

Zavedení a provoz operačního systému Windows ze sítě

Boot up and operation of Windows operating system
over a network

Tomáš Kusák



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Tomáš KUSÁK**
Osobní číslo: **A08064**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Informační a řídicí technologie**

Téma práce: **Zavedení a provoz operačního systému Windows ze sítě**

Zásady pro vypracování:

1. Vypracujte literární rešerši na téma zavedení a provoz operačního systému ze sítě.
2. Navrhněte a prakticky realizujte nejvhodnější řešení pro operační systém Windows.
3. Definujte požadavky pro praktickou realizaci.
4. Věnujte se problematice zabezpečení a správy.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. TULLOCH, Mitch ; NORTHRUP, Tony; HONEYCUTT, Jerry. Windows 7 Resource Kit. 1st edition. Redmond (Washington) : Microsoft Press, 2009. 1760 s. ISBN 0735627002, 978-0735627000.
2. BOTT, Ed; SIECHERT, Carl; STINSON, Craig. Windows 7 Inside Out. 1st edition. Redmond (Washington) : Microsoft Press, 2009. 1056 s. ISBN 0735626650, 978-0735626652.
3. POELKER, Christopher; NIKITIN, Alex. Storage Area Networks For Dummies. 2nd edition. Hoboken (New Jersey) : Wiley Publishing, Inc., 2009. 456 s. ISBN 978-0-470-38513-5.
4. Linux : Dokumentační projekt. [s.l.] : Computer Press, 2008. 1336 s. Dostupné z WWW: [http://ii.iinfo.cz/r/kd/LDP_4.pdf]. ISBN 978-80-251-1525-1.
5. KOHOUT, Petr. Nasazení bezdiskových pracovních stanic s OS Linux v síti FAI UTB. Zlín, 2008. 70 s. Bakalářská práce. UTB ve Zlíně.

Vedoucí bakalářské práce:

doc. Ing. Martin Sysel, Ph.D.

Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce:

25. února 2011

Termín odevzdání bakalářské práce:

7. června 2011

Ve Zlíně dne 25. února 2011

prof. Ing. Vladimír Vašek, CSc.
děkan



prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Tato bakalářská práce popisuje možné způsoby zavedení a provozu operačního systému Microsoft Windows přes síť.

V teoretické části jsou popsány různé způsoby, jak tento problém řešit - zavedení a provoz systému ze síťového disku přes protokol iSCSI, komerční řešení CCBoot, Windows PE.

Praktická část se věnuje realizaci některých způsobů, které byly popsány v teoretické části - zavedení Windows 7 ze síťového disku pomocí protokolu iSCSI a zavedení Windows PE ze sítě přes protokoly PXE, HTTP a iSCSI.

Klíčová slova: Microsoft, Windows, Linux, PXE, iSCSI, zavádění systému, síť, CCBoot

ABSTRACT

This bachelor thesis describes possible ways how to boot up and use Microsoft Windows operating system over a network.

Theoretical part contains description of various ways how to solve this problem - boot up and operation of system from iSCSI target, commercial solution CCBoot, Windows PE.

Practical part is dedicated to realization of some ways that were described in theoretical part - boot up of Windows 7 from iSCSI target and boot up of Windows PE over a network via PXE, HTTP and iSCSI protocols.

Keywords: Microsoft, Windows, Linux, PXE, iSCSI, boot, network, CCBoot

Děkuji svému vedoucímu bakalářské práce doc. Ing. Martinu Syslovi, Ph.D. za to, že mi ochotně věnoval spoustu svého času a poskytl mnoho cenných rad a doporučení.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně dne 22. května 2011

.....
podpis diplomanta

OBSAH

ÚVOD	11
I TEORETICKÁ ČÁST	12
1 ÚVOD DO SÍTOVÉHO ZAVÁDĚNÍ OPERAČNÍHO SYSTÉMU	13
1.1 ZAVÁDĚNÍ SYSTÉMU Z LOKÁLNÍHO PEVNÉHO DISKU	13
1.2 VÝHODY ZAVÁDĚNÍ ZE SÍTĚ	13
1.2.1 Centrální správa všech počítačů	13
1.2.2 Zvýšená odolnost systému před zásahy uživatele	14
1.2.3 Vyšší spolehlivost oproti lokálnímu pevnému disku	14
1.2.4 Nižší cena řešení jako celku	14
1.3 MOŽNOSTI PŘI ZAVÁDĚNÍ	14
1.3.1 In-RAM řešení.....	15
1.3.2 OS - Streaming	15
1.4 POSTUP PŘI ZAVÁDĚNÍ SYSTÉMU ZE SÍTĚ	15
1.4.1 Funkce BIOSu	15
1.4.2 Oficiální Boot ROM.....	16
1.4.3 Alternativní Boot ROM.....	16
1.5 PROTOKOLY POUŽÍVANÉ PRO ZAVÁDĚNÍ SYSTÉMU	16
1.5.1 PXE	16
1.5.2 iSCSI	17
1.5.3 HTTP.....	19
1.6 ZPŮSOBY ZAVÁDĚNÍ SYSTÉMU POPISOVANÉ ZDE	20
1.6.1 Zavedení systému přes protokol iSCSI	20
1.6.2 Komerční řešení - program CCBoot	20
1.6.3 Zavedení Windows PE ze sítě.....	20
1.6.4 Virtualizace Windows na systému Linux.....	20
1.6.5 Komerční řešení - SANDeploy Boot Server	20
2 ZAVÁDĚNÍ SYSTÉMU PŘES PROTOKOL iSCSI	21
2.1 STRUKTURA ZAVÁDĚNÍ	21
2.1.1 Požadavky na server	21
2.1.2 Požadavky na klienta.....	21
2.1.3 Požadavky na síťové propojení	21
2.1.4 Postup při zavádění operačního systému.....	22
2.2 PROBLÉMY PŘI SÍTOVÉM ZAVÁDĚNÍ WINDOWS.....	23
2.2.1 Windows při zavádění zapisují na disk	23
2.2.2 Windows nepodporují rozdílné hardwarové konfigurace	23
2.2.3 Síťově zavedená Windows mohou ohrozit lokální pevný disk pracovní stanice.....	24
2.2.4 Další problémy	24

3	KOMERČNÍ ŘEŠENÍ - PROGRAM CCBOOT.....	25
3.1	POPIS PROGRAMU	25
3.2	VLASTNOSTI ŘEŠENÍ	27
3.2.1	Výhody řešení.....	27
3.2.2	Nevýhody řešení.....	28
3.3	POPIS A NASTAVENÍ SERVERU.....	29
3.3.1	Instalace serveru	29
3.3.2	Popis základního nastavení	29
3.3.3	Přidání nového klienta.....	34
3.4	POPIS KLIENSKÉ APLIKACE.....	37
3.4.1	Instalace aplikace CCBoot Client.....	37
3.4.2	Popis základního nastavení	37
3.4.3	Upload image disku lokálního počítače na server.....	38
3.4.4	Další volby klientské aplikace.....	38
3.5	PRAKTICKÉ ZKUŠENOSTI S PROGRAMEM CCBOOT.....	39
4	WINDOWS PE	41
4.1	ZÁKLADNÍ VLASTNOSTI	41
4.1.1	Možnosti zavedení	41
4.1.2	Nevýhody a problémy	42
4.2	DRUHY WINDOWS PE	43
4.2.1	Oficiální vydání.....	43
4.2.2	Neoficiální vydání	44
4.3	POUŽÍVÁNÍ WINDOWS PE.....	46
4.3.1	Požadavky na image.....	46
4.3.2	Popis řešení	46
4.3.3	Výhody řešení.....	47
4.3.4	Nevýhody řešení.....	47
4.3.5	Alternativní řešení.....	48
5	DALŠÍ MOŽNOSTI ZAVEDENÍ WINDOWS ZE SÍTĚ.....	49
5.1	VIRTUALIZACE WINDOWS NA SYSTÉMU LINUX	49
5.1.1	Postup zavádění systému.....	49
5.1.2	Výhody řešení.....	49
5.1.3	Nevýhody řešení.....	50
5.2	KOMERČNÍ ŘEŠENÍ - SANDEPLOY BOOT SERVER	50
II	PRAKTICKÁ ČÁST	51
6	ZAVÁDĚNÍ SYSTÉMU PŘES PROTOKOL iSCSI.....	52
6.1	PXE SERVER	52
6.1.1	Nastavení statické IP adresy.....	52
6.1.2	Nastavení služby TFTP	53
6.1.3	Obsah kořenového adresáře TFTP serveru	53
6.1.4	Nastavení služby DHCP.....	54
6.1.5	Další podpůrné soubory nutné pro instalaci a zavedení Windows.....	55

6.2	iSCSI SERVER.....	56
6.2.1	Nastavení síťového rozhraní	56
6.2.2	Připojení fyzických disků a vytvoření logických jednotek.....	56
6.2.3	Vytvoření disku sdíleného protokolem iSCSI.....	56
6.3	INSTALACE WINDOWS NA iSCSI TARGET	59
6.3.1	Využití instalačního média jako druhého bootovatelného zařízení.....	59
6.3.2	Připojení iSCSI disku z Windows 7 a instalace na něj	60
6.3.3	Instalace přes Windows PE	61
6.3.4	Použití El-Torito CD	61
6.3.5	Instalace přes síťový adaptér přímo obsahující gPXE.....	63
6.3.6	Další možnosti instalace.....	65
7	WINDOWS PE	66
7.1	ÚVOD	66
7.1.1	Vytvářený image se systémem	66
7.1.2	Další možnosti při vytváření image.....	66
7.1.3	Nastavení sítě	66
7.2	ZAVÁDĚNÍ PROGRAMŮ ZE SÍTĚ	67
7.2.1	Síťový disk s programy	67
7.2.2	Spouštění programů na Windows PE.....	67
7.2.3	Vytváření balíčků s programy a instalačních skriptů	68
7.3	VYTVORENÍ SPUSTITELNÉHO IMAGE SE SYSTÉMEM.....	70
7.3.1	Postup při vytváření image.....	70
7.4	VYUŽITÍ HTTP PRO INSTALACI BALÍČKŮ S PROGRAMY.....	75
7.4.1	HTTP server	75
7.4.2	Úprava obrazu Windows PE	76
7.4.3	Výhody a nevýhody řešení	77
7.5	BOOTOVÁNÍ PŘES PXE (STANDARDNÍ ZPŮSOB)	78
7.5.1	Příprava souborů	78
7.5.2	Nastavení serveru	79
7.5.3	Postup při bootování	81
7.5.4	Výhody řešení.....	82
7.5.5	Nevýhody řešení.....	82
7.6	BOOTOVÁNÍ PŘES PXE (STAŽENÍ ISO OBRAZU)	82
7.6.1	Obsah ISO obrazu	82
7.6.2	Vytváření ISO obrazu.....	83
7.6.3	Nastavení serveru	84
7.6.4	Postup při bootování	85
7.6.5	Výhody řešení.....	85
7.6.6	Nevýhody řešení.....	85
7.7	BOOTOVÁNÍ PŘES HTTP (STAŽENÍ ISO OBRAZU)	86
7.7.1	ISO obraz.....	86
7.7.2	Nastavení serveru	86
7.7.3	Postup při bootování	87
7.7.4	Výhody řešení.....	87
7.7.5	Nevýhody řešení.....	88

7.8	BOOTOVÁNÍ PŘES PROTOKOL iSCSI (STAŽENÍ DO RAM).....	88
7.8.1	Příprava	88
7.8.2	Přesun souborů na disk.....	89
7.8.3	Nastavení serveru	89
7.8.4	Výhody a nevýhody řešení	89
7.9	VÝBĚR OPERAČNÍHO SYSTÉMU PŘI SPUŠTĚNÍ POČÍTAČE.....	90
7.9.1	Nutné podmínky pro vytvoření menu.....	90
7.9.2	Vytváření jednoduchého menu.....	90
7.9.3	Význam jednotlivých položek skriptu.....	92
7.10	SROVNÁNÍ ŘEŠENÍ Z HLEDISKA RYCHLOSTI BOOTOVÁNÍ	93
7.11	ALTERNATIVNÍ ZPŮSOB VYTVOŘENÍ IMAGE SE SYSTÉMEM.....	95
7.11.1	Stažení projektu Win7PE_SE	95
7.11.2	Prostředí programu WinBuilder	96
7.11.3	Nepřipojení lokálních disků při startu Windows	97
7.11.4	Instalace programu přímo do Windows PE.....	97
7.11.5	Vytvoření image se systémem.....	100
7.12	PŘÍNOS PRO ADMINISTRACI POČÍTAČŮ NA FAI UTB.....	101
ZÁVĚR		103
ZÁVĚR V ANGLIČTINĚ.....		104
SEZNAM POUŽITÉ LITERATURY.....		105
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK		110
SEZNAM OBRÁZKŮ		114
SEZNAM TABULEK.....		115
SEZNAM PŘÍLOH.....		116

ÚVOD

Cílem této práce je představit rozdílné způsoby zavedení a provozu systému Microsoft Windows ze sítě a prakticky realizovat nejvhodnější řešení z nich.

Běžný způsob zavádění MS Windows spočívá v nutnosti mít v lokálním počítači nainstalován pevný disk, na němž se nachází místní spustitelná kopie MS Windows. Tento způsob zavádění je vhodný pro počítače používané v domácím prostředí, jako přenosné, nebo v malé společnosti, kde se uplatňuje výhoda nezávislosti provozu systému na existenci okolní sítě.

Pokud je ovšem daný počítač využíván ve velké společnosti, v níž je možné garantovat nejen připojení počítače k síti, ale rovněž i kvalitu samotné sítě, nabízí se vhodnější řešení, jak zavádět a spravovat operační systém. Toto řešení vychází z použití jednoho centrálního prvku, který obsahuje spustitelný image operačního systému, jež je přes síť distribuován na pracovní stanice, které z něj následně zavedou operační systém. Při použití tohoto řešení odpadá nutnost starat se o každou pracovní stanici zvlášť, což výrazně šetří čas správci sítě a umožňuje efektivní správu a rychlejší reakci na požadované změny v softwarové konfiguraci počítače.

V teoretické části práce budou probrány možné způsoby, pomocí nichž lze systém MS Windows zavést přes síť. Bude diskutováno nekomerční řešení, kdy server běží na operačním systému GNU/Linux, i komerční řešení, kdy se jako server využívá aplikace pro serverový systém Windows. Mezi popisované způsoby patří zavedení plné verze Windows ze síťového disku přes protokol iSCSI a různé způsoby zavedení Windows PE. Praktická část obsahuje realizaci vybraných teoretických řešení.

Zavedení a používání plné verze operačního systému Windows přes síť komplikuje fakt, že pro tento způsob zavádění existuje velmi slabá oficiální podpora. Situace je taková, že každá majoritní verze Windows s sebou přináší změny, jež téměř znemožňují použití funkčního řešení, které bylo možné aplikovat na verzi předchozí. S nadsázkou by se dalo říct, že se společnost Microsoft snaží zavedení svého operačního systému ze sítě co nejvíce znesnadnit. Důvodem k tomu může být snaha zvýšit prodej již hotových řešení na bázi virtualizace nebo strach ze zneužití dané technologie.

I. TEORETICKÁ ČÁST

1 ÚVOD DO SÍŤOVÉHO ZAVÁDĚNÍ OPERAČNÍHO SYSTÉMU

Aby bylo možno v operačním systému pracovat, musí se nejdříve zavést, tzv. naboootovat. Nejběžnější způsob zavádění operačního systému je z pevného disku v lokálním počítači. V tomto případě se po spuštění počítače provede POST, načte MBR z aktivního spouštěcího disku, předá řízení prvnímu sektoru aktivního oddílu a spustí zavaděč operačního systému. Operační systém se potom zavede z lokálního pevného disku. [1, s.45]

1.1 Zavádění systému z lokálního pevného disku

Zavádění operačního systému z lokálního pevného disku je vhodné, pokud je počítač izolován od sítě, případně je síť, ke které je připojen, nespolehlivá. Nezastupitelnou úlohu má rovněž v domácích a menších podnikových sítích, kde by se zavádění operačního systému ze sítě nevyplatilo. Ve větších sítích je ovšem tento způsob méně vhodný.

1.2 Výhody zavádění ze sítě

1.2.1 Centrální správa všech počítačů

V případě, že se podniková síť skládá z velkého množství počítačů, je velmi pracné starat se o každý počítač zvlášť. I kdyby měl administrátor připraven obraz systému, který na daný počítač v případě havárie lokálního pevného disku nebo poškození stávající instalace Windows nahraje, v případě společnosti, která používá stovky počítačů, nebude dělat nic jiného, než běhat od jednoho počítače ke druhému. V tomto případě se jeví využití centrálního serveru, z něž by všechny stanice bootovaly, jako výhodné řešení. Administrátor se už nemusí starat o každou stanici zvlášť, pouze stanice nastaví tak, aby zaváděly operační systém ze sítě. Veškeré změny v operačním systému, jako je instalace programů, updatů, nebo dokonce i upgrade celého systému se děje pouze na jednom místě, na serveru. Pozitivní je rovněž rychlost, s jakou tato změna nastane. Stačí, aby se stanice restartovala. Po restartu okamžitě používá upravený operační systém.

1.2.2 Zvýšená odolnost systému před zásahy uživatele

Zavádění systému ze sítě má další pozitiva. Na serveru se může vyskytovat více operačních systémů současně. Určitá skupina počítačů může mít stejný image se systémem. To, který image daný počítač zavede, se nastavuje přímo na serveru a je možné, aby se v denních hodinách automaticky zaváděl jiný operační systém než v noci. Zvyšuje se také odolnost celého systému před zásahy uživatele. Zavádění ze sítě může být nastaveno tak, že se na danou pracovní stanici zavede systém buď ve stavu, ve kterém byl, když byla pracovní stanice vypnuta, nebo ve stavu po čisté instalaci. Vše záleží na nastavení na jediném centrálním prvku.

1.2.3 Vyšší spolehlivost oproti lokálnímu pevnému disku

Přestože je operační systém zaváděn z jednoho centrálního prvku, což by mohlo vzbuzovat obavy o spolehlivosti tohoto řešení, je toto řešení, při správně navržené infrastruktuře sítě a vhodné volbě serveru, spolehlivější, než bootování z lokálního pevného disku. Ve větší síti je možno využít rozdělení zátěže na více prvků, případně zřídit záložní hot-site¹, která zrcadlí server.

1.2.4 Nižší cena řešení jako celku

V neposlední řadě je nutné zmínit finanční dopady tohoto řešení. Z počátku se mohou projevit zvýšené náklady na inovaci sítě a nákup vhodného serveru. Postupem času se ovšem tyto náklady vrátí v ceně za lokální pevné disky a v celkové lepší náladě správců, kteří se budou moci lépe věnovat skutečným problémům svých uživatelů a ne stále dokola rutinně obnovovat systém na jednotlivých pracovních stanicích.

