/custom/customcd/isoroot/isolinux/syslinux.cfg`
10. Vytvoření ISO obrazu disku:  
`# /usr/sbin/sysresccd-custom isogen my_srcd`
11. Synchronizace a odpojení disků:  
`# cd / ; umount /mnt/custom ; sync`
12. Vypálení ISO obrazu na nové CD – výsledkem přípravy je obraz CD ve standardním formátu ISO umístěný v `/mnt/custom/customcd/isofile/sysresccd-new.iso`, který je potřeba vypálit na CD pomocí některého z zapisovacích programů (cdrecord, Nero...).
13. Nabootování z nového CD.

Další podrobnosti o přípravě vlastní verze lze nalézt na stránkách projektu [4].

## 5.4 Závěr

Cílem kapitoly bylo nastínit možnosti zálohování/obnovy diskových oddílů Windows se souborovým systémem NTFS pomocí dostupných nástrojů a možnosti použití volně šiřitelných nástrojů. Kombinace SystemRescueCD a nástroje Partimage je používána ve škole druhým rokem a pro daný účel se osvědčila.

## Kapitola 6

# Další provoz systému

Úkony nutné pro další provoz systému z pohledu zálohování a bezpečnostních aktualizací pro operační systém FreeBSD byly uvedeny v bakalářské práci autora [8] v kapitole 5.

### 6.1 Softwarové zrcadlení disků

Jako ochrana před selháním disku byla navíc odzkoušena podpora pro softwarové zrcadlení disků v operačním systému FreeBSD 6.2. Server, na který byl software Samba instalován, obsahoval 2x 36 GB a 2x 72 GB SCSI disky. Jelikož SCSI disky jsou relativně drahé při nižší kapacitě, byl server, vzhledem k potřebné diskové kapacitě, dovybaven dvojicí IDE disků s kapacitou 320 GB na disk. Mezi dvojicemi disků bylo vytvořeno softwarové zrcadlení. Využití zrcadlených dvojic disků bylo v systému bylo rozděleno následovně:

- 36 GB uložení operačního systému a jeho softwarového vybavení;
- 72 GB uložení cestovních profilů uživatelů Samba serveru;
- 320 GB uložení uživatelských domovských adresářů.

Použití IDE disků se v řešené síti střední školy neukázalo být překážkou, co se týče propustnosti a odezvy serveru.

Pro realizaci zrcadlení byl použit modul jádra *geom\_mirror*. Tento modul přináší podporu funkcionality zrcadlení disků do jádra operačního systému. Zrcadlení může být kromě samostatných disků provedeno i na systémovém bootovacím disku. Konfigurace zrcadlení je jednoduchá a přímočará.

Předpokládejme, že disky v systému, které chceme zrcadlit, nesou označení *ad4* a *ad6*. Zrcadlení těchto disků ustavíme následujícím způsobem:

```
# gmirror -v data ad4 ad6
# gmirror load
# newfs -U /dev/mirror/data
```

Název vytvořeného zrcadlení je *data*. První příkaz provede uložení metadat a ustavení zrcadlení nad uvedenými disky. Druhý příkaz provede inicializaci a načtení modulu jádra *geom\_mirror* a poslední příkaz vytvoří na zrcadlených discích nový souborový systém.

Po provedení těchto kroků jsou zrcadlené disky připravené k použití a můžeme se pokusit o připojení zrcadlených disků do adresářového stromu:

```
# mount /dev/mirror/data /mnt
```

Stavové informace o zrcadlených discích je možné zobrazit pomocí příkazů:

```
# gmirror list
# gmirror status
```

Pro automatickou podporu zrcadlených disků po startu systému a jejich automatické připojení je potřeba provést následující úpravy:

- do souboru `/boot/loader.conf` přidat řádek, který zajistí načtení modulu jádra `geom_mirror` při startu systému:  
`geom_mirror_load="YES"`
- do souboru `/etc/fstab` přidat řádek, který zajistí připojení do požadovaného místa adresářového stromu, například:  
`/dev/mirror/data /samba/data ufs rw 1 1`

### 6.1.1 Zrcadlení systémového disku

Postup vytvoření softwarového zrcadlení na systémového disku je složitější. Následující seznam naznačuje potřebné kroky:

- instalace operačního systému na první disk, v nejjednodušším případě do jediného oddílu `/` (`root`);
- vytvoření nového zrcadlení s komponentou pouze druhého disku (zatím nekompletní zrcadlo pouze s jedním diskem);
- vytvoření oddílů na novém zrcadlení;
- uložení zaváděcího kódu pro bootování;
- vytvoření souborového systému;
- dočasné připojení zrcadlení;
- překopírování systémového disku na zrcadlení (vhodným způsobem, aby byla zachována oprávnění souborů – například pomocí programů `dump/restore`);
- úprava zkopírovaných souborů `/etc/fstab` a `/boot/loader.conf`;
- nový start systému a naboťování z druhého disku s vytvořeným nekompletním zrcadlením (například změnou pořadí bootování v biosu nebo fyzickým přehozením disků);
- po naboťování systému přidání prvního disku do zrcadlení; po provedení tohoto kroku dojde k synchronizaci obsahu disků a zrcadlení systémového disku je uvedeno do provozu.

Další informace lze nalézt ve FreeBSD Handbook [2], kapitola 19.

# Kapitola 7

## Závěr

Cílem práce bylo nahrazení serveru Windows 2000, který zastával roli primárního řadiče domény školní počítačové sítě se stanicemi Windows, novým serverem s operačním systémem rodiny BSD a instalace software Samba do role primárního řadiče domény a tiskového serveru.

Tento cíl se podařilo splnit a celý systém má za sebou již několik měsíců bezproblémového chodu. Větší hardwarový problém se vyskytl jenom při instalaci samotného serveru s řadičem SCSI. Instalace samotného operačního systému a balíku Samba byla celkově bez větších komplikací.

Dalším úkolem bylo navrhnout systém pro zjednodušení instalace mnoha počítačů se stejnou hardwarovou konfigurací v prostředí školních učeben. Popsaná varianta založená na volně šiřitelném softwaru se při dlouhodobém provozu v daném prostředí osvědčila.

Pro autora byl tento projekt přínosem hlavně ve získání praktických zkušeností se sítěmi Windows založenými na SMB protokolu, tiskovými službami, s operačními systémy FreeBSD a Linux a zkušenostmi s dlouhodobým provozem školní počítačové sítě s několika sty uživateli.

Instalace a provoz systému v prostředí školy je typický svojí podobností v prostředí různých škol – několik učeben s výpočetní technikou, které jsou obvykle vybaveny stejným nebo podobným hardwarem a počet uživatelů mnohonásobně převyšující počet stanic na škole. Uživatelé se obměňují nárazově jedenkrát do roka, s příchodem nových studentů a odchodem absolventů. Potřeba vytváření/rušení uživatelů během školního roku je spíše výjimečná. Trvanlivost uživatelských účtů je dána typem studijního programu na 4 nebo 8 let. Žádná uživatelská data nejsou ukládána na lokální disky a nezáleží na které stanici v učebnách se uživatel přihlásí. Uživatelé migrují a přihlašují se na různých stanicích v různých učebnách. Tímto se prostředí školy liší od ostatních prostředí, například firemních.

Díky těmto vlastnostem je popsané řešení a jeho nasazení do značné míry použitelné i v prostředí jiné školy s provedením pouze drobných úprav. Další realizace byla uvedena do provozu na základní škole v obci Nová Říše.

## Další vývoj

Dalšími možnými kroky pro zjednodušení správy Samba serveru by mohl být návrh a implementace rozhraní pro snadnější správu uživatelů (vytváření, mazání, změny hesel, diskových kvót, oprávnění...) a případně dalších úkonů pro obsluhu, která nemá zkušenosti

s ovládáním operačních systémů typu Unix a s rozhraním konzole s příkazovou řádkou. Rozhraní by mohlo být vytvořeno jako webová aplikace. Neexistence komplexního grafického uživatelského rozhraní pro správu systému může být překážkou vedoucí v některých prostředích až k výběru jiné, komerční a mnohonásobně dražší varianty řešení.