1.3 Možnosti při zavádění

Zavádění může probíhat buď jako In-RAM řešení, při kterém se do operační paměti cílového počítače nejdříve stáhne celý image² se systémem jako jeden soubor a ten se

¹ Hot-site je záložní systém, který dokáže při výpadku původního systému okamžitě převzít jeho funkci.

² Kompletní disk s nainstalovaným operačním systémem uložený do jednoho souboru.

následně spustí, nebo jako OS-Streaming, při němž je systém ze serveru načítán soubor po souboru.

1.3.1 In-RAM řešení

V případě použití In-RAM řešení odpadá nutnost mít počítač neustále připojený k síti. Připojení k síti je nutné pouze při startu počítače, kdy se do RAM startujícího počítače stáhne jako jeden celek kompletní image s operačním systémem. Image vytvoří v operační paměti virtuální disk, který může být využíván nezávisle na dostupnosti, stabilitě a propustnosti sítě. Nevýhoda tohoto řešení ovšem spočívá v tom, že je operační systém přenesen naráz jako jeden komplet, což znamená, že jsou přeneseny i soubory, které nebudou po zavedení systému vůbec použity.

1.3.2 OS - Streaming

Hlavní výhodou OS-Streaming řešení je menší množství přenášených dat a tedy i menší zatížení sítě. Konkrétní soubor je ze serveru na cílový počítač přenesen až v okamžiku, kdy je skutečně potřeba a nepřenáší se tedy nic zbytečného. Nevýhodou tohoto řešení je nutnost být neustále připojen k síti. Jakákoliv porucha sítě může takto zavedený operační systém vyřadit z provozu. Nepříjemné může být také kolísání propustnosti sítě, například při spuštění více počítačů současně, což se projeví i na již zavedených systémech.

1.4 Postup při zavádění systému ze sítě

1.4.1 Funkce BIOSu

Po zapnutí počítače se spustí část BIOSu zvaná POST, která provede kontrolu nezbytných komponent nutných pro start systému. BIOS dále v průběhu fáze POST vyhledá zařízení s rozšiřujícím firmwarem, který přidává funkce specifické pro dané zařízení, a inicializuje je.

BIOS za účelem vyhledání doplňkového firmwaru prohledá speciální oblast paměti (C0000h až DFFFFh) určenou pro ROM obrazy rozšiřujících karet a pokud v ní najde hodnotu 0x55h následovanou hodnotou 0xAAh, interpretuje třetí bajt jako velikost ROM v násobcích 512 B. Čtvrtý bajt obsahuje offset definující spouštěcí bod, kterému je následně předáno řízení. Od tohoto okamžiku přebírá kontrolu nad počítačem program

v ROM, který pomocí služeb BIOSu zaregistruje vektory přerušení. Nyní je zařízení (mající vlastní firmware) připraveno k použití. [2]

Načtení ROM se speciálním firmwarem se používá k zavedení systému ze sítě. Daná ROM se obvykle nachází v EEPROM paměti síťové karty a obsahuje program potřebný pro zahájení zavádění operačního systému.

1.4.2 Oficiální Boot ROM

Po zakoupení síťové karty je v kartě nahrán oficiální firmware, který obsahuje velmi omezenou funkcionalitu. Obvykle podporuje pouze protokol PXE (pokud vůbec) a neumožňuje využít žádnou z rozšířených možností bootování.

1.4.3 Alternativní Boot ROM

Pokud má daná síťová karta patičku pro vložení Boot ROM, případně má firmware uložen v přepisovatelné flash paměti (např. karta Intel PRO/1000 GT), může být původní firmware nahrazen alternativní Boot ROM. Často používanou alternativní Boot ROM je program gPXE.

Program gPXE je zavaděč operačního systému, který je schopen zavést operační systém přes protokoly PXE, iSCSI, AoE a HTTP. Program je vydán pod licencí GPL, jeho předchůdcem je projekt Etherboot. V roce 2010 se vývoj programu roztrhl na dvě větve, původní gPXE a novou iPXE, která by měla být oficiální náhradou za gPXE. Funkčnost obou programů je ovšem téměř shodná. [3][4]

Program gPXE může být rovněž zaveden na cílový počítač, aniž by bylo nutné přepisovat původní firmware síťové karty. V tomto případě se program stáhne jako NBP (Network Bootstrap Program) přes protokol PXE.

1.5 Protokoly používané pro zavádění systému

1.5.1 PXE

Zkratka PXE znamená Preboot Execution Environment. Tento protokol byl uveden firmou Intel v roce 1999 a stal se světovým standardem pro zavádění operačního systému ze sítě. Podporu lze nalézt ve většině dnešních síťových adaptérů. Protokol je typu klient-server

a skládá se z protokolů DHCP a TFTP, na transportní vrstvě zajišťuje přenos dat protokol UDP. Při stahování image se systémem se používají porty 67 (DHCPDISCOVER), 68 (DHCPOFFER), 69 (TFTP přenos souborů). [5]

Zavedení systému probíhá takto:

- Spustí se klientský počítač, BIOS provede POST a načte Boot ROM na síťové kartě
- Řízení se předá Boot ROM na síťové kartě, začne se používat protokol PXE
- Počítač vyšle DHCP broadcast s žádostí o přidělení IP adresy a dalších informací (DHCPDISCOVER)
- DHCP server ve své odpovědi (DHCPOFFER) zašle klientovi informace nutné pro připojení k síti (IP adresa, síťová maska atd.) a cestu k NBP (Network Bootstrap Program)
- Klient se připojí k síti a pomocí protokolu TFTP stáhne NBP, který zavede do paměti a předá mu řízení
- NBP začne zavádět operační systém ze sítě (obvykle také protokolem TFTP), NBP zde slouží stejnému účelu jako bootloader u systému zaváděného z lokálního pevného disku

Z důvodu, že se pro přenos souborů využívá protokol TFTP, je přenos příliš pomalý a nevhodný pro sítě s větší odezvou. Základní problém tohoto protokolu je, že musí být doručení každého vyslaného paketu potvrzeno příjemcem a teprve po doručení potvrzení o doručení předchozího paketu (ACK) zpět na server se vysílá další paket (běžně 512B). Každý paket se tedy potvrzuje zvlášť. V daném okamžiku je v síti mezi odesílatelem a příjemcem vždy maximálně jeden paket. Dalším problémem protokolu PXE byla špatně napsaná specifikace, která obsahovala protichůdné informace a znemožňovala plné využití protokolu jako celku [6].

1.5.2 iSCSI

Protokol iSCSI (Internet Small Computer System Interface) je úprava protokolu SCSI pro přenos dat pomocí protokolu IP. Jedná se o protokol typu klient-server, data se přes síť přenášejí jako sada SCSI příkazů. Na transportní vrstvě je využit protokol TCP, výchozím portem je 3260, iSCSI je možno směrovat.

Server se nazývá *Target* a obsahuje disk sdílený přes protokol iSCSI. Sdíleným diskem může být buď fyzický disk (jednotka) v serveru nebo image soubor. [7, s. 188]

Adresování disku je následující [8] :

iscsi:<nazevserveru>:<protokol>:<port>:<LUN>:<nazevcile>

Pole	Popis
nazevserveru	Název serveru může obsahovat buď platné doménové jméno, nebo IP (IPv4/IPv6) adresu serveru.
protokol	Uvede se buď hodnota 6 (TCP), nebo se pole ponechá prázdné (v tomto případě se použije výchozí hodnota 6).
port	Port, na kterém iSCSI server naslouchá, pokud se neuvede, bude použit výchozí port 3260.
LUN	LUN (Logical Unit Number). Do pole se zapíše číslo logické jednotky ve formě čtyř skupin po čtyřech hexadecimálních znacích (např. 4752-3A4F-6b7e-2F99). Pokud se pole nevyplní, bude použita hodnota 0.
nazevcile	IQN (iSCSI Qualified Name). Do pole se zadá jméno, které unikátně identifikuje iSCSI target. Obvykle se zapisuje ve tvaru (yyyy reprezentuje rok, mm měsíc): <i>iqn.yyyy-mm.preveracene.domenove.jmeno:pojmenovani_uloziste</i>

Tab. 1: Parametry adresování protokolu iSCSI

Klient se nazývá *Initiator*. Pro připojení k iSCSI serveru je potřebný speciální software³, který se musí do starších operačních systémů, např. Windows XP, doinstalovat. V novějších operačních systémech, jako např. Windows 7, je již tento software součástí systému. Po připojení iSCSI jednotky v běžícím operačním systému se tato jednotka tváří,

³ V prostředí Windows se používá Microsoft iSCSI Software Initiator.

jako by byla lokální pevný disk a lze s ní následně pracovat stejně, jako s běžným lokálním pevným diskem.

Postup při zavádění operačního systému (popis pro zavaděč gPXE⁴) [9]:

- Spustí se klientský počítač, BIOS provede POST a načte Boot ROM na síťové kartě
- Řízení se předá Boot ROM na síťové kartě, začne se používat gPXE zavaděč
- Počítač vyšle DHCP broadcast s žádostí o přidělení IP adresy a dalších informací (DHCPDISCOVER)
- DHCP server ve své odpovědi (DHCPOFFER) zašle klientovi informace nutné pro připojení k síti (IP adresa, síťová maska atd.) a informace nutné pro zavedení operačního systému přes iSCSI (IP adresa serveru, protokol, port, LUN, IQN)
- Zavaděč využije přerušení BIOSu 0x13h, namapuje vzdálený iSCSI disk jako lokální jednotku a označí ji jako aktivní spouštěcí oddíl 0x80h, následně předá řízení operačnímu systému. Vzdálená jednotka je operačnímu systému transparentně prezentována jako lokální.
- Operační systém se začne zavádět z lokální jednotky. V první fázi zavádění (reálný mód) používá pro přístup k iSCSI disku přerušení 0x13h, po přechodu do chráněného módu začne používat vlastní ovladače pro přístup k disku.

Informace o iSCSI disku jsou systému předány pomocí iBFT tabulky (iSCSI Boot Firmware Table). Tabulka se musí nacházet v paměti mezi 512K a 1024K a je vyhledána pomocí hlavičky [10].

1.5.3 HTTP

Protokol HTTP (Hypertext Transfer Protocol) nahrazuje při stahování image systému protokol TFTP. Jeho hlavní výhodou je v tom, že pro přenos dat na transportní vrstvě používá protokol TCP. Je tedy možné využít metodu okénka a potvrzovat větší množství doručených dat jako jeden celek, čímž se zefektivňuje využití sítě. V jeden okamžik může

⁴ gPXE je alternativní zavaděč umožňující síťovému adaptéru zavést systém přes protokol iSCSI, viz. 1.4.3.

být na síti větší množství paketů. Další výhodou protokolu HTTP je ta, že je směrovatelný a díky portu 80, který je obvykle povolený na všech firewallech snadno dostupný. Lze jej tedy použít pro zavádění systému i z jiné než lokální sítě [6].

1.6 Způsoby zavádění systému popisované zde

1.6.1 Zavedení systému přes protokol iSCSI

Plná verze Windows je zaváděna pomocí protokolu iSCSI ze sdíleného síťového disku. Vše se děje transparentně a koncový uživatel nepozná rozdíl oproti zavádění Windows z lokálního disku. Celý postup je založen na open-source řešení využívající server postavený na operačním systému Linux. Pro zavádění systému je využit zavaděč gPXE. Tento způsob se zdá být nejvhodnější a je realizován v praktické části práce.

1.6.2 Komerční řešení - program CCBoot

Plná verze Windows je zaváděna protokolem iSCSI. Vše se děje transparentně a koncový uživatel nepozná rozdíl oproti zavádění Windows z lokálního disku. K zavádění systému se využívá komerční program CCBoot, jehož autorem je čínská firma Youngzsoft. Toto řešení využívá stejného principu, jako open-source řešení zmíněné výše. Hlavní rozdíl je v tom, že se jedná o hotové řešení, které umožňuje nastavit server i klienta pomocí pár kliknutí.

1.6.3 Zavedení Windows PE ze sítě

Windows PE je zjednodušená verze Windows, primárně určená pro servisní účely. V praktické části bude popsáno, jak systém zavádět pomocí protokolu PXE, HTTP a iSCSI.

1.6.4 Virtualizace Windows na systému Linux

Nejdříve se ze sítě nabojuje operační systém Linux, následně je na tomto systému virtualizován Windows. Virtuální disk s Windows se nachází na sdílené síťové jednotce. Kapitola obsahuje krátké pojednání o možnosti zavedení Windows tímto způsobem.

1.6.5 Komerční řešení - SANDeploy Boot Server

All-in-one řešení pro zavedení systému Windows pomocí protokolu iSCSI.

2 ZAVÁDĚNÍ SYSTÉMU PŘES PROTOKOL iSCSI

Tato kapitola se zabývá způsobem, jak ze vzdáleného disku, který je připojen protokolem iSCSI, zavést plnou verzi Windows tak, aby koncový uživatel nepoznal rozdíl oproti zavádění z pevného disku lokálního počítače. Zaváděným systémem bude Windows 7 Professional. Na serveru bude použit operační systém Linux a jako zavaděč se využije open-source řešení gPXE. Slovo *Windows* dále v textu se vztahuje na Windows 7.

2.1 Struktura zavádění

2.1.1 Požadavky na server

K zavedení Windows bude potřeba, aby na straně serveru běžely následující služby:

- DHCP a TFTP poskytující základ pro zavedení gPXE přes protokol PXE
- iSCSI zajišťující zpřístupnění disku s Windows přes protokol iSCSI

Všechny služby mohou běžet na jednom fyzickém serveru, ale vhodnější je rozdělit je na 2 fyzické servery. Server, který poskytuje podporu pro PXE a server, který zpřístupňuje disky přes protokol iSCSI. Server poskytující disk s operačním systémem musí být dostatečně výkonný, aby zvládal obsluhovat více klientů současně. Pokud má server dostatek operační paměti, může být image s operačním systémem umístěn v ní. Síťové rozhraní na serveru musí být minimálně 1 Gbit/s.

2.1.2 Požadavky na klienta

Klientský počítač musí být vybaven síťovým adaptérem, který je schopen zavést operační systém přes protokol PXE. Klient musí být dále nastaven tak, aby první zařízení, ze kterého se má operační systém zavádět, byla síť. Síťové rozhraní na klientské stanici musí být minimálně 100 Mbit/s.

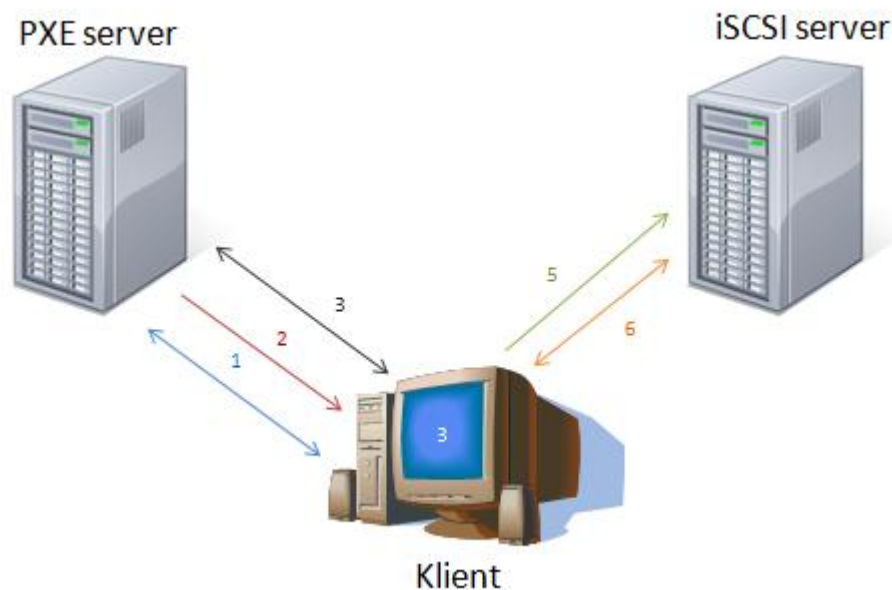
2.1.3 Požadavky na síťové propojení

Z důvodu přenosu velkého množství dat mezi klientem a serverem se doporučuje použít síť s celkovou propustností 1 Gbit/s a vyšší. Vhodné je síť zálohovat pomocí redundantních propojení.

2.1.4 Postup při zavádění operačního systému

Postup při zavádění operačního systému je potom následující:

- 1) Klient se snaží naboťovat přes PXE, od PXE serveru (DHCP) získá IP adresu a potřebné informace vyžadované protokolem PXE, jako NBP je použit obraz s gPXE
- 2) Klient si přes protokol TFTP stáhne zavaděč gPXE, spustí jej a předá mu řízení
- 3) gPXE znovu provede dotaz DHCP, znovu dostane přidělenou IP adresu a další informace, tentokrát se ovšem přenesou informace nutné pro zavedení systému z iSCSI disku
- 4) gPXE dle konfigurace připojí iSCSI disk a označí jej v BIOSu jako primární aktivní oddíl
- 5) Klient začne zavádět operační systém z připojeného iSCSI disku stejně, jako by jej zaváděl z lokálního (SCSI) disku, disk je připojen přímo v BIOSu (pro OS transparentní)
- 6) Operační systém používá pro přístup k disku zpočátku přerušení INT 0x13h, po přechodu do chráněného módu začne pro přístup k iSCSI disku používat vlastní ovladače



Obr. 1: Postup při zavádění operačního systému pomocí protokolu iSCSI

2.2 Problémy při síťovém zavádění Windows

Postup zavádění Windows je dobře popsán v bakalářské práci p. Havránka [11]. Zde budou zmíněny pouze informace týkající se zavádění Windows ze sítě.

2.2.1 Windows při zavádění zapisují na disk

Operační systém Windows při svém bootování z disku nejen čte, ale i na něj zapisuje⁵. Tento fakt je z hlediska zavádění více počítačů současně z jednoho společného síťového disku (image) nepříjemný, protože se nesmí do sdíleného síťového disku zapisovat. Problém lze vyřešit pomocí technologie *Copy-On-Write*, při které jsou data čtena ze sdíleného disku, ale zápisy jsou odkláněny mimo sdílený disk. Toto je možné implementovat buď na straně serveru, kdy jsou zapsaná data jednotlivých pracovních stanic ukládána do speciálních souborů (každá stanice má svůj), nebo na straně klienta, kdy jsou zápisy na pevný disk přesměrovávány do operační paměti daného klienta. Při čtení se nejdříve projdou přesměrovaná data, a pokud se v nich požadovaný soubor nenachází, je načten ze sdíleného disku se systémem.

2.2.2 Windows nepodporují rozdílné hardwarové konfigurace

Pokud je HW konfigurace bootujícího počítače mírně odlišná od počítače, na němž byl Windows nainstalován, např. změna umístění optické mechaniky nebo změna rozlišení monitoru, Windows se s touto změnou vypořádají a operační systém naběhne. Pokud se ovšem změna týká čipové sady, například z *Intel* na *AMD*, s největší pravděpodobností skončí zavádění systému chybou *BSOD*.

Zavádění systému z iSCSI disku je dokonce tak citlivé, že pouhá změna síťového adaptéru, přes který jsou Windows zaváděna, způsobí *BSOD 0x7b*. Tento jev se (u Windows 7) projeví dokonce ve chvíli, kdy jsou v počítači dva síťové adaptéry (hlavní a záložní) a pouze se přehodí síťové kabely mezi těmito adaptéry tak, aby Windows bootovala

⁵ Při startu Windows 7 je z disku čteno přibližně 260 MiB dat a na disk zapsáno okolo 17 MiB dat. Hodnoty jsou pouze orientační a platí pro čistou instalaci Windows 7 Professional x86 a práci s diskem od načtení zavaděče do úspěšného přihlášení do Windows.

přes záložní adaptér [12].⁶ Windows (Windows 7) tedy pojedou pouze na počítači, přes který byla původně na iSCSI disk nainstalována. Z tohoto důvodu je nutné nainstalovat Windows (Windows 7) přímo na iSCSI disk.

2.2.3 Sítově zavedená Windows mohou ohrozit lokální pevný disk pracovní stanice

I v případě, že bude lokální pevný disk skryt před uživatelem, bude stále pro jádro systému přístupný a bude obtížné zaručit, aby na něj Windows v žádném případě nikdy nic nezapsala. Jediné skutečně spolehlivé řešení je fyzické odpojení lokálního pevného disku z pracovní stanice.

2.2.4 Další problémy

Při zavádění Windows jsou data posílána přes výchozí bránu [13]. Je tedy nutné mít sítové zařízení na 3. vrstvě modelu ISO/OSI, které bude data směřovat zpět do sítě, ze které přišla. V případě sítě na UTB to znamená, že veškerá data při zavádění Windows půjdou přes L3 switch v budově U13. Tento jev lze obejít vhodným nastavením DHCP serveru, při němž se při zavádění Windows použije jako výchozí brána IP adresa iSCSI serveru z něž jsou Windows zaváděna a po zavedení se použije IP adresa výchozí brány v dané VLAN.

Dalším problémem je automatická změna názvu počítače tak, aby měl každý počítač po zavedení unikátní NetBIOS jméno.

Windows je dále nutno upravit tak, aby zbytečně nepřístupoval na (sítový) pevný disk. Z tohoto důvodu je nutno zakázat služby jako *Defragmentace disku*, *Superfetch*, *Windows Defender*, *Windows Search*, *Windows Update*, *Windows Zálohování*, případně i *Plánovač úloh* a *Protokol událostí systému Windows*. Tento výčet není úplný ani závazný, slouží pouze jako návrh.

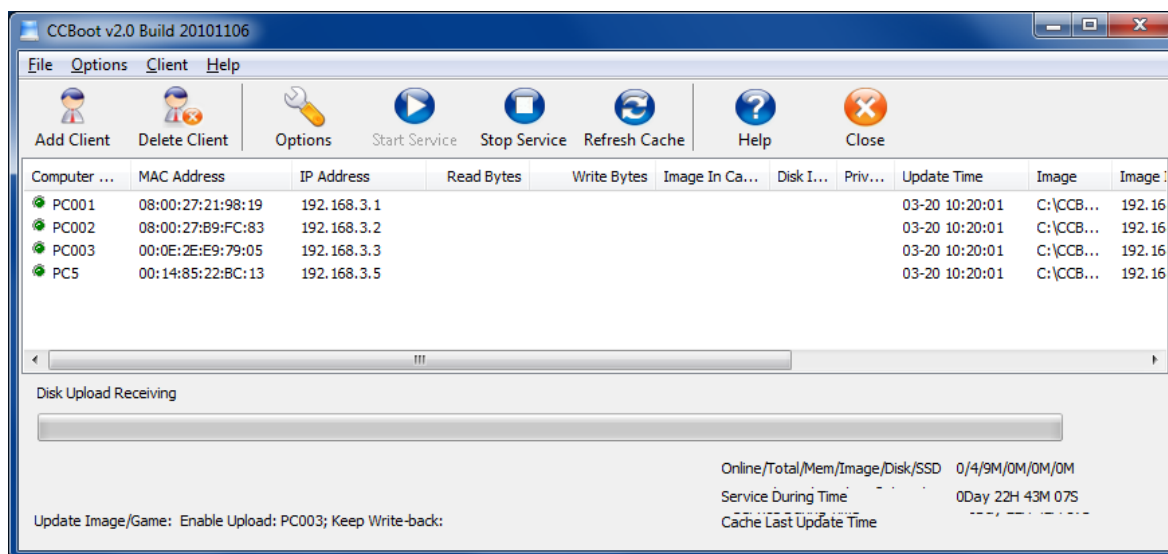
⁶ Tento problém by mělo být možno odstranit pomocí nástroje BindView, který je součástí sady WDK (Windows Developer Kit).

3 KOMERČNÍ ŘEŠENÍ - PROGRAM CCBOOT

Program CCBoot je komerční řešení čínské společnosti Youngzsoft umožňující bezdiskové bootování Windows na lokálních stanicích. Řešení se skládá ze dvou částí, programu, který tvoří serverovou část, a aplikace, která se instaluje na klienta a umožňuje vylepšenou komunikaci klienta se serverem. Samotný princip zavádění OS je naprosto shodný s kapitolou 2 - Zavádění systému přes protokol iSCSI. V době psaní této práce byla k dispozici verze 2.0 Build 20101106 a tudíž se následující popis bude vztahovat na ni.

3.1 Popis programu

Program CCBoot lze stáhnout ze stránek společnosti Youngzsoft [14]. Jedná se o jednoduchou okenní aplikaci, kde se dá vše potřebné nastavit na pár kliknutí. Hlavní částí aplikace je serverová část, kterou je možno nainstalovat na počítač s operačním systémem MS Windows 2000 / XP / Server 2003 / Vista / 7 / Server 2008.



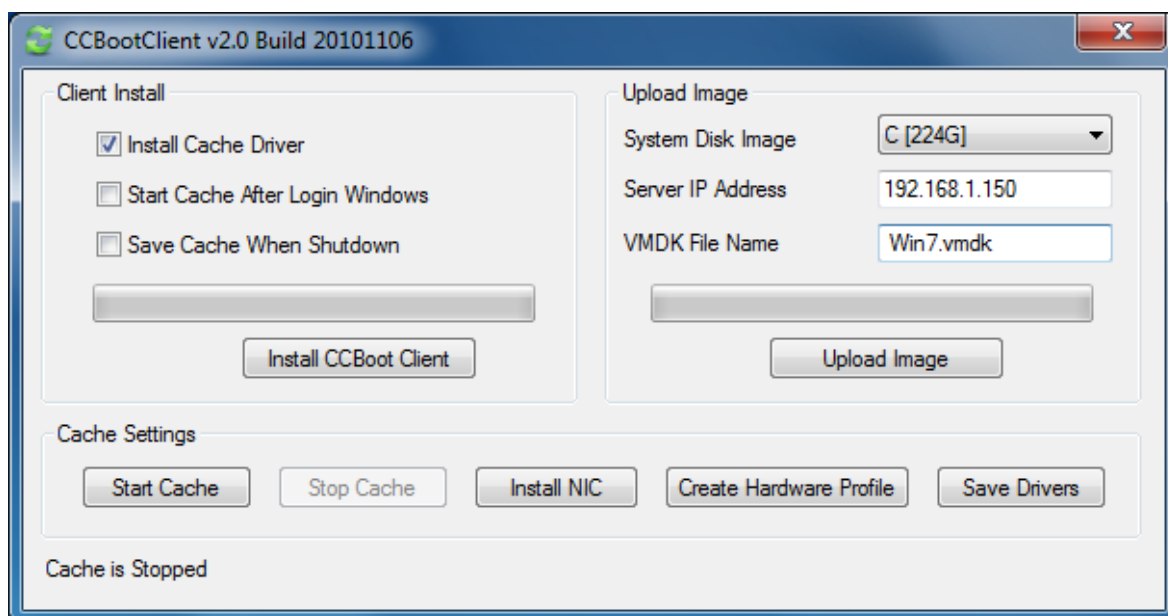
Obr. 2: Okno aplikace CCBoot - serverová část

Jádro programu běží na serveru jako služba "CCBoot". Různá nastavení lze provést pomocí aplikace CCBoot. V nabídce "File" se nacházejí položky pro spuštění / pozastavení / zastavení služby. Nabídka "Options" obsahuje položku "Settings" pomocí které je možno specifikovat globální nastavení společné pro všechny klientské počítače.

V nabídce "*Client*" se nacházejí položky pro práci s klienty jako přidání / odebrání / editace / probuzení po LAN a podobně. Poslední nabídka vpravo, "*Help*" nabízí možnost zobrazit nápovědu a registraci programu.

Nápověda programu je ve formátu PDF a obsahuje podrobnou dokumentaci jednotlivých kroků a nastavení potřebných pro zprovoznění zavádění jednotlivých verzí systému Windows.

Pro spolupráci klienta se serverem je potřeba do zaváděného image systému nainstalovat klientský program CCBoot a provést základní nastavení týkající se vyrovnávací paměti pro ukládání zapisovaných dat.



Obr. 3: Okno aplikace CCBoot - klientská část

Klientský program nainstaluje do systému potřebné ovladače a umožní následné zavedení systému ze serveru.

3.2 Vlastnosti řešení

3.2.1 Výhody řešení

Bootování pracovních stanic pomocí programu CCBoot s sebou přináší spoustu výhod. Mezi hlavní patří [15]:

- Jednoduché a intuitivní ovládání, v jednom programu je zahrnut DHCP, TFTP i iSCSI server.
- Možnost instalovat OS přímo na server, instalovat OS na jednoho klienta a potom jej přesunout na server, možnost instalovat OS ve virtuálním stroji (vmdk disk) a potom jej na serveru připojit.
- Z jednoho image na serveru startuje více počítačů současně, využívá se technologie copy-on-write, při které se data čtou ze společného image, ale zápisy jsou odklány jinam.
- Zápisy na disk (na straně klienta) jsou udržovány v operační paměti lokálního počítače, pokud je vymezený prostor v RAM zaplněn, jsou posílány přes síť na server. Na straně serveru se přijatá data ukládají nejdříve do RAM, pokud je vymezené místo v RAM zaplněno, data jsou ukládána na pevný disk serveru.
- Každý klient je identifikován svou MAC adresou a může mít svoje vlastní nastavení nezávisle na jiném klientovi.
- Po restartu počítače může daný klient (dle jeho nastavení) načíst buď čistý image se systémem (bez uložených změn, které udělal před restartem), nebo může načíst systém ve stavu, v jakém jej před restartem zanechal.
- Podpora různých hardwarových profilů, každý klient může mít svůj vlastní HW profil nezávisle na jiném klientovi.
- Image s operačním systémem je automaticky upraven klientskou částí aplikace CCBoot, nejsou tedy potřeba žádné manuální nastavení operačního systému.
- Možnost redundance a rozdělení zátěže. CCBoot server může současně běžet na více fyzických strojích a každý bootující počítač může mít nastaven hlavní server a záložní server.

3.2.2 Nevýhody řešení

Ačkoliv se program CCBoot může zdát jako ideální řešení, obsahuje i několik nevýhod:

- Cena. Za každý připojený počítač je nutno zaplatit licenční poplatek ve výši \$10. Jistým zmírňujícím prostředkem zde může být to, že je nutno nakoupit pouze tolik licencí, kolik bude současně spouštěno počítačů v daném okamžiku. Na počítače, které tímto způsobem nebudou bootovat, není nutno kupovat licenci. [16]
- Server musí být neustále připojen k internetu. Každé 4 hodiny je ověřována licence programu. Pokud se nepodaří spojit se domácím aktivačním serverem, začne běžet lhůta 12 hodin, po které přestane server fungovat.
- Částečná nefunkčnost (viz. 3.5 Praktické zkušenosti s programem CCBoot).

3.3 Popis a nastavení serveru

Jednotlivé kroky se liší v závislosti na operačním systému, který je zaváděn. Z důvodu, že se při praktickém testování programu nepodařilo Windows zavést (viz. 3.2.2) a z důvodu, že jsou již všechny nutné informace uvedeny v příloženém PDF k programu (a nemá smysl je doslova opisovat), budou zde popsány pouze základní principy nastavení serveru. Pro podrobné informace prosím zkonzultujte dokumentaci v PDF.

3.3.1 Instalace serveru

Z webu výrobce [17] se stáhne soubor "*CCBoot v2.0 Build 20101106*" a nainstaluje se na server. Po úspěšné instalaci a spuštění programu se objeví okno CCBoot (*Obr. 2*). Nyní se provede nastavení pro zavádění konkrétní verze Windows.

3.3.2 Popis základního nastavení

Základní nastavení serveru lze provést kliknutím na ikonu "**Options**" v hlavním okně programu. Objeví se dialog s pásem karet.

Karta **DHCP Settings**:

Na této kartě se nastavuje DHCP server.

- Musí být zaškrtnuty volby "**Start DHCP**" a "**Start TFTP**".
- "**DHCP Server IP**" obsahuje IP adresu, kterou má tento server.
- Pomocí "**IP Allocated Start**" a IP "**Allocated End**" lze nastavit rozsah adres přidělovaný klientům.
- Nastavení hodnot, které budou přes DHCP předány klientovi: síťová maska ("**IP Mask**"), výchozí brána ("**IP Gateway**") a adresa DNS serveru ("**DNS Address**").

DHCP Settings Client Default Settings Server Cache Settings Other Settings

Start DHCP Start TFTP

DHCP Server IP 192.168.1.150

IP Allocated Start 192.168.3.1

IP Allocated End 192.168.3.50

IP Mask 255.255.0.0

IP Gateway 192.168.1.254

DNS Address 1 8.8.8.8

DNS Address 2 8.8.4.4

Scan DHCP

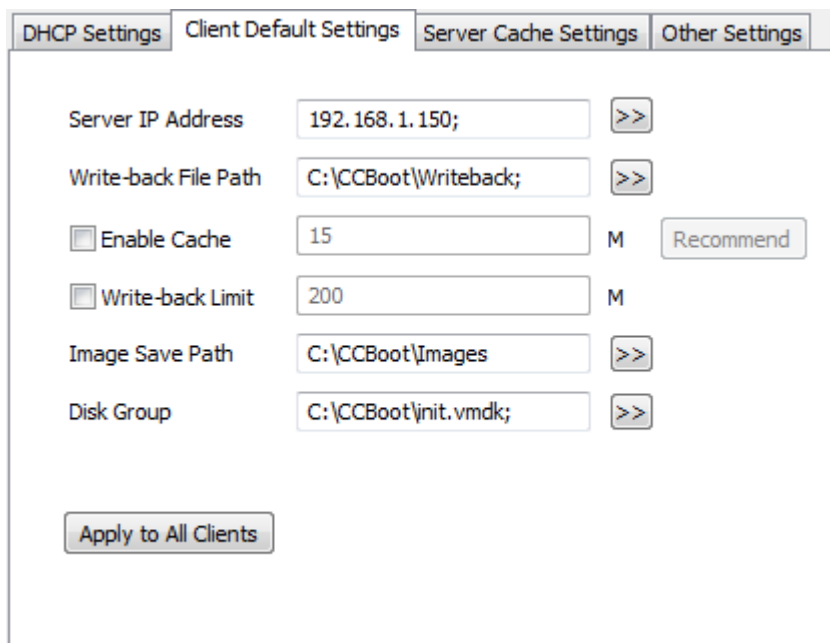
Obr. 4: Nastavení DHCP v programu CCBoot

Karta **Client Default Settings**:

Hodnoty zde nastavené slouží jako výchozí hodnoty pro nově vytvořeného klienta. Dané hodnoty lze později upravit u každého klienta zvlášť.

- Volba "**Server IP Address**" obsahuje adresu serveru, ze kterého bude zaváděn operační systém. Při vyplnění více adres se provede pokus zavedení systému z první vyplněné adresy, a pokud pokus selže, provede se pokus o zavedení systému z dalších vyplněných adres.
- Ve "**Write-back File path**" se volí umístění, do kterého se budou ukládat data, která byla při pokusu klienta zapsat je na disk přeměrována zpět na server.
- Volbou "**Enable Cache**" lze povolit nebo zakázat vyrovnávací paměť v RAM nabootovaného počítače. Tato paměť slouží jako dočasné úložiště pro data, která se klient snažil zapsat na pevný disk.
- Volba "**Write-back Limit**" umožňuje nastavit limit pro množství uložených dat, která byla při pokusu klienta zapsat na pevný disk přeměrována na server.

- "**Image Save Path**" obsahuje cestu pro ukládání obrazů operačních systémů, do tohoto umístění se ukládají uploadnuté image Windows XP/2003 a obrazy systémů instalovaných přímo na server (Windows Vista/7/Server 2008).
- V "**Disk Group**" je cesta k bootovatelnému image se systémem.



Obr. 5: CCBboot - volba výchozího nastavení pro klienty

Karta **Server Cache Settings**:

Zde se nastavují hodnoty týkající se vyrovnávací paměti serveru. Vyrovnávací paměť je uložena v RAM.

- Zaškrtnutí volby "**Enable Cache**" povolí používání operační paměti serveru jako vyrovnávací paměť.
- Volba "**Enable Huge Memory Access**" umožňuje používat více jak 2 GiB operační paměti.
- Hodnota v "**System Image Read Cache**" určuje, kolik MiB z image se systémem může být uloženo ve vyrovnávací paměti.
- Hodnota v "**Game Disk Read Cache**" udává, kolik MiB s připojeného Game disku může být uloženo ve vyrovnávací paměti. Game disk je fyzický disk na serveru, který je namapován jako druhý (nesystémový) disk v nabootevaném klientském počítači.

Pro Game disk platí stejná pravidla jako pro zaváděný image - zápisy na disk jsou odklány a pouze jeden vybraný klient (tzv. Super Client) může na disk zapisovat přímo.

- Hodnota v "**Clients Write-back Cache**" udává, jaké množství z dat, která byla přeměrována na server v důsledku pokusu klienta zapsat data na lokální disk, bude uloženo v RAM serveru. Po dosažení této hodnoty se data ukládají na disk serveru do adresáře, který je specifikován "*Write-back File Path*".
- "**Enable SSD Cache**" umožní používat SSD disk jako vyrovnávací paměť. Tato volba je vhodná, pokud je v serveru instalován SSD disk. Tento disk potom slouží jako prostředník mezi vyrovnávací pamětí v RAM a vyrovnávací pamětí na pevném disku.
- Volby "**Auto Update Cache**" a "**Update Cache Time**" slouží pro Game disk. Tyto hodnoty určují, zda se má cache Game disku po změně souborů na něm ihned aktualizovat nebo zda se má aktualizovat až po určité době v sekundách od posledního zápisu na disk.