# Literatura

- [1] Robert Eckstein, David Collier-Brown, and Peter Kelly. *Samba (český překlad)*. Computer Press, 2001.
- [2] The FreeBSD Documentation Project. *FreeBSD Handbook*.  
[http://www.freebsd.cz/doc/en\\_US.ISO8859-1/books/handbook/index.html](http://www.freebsd.cz/doc/en_US.ISO8859-1/books/handbook/index.html)  
(duben 2007).
- [3] WWW stránky. *Program Partimage*. <http://www.partimage.org/> (duben 2007).
- [4] WWW stránky. *Projekt SystemRescueCD*. <http://www.sysresccd.org/> (duben 2007).
- [5] John H. Terpstra. *Samba-3 by Example*.  
<http://us4.samba.org/samba/docs/man/Samba-Guide/> (duben 2007).
- [6] Jay Ts, Robert Eckstein, and David Collier-Brown. *Using Samba 2nd Edition*. O'Reilly & Associates, 2003.  
[http://us4.samba.org/samba/docs/using\\_samba/toc.html](http://us4.samba.org/samba/docs/using_samba/toc.html) (duben 2007).
- [7] Jelmer R. Vernooij, John H. Terpstra, and Gerald Carter. *The Official Samba-3 HOWTO and Reference Guide*.  
<http://us4.samba.org/samba/docs/man/Samba-HOWTO-Collection/> (duben 2007).
- [8] Martin Zadina. *Nasazení OS xBSD v síti pro střední školu*. VUT FIT, 2005.  
Bakalářská práce.

## Dodatek A

# Konfigurační soubory

### A.1 Konfigurační soubor tiskového podsystemu – printcap

```
#laserova tiskarna HP v ucebne pisarna
#pripojena k siti pomoci hw printserveru
ljpis:\
    :lp=\
    :rm=ljpis:\
    :rp=lpt1:\
    :lf=/var/spool/lpd/ljpis.log:\
    :sd=/var/spool/lpd/ljpis:\
#
#laserova tiskarna HP v ucebne IVT
#pripojena k siti pomoci hw printserveru
ljivt:\
    :lp=\
    :rm=ljivt:\
    :rp=L1:\
    :lf=/var/spool/lpd/ljivt.log:\
    :sd=/var/spool/lpd/ljivt:\
#
#laserova barevna tiskarna Epson v ucebne IVT
#pripojena ke stanici s Windows
#preposlani tiskove ulohy pomoci skriptu smbprint
ljivtcolor:\
    :lp=/dev/null:\
    :lf=/var/spool/lpd/ljivtcolor.log:\
    :sd=/var/spool/lpd/ljivtcolor:\
    :sh:\
:if=/usr/local/samba/bin/smbprint:
```

### A.2 Konfigurační soubor Samby smb.conf

```
[global]
workgroup = GYMN
```

```

netbios name = PROLIANT
passdb backend = tdbsam
wins support = Yes
printing = bsd
;
logon script = %a.bat
logon path = \\%L\profiles\%U\%a
logon drive = H:
;
domain logons = Yes
security = user
os level = 34
local master = Yes
domain master = Yes
;
printcap name = /etc/printcap
printer admin = root

[printers]
comment = All Printers
printable = yes
path = /var/spool/samba
writable = no

[print$]
comment = Printer Driver Download Area
path = /samba/profiles/drivers
browseable = yes
writeable = no
write list = root
;
[homes]
comment = Home Directories
valid users = %S
read only = No
browseable = No
;
create mask = 711
directory mask = 711
map archive = Yes
map hidden = Yes
map system = Yes

[netlogon]
comment = Network Logon Service
path = /samba/profiles/netlogon
public = no
writeable = No