The screenshot shows the 'Server Cache Settings' window in CCBoot. It features four tabs: 'DHCP Settings', 'Client Default Settings', 'Server Cache Settings' (which is active), and 'Other Settings'. The active tab contains the following settings:

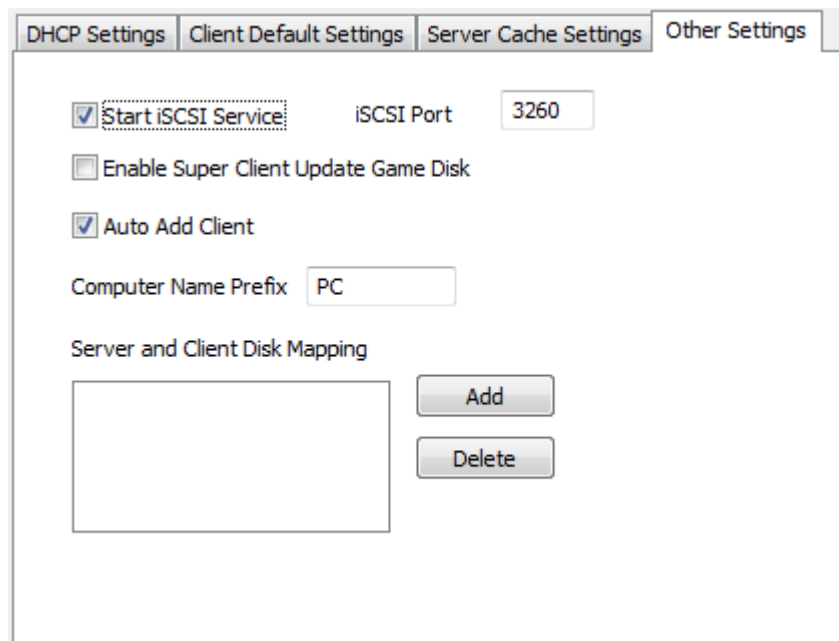
- Enable Cache**
- Enable Huge Memory Access**
- Available Physical Memory: 1242 M (with a 'Recommend' button)
- System Image Read Cache: 10 M
- Game Disk Read Cache: 10 M
- Clients Write-back Cache: 0 M
- Enable SSD Cache** (with an 'SSD Cache' button)
- SSD Path: [empty text box]
- SSD Size: 0 M
- Auto Update Cache**
- Update Cache Time**: [empty text box]

Obr. 6: CCBoot - nastavení vyrovnávací paměti serveru

Karta Other Settings:

Umožňuje nastavit zbývající volby.

- **"Start iSCSI Service"** spustí iSCSI službu, **"iSCSI Port"** obsahuje port, na kterém služba běží (výchozí hodnota pro iSCSI je 3260).
- **"Enable Super Client Update Game Disk"** umožní, aby mohl některý z klientů přímo ukládat na Game disk.
- **"Auto Add Client"** automaticky přidá počítač, který získal adresu z nastaveného DHCP serveru, jako klienta a přiřadí mu výchozí hodnoty nastavené v *"Client Default Settings"*.
- **"Server and Client Disk Mapping"** umožňuje nastavit přiřazení místního disku na serveru k disku, který má naboatovaný klient připojený jako druhý disk (písmena jednotek).



Obr. 7: CCBoot - ostatní globální nastavení

3.3.3 Přidání nového klienta

Nový klient je do seznamu klientů (hlavní okno programu) přidán buď automaticky, jakmile se daný klient (identifikován MAC adresou) pokusí poprvé získat údaje z DHCP serveru (pokud je v "*Other Settings*" zaškrtnuta položka "*Auto Add Client*"), nebo může být přidán manuálně.

Pokud byl klient přidán automaticky, vytvořilo se spojení MAC adresa - dynamicky přidělená IP adresa a daný počítač se objevil v seznamu klientů. Tento počítač má nyní zděděná nastavení z "*Client Default Settings*". Nastavení vlastností daného klienta lze provést poklepnutím na položku daného klienta v seznamu klientů.

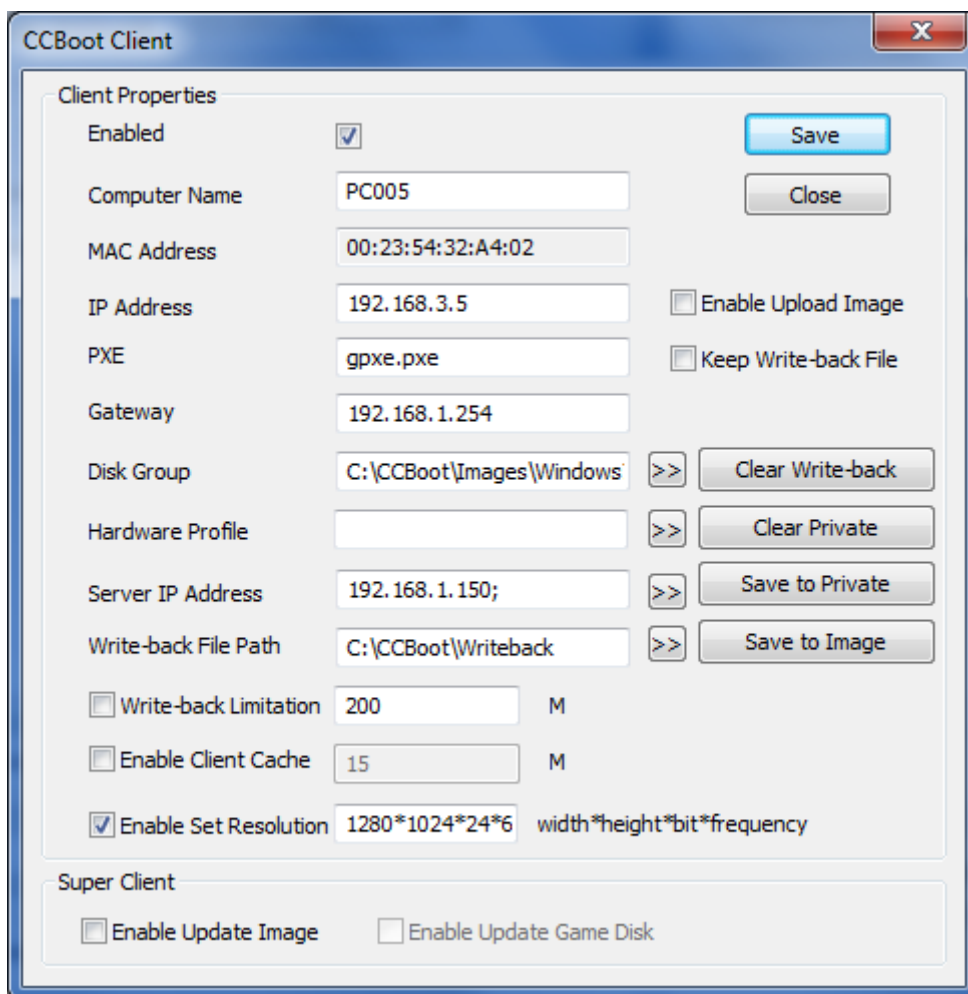
Manuální přidání klienta lze provést kliknutím na ikonu "*Add Client*" v hlavním okně programu. Otevře se dialog, ve kterém lze nastavit vlastnosti pro daného klienta.

Popis vlastností daného klienta:

- Volba "**Enabled**" určuje, zda má daný klient bootování povoleno nebo zakázáno.
- Položka "**Computer Name**" obsahuje název, pod kterým bude daný klient zobrazen v seznamu klientů.
- Položka "**MAC Address**" obsahuje MAC adresu daného klienta. Tato hodnota je buď vyplněna automaticky (pokud byl klient přidán automaticky) nebo může být vyplněna manuálně. Při manuálním vyplňování lze nastavit, že pokud se později připojí klient s danou MAC adresou, budou mu automaticky přiřazeny zde manuálně předvyplněné vlastnosti a nebudou na něj aplikována nastavení z "*Client Default Settings*".
- V položce "**IP Address**" je nutno vyplnit IP adresu klienta. Pokud byl klient přidán automaticky, je tato adresa předvyplněna na adresu, která byla klientovi přidělena serverem DHCP.
- Položka "**PXE**" určuje obraz zavedený protokolem PXE. Ve výchozím nastavení je to "*gpxe.pxe*".
- "**Gateway**" určuje výchozí bránu předávanou klientovi.
- V "**Disk Group**" je možno vybrat obraz se systémem a Game disk.

- V položce "**Hardware Profile**" je možno vybrat hardwarový profil daného počítače. HW profil je nutno nejdříve vytvořit na daném klientovi.
- Položka "**Server IP Address**" obsahuje IP adresu serveru, ze kterého se bude zavádět systém.
- Položka "**Write-back File Path**" určuje adresář na disku serveru pro ukládání přesměrovaných zápisů klienta. Zde je možno nastavit specifickou cestu pro daného konkrétního klienta.
- Hodnota v "**Write-back Limitation**" určuje omezení ukládaných dat na server pro daného klienta. Doporučuje se žádné omezení nezapínat.
- Volba "**Enable Client Cache**" zapíná vyrovnávací paměť pro odkloněné zápisy v RAM nabootovaného počítače.
- Volba "**Enable Set Resolution**" umožňuje nastavit rozlišení obrazovky daného klienta.
- Volby v části "**Super Client**": "**Enable Update Image**" umožňuje klientovi přímo modifikovat image, ze kterého nabootoval. Zápisy jsou místo odklání směřovány přímo do systémového image. Tato volba slouží k úpravě image se systémem z jednoho vybraného počítače. Volba "**Enable Update Game Disk**" je k dispozici po zaškrtnutí volby "*Enable Super Client Update Game disk*" v "*Other Settings*" a umožňuje, aby daný klient mohl přímo zapisovat na sdílený serverový disk.
- Volba "**Enable Upload Image**" v hlavním okně dialogu (pod tlačítky) slouží pro povolení/zakázání uploadu image disku přes CCBoot klientskou aplikaci, která je nainstalována na pevném disku referenčního počítače. Takto se dá na server nahrát image disku z již existujícího počítače.
- Volba "**Keep Write-back File**" umožní, aby měl klient po restartu svoje uložená data. Pokud není zaškrtnuto, data klienta jsou při jeho restartu automaticky smazána a klient nabíhá z čistého image.
- Tlačítko "**Clear Write-back**" manuálně smaže data, která si klient uložil (přesměrované zápisy na lokální disk).

- Tlačítko "**Save to Private**" uloží momentální stav disku klienta v daném okamžiku při stisknutí (ovládáno ze serveru). Po restartu bude stav klienta obnoven do původního stavu nezávisle na existenci Write-back souboru.
- Tlačítko "**Clear Private**" smaže data uložená tlačítkem "*Save to Private*".
- Tlačítko "**Save to Image**" uloží data, která klient zapsat do "Write-back" souboru do hlavního image se systémem, ze kterého klient bootuje. Aby byla data dostupná, musí být zaškrtnutá položka "*Keep Write-back File*".



Obr. 8: CBoot - nastavení jednoho daného klienta

3.4 Popis klientské aplikace

Z důvodu využití možnosti ukládání zápisů směřovaných na lokální pevný disk do RAM lokálního počítače musí být v image klientského počítače nainstalována aplikace CCBoot Client. Tato aplikace lze stáhnout z webu výrobce [17].

3.4.1 Instalace aplikace CCBoot Client

Po stažení, instalaci a spuštění aplikace *CCBoot Client* (CCBootClient v2.0 Build 20101106) na referenční počítač se objeví okno s možnostmi (*Obr. 3*).

3.4.2 Popis základního nastavení

Nyní se musí provést volby týkající se cache. Po nastavení cache bude počítač restartován a následně mohou být provedeny další úkony.

Nastavení cache:

- Volba "**Install Cache Driver**" nainstaluje ovladač vyrovnávací paměti. Tato volba musí být aktivována, jinak vyrovnávací paměť v RAM lokálního počítače nebude fungovat.
- Pokud je volba "**Start Cache After Login Windows**" zaškrtnuta, bude vyrovnávací paměť spuštěna až po přihlášení do systému Windows. Nezaškrtnutá volba znamená spuštění vyrovnávací paměti již v raném stádiu zavádění, což sníží objem přenášených dat po síti, ale na některých systémech může vyvolat BSOD.
- Volba "**Save Cache When Shutdown**" zajistí, aby se při vypnutí počítače uložil obsah lokální cache na server.
- Tlačítkem "**Install CCBoot Client**" se provedou nastavení týkající se cache a objeví se volba "*Do you want to install NIC drivers ?*". Při volbě "Yes" se zobrazí výběr ovladačů různých síťových adaptérů. Zde je možno vybrat, jaké ovladače do systému zahrnout. Tato volba je vhodná pro případ, kdy se bude výsledný image bootovat na počítačích s různými síťovými adaptéry. Následuje restart systému.

V tomto bodě je základní nastavení hotovo a image se systémem se může začít používat.

3.4.3 Upload image disku lokálního počítače na server

Pokud byl předchozí krok proveden na počítači, který byl naboťován z lokálního pevného disku, je potřeba daný systém přesunout na CCBoot server. CCBoot klient automaticky udělá image lokálního disku ve formátu *vmdk* a nahraje jej na CCBoot server.

Na CCBoot serveru musí být u daného klienta zaškrtnuta volba "*Enable Upload Image*".

Po restartu referenčního počítače je potřeba znovu spustit aplikaci CCBoot Client a provést následující nastavení:

- Vybrat v "**System Disk Image**" lokální pevný disk, který obsahuje instalaci Windows.
- Nastavit IP adresu CCBoot serveru ("**Server IP Address**").
- Zvolit název souboru, pod kterým bude image disku na serveru uložen ("**VMDK File Name**").
- Kliknout na tlačítko "**Upload Image**" a počkat, než se image uloží na server.
- Po nahrání image na server na serveru u daného klienta odškrtnout volbu "*Enable Upload Image*".

Nyní je obraz disku s Windows uložen na serveru a může být využit pro bootování bezdiskových stanic.

3.4.4 Další volby klientské aplikace

- Tlačítkem "**Start Cache**" se manuálně spustí lokální cache.
- Tlačítkem "**Install NIC**" je možné nainstalovat ovladače pro různé síťové karty.
- Tlačítko "**Create Hardware Profile**" spustí dialog pro vytvoření HW profilu. Tato možnost je vhodná, pokud bude stejný image používán na více rozdílných HW konfiguracích. Různé HW konfigurace (pokud byly vytvořeny) jsou uloženy přímo v image se systémem a na základě volby v nastavení daného klienta se některá z konfigurací použije. Vytvářený HW profil se musí uložit do image na serveru. Pokud je HW profil vytvářen na počítači naboťovaném ze sítě, musí být v nastavení daného klienta zaškrtnuta volba "*Enable Update Image*", případně před startem klienta zaškrtnutá volba "*Keep Write-back File*" a po vypnutí klienta tato volba odškrtnuta

a stisknuto tlačítko "*Save to Image*". Pokud je HW profil vytvářen na počítači nabootevaném z pevného disku, musí se obraz disku znovu nahrát na server.

Je možné, že bude nutné nainstalovat určité ovladače pouze na klienty, kteří používají určitý hardwarový profil. V tomto případě je nutno klienta spustit ze sítě (v nastavení klienta na serveru použít daný HW profil) a následně do nabootevaného systému nainstalovat dané ovladače. Po instalaci restartovat počítač, spustit aplikaci *CCBoot Client* a kliknout na tlačítko "**Save Drivers**". Změny musí být uloženy do image se systémem na serveru.

3.5 Praktické zkušenosti s programem CCBoot

Při testování v domácích podmínkách se ukázalo, že většina výhod, které tento program nabízí, nefunguje tak, jak by měla. Například se pomocí přiloženého návodu nepodařilo rozběhnout Windows XP tak, aby nepadal (opakovaná BSOD před přihlášením nebo po přihlášení), rovněž se objevily problémy s přesunem image disku z lokálního počítače na server.

Při použití doporučeného postupu se Windows 7 vůbec nepodařilo na server nainstalovat (při instalaci se objevila hláška, že BIOS počítače nepodporuje bootování z daného disku, viz. *Obr. 12: Chyba při instalaci Windows na iSCSI disk* na straně 62). Největšího úspěchu bylo dosaženo při instalaci přes NIC *Intel PRO/1000 GT* s přeflashovanou Boot ROM z originální na *gPXE 1.0.0*, v tomto případě se Windows nainstalovala na iSCSI disk, ale zavaděč zapsala na disk lokální.

Při snaze nainstalovat Windows 7 ve virtuálním prostředí a následném připojení "*vmdk*" disku na server byla nutná manuální úprava registru, v tomto případě Windows sice naběhla, ale pouze ve virtuálním počítači (na fyzickém byla BSOD 0x7b) a při startu strávila dlouhou dobu čekáním v nečinnosti, než se dostala k přihlášení.

CCBoot server rovněž vykazoval určitou nestabilitu, služba občas samovolně přestala fungovat (obvykle po neúspěšném bootování klientského počítače) a jediný způsob, jak ji zprovoznit bylo fyzické restartování celého serveru (jiný způsob při testování nefungoval). Z tohoto důvodu se program CCBoot (verze 2.0 Build 20101106) jeví spíše jako nefunkční řešení, které má do ideálního řešení hodně daleko. V každém případě je možné, že se

uvedené problémy vyskytovaly pouze v důsledku použité testovací konfigurace a při jiné konfiguraci serveru, lokální síti a jiné hardwarové konfiguraci bootujícího počítače by vše proběhlo podle inzerovaných výhod. Toto se bohužel nepodařilo potvrdit.

4 WINDOWS PE

Windows PE (Preinstall Environment) je speciální verze Windows, vyznačující se schopností naboootovat z mnoha různých typů médií. Tento systém byl primárně určen jako náhrada systému MS-DOS, který se používal jako základ pro běh první fáze instalačního procesu při instalaci plnohodnotného Windows na pevný disk. Snahou bylo vytvořit operační systém, který bez nutnosti instalace na pevný disk poskytne nezbytné minimum rozhraní Win32 API a podpory pro 32-bitové ovladače tak, aby v něm mohla běžet instalace Windows. Kromě oficiálních Windows PE existují také neoficiální edice, které částečně odstraňují nedostatky, jimiž oficiální vydání trpí. [18, s. 273]

4.1 Základní vlastnosti

Následující popis se týká oficiálních Windows PE, která jsou vydána společností Microsoft.

4.1.1 Možnosti zavedení

Windows PE se vyznačují vestavěnou podporou sítě a schopností naboootovat téměř z jakéhokoliv typu média. V poslední verzi (3.0) jsou podporovány tyto možnosti:

- Pevný disk
- CD/DVD
- USB flash disk
- PXE server
- WDS⁷

Celková velikost Windows PE je dle verze, nainstalovaných komponent a přidávaných programů v rozmezí 120 – 700 MiB, což ji činí oproti plné verzi Windows vhodným

⁷ Windows Deployment Services je technologie společnosti Microsoft určená pro instalaci operačního systému Windows přes síť. Při použití této technologie probíhá instalace Windows na koncové počítače z centrálního prvku v síti a odpadá nutnost používat CD/DVD media. WDS je zahrnuta jako jedna z rolí ve Windows Server 2008, lze ji rovněž sehnat jako instalační balíček pro Windows Server 2003 SP2.

kandidátem na zavedení ze sítě. Windows PE jsou od začátku navržena jako read-only, což znamená, že ze zdrojového disku pouze čtou. Všechny zápisy na pevný disk jsou buď zahozeny, nebo virtualizovány. Naopak plná verze Windows při startu i provozu neustále čte a zapisuje, což bez dodatečných řešení na straně serveru přímo vylučuje možnost zavedení ze sítě.

4.1.2 Nevýhody a problémy

Ačkoliv se Windows PE jeví jako vhodný kandidát pro zavádění ze sítě, ze své podstaty minimalistického OS plynou mnohá omezení, jež komplikují využití Windows PE jako plnohodnotného operačního systému. Jako největší nedostatek pro nasazení v jakékoliv síti se jeví schopnost provozu pouze s jedním uživatelským účtem. Uživatel je ihned po startu počítače přihlášen pod účtem *SYSTEM* a rovněž všechny akce i spuštěné procesy jsou prováděny s právy uživatele *SYSTEM*⁸. V případě, že jsou Windows PE spuštěna na počítači, kde je již systém Windows lokálně instalován, mohou ohrozit již nainstalovaný systém, protože neberou ohled⁹ na přístupová práva k souborům lokálně instalovaného systému. Jakýkoliv spuštěný program nebo akce uživatele v prostředí Windows PE může ohrozit již nainstalovaný systém na pevném disku, což v konečném důsledku může vážně narušit bezpečnost celého síťového prostředí.

Mezi další nevýhody patří absence *Exploreru* jako desktopového prostředí. Jako výchozí shell¹⁰ je nastaven *Cmd*¹¹. Po úspěšném startu a automatickém přihlášení se před uživatelem objeví příkazový řádek, pomocí nějž lze ovládat operační systém, případně spouštět další programy. Ovládání operačního systému se tedy spíše podobá používání *MS-DOSu*, případně terminálu v Linuxu. Běžně používaný shell, *Explorer*, není

⁸ "Uživatel" *SYSTEM* má větší oprávnění než uživatelský účet Administrátor.

⁹ "Uživatel" *SYSTEM* má ve výchozím nastavení přístup úplně ke všem souborům a složkám na pevném disku.

¹⁰ Shell je označení programu, který vytváří v počítači rozhraní pro uživatele.

¹¹ *Cmd.exe* je shell v operačním systému Microsoft Windows poskytující v tomto systému rozhraní příkazového řádku.

ve Windows PE oficiálně podporován, takže jediná možnost je použít buď jiný shell podobný Exploreru, nebo Explorer do Windows PE dostat neoficiálně. V obou případech se jedná o velmi špatně dokumentované a zdlouhavé postupy.

Windows PE rovněž nepodporuje rozhraní *DirectX* a zvuk. Instalace programů je možná pouze manuálně v offline¹² režimu nakopírováním souborů daného programu do daného umístění a manuální úpravou registru Windows. Toto je velmi pracné a prakticky použitelné pouze pro velmi jednoduché programy. Velmi vhodné se zde jeví použití přenosných verzí¹³ programů, které se nemusí instalovat. Daný program stačí zkopírovat na lokální disk a spustit. Není potřeba předchozí instalace.

Z důvodu, že Windows PE obsahuje pouze podmnožinu celkového Win32 API, není zajištěno, že je schopen spustit úplně všechny programy. Drobný problém může činit rovněž fakt, že se samovolně restartuje po uplynutí určité doby. Tato doba záleží na konkrétní verzi a slouží jako vestavěná ochrana proti používání Windows PE jako hlavního operačního systému.

4.2 Druhy Windows PE

4.2.1 Oficiální vydání

Za oficiálním vydáním Windows PE stojí společnost Microsoft, která stejně jako pro hlavní Windows poskytuje i u tohoto produktu technickou podporu. Windows PE existuje v několika verzích, které se z pohledu běžného uživatele a omezení v používání (viz. 4.1.2. Nevýhody a problémy) příliš neliší. Ve všech verzích platí omezení na uživatele SYSTEM, shell v podobě příkazové řádky, instalaci programů a podobně. Rozdíl v jednotlivých verzích se nachází spíše uvnitř v systému, což je důsledek toho, že je každá verze postavena na jiné verzi plného systému Windows.

Verze 1.x je postavena na jádru Windows XP/2003. Tato verze nebyla určena pro širokou veřejnost, oficiálně šla sehnat pouze přes smlouvu *Software Assurance*, kterou měly

¹² Úprava daného neběžícího operačního systému z jiného běžícího operačního systému.

¹³ Programy, jež lze přímo spustit bez potřeby předchozí instalace lze nalézt např. zde [32].

uzavřenu pouze střední a větší společnosti. Pro bootování ze sítě šlo oficiálně použít pouze PXE In-RAM řešení, kdy se celý ISO obraz systému stáhl do operační paměti a teprve z ní se zavedl operační systém.

S příchodem Windows Vista se na trhu objevila **verze 2.0**, tato verze přinesla zásadní změnu v uložení obrazu systému, kdy se místo ISO obrazu, jež je založený na sektorech začal používat formát *WIM*. Formát WIM (Windows Imaging Format) byl původně vyvinut za účelem změny hlavního instalačního procesu Windows pro Windows Vista. Jedná se o image celého systému, který je založen na souborech. Jako hlavní výhoda tohoto řešení se jeví možnost lepší komprimace dat a uložení vícenásobně používaného souboru pouze jednou, což v konečném důsledku zmenší velikost výsledného image a umožní efektivnější uložení dat na instalační médium. Bootovací proces je založen na PXE. Nejdříve se ze serveru protokolem TFTP stáhne zavaděč systému, který se spustí. Následně si Windows stáhne *BCD* záznam a soubory "*boot.sdi*" a "*boot.wim*", které uloží do RAM. Spojením těchto 2 souborů se vytvoří virtuální systém souborů, z nějž následně Windows naboootuje.

[19]

Poslední vydanou verzí je **3.0**, jež je založená na jádru Windows 7. Tato, kromě drobných změn při vytváření image systému, nepřináší z hlediska bootování systému žádné převratné změny. Verze 2.0 a 3.0 lze vytvořit pomocí balíků *Windows AIK*¹⁴ nebo *Windows OPK*¹⁵, které lze stáhnout ze stránek společnosti Microsoft.

4.2.2 Neoficiální vydání

V důsledku omezení a nedostupnosti oficiálních Windows PE pro běžné uživatele (týká se verze 1.x) vzniklo několik neoficiálních verzí, které si kladly za cíl odstranit některá

¹⁴ Windows Automated Installation Kit je balík nástrojů, který umožňuje upravit instalaci Windows a zjednodušuje nasazení Windows v podnikové sféře.

¹⁵ Windows OEM Preinstallation Kit je sada nástrojů sloužící pro usnadnění předinstalace Windows určená pro výrobce počítačů.

omezení a umožnit používání Windows PE i běžným lidem (bez speciální smlouvy). Ačkoliv mají tyto systémy v názvu *PE* a lze u nich aplikovat podobný princip zavedení ze sítě jako u oficiálních Windows PE, jsou postaveny od začátku nezávisle na oficiálním vydání a tvoří úplně vlastní větev spravovanou nadšenci mimo Microsoft.

Mezi nejznámější odnože patří **BartPE** založené na Windows XP/2003. K vytvoření image s BartPE lze použít freewarový nástroj *PE Builder* vytvořený Bartem Lagerweijem a instalační médium Windows XP/2003. Nejvýraznější změna v BartPE oproti Windows PE 1.x je grafické rozhraní používající *Nu2Menu*, případně *XPE* a možnost snadného rozšíření pomocí předpřipravených pluginů. Více informací o přípravě BartPE lze nalézt v práci p. Havránka [11].

Konkurencí k Windows PE 2.0 je **VistaPE**, která existuje jako jeden z projektů v rámci programu *WinBuilder*. K vytvoření image je zapotřebí nástroj WinBuilder, Windows AIK a instalační médium Windows Vista. Po dokončení průvodce je hotová adresářová struktura, kterou můžeme využít pro bootování ze sítě. Grafické rozhraní se velmi blíží klasickému motivu ve Windows Vista, hlavním problémem je ale automatické přihlášení a práce pod účtem SYSTEM.

Dalším kandidátem na zavedení přes síť je **My_7PE**. Tento systém je založen na Windows 7 a konkuruje Windows PE 3.0. Vytváření probíhá automaticky pomocí předpřipraveného skriptu, který běží v rozhraní příkazové řádky a z uživatelského hlediska nabízí pouze velmi omezené volby. Tak jako VistaPE obsahuje grafické rozhraní podobné klasickému motivu ve Windows a procesy běžící pod uživatelem SYSTEM. Systém je možné vytvořit buď z Windows AIK, nebo přímo z nainstalovaných Windows 7 x86 (skript využije image Windows RE, který je obsažen v nainstalovaném Windows 7). Výstupem ze skriptu je adresářová struktura, jež umožňuje zavedení systému ze sítě stejným způsobem jako oficiální PE 3.0.

Posledním kandidátem na zavedení ze sítě je **Win7PE**. Tuto distribuci je možné vytvořit pomocí programu *WinBuilder*. K vytvoření je nutné mít instalační médium s Windows 7 (v anglické verzi) a dále je nutné mít v počítači nainstalován Windows AIK 3.0 (rovněž v anglické verzi). Win7PE obsahuje grafické prostředí velmi podobné plnohodnotným Windows 7, pozitivem je rovněž velké množství aplikací dostupných ve výchozím sestavení systému, podpora DirectX a uživatelské procesy běžící pod účtem "λ[]".

4.3 Používání Windows PE

4.3.1 Požadavky na image

Upravený obraz Windows PE musí být přizpůsoben tak, aby obsahoval grafické rozhraní umožňující uživateli ovládní systému, na které je zvyklý z plné verze Windows. Rovněž musí být zajištěno, aby nepřipojoval lokální pevný disk a aby dokázal spouštět základní aplikace nutné pro běžnou práci.

4.3.2 Popis řešení

Systém se bude zavádět zkopírováním celého image do RAM a následným nabofováním systému z ní. K tomuto účelu bude potřeba, aby byl výsledný obraz se systémem co nejmenší a aby veškeré zápisy zůstávaly v RAM lokálního počítače.

Aby byla tvorba image co nejjednodušší a zároveň měl co nejmenší velikost, budou jednotlivé aplikace uloženy na serveru a až na požádání staženy do klientského počítače.

Použije se tento model:

- 1) Obraz celého systému se stáhne do RAM lokálního počítače
- 2) Operační systém se zavede kompletně z RAM (ze staženého obrazu)
- 3) Systém vytvoří virtuální úložné místo (jednotku) v operační paměti
- 4) Po zavedení se protokolem SMB připojí síťový disk, na kterém budou přenosné verze programů
- 5) Na ploše se zobrazí seznam dostupných programů, které je možné v danou chvíli stáhnout ze síťového disku. Výběr programu je řešen sadou skriptů
- 6) Uživatel si ze seznamu vybere program, který chce spustit, tím spustí skript, který mu daný konkrétní program zkopíruje na lokální počítač
- 7) Uživatel program spustí

Veškeré programy jsou tedy uloženy mimo hlavní image systému a jsou pro systém dostupné pomocí sdíleného síťového disku.

4.3.3 Výhody řešení

Seznam programů může být rovněž uložen na síťovém disku. V tomto případě by si Windows PE nejdříve dynamicky zjistil, které programy jsou pro něj v danou chvíli dostupné, a teprve tento seznam by nabídl uživateli. Výhoda tohoto řešení je, že stačí vytvořit jeden image systémem, který se nemusí často měnit. Všechny změny v dostupných programech (přidání, odebrání, změna verze) by se děla přímo na serveru nezávisle na image s Windows PE. Drobná nevýhoda tohoto řešení spočívá v možnosti spouštět pouze přenosné verze programů, které se nemusí instalovat, toto ovšem není příliš velký problém, protože mnoho často používaných programů (pro běžnou práci) jako *OpenOffice*, *Firefox*, *Opera*, *Google Chrome*, *XAMPP*, *Blender*, *Gimp*, *Nvu*, *Putty*, *Skype*, *7-zip* existují dnes i jako přenosné verze a často zahrnují shodnou funkcionalitu s verzí instalovanou.

Ke zvýšení bezpečnosti by se dalo využít toho, že by byla sdílená jednotka na síti pro klienty dostupná pouze v režimu read-only. Ke snížení zatížení sítě při přenosu jednotlivých aplikací by jednotlivé programy mohly být již na serveru komprimovány, přenášeny v zkomprimované formě a na lokální počítači dekomprimovány. Toto řešení může být ovšem o něco složitější prakticky implementovat, vyžadovalo by to začlenit např. 7-zip do již standardního image Windows PE a následně rozšířit skript pro stažení programu o automatickou dekomprimaci staženého souboru pomocí programu 7-zip.

4.3.4 Nevýhody řešení

Drobná nevýhoda může být fakt, že Windows PE nedokáže vytvořit v operační paměti lokálního počítače větší místo pro ukládání dočasných dat než 512 MiB. Na lokální stanici by tedy nebylo možno stáhnout víc, jak 510 MiB dat jednotlivých programů (určité místo využije samotný Windows PE a programy umožňující stahování balíčků), tj. v jednom okamžiku by se na lokální stanici dal používat pouze (velikostně) omezený počet aplikací, pokud by se nově stahovaná aplikace do umístění v RAM nevešla, musela by se už dříve stažená a nepoužívaná aplikace z disku odstranit a tím na něm uvolnit místo. Pokud by se navíc používala komprimace dat a následné rozbalování na pracovní stanici, mohla by nastat situace, že stažená data není kam rozbalit.

4.3.5 Alternativní řešení

System se bude zavádět zkopírováním celého image do RAM a následným naboováním systému z ní. Základním image již v sobě obsahuje všechny potřebné programy. Mezi výhody tohoto řešení patří možnost daný program do Windows PE "nainstalovat", tj. udělat potřebné změny v registrech systému. Nevýhodou je, že se jednorázově stahuje celý image i s programy, které nemusí být vůbec potřeba, čímž se zbytečně zatěžuje síť.

5 DALŠÍ MOŽNOSTI ZAVEDENÍ WINDOWS ZE SÍTĚ

Tato kapitola se věnuje dalším možnostem, jak systém Windows zavést ze sítě.

5.1 Virtualizace Windows na systému Linux

Windows běží jako virtualizovaný hostovaný systém na hostitelském systému Linux, který je kompletně zaveden ze sítě. Toto řešení využívá předchozích poznatků bakalářské práce pana Kohouta [20].

5.1.1 Postup zavádění systému

Nejdříve je na bezdiskové stanici ze sítě naboootován operační systém Linux, který pomocí protokolu NFS nebo iSCSI připojí síťový disk obsahující soubor (virtuální disk) se systémem Windows. Po automatickém přihlášení do systému Linux je automaticky v celoobrazovkovém režimu spuštěn virtualizační nástroj *KVM* nebo *VirtualBox*, který automaticky otevře soubor virtuálního disku na sdílené síťové jednotce a naboootuje jeho obsah. Uživatelé pracují s virtualizovaným operačním systémem stejně, jako kdyby byl nainstalován na lokálním pevném disku pracovní stanice.

5.1.2 Výhody řešení

- Virtualizovaný systém nemá přímý přístup k hardwaru hostitelského počítače, dokonalá ochrana lokálního disku pracovní stanice.
- Unifikovaná platforma pro spouštění virtuálního disku s jakýmkoliv operačním systémem - Windows XP/Vista/7/2008 (teoreticky i budoucí verze Windows), nezávislá na hardwaru hostitelského počítače. Virtualizovanému systému je vždy prezentován unifikovaný hardware napříč rozdílnou konfigurací hostitelských počítačů.
- Snadná příprava virtualizovaného operačního systému. Systém se jednoduše nainstaluje do virtualizačního prostředí (VirtualBoxu, KVM) na správcově lokálním počítači, upraví se dle potřeb a celý virtuální disk se přesune na server.
- Spuštění více počítačů současně z jednoho sdíleného virtuálního disku by mohl řešit samotný virtualizační nástroj.

Z výhod vyplývá, že odpadají téměř všechny problémy popisované v kapitole 2.2. Stále je ovšem nutné vyřešit rozdílná jména jednotlivých počítačů a odstranit zbytečné zápisy / čtení z disku.

5.1.3 Nevýhody řešení

- Virtualizovaný systém nemá přímý přístup k hardware hostujícího počítače.
- Ztráta výkonu v důsledku virtualizace.

5.2 Komerční řešení - SANDeploy Boot Server

SANDeploy Boot Server je all-in-one řešení společnosti SANDeploy International Limited umožňující bezdiskové zavedení operačního systému [21]. Řešení využívá stejného principu, jako *Zavádění systému přes protokol iSCSI* (kapitola 2) a program *CCBoot* (kapitola 3).

Jedná se o malý program, který se instaluje na Windows Server a zde poskytuje služby DHCP, TFTP a iSCSI. Nastavení těchto služeb je možné přes přehledné grafické rozhraní, které se přidává jako modul snap-in do konzoly MMC (Microsoft Management Console).

Z podporovaných technologií je zde technologie umožňující z jednoho image zavádět více počítačů současně. Systém může být na serveru uložen buď jako jeden image soubor, nebo může být nainstalován na fyzickém oddílu. Program rovněž umožňuje zavést po síti obsah CD/DVD disku.

Cena řešení pro neomezený počet připojení je \$545.95, což je přibližně 9200 Kč (cena zjištěna k datu 10.5.2011).

II. PRAKTICKÁ ČÁST

6 ZAVÁDĚNÍ SYSTÉMU PŘES PROTOKOL iSCSI

Zde je popis základního nastavení jednotlivých prvků nutných pro zavedení systému. Jednotlivé prvky jsou PXE server, iSCSI server a klientský počítač.

6.1 PXE server

Jako PXE server slouží počítač s operačním systémem *Debian Linux* (verze 6, Squeeze).

Po základní instalaci je potřeba přidat balíčky **tftpd-hpa** (TFTP server) a **dhcp3-server** (DHCP server).

Instalace balíčků se provede v terminálu s právy uživatele root příkazem:

```
apt-get install tftpd-hpa dhcp3-server
```

6.1.1 Nastavení statické IP adresy

Pro nastavení statické IP adresy serveru je nutno editovat soubor **/etc/network/interfaces**.

Pro testovací prostředí byly zvoleny následující hodnoty:

Parametr	IPv4 adresa
IP adresa serveru	192.168.2.50
Subsíťová maska	255.255.0.0
Adresa síť	192.168.0.0
Broadcastová adresa	192.168.255.255
Výchozí brána	192.168.1.254

Tab. 2: Nastavení statické IP adresy PXE serveru

V případě, že je server připojen k síti přes adaptér *eth0* [22, s.94] bude obsah konfiguračního souboru vypadat následovně:

```
allow-hotplug eth0
iface eth0 inet static
address    192.168.2.50
netmask    255.255.0.0
network    192.168.0.0
broadcast  192.168.255.255
gateway    192.168.1.254
```

6.1.2 Nastavení služby TFTP

V případě zde byla jako kořenový adresář TFTP serveru zvolena cesta **/tftpboot**.