```

```

browsable = No
;
create mask = 711
directory mask = 711
map archive = Yes
map hidden = Yes
map system = Yes

[profiles]
comment = Profile Share
path = /samba/profiles/profiles
writable = Yes
browsable = No
create mask = 711
directory mask = 711
map archive = Yes
map hidden = Yes
map system = Yes

[public]
comment = Pro sdileni souboru
path = /samba/data/shares/public
writable = Yes
oplocks = No
level2 oplocks = No

[software]
comment = Software
path = /samba/data/shares/software
writable = Yes
oplocks = No
level2 oplocks = No

```

### A.3 Přihlašovací skript WinXP.bat

```

net time \\proliant /set /yes
net use p: \\proliant\public
net use s: \\proliant\software
rundll32 printui.dll,PrintUIEntry /in /n "\\proliant\ljpis"
rundll32 printui.dll,PrintUIEntry /in /n "\\proliant\ljivt"
rundll32 printui.dll,PrintUIEntry /in /n "\\proliant\ljivtcolor"

```

### A.4 Skript autorun.sh

```

#!/bin/sh
echo "System obnovy"
echo "Zadejte cislo akce, ktera se ma provest:"

```

```

echo " 1. - obnovit obraz IVT - Windows"
echo " 2. - obnovit obraz IVT - kompletni disk"
echo " 3. - obnovit obraz pisarna - kompletni disk"
echo " 4. - obnovit obraz 7x nove PC pro kancelar a zemepis"
echo " 5. - obnovit obraz 20x nove PC ucebna"
echo -n "-> "
read A
case $A in
  1) partimage -b -f3 restore /dev/hda1 /mnt/image/windows.06-08-09a.img.000
    ;;
  2) gzcat /mnt/image/windows.06-08-10.cat.gz > /dev/hda
    ;;
  3) gzcat /mnt/image/win-pis.06-08-11.cat.gz > /dev/hda
    ;;
  4) partimage -b -f3 restore /dev/sda1 /mnt/image/win7x.img.000
    ;;
  5) partimage -b -f3 restore /dev/sda1 /mnt/image/win20x.img.000
    ;;
  *) echo "Neplatna volba!"
    exit 0
    ;;
esac

echo "Obnova dokoncena"
echo "Stisknete libovolnou klavesu pro restart..."
read
shutdown -r now

```

## A.5 Skript user\_add.sh

```

#!/bin/sh
#vytvoreni uzivatele v Unixu a Sambe
#$1, $2, $3, $4, $5
#login, groupname, firstname, lastname, smbpassword
#uzivateli je vygenerovano do unixu nahodne heslo
#jelikoz se autentizuje pres sambu, neni treba
#je mozne ho ziskat v pripade potreby z promenne UNIXPASSWD
#
#vytvorime uzivatele v unixu
UNIXPASSWD='pw useradd -n $1 -c "$4 $3" -d /home/$2/$1 -g $2 -m | cut -d: -f1'
#vytvorime uzivatele v Sambe a nastavime heslo
printf %b "$5\n$5" | smbpasswd -a -s $1

```

## Dodatek B

# Popis parametrů

### B.1 Přehled důležitých parametrů souboru `smb.conf` pro tiskové služby

#### B.1.1 Parametry speciální sekce [global]

**printing = bsd** – říká Sambě, že má používat příkazy tiskového podsystému BSD (LPR/LPD). Obecně tento parametr informuje Sambu o tiskovém podsystému, který má očekávat. Samba podporuje podsystémy CUPS, LPD, LPRNG, SYSV, HPUX, AIX, QNX a PLP. Každý z těchto podsystémů používá odlišné příkazy pro ovládání tisku.

Tento parametr uvedený v globální sekci je následně použit jako výchozí hodnota pro všechna tisková sdílení. Parametr může být též uveden u samotného tiskového sdílení a obejít tak výchozí nastavení v globální sekci.

**load printers = yes** – říká Sambě, že má automaticky vytvořit tisková sdílení pro všechny tiskárny tiskového podsystému dle souboru `printcap`. Všechna vytvořená sdílení jsou zveřejněna v prohlízacích seznamech Samby. Při použití tohoto parametru není nutné vytvářet pro každou tiskárnu tiskové sdílení v souboru `smb.conf`. Každé automaticky vytvořené tiskové sdílení přebírá nastavení uvedené v obecné sekci [printers] souboru `smb.conf`. V případě nastavení parametru na hodnotu *no* je potřeba vytvořit požadovaná tisková sdílení v souboru `smb.conf` manuálně.