TFTP službu je možné spouštět přes server *xinetd*. Zde je ukázáno, jak spouštět službu samostatně. Nastavení serveru se provede v souboru **/etc/default/tftpd-hpa**. Obsah souboru by měl být následující:

```
# /etc/default/tftpd-hpa
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/tftpboot"
TFTP_ADDRESS="0.0.0.0:69"
TFTP_OPTIONS="--secure"
RUN_DAEMON="yes"
```

6.1.3 Obsah kořenového adresáře TFTP serveru

Kořenový adresář TFTP serveru **/tftpboot** musí obsahovat NBP soubor s programem gPXE. Tento soubor lze stáhnout ze stránek určených k vytváření image programu gPXE [23].

Nastavení pro vygenerování image je následující:

- Volba "**Choose an output format:**" musí být nastavena na "**PXE bootstrap loader keep [Keep PXE stack method 1] (.kpxe)**".
- Volba "**Choose a NIC type:**" musí být nastavena na "**undionly**". Je možné zvolit volbu "*all-drivers*", případě vybrat přímo typ čipu na síťovém adaptéru, ale z praktického testování vyplývá, že tyto volby nemají na úspěšnost bootování žádný vliv.

Nakonec je potřeba kliknout na tlačítko "**Get Image**" a vygenerovaný soubor uložit do adresáře **/tftpboot** pod názvem "**undionly.kpxe**", tak aby platila cesta:

```
/tftpboot/undionly.kpxe
```

V případě nefunkčnosti [23] je možné image gPXE zkompilevat ze zdrojových kódů. K tomuto účelu je potřeba doinstalovat balíčky **git-core**, **make** a **gcc**, přepnout se do pracovního adresáře a provést příkazy:

```
git clone git://git.etherboot.org/scm/gpxe.git
cd gpxe/src
```

```
make bin/undionly.kpxe
```

Vytvořený soubor "*undionly.kpxe*" se nachází v podadresáři "*gpxe/src/bin*" ve zvoleném pracovním adresáři.

6.1.4 Nastavení služby DHCP

Nastavení služby DHCP se provede v souboru */etc/dhcp/dhcpd.conf*.

V testovacím prostředí bylo s ohledem na povahu bootování zvoleno toto nastavení:

Parametr	Hodnota
Doba zapůjčení adresy	1800 s
Maximální doba zapůjčení adresy	3600 s
Přidělovaný rozsah adres	192.168.3.1 - 192.168.3.99
Subsíťová maska	255.255.0.0
Výchozí brána při zavádění OS	192.168.1.199
Výchozí brána po zavedení OS	192.168.1.254
Adresa PXE serveru	192.168.2.50
Adresa iSCSI serveru	192.168.1.199

Tab. 3: Nastavení služby DHCP na PXE serveru

Po spuštění počítače bude přes protokol PXE provedena DHCP žádost a následně se protokolem TFTP stáhne soubor "*undionly.kpxe*" (program gPXE). Po spuštění programu gPXE ("*undionly.kpxe*") se znovu provede DHCP žádost, server tentokrát odpoví uvedením cesty k disku sdílenému protokolem iSCSI ("*iscsi:192.168.1.199:::Windows7*").

Celý obsah souboru vypadá následovně [24]:

```
default-lease-time 1800;
max-lease-time 3600;
authoritative;
```

```
option space gpxe;
option gpxe-encap-opts code 175 = encapsulate gpxe;
option gpxe.keep-san code 8 = unsigned integer 8;
```

```
subnet 192.168.0.0 netmask 255.255.0.0 {
    range 192.168.3.1 192.168.3.99;
    if exists user-class and option user-class = "gPXE" {
        filename "";
        option routers 192.168.1.199;
        option root-path "iscsi:192.168.1.199::::Windows7";
        option gppe.keep-san 1;
    } else {
        option routers 192.168.1.254;
        next-server 192.168.2.50;
        filename "undionly.kpae";
    }
    option subnet-mask 255.255.0.0;
    option broadcast-address 192.168.255.255;
    option domain-name-servers 8.8.8.8, 8.8.8.4;
}
```

V případě, že server obsahuje více síťových rozhraní, je vhodné službu DHCP omezit pouze na vybraná rozhraní. Toto se provede v souboru `/etc/default/isc-dhcp-server`.

V případě, že má být služba omezena pouze na rozhraní `eth0`, bude soubor obsahovat:

```
INTERFACES="eth0"
```

6.1.5 Další podpůrné soubory nutné pro instalaci a zavedení Windows

V různých fázích instalace a spuštění Windows budou potřeba další soubory, tyto soubory pocházejí z projektu SYSLINUX / PXELINUX [25] [26] a je možné sehnat je z balíku `syslinux-common`. Soubory se po instalaci balíčku nacházejí v adresáři `/usr/lib/syslinux`.

V případě, že soubor v balíku není, je možné, že bude v balíčku stažitelném zde [27]. Zde používaná verze je 4.03.

Na jednotlivé soubory obsažené v balíku bude v práci odkazováno v okamžiku, kdy bude daný soubor potřeba. Soubor `/tftpbboot/pxelinux.cfg/default` se v balíku nenachází a v případě potřeby se musí manuálně vytvořit. Ostatní soubory jsou obsaženy v balíku.

6.2 iSCSI server

Jako iSCSI server je na návrh vedoucího práce využit systém *Openfiler* (verze 2.3).

Openfiler je speciálně uzpůsobený operační systém (založený na linuxové distribuci rPath), který je určen pro zařízení typu NAS a SAN. Mezi jeho hlavní výhody patří široká podpora protokolů pro sdílení souborů - NFS, SMB/CIFS, HTTP, FTP, podpora autentizace přes LDAP a možnost funkce jako iSCSI target a iSCSI initiator. [28]

Zde bude využito možnosti použití systému Openfiler jako iSCSI target.

6.2.1 Nastavení síťového rozhraní

V rámci testovacího prostředí je serveru přidělena statická IP adresa *192.168.1.199*, ostatní nastavení odpovídají popisu v kapitole 6.1.1.

6.2.2 Připojení fyzických disků a vytvoření logických jednotek

Z důvodu rozsahu práce zde nebude uvedeno základní nastavení systému, připojování fyzických disků a vytváření logických jednotek. Všechny kroky jsou detailně popsány v *Openfiler 2.3 Administrator Guide* [29]. Základní princip spočívá v připojení pevného disku, přidání daného disku do "*Volume Group*", čímž se z více fyzických disků vytvoří jedno spojené logické místo a následné rozdělení tohoto místa na oddíly (*Volumes*).

6.2.3 Vytvoření disku sdíleného protokolem iSCSI

Nejdříve se dle návodu ve vybrané "*Volume Group*" vytvoří "*Volume*", který bude následně sdílen prostřednictvím protokolu iSCSI. Nutná velikost svazku je nejméně 20 GiB, doporučený souborový systém je iSCSI.

Select Volume Group

Please select a volume group to display.

windows_images

Volumes in volume group "windows_images" (40928 MB)

Free (39%)
windows7 (56%)
win_pe (5%)

Volume name	Volume description	Volume size	File system type	File system size	FS used space	FS free space	Delete	Properties	Snapshots
windows7	Windows7	22720 MB	iSCSI	Not applicable	Not applicable	Not applicable	In use	Edit	Create
win_pe	Win_PE	2048 MB	iSCSI	Not applicable	Not applicable	Not applicable	In use	Edit	Create

0 MB allocated to snapshots
16160 MB of free space left

Volumes section

- Manage Volumes
- Volume Groups
- Block Devices
- Add Volume
- iSCSI Targets
- Software RAID

Support resources

- Report bug
- Get support
- Forums
- Admin Guide

Obr. 9: Openfiler - seznam vytvořených svazků ve skupině "windows_images"

Následně se daný svazek (volume) musí vysdílet pomocí protokolu iSCSI. To se provede kliknutím na odkaz "iSCSI Targets", vyplněním názvu cíle v položce "Target IQN", v případě zde je to "Windows7", a následným vyplněním vlastností pro nově vytvořený cíl.

Nastavení bylo zvoleno takto:

Atribut	Hodnota
HeaderDigest	None
DataDigest	None
MaxConnections	1
InitialR2T	Yes
ImmediateData	No
MaxRecvDataSegmentLength	131072
MaxXmitDataSegmentLength	131072

Tab. 4: Openfiler - nastavení parametrů pro iSCSI target

Atribut	Hodnota
MaxBurstLength	262144
FirstBurstLength	262144
DefaultTime2Wait	2
DefaultTime2Retain	20
MaxOutstandingR2T	8
DataPDUInOrder	Yes
DataSequenceInOrder	Yes
ErrorRecoveryLevel	0
Wthreads	16
QueuedCommands	32

Tab. 5: Openfiler - nastavení parametrů pro iSCSI target (pokračování)

Nyní je potřeba přepnout se na záložku "LUN Mapping", vybrat dříve vytvořený svazek (volume), nastavit "R/W Mode" na "write-thru", "Transfer Mode" na "blockio" a kliknout na tlačítko "Map".

Pokud bylo vše nastaveno tak, jak bylo uvedeno zde, je nový iSCSI disk dostupný na adrese **192.168.1.199:::Windows7**.

The screenshot displays the Openfiler web interface with the 'LUN Mapping' tab selected. The interface shows a table of mapped LUNs and a section for mapping a new LUN to the target 'Windows7'.

LUNs mapped to target: Windows7

LUN Id.	LUN Path	R/W Mode	SCSI Serial No.	SCSI Id.	Transfer Mode	Unmap LUN
0	/dev/windows_images/windows7	write-thru	shaMo2-BVgS-X7Mu	shaMo2-BVgS-X7Mu	blockio	<input type="button" value="Unmap"/>

Map New LUN to Target: "Windows7"

Name	LUN Path	R/W Mode	SCSI Serial No.	SCSI Id.	Transfer Mode	Map LUN
Win_PE	/dev/windows_images/win_pe	write-thru	2XFDcT-8WbA-HgRx	2XFDcT-8WbA-HgRx	blockio	<input type="button" value="Map"/>

The interface also includes a navigation menu at the top (Status, System, Volumes, Quota, Shares, Services, Accounts) and a sidebar with 'Volumes section' (Manage Volumes, Volume Groups, Block Devices, Add Volume, iSCSI Targets, Software RAID) and 'Support resources' (Report bug, Get support, Forums, Admin Guide).

Obr. 10: Openfiler - přidružení svazku k danému iSCSI targetu

Openfiler (verze 2.3) bohužel nepodporuje Copy-On-Write mechanismus umožňující spouštět více Windows současně z jednoho disku. Tento problém bude řešen později. Nejdříve je potřeba najít způsob, jak Windows na iSCSI disk dostat.

6.3 Instalace Windows na iSCSI target

Z důvodu, že je na systém Openfiler velmi problematické přesunout již hotový image disku z klientského počítače s instalací Windows 7, byla zvolena možnost instalace Windows 7 přímo na iSCSI target. Pro instalaci byly využity postupy uvedené zde [13].

6.3.1 Využití instalačního média jako druhého bootovatelného zařízení

Pro instalaci Windows přímo na iSCSI disk musí být tento disk nejdříve připojen v BIOSu. Princip instalace spočívá v nastavení BIOSu tak, že první zařízení, ze kterého se počítač snaží bootovat je síť, druhé zařízení je optická mechanika. V optické mechanice se nachází instalační DVD s Windows 7. Síť je nastavena tak, že pomocí protokolu PXE se na cílový počítač zavede gPXE. gPXE následně připojí iSCSI disk a po neúspěšném pokusu o zavedení systému z něj (na iSCSI disku žádný systém zatím není) nechá připojený iSCSI disk zaregistrovaný jako jednotku v BIOSu a předá řízení druhému bootovatelnému zařízení v pořadí - DVD ROM s instalačním médiem systému Windows 7.

Následně se spustí instalační proces Windows 7, program *Setup* najde připojený iSCSI disk a nabídne na něj instalaci systému. Při výběru, kam operační systém nainstalovat se vybere daný iSCSI disk a spustí se instalace. První zavedení systému z iSCSI disku se objeví už v průběhu instalace po nakopírování image systému z instalačního DVD na disk a restartu počítače. Instalace pokračuje až do bodu, kdy je systém úspěšně nainstalován na iSCSI disku. Následně se může vyjmout instalační DVD, systém startuje z iSCSI disku stejně, jako z lokálního disku.

Toto se, bohužel, při praktickém testování postupu nestalo. Nastavení BIOSu bylo shodné s výše uvedeným, nastavení sítě rovněž odpovídalo výše uvedenému (platí zde konfigurace serveru uvedená v kapitole 6.1), v DVD mechanice bylo vloženo DVD s Windows 7 (MSDNAA Professional x86 Czech), systém úspěšně nabootoval ze sítě a program gPXE připojil iSCSI disk, problém ovšem byl, že BIOS nepředal řízení druhému bootovatelnému zařízení v pořadí.

Postup byl zkoušen na více počítačích, u všech se objevil podobný problém. V programu *VirtualBox* následovalo zatuhnutí systému, na fyzickém počítači s deskou *Gigabyte GA-8I915PL-G* a BIOSem *AWARD* se po neúspěšném zavedení systému ze sítě objevila hláška "*PRESS ANY KEY TO REBOOT*", po stisku libovolné klávesy se BIOS znovu pokoušel zavést systém ze sítě a situace se opakovala. Na netbooku *Asus EEE PC 1000H* s BIOSem *AMI* se po neúspěšném zavedení systému ze sítě objevila hláška "*Insert bootable device and press any key*", po stisku libovolné klávesy následovalo nové bootování ze sítě a situace se opakovala.

```
UNDI code segment 9F00:0B20, data segment 9E00:1000 (632-639kB)
UNDI device is PCI 00:03.0, type UBOX PXE/UNDI
632kB free base memory after PXE unload
gPXE initialising devices...

gPXE 1.0.1 -- Open Source Boot Firmware -- http://etherboot.org
Features: AoE HTTP iSCSI DNS TFTP bzImage COMBOOT ELF Multiboot NBI PXE PXEXT

net0: 08:00:27:21:98:19 on UNDI (open)
  [Link:up, TX:0 TXE:0 RX:0 RXE:0]
DHCP (net0 08:00:27:21:98:19)... ok
net0: 192.168.3.1/255.255.0.0 gw 192.168.1.254
Booting from root path "iscsi:192.168.1.199:::Windows7"
Registered as BIOS drive 0x80
Booting from BIOS drive 0x80
Boot failed
Preserving connection to SAN disk
Could not boot from root path "iscsi:192.168.1.199:::Windows7": Not an executable image (0x2e852001)
No more network devices

Cannot remove PXE stack!
```

Obr. 11: Instalace Windows 7 přímo na iSCSI disk, systém se nesnaží bootovat z druhého zařízení

Tento postup se neukázal jako funkční, bylo tedy rozhodnuto vyzkoušet další postupy.

6.3.2 Připojení iSCSI disku z Windows 7 a instalace na něj

Dalším nápadem bylo připojit iSCSI disk jako lokální jednotku ve Windows 7 a spustit instalaci na disk přímo z prostředí Windows 7. Program *Setup* vypsal, že na danou jednotku nemůže instalovat, údajně je to možné z prostředí Windows PE.

6.3.3 Instalace přes Windows PE

Ačkoliv se využití Windows PE zdálo dobrou volbou, objevil se problém v tom, že oficiální Windows PE nativně neobsahují iSCSI iniciator, bylo tedy nutné daný iniciator do systému přidat. To se bohužel nepovedlo, příkaz *iscsicpl* nic neprovedl, byl využit návod zde [30].

6.3.4 Použití El-Torito CD

Postup vychází z 6.3.1. Princip spočívá v úpravě konfigurace serveru tak, aby po neúspěšném zavedení systému z iSCSI disku (disk zůstává v BIOSu připojen) bylo možno ze serveru pomocí protokolu TFTP stáhnout a spustit malý operační systém El-Torito, který následně předá řízení optické mechanice a spustí instalaci Windows 7 z média v ní.

Do kořenového adresáře TFTP serveru je nutno stáhnout soubory "*memdisk.bin*" a "*sbootmgr.dsk*" [13], zkopírovat do něj z balíčku SYSLINUX (viz. 6.1.5) soubor "*gpxelinux.0*" a vytvořit v něm adresář "*pxelinux.cfg*" a v něm soubor "*default*".

Budou tedy platit cesty:

```
/tftpboot/memdisk.bin  
/tftpboot/sbootmgr.dsk  
/tftpboot/gpxelinux.0  
/tftpboot/pxelinux.cfg/default
```

Obsah souboru **/tftpboot/pxelinux.cfg/default** bude následující:

```
label torito  
kernel memdisk.bin  
append initrd=sbootmgr.dsk
```

V adresáři "*tftpboot*" se samozřejmě nachází soubor "*undionly.kpxe*". Konfigurační soubory DHCP a TFTP daemonů jsou shodné s kapitolou 6.1.

Pro spuštění instalace tímto způsobem je nutno restartovat klientský počítač, počkat než program gPXE připojí iSCSI disk a stisknout klávesy CTRL+B (až na druhou výzvu). Do příkazového řádku je potřeba zadat:

```
chain tftp://192.168.2.50/gpxelinux.0
```

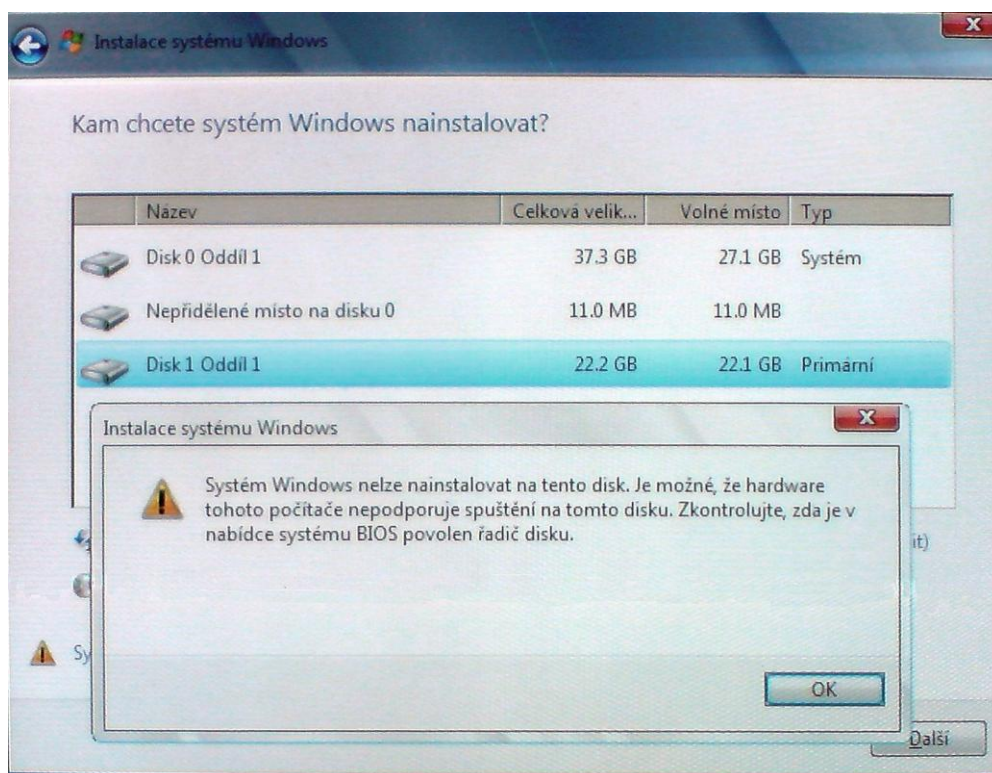
a po zavedení souborů do lokálního počítače napsat řetězec: `torito`.

System El-Torito předá řízení optické mechanice, spustí se instalace Windows 7 (z instalačního DVD). Při načítání souborů z instalačního média si lze všimnout, že toto načítání plně řídí systém El-Torito (spuštění instalačního procesu trvá zřejmě déle, než při přímém bootování z instalačního média).

V případě, že se po zadání `chain tftp://192.168.2.50/gpxelinux.0` načítání zasekne, je možno místo souboru "`gpxelinux.0`" použít soubor "`pxelinux.0`", tento soubor je možno sehnat ze starších balíčků SYSLINUX (např. 3.63), případně z přílohy k této práci.

Tímto způsobem se podařilo zajistit registraci iSCSI disku jako jednotky v BIOSu a současně spustit instalaci Windows 7 z instalačního média.

Instalace pokračovala do bodu, kdy se měl zvolit disk, na který se mají Windows nainstalovat, připojený iSCSI disk se sice zobrazil jako jedna z jednotek, ale při jeho výběru se objevila hláška "*System Windows nelze nainstalovat na tento disk. Je možné, že hardware tohoto počítače nepodporuje spuštění na tomto disku. Zkontrolujte, zda je v nabídce systému BIOS povolen řadič disku.*"



Obr. 12: Chyba při instalaci Windows na iSCSI disk

Přes tento bod se nepodařilo dostat dál. Daný postup byl vyzkoušen na několika domácích počítačích a po domluvě s vedoucím práce i na 2 různých školních počítačích s několika rozdílnými síťovými adaptéry (*Belkin Ver. 2000 ee*, *3Com 3C905CX-TX-M*, *Edimax s čipem RTL 8169SC*, integrovaný adaptér *Intel* na desce jednoho z počítačů). Přesto, že byly vyzkoušeny všechny možné způsoby a nastavení BIOSu daných počítačů, řešení nevedlo ke zdárnému výsledku.

6.3.5 Instalace přes síťový adaptér přímo obsahující gPXE

Po předchozích neúspěších byla snaha pokračovat dál a vyzkoušet další možnosti. Jednou z nich bylo naflashovat program gPXE přímo jako Boot ROM do síťové karty. K tomuto byla potřeba síťová karta s možností flashování image. Na vlastní náklady byla tedy zakoupena NIC *Intel PRO/1000 GT* (daný adaptér má flashovatelnou EEPROM) a provedena riskantní výměna oficiálního PXE firmwaru za neoficiální image s *gPXE 1.0.1+*. Po flashnutí karty se celý start počítače choval divně (BIOS nebral ohled na nastavení v programu *Setup* a neustále startoval s defaultními hodnotami) a karta se vůbec neinicializovala. Dále byl vyzkoušen image s *gPXE 1.0.0*. Tento fungoval a po provedení programu POST se z karty spustil program gPXE. Následně byl ze serveru spuštěn systém El-Torito, přes který se spustila instalace Windows 7 z DVD.

Instalační program našel iSCSI disk a umožnil na něj instalovat. Celá instalace proběhla na první pohled v pořádku. Problém ale byl, že instalační program sice nainstaloval Windows na iSCSI disk, ale zavaděč zapsal na lokální pevný disk klientského počítače, ne na síťový iSCSI disk. Stejný pokus byl proveden s Windows Server 2008 R2 Standard (MSDNAA), výsledek byl zcela shodný. Při odpojení lokálního fyzického disku z počítače instalační program nedovolil na iSCSI disk instalovat s hláškou výše (kapitola 6.3.4).

Posledním testovaným způsobem instalace bylo použití iSCSI disku, který poskytuje program *CCBoot* (viz. kapitola 3). Vestavěné gPXE v síťové kartě jej pomocí služby DHCP, kterou poskytnul program *CCBoot*, našlo a připojilo. Pomocí systému El-Torito byla spuštěna instalace. Výsledek byl přesně stejný, jako při instalaci na iSCSI disk vytvořený v systému *Openfiler*. Systém se na disk nainstaloval, ale zavaděč (*Bootmgr* a *BCD*) zapsal na lokální disk počítače, z něž byl instalován.

V tomto bodě bylo nutno konstatovat, že BIOS počítače, přes veškerou snahu o zprovoznění, bootování z iSCSI disku skutečně nepodporuje.

Situace byla řešena dotazem v několika internetových diskuzích, asi nejlepší odpověď poskytl člověk jménem Andrew Bobulsky dne 1.4.2011 skrze gPXE mailing list:

Jeho odpověď byla (část popisující problém):

The infamous error that you are getting, "Windows cannot be installed to this disk," is, as I found out(1), an issue that's caused by a combination of Windows' inability to resolve ARC paths for some system BIOSes in the presence of BIOS INT 13h hooks like the one gPXE uses to attach its SAN target.

*Some of the troubleshooting steps, like attaching an internal hard drive, allow you to "trick" (for lack of a better word) Windows into resolving these ARC paths correctly and proceeding with the iSCSI installation. The problem is that it's hit or miss as to whether or not that will work for your BIOS. In your case, adding a drive presented Windows with two installation sources, but the ARC path for your iSCSI disk still wasn't available to the Windows installer. As a result, it only considered your local disk to be bootable, and wrote the BCD and copied BOOTMGR to *it* while placing everything else on the SAN. The SAN disk will get its MBR written, so it'll *try* to boot, but since there's no actual boot loader on it, it can't boot without the other [local] drive being available for that data.*

(1):<http://social.technet.microsoft.com/Forums/en-US/w7itproinstall/thread/cea6177e-9cb2-420e-bbc0-0cac487e51e2>

Volný překlad:

Chyba, kterou dostáváte, "Windows nemůže být nainstalován na tento disk", je, jak jsem zjistil (1), problém způsobený kombinací neschopnosti Windows detekovat ARC cesty u některých BIOSů pokud je používáno přerušování BIOSu INT 13h, které používá gPXE k připojení SAN cíle.

Některé kroky k odstranění poruch, jako připojení interního harddisku, Vám dovolí obelstít Windows do stavu, kdy rozluští tyto ARC cesty správně a pokračují v instalaci na iSCSI disk. Problém je, že se musí použít metoda pokus-omyl a zjistit, co bude fungovat pro daný BIOS. Ve Vašem případě přidání jednotky představovalo pro Windows dva instalační zdroje, ale ARC cesty iSCSI disku stále nebyly dostupné instalátoru Windows. Jako výsledek považoval za bootovatelný pouze lokální disk, zapsal na něj BCD a zkopíroval na něj BOOTMGR, zatímco všechna ostatní data zapsal na SAN. SAN disk může mít MBR zapsán, takže se z něj systém snaží bootovat, ale protože neobsahuje zavaděč systému, nelze nabootovat bez dalšího [lokálního] disku, který je dostupný pro data.

ARC cesty jsou podle zdroje, který je uveden jako (1) v textu mailu, cesty, pomocí nichž Windows identifikují jednotky. ARC cesta vypadá (podle zdroje (1) uvedeného v mailu) například takto: multi(0)Disk(0)rdisk(0).

V mailu byla dále rada zkusit sejmout image pevného disku a přesunout tento image na server. Tento způsob byl ovšem nerealizovatelný z důvodu, že byl serverem Openfiler.

V dalším mailu člověk jménem Michael Brown radil zkusit zavaděč iPXE [31] (místo gPXE), nebo k instalaci na iSCSI server využít službu WDS (Windows Server 2008).

Byla tedy provedena kompilace image s programem *iPXE 1.0.0+* a daný image následně naflashován na adaptér *INTEL PRO/1000 GT*. Program iPXE nabídl lepší (grafickou) konfiguraci parametrů, ale výsledek při instalaci Windows na iSCSI target byl zcela shodný, jako při použití programu gPXE.

6.3.6 Další možnosti instalace

Po neúspěších s přímou instalací Windows na iSCSI target metodami popsány výše bylo zvažováno použití technologie WDS a manuální přesunutí zavaděče na iSCSI disk.

Nakonec ale bylo, po dlouhém a pracném testování předchozího způsobu instalace, rozhodnuto tento způsob zavádění Windows ze sítě opustit (pokud se objevily takové problémy s instalací, pravděpodobně budou velké problémy i se spouštěním a provozem) a prozkoumat další způsoby zavedení Windows ze sítě.

Celý postup by pravděpodobně fungoval na serverových síťových adaptérech, které nativně protokol iSCSI podporují, jako je například *Intel PRO/1000 PT Server Adapter* nebo *QLogic 4000 Series*. Problém je ovšem v ceně tohoto řešení, která začíná na 2000 Kč (odhad) za jednu pracovní stanici.

Nasazení gPXE jako zavaděče pro iSCSI se zdálo levným, praktickým a univerzálním řešením. Bohužel tento program nesplnil, co sliboval.

7 WINDOWS PE

Tato kapitola je věnována praktické realizaci vytvoření image se systémem Windows PE a jeho následným zavedením pomocí protokolů PXE, HTTP a iSCSI na cílovou stanici.

7.1 Úvod

7.1.1 Vytvářený image se systémem

Zde vytvářený systém bude Windows PE 3.0. Systém bude pouze základní, grafické rozhraní bude řešeno jednoduchým souborovým manažerem, lokální disky se nebudou po startu automaticky připojovat a instalované programy se budou stahovat jako *7-zip* balíčky ze SMB sdíleného disku.

Pozn.: Přestože nebudou pevné disky lokálního počítače při startu automaticky připojeny, stále je možné, že si potenciální útočník lokální disky znovu připojí (např. nástrojem *Diskpart*) a následně na nich provede změny.

7.1.2 Další možnosti při vytváření image

Z důvodu celkového rozsahu této práce zde není primárním cílem vytvořit Windows PE se stoprocentní funkčností plné verze Windows, ale spíše jej zavést ze sítě. Administrátor má možnost vytvořit si Windows PE podle svých vlastních potřeb. K vytvoření může být použit základ *PE 2.0*, *PE 3.0*, *VistaPE*, *My_7PE*, *Win7PE*. To, jaká možnost k vytvoření Windows PE bude použita, není důležité. Důležité je, aby vytvořený image podporoval adresářovou strukturu, která je nutná pro zde diskutované zavedení Windows ze sítě, případně níže uvedené skripty pro zavádění jednotlivých programů ze síťového disku.

7.1.3 Nastavení sítě

Nastavení sítě (IP adresy) použité pro zavádění Windows PE je shodné s nastavením použitým pro zavádění plné verze Windows z iSCSI disku (kapitola 6.1). Konfigurační soubory serveru jsou v příloze.

7.2 Zavádění programů ze sítě

7.2.1 Síťový disk s programy

Síťový disk s programy je připojen protokolem SMB při startu Windows PE (viz 7.3.1).

Adresářová struktura disku je následující:

```
\Balicky  
\Skripty
```

V adresáři "*Balicky*" se nacházejí balíčky se samotnými programy. Balíček se vytvoří tak, že se spustitelná (přenositelná) verze programu nastaví na lokálním počítači (provede se uživatelské nastavení vzhledu a podobně) a následně se adresářová struktura aplikace zkomprimuje programem 7-zip tak, aby se vytvořil balíček "*.7z" s programem. Tento balíček se následně zkopíruje na sdílený disk do složky "*Balicky*".

Adresář "*Skripty*" obsahuje sadu dávkových souborů, které se starají o kopírování a instalaci programu na lokální stanici s běžícím Windows. Ke každému jednomu balíčku je vždy přiřazen konkrétní skript, který za daný balíček odpovídá.

Po zavedení Windows PE se obsah adresáře "*Skripty*" na síťové jednotce automaticky zkopíruje do lokálního adresáře "*X:\Programy\Nainstalovat*" na lokálním počítači a adresář "*X:\Programy*" se stane výchozím pracovním adresářem.

7.2.2 Spouštění programů na Windows PE

Po naboování systému je dostupný lokální disk "*X:*" vytvořený v RAM a síťová jednotka "*Z:*" obsahující jednotlivé programy.

Na disku "*X:*" se nacházejí adresáře:

```
X:\Temp\Instemp  
X:\Temp\Nastroje  
X:\Temp\Programy  
X:\Programy\Nainstalovat  
X:\Programy\Spustit
```

V adresáři "X:\Programy\Nainstalovat" se nacházejí instalační skripty jednotlivých programů. Adresář "X:\Programy\Spustit" obsahuje zástupce již nainstalovaných programů. Dvojitým kliknutím na instalační skript daného programu ve složce "Nainstalovat" se spustí kopírování daného programu ze síťového disku do adresáře "X:\Temp\Instemp", následná dekomprimace programu pomocí nástroje 7-zip do složky "X:\Temp\Programy" a vytvoření zástupce na daný program do adresáře "X:\Programy\Spustit".

Adresář	Význam
X:\Temp\Instemp	Slouží jako dočasný adresář pro uložení staženého 7z balíčku.
X:\Temp\Nastroje	Obsahuje nástroje nutné pro stažení a instalaci jednotlivých programových balíčků ze sdílené složky.
X:\Temp\Programy	Obsahuje nainstalované programy (rozbalené balíčky).
X:\Programy\Nainstalovat	Obsahuje skripty pro instalaci jednotlivých programů.
X:\Programy\Spustit	Obsahuje zástupce na již nainstalované programy.

Tab. 6: Význam jednotlivých uživatelských adresářů ve Windows PE

Cílem tohoto řešení je umožnit uživateli pohodlně instalovat a spouštět aplikace. Uživatel nemusí procházet adresářovou strukturu celého OS proto, aby si spustil a nainstaloval program. Jednoduše se přepne do adresáře "X:\Programy\Nainstalovat" a provede instalaci. Nainstalovaný program pak spustí poklepnutím na zástupce v "X:\Programy\Spustit".

7.2.3 Vytváření balíčků s programy a instalačních skriptů

Vytvoření "*.7z" balíčku s programem je ukázáno na webovém prohlížeči Opera.

Nejdříve se z webových stránek [32] stáhne program *OperaPortable*, který se nainstaluje do lokální složky. Spustí se "*OperaPortable.exe*" a provedou se nutná uživatelská nastavení. Za pomoci VBS skriptu [33] se vytvoří zástupce na (zatím) neexistující soubor, který se ve výsledku bude nacházet v "X:\Temp\Programy\Opera\OperaPortable.exe". Zástupce "*Opera.lnk*" se umístí do složky se souborem "*OperaPortable.exe*".

Nyní se všechny soubory a složky v adresáři se souborem "*OperaPortable.exe*" zkomprimují nástrojem *7-zip* do archivu "*opera.7z*" a tento soubor se zkopíruje na sdílený síťový disk do adresáře "*Balicky*".

Celá operace se završí napsáním jednoduchého skriptu "**Opera.cmd**", který se umístí na sdílený síťový disk do složky "*Skripty*". Výsledný skript může vypadat třeba takto (v případě zde je síťová jednotka dostupná pod písmenem "Z:"):

```
echo Instalace programu Opera
echo -----
set balicky=Z:\Balicky
set insprogr=X:\Temp\Programy
set temp=X:\Temp\Instemp

IF EXIST %insprogr%\Opera\OperaPortable.exe GOTO END
copy %balicky%\opera.7z %temp%\opera.7z /Y /Z
X:\Temp\Nastroje\7za.exe x %temp%\opera.7z -o%insprogr%\Opera
copy %insprogr%\Opera\Opera.lnk X:\Programy\Spustit
del %temp%\opera.7z

:END
echo Instalace ukoncena
```

7.3 Vytvoření spustitelného image se systémem

7.3.1 Postup při vytváření image

K vytvoření Windows PE 3.0 [34] lze použít balík *Windows AIK 3.0*, který je možno stáhnout ze stránek společnosti Microsoft. Po instalaci balíku do lokálního počítače se spustí "**nabídka Start** → **Všechny programy** → **Microsoft Windows AIK** → **Příkazový řádek nástrojů pro nasazení**"¹⁶. Zde se budou provádět níže uvedené příkazy.

Nejdříve se zkopírují nezbytné soubory nutné pro vytvoření Windows PE, k tomu se využije vestavěný skript "*copype.cmd*", který jako argumenty přijímá cílovou architekturu (x86) a pracovní složku, do které se mají nezbytné soubory nakopírovat (*c:\winpe_x86*).

```
copype.cmd x86 c:\winpe_x86
```

Ve složce "*c:\winpe_x86*" se nachází image systému, soubor "*winpe.wim*". Nyní se tento image pomocí nástroje *Dism* připojí do lokálního adresáře "*c:\winpe_x86\mount*". Tím se získá přístup k souborům, které se nachází uvnitř (příkaz i parametry jsou na jednom řádku).

```
Dism /Mount-Wim /WimFile:c:\winpe_x86\winpe.wim /index:1  
/MountDir:c:\winpe_x86\mount
```

Nyní se v adresáři "*mount*" vytvoří 5 nových adresářů: "*Temp\Instemp*", "*Temp\Nastroje*", "*Temp\Programy*", "*Programy\Nainstalovat*" a "*Programy\Spustit*", tyto adresáře budou později sloužit pro spouštění programů, které jsou umístěny na sdíleném síťovém disku.

```
mkdir c:\winpe_x86\mount\Temp\Instemp  
mkdir c:\winpe_x86\mount\Temp\Nastroje  
mkdir c:\winpe_x86\mount\Temp\Programy  
mkdir c:\winpe_x86\mount\Programy\Nainstalovat  
mkdir c:\winpe_x86\mount\Programy\Spustit
```

¹⁶ Daný program je nutno spouštět s oprávněním Administrátora.

Aby se snížilo při přenosu jednotlivých aplikací zatížení sítě, budou tyto aplikace na serveru komprimovány programem 7-zip. Aby bylo možné aplikaci na lokálním počítači spustit, musí být nejdříve dekomprimována. K tomu bude potřeba program 7-zip ve verzi pro příkazovou řádku. Program se dá stáhnout třeba zde [35].

Po rozbalení staženého zip archivu se program "7za.exe" zkopíruje do adresáře "Temp" tak, aby platila cesta:

```
c:\winpe_x86\mount\Temp\Nastroje\7za.exe.
```

Po spuštění Windows se automaticky otevře program Explorer++, který bude sloužit pro instalaci a spouštění programů. Explorer++ je možné stáhnout na stránce výrobce [37]. Po stažení a rozbalení je nutno v adresáři se souborem "Explorer++.exe" vytvořit soubor "config.xml", spustit Explorer++ a v menu "Tools → Options" na první záložce nastavit volby "On Startup" na "Load default folder", v "General settings" zaškrtnout volbu "Run in portable mode" a do pole "Default new tab folder:" vložit "X:\Programy\".