**show add printer wizard = yes** – ovládá zobrazení ikony pro přidání další tiskárny ve složce tiskáren při prohlížení Samba serveru. Zobrazení ikony je potřebné pro spuštění průvodce přidáním tiskárny při nahrávání ovladačů tiskárny na Samba server do sdílení [print\$] a jejich asociaci s tiskárnou.

**max print jobs = 100** – nastavuje limit tiskových úloh, které mohou být aktivní na Samba serveru v jednom okamžiku. Nastavení na hodnotu 0 znamená, že limit není stanoven. Při překročení počtu tiskových úloh je při odesílání další úlohy klientem na server klientovi vráceno chybové hlášení o nedostatku místa na serveru.

**printcap name = /etc/printcap** – říká Sambě, kde má hledat soubor `printcap` s informacemi o dostupných tiskárnách tiskového podsystému.

**printer admin = @printadmins** – členové skupiny `printadmins` budou oprávněni k přidávání ovladačů tiskáren na server a k nastavování vlastností tiskáren. Uživatel `root` je implicitně vždy správcem tiskáren. Znak „@“ předchází názvu skupiny systému Unix uvedené v souboru `/etc/group`. Tento parametr může být specifikován i u jednotlivých tiskových sdílení.

**lpq cache time = 20** – určuje časování výsledku příkazu `lpq`. Redukuje počet volání příkazu `lpq` a snižuje tak zátěž vysoce zatíženého tiskového serveru.

**use client driver = no** – nastavení parametru na hodnotu `yes` se projeví pouze u klientů s operačními systémy Windows NT/2000/XP. Výchozí hodnotou je `no` a nesmí být tento parametr povolen (nastaven na hodnotu `yes`) pro tisková sdílení, která mají nainstalován na Samba serveru tiskové ovladače.

### B.1.2 Nastavení sekce [printers]

Tato sekce má roli zástupce pro všechny tiskárny. Parametry specifikované v této sekci jsou výchozí pro všechna tisková sdílení a mohou být obejity nastavením příslušného parametru v sekci konkrétního tiskového sdílení.

**comment =** – parametr nastavuje komentář k tiskovému sdílení, který je viditelný u klienta při prohlížení sítě.

**printable = yes** – tiskové sdílení musí být deklarováno jako „printable“ (tisknutelné). Tento parametr je použit Sambou pro rozlišení tiskových a souborových sdílení.

**path = /var/spool/samba** – musí ukazovat do adresáře, který je určen pro uložení příchozích tiskových úloh Sambou. Tento adresář nesmí být stejný jako adresář specifikovaný pro účel tiskové fronty v použitém tiskovém podsystému. Typicky je použit adresář s oprávněním zápisu pro všechny a nastaveným `sticky` bitem.

**browsable = no** – tento parametr má vždy hodnotu `no` pokud `printable = yes`. Způsobuje neviditelnost tiskového sdílení v seznamu souborových sdílení (tisková sdílení jsou viditelná ve speciální složce tiskáren).

**public = yes** – určuje, jestli se k tiskovému sdílení může připojit uživatel bez provedení autentizace

### B.1.3 Parametry pro libovolnou sekci [tiskove\_sdileni]

Jsou stejné jako parametry uvedené v sekci [printers]. Může být dále vhodné specifikovat pro jednotlivé tiskárny následující parametry:

**hosts allow = 192.168.1., 192.168.2.** – umožňuje tisk na tiskárně pouze z podsítí 192.168.1. a 192.168.2.

**hosts deny = 192.168.1.99, 192.168.2.80** – zakazuje uvedeným adresám tisk na tiskárně, přestože jejich podsítě byly uvedeny v parametru `hosts allow`. Místo IP adres může být uvedeno i jméno NetBIOS.