Změnu nastavení je nutno zkontrolovat v souboru "config.xml" a ujistit se, že je nastaveno:

```
<Setting name="NewTabDirectory">X:\Programy</Setting>  
a Directory="X:\Programy".
```

Následně se soubory "Explorer++.exe" a "config.xml" zkopírují do složky

```
c:\winpe_x86\mount\Temp\Nastroje.
```

Dále se vytvoří soubor "Vypnout pocitac.cmd", jehož obsahem bude:

```
wpeutil shutdown
```

a zkopíruje se do "c:\winpe_x86\mount\Programy".

Odpojení lokálních disků se provede pomocí úpravy registru Windows PE [30] [36].

Nejdříve se systémový registr Windows PE připojí do podklíče "*HKLM\pe_sys*" na lokálním počítači:

```
REG LOAD HKLM\pe_sys
C:\winpe_x86\mount\Windows\System32\config\SYSTEM
```

dále je nutno do něj vložit následující hodnoty:

```
REG ADD HKLM\pe_sys\ControlSet001\Services\MountMgr /v NoAutoMount
/t REG_DWORD /d 1 /f

REG ADD HKLM\pe_sys\ControlSet001\Services\partmgr\Parameters /v
SanPolicy /t REG_DWORD /d 3 /f
```

a nakonec jej odpojit příkazem:

```
REG UNLOAD HKLM\pe_sys
```

Toto nastavení zajistí, že se při spuštění Windows PE nebudou automaticky připojovat lokální disky.

Změna rozlišení obrazovky na 1024x768 se provede vytvořením souboru "**peoptions.xml**" [38], do nějž se vloží:

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="windowsPE">
    <component name="Microsoft-Windows-Setup"
processorArchitecture="x86"
publicKeyToken="31bf3856ad364e35" language="neutral"
versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"xmlns
:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <Display>
        <ColorDepth>32</ColorDepth>
        <HorizontalResolution>1024</HorizontalResolution>
        <VerticalResolution>768</VerticalResolution>
      </Display>
    </component>
  </settings>
</unattend>
```

"*peoptions.xml*" se následně zkopíruje do "*c:\winpe_x86\mount\Windows*".

Dále je nutno upravit soubor "*c:\winpe_x86\mount\Windows\System32\startnet.cmd*" tak, aby obsahoval následující text:

```
@ECHO off
wpeinit /unattend=X:\Windows\peoptions.xml
net use Z: <síťová jednotka> > NUL
xCopy Z:\Skripty X:\Programy\Nainstalovat
X:\Temp\Nastroje\Explorer++.exe
```

Soubor "*startnet.cmd*" se spustí po zavedení systému a zajistí změnu rozlišení obrazovky, připojení síťové jednotky, zkopírování instalačních skriptů a spuštění programu Explorer++.

Rovněž je možno zvětšit úložné místo, které bude virtuálně existovat v operační paměti z původních 32 MiB na 512 MiB. Toto místo se použije pro lokální uložení programů stažených ze sítě. Velikost místa lze nastavit příkazem:

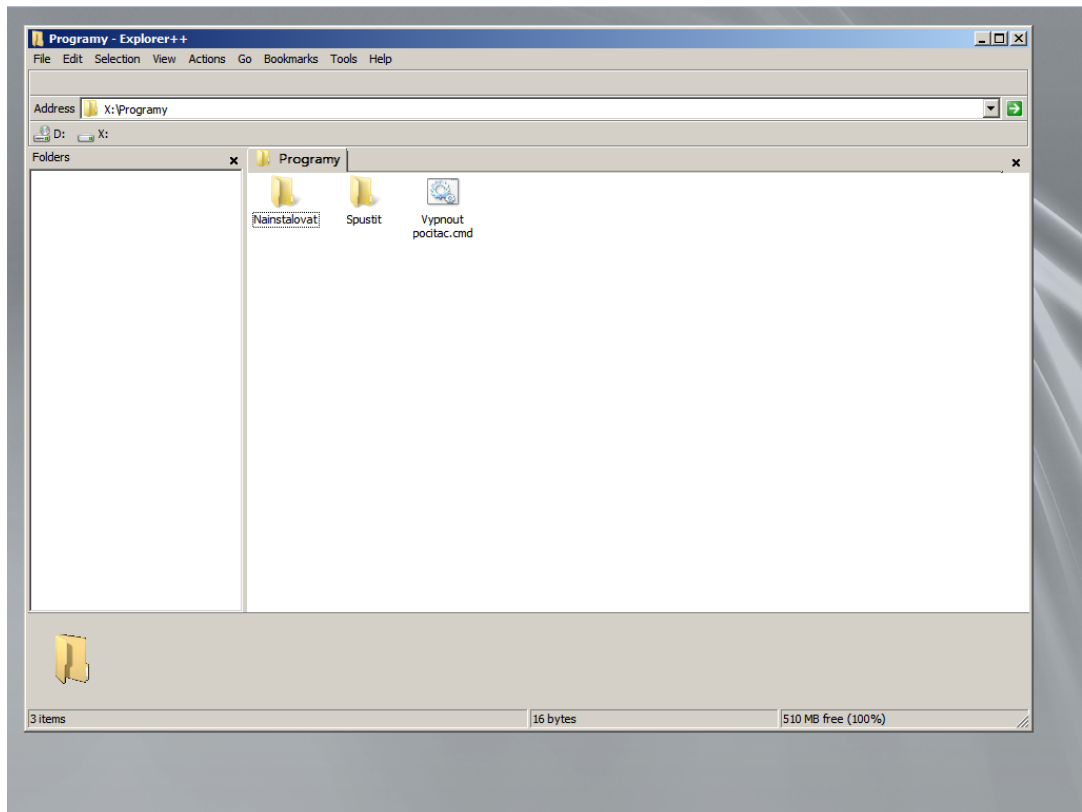
```
dism /image:c:\winpe_x86\mount /Set-ScratchSpace:512
```

Následně se provede uložení změn do image:

```
Dism /Unmount-Wim /MountDir:C:\winpe_x86\mount /Commit
```

Soubor "*winpe.wim*" nyní obsahuje bitovou kopii Windows PE.

Po zavedení vypadá vytvořený image s Windows PE takto:



Obr. 13: Jednoduchý image s Windows PE 3.0

7.4 Využití HTTP pro instalaci balíčků s programy

V kapitolách 7.2.1 až 7.2.3 byla ukázána instalace programů do běžícího Windows PE. Jednotlivé programy mají formu 7-zip balíčků, které se na požádání přes skript stáhnou do operační paměti běžícího počítače, kde se rozbalí a umožní své spuštění. Byl představen jednoduchý model skriptů, který tuto činnost zabezpečuje. Původní myšlenka byla stahovat programy ze sdíleného síťového disku připojeného protokolem SMB. Nyní tato myšlenka bude rozšířena o možnost zavedení a instalaci programů z HTTP serveru.

Struktura i instalace programů je velmi podobná instalaci ze síťového SMB disku, pouze je nutné zajistit, aby se balíčky stahovaly z HTTP serveru. K tomuto účelu bude využit program *Wget* [45], který lze stáhnout zde [46]. Struktura adresářů na vytvořeném Windows PE je shodná se strukturou popsanou v kapitole 7.2.2.

Stahování balíčků protokolem HTTP je alternativa k již dřívějšímu řešení pomocí sdíleného disku a může být použito úplně ve všech způsobech zavádění Windows PE ze sítě.

7.4.1 HTTP server

Předpokládá se, že HTTP server je dostupný na adrese "192.168.1.100" přes port 80. Pozn. server může být přístupný i přes doménové jméno (FQDN), v tomto případě se jednoduše nahradí všechny výskyty IP adresy daným doménovým jménem.

V adresáři, který je dostupný jako kořenový (zde byl pro názornost použit kořenový adresář serveru) je nutno vytvořit složky "*Balicky*" a "*Skripty*", tak aby platily cesty

```
http://192.168.1.100/Balicky
```

```
http://192.168.1.100/Skripty
```

Složka "*Balicky*" bude stejně jako na sdíleném síťovém disku obsahovat vytvořené 7-zip balíčky s programy. Jednotlivé balíčky se vytvářejí úplně stejně jako v předchozím případě (7.2.3). Drobná změna se týká vytvářeného skriptu, kde se místo kopírování ze síťového disku využije nástroj *Wget*.

Vytvoření skriptu bude, tak jako v předchozím případě, předvedeno na programu *Opera*.

Předpokládá se, že se balíček "opera.7z" již nachází na serveru a že je dostupný na této adrese:

```
http://192.168.1.100/Balicky/opera.7z
```

Skript "**Opera.cmd**" potom bude vypadat:

```
echo Instalace programu Opera
echo -----
set insprogr=X:\Temp\Programy
set temp=X:\Temp\Instemp

IF EXIST %insprogr%\Opera\OperaPortable.exe GOTO END
X:\Temp\Nastroje\wget.exe -O %temp%\opera.7z
http://192.168.1.100/Balicky/opera.7z
X:\Temp\Nastroje\7za.exe x %temp%\opera.7z -o%insprogr%\Opera
copy %insprogr%\Opera\Opera.lnk X:\Programy\Spustit
del %temp%\opera.7z

:END
echo Instalace ukoncena
```

pozn.

"X:\Temp\Nastroje\wget.exe -O %temp%\opera.7z http://192.168.1.100/Balicky/opera.7z"
musí být na jednom řádku (zde je z důvodu formátování zalomeno).

Takto vytvořený skript (spolu s dalšími skripty pro ostatní programy) se zkomprimuje programem 7-zip do souboru "skripty.7z" a umístí se na server tak, aby byl soubor dostupný na:

```
http://192.168.1.100/Skripty/skripty.7z
```

7.4.2 Úprava obrazu Windows PE

V části 7.3.1 byl podrobně popsán postup při vytváření image s Windows PE. Zde budou popsány pouze změny, které se musí udělat, aby bylo možno stahovat z HTTP serveru.

Nejdříve je nutno image se systémem "*c:\winpe_x86\winpe.wim*" připojit do složky "*c:\winpe_x86\mount*".

Do připojeného image se kromě souborů "*7za.exe*", "*Explorer++.exe*" a "*config.xml*" přidá také soubor "*wget.exe*" tak, aby platila cesta

```
c:\winpe_x86\mount\Temp\Nastroje\wget.exe
```

Dále je nutno upravit soubor "*c:\winpe_x86\mount\Windows\System32\startnet.cmd*" tak, aby obsahoval následující text:

```
@ECHO off
set temp=X:\Temp\Instemp
wpeinit /unattend=X:\Windows\peoptions.xml
X:\Temp\Nastroje\wget.exe -O %temp%\skripty.7z
http://192.168.1.100/Skripty/skripty.7z
X:\Temp\Nastroje\7za.exe x %temp%\skripty.7z -
oX:\Programy\Nainstalovat
del %temp%\skripty.7z
X:\Temp\Nastroje\Explorer++.exe
```

Soubor "*c:\winpe_x86\winpe.wim*" je nutno odpojit. Nyní je vytvořen image Windows PE schopný stahovat programy pomocí protokolu HTTP.

7.4.3 Výhody a nevýhody řešení

Hlavní výhodou a současně i nevýhodou je využití HTTP serveru místo SMB sdíleného síťového disku. V síti nemusí být zpřístupněn sdílený disk, naopak se musí vytvořit webový server. Toto řešení se zdá být výhodné, pokud již klient bootuje ISO obraz pomocí protokolu HTTP (kapitola 7.7). Přenos souborů protokolem HTTP by měl být teoreticky o něco méně náchylný na větší latence sítě (rychlost přenosu dat by při vyšších odezvách sítě neměla výrazně klesat). Při použití protokolu SMB2 by se ovšem neměly projevat výrazné rozdíly.

7.5 Bootování přes PXE (standardní způsob)

Předpokládá se, že je úspěšně splněn předchozí bod a je vytvořen image s operačním systémem Windows PE. V této části bude ukázáno, jak nastavit image se systémem tak, aby jej bylo možné zavést doporučeným způsobem.

7.5.1 Příprava souborů

Tento postup vychází z [39]. Na disku "C:" je nutno vytvořit pracovní složku "*pe_temp*", a do ní nakopírovat potřebné soubory. Aby byl popis maximálně zjednodušen, je uveden ve formě příkazů.

V nabídce "**Start** → **Všechny programy** → **Microsoft Windows AIK**" se spustí "**Příkazový řádek nástrojů pro nasazení**" a provedou se následující příkazy:

```
Dism /Mount-Wim /WimFile:c:\winpe_x86\winpe.wim /index:1
/MountDir:c:\winpe_x86\mount
mkdir c:\pe_temp

copy c:\winpe_x86\mount\Windows\Boot\PXE\*. * c:\pe_temp

copy "c:\Program Files\Windows
AIK\Tools\PETools\x86\boot\boot.sdi" c:\pe_temp

copy c:\winpe_x86\winpe.wim c:\pe_temp\boot.wim
```

Nyní se musí nastavit bootovací záznam:

```
Bcdedit -createstore c:\pe_temp\BCD

Bcdedit -store c:\pe_temp\BCD -create {ramdiskoptions} /d "Ramdisk
options"

Bcdedit -store c:\pe_temp\BCD -set {ramdiskoptions}
ramdiskdevice Boot

Bcdedit -store c:\pe_temp\BCD -set {ramdiskoptions} ramdiskpath
\Boot\boot.sdi

Bcdedit -store c:\pe_temp\BCD -create /d "Windows PE" /application
osloader
```

příkaz vrátí GUID hodnotu, touto hodnotou se nahradí {guid} v následujících příkazech:

```
Bcdedit -store c:\pe_temp\BCD -set {guid} systemroot \Windows
```

```
Bcdedit -store c:\pe_temp\BCD -set {guid} detecthal Yes
```

```
Bcdedit -store c:\pe_temp\BCD -set {guid} winpe Yes
```

```
Bcdedit -store c:\pe_temp\BCD -set {guid} osdevice  
ramdisk=[Boot]\Boot\boot.wim, {ramdiskoptions}
```

```
Bcdedit -store c:\pe_temp\BCD -set {guid} device  
ramdisk=[Boot]\Boot\boot.wim, {ramdiskoptions}
```

nastavení BOOTMGR, za {guid} se dosadí GUID hodnota:

```
Bcdedit -store c:\pe_temp\BCD -create {bootmgr} /d "Windows  
BootManager"
```

```
Bcdedit -store c:\pe_temp\BCD -set {bootmgr} timeout 0
```

```
Bcdedit -store c:\pe_temp\BCD -displayorder {guid}
```

dále se v "*Příkazový řádek nástrojů pro nasazení*" (Windows AIK) provede příkaz:

```
Dism /Unmount-Wim /MountDir:C:\winpe_x86\mount /discard
```

Nyní se obsah adresáře "c:\pe_temp" zkopíruje na PXE server.

7.5.2 Nastavení serveru

Tato část se provádí na serveru běžícím na Linuxu. V této části budou použity soubory z balíčku, který je popsán v kapitole 6.1.5. V adresáři "**tftpboot**" je nutno nakopírováním a vytvořením souborů vytvořit tuto strukturu:

```
/tftpboot/gpxelinux.0  
/tftpboot/pxelinux.cfg/default
```

Nyní se v adresáři "*tftpboot*" vytvoří adresář "*Boot*":

```
mkdir -p /tftpboot/Boot
```

a zkopírují se do něj soubory "BCD", "boot.sdi", "boot.wim", "bootmgr.exe" a "pxeboot.n12" ze složky "c:\pe_temp", tak aby platily cesty:

```
/tftpboot/Boot/BCD
/tftpboot/Boot/boot.sdi
/tftpboot/Boot/boot.wim
/tftpboot/Boot/bootmgr.exe
/tftpboot/Boot/pxeboot.n12
```

dále je nutno přejmenovat soubor "pxeboot.n12" na "pxeboot.0"

```
mv /tftpboot/Boot/pxeboot.n12 /tftpboot/Boot/pxeboot.0
```

Nyní se upraví dané konfigurační soubory do tvaru:

/etc/dhcp/dhcpd.conf:

```
default-lease-time 1800;
max-lease-time 3600;
authoritative;

subnet 192.168.0.0 netmask 255.255.0.0 {
    range 192.168.3.1 192.168.3.99;
    option subnet-mask 255.255.0.0;
    option broadcast-address 192.168.255.255;
    option domain-name-servers 8.8.8.8, 8.8.8.4;
    option routers 192.168.1.254;
    next-server 192.168.2.50;
    filename "gpxelinux.0";
}
```

/etc/default/tftpd-hpa:

```
# /etc/default/tftpd-hpa
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/tftpboot"
TFTP_ADDRESS="0.0.0.0:69"
TFTP_OPTIONS="--secure -m /etc/tftp_remap.conf"
RUN_DAEMON="yes"
```

Dále se vytvoří soubor `"/etc/tftp_remap.conf"`, který bude sloužit pro automatické nahrazování `"\"` používané u Windows na `"/` používané v systému Linux.

Obsah `/etc/tftp_remap.conf` [40]:

```
re bootmgr\ .exe /Boot/bootmgr.exe
rgG [\] /
```

Do `/tftpboot/pxelinux.cfg/default` vložit [41]:

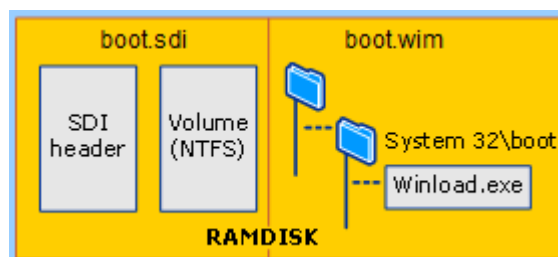
```
default Win_PE
label Win_PE
kernel Boot/pxeboot.0
```

7.5.3 Postup při bootování

Popis založen na [19] a [39] :

- 1) Klient si z PXE serveru stáhne soubor `"gpxelinux.0"` (NBP) a spustí jej (umožňuje zobrazit menu s výběrem operačního systému, automaticky vybrán Windows PE)
- 2) `"gpxelinux.0"` zavede `"pxeboot.0"` (NBP Windows PE) a spustí jej
- 3) `"pxeboot.0"` stáhne soubory `"Bootmgr.exe"` a `"BCD"`
- 4) `"Bootmgr.exe"` přečte informace v `"BCD"` a na jejich základě stáhne soubory `"boot.sdi"` a `"boot.wim"`
- 5) `"Bootmgr.exe"` připojí image systému `"boot.wim"`
- 6) Systém z image `"boot.wim"` nabootuje a provede přednastavené skripty

Soubor `"boot.sdi"` obsahuje NTFS svazek. Po spojení souborů `"boot.sdi"` a `"boot.wim"` vznikne výsledný ramdisk. Obr. 14 ukazuje výsledné složení ramdisku [19].



Obr. 14: Složení ramdisku Windows PE

7.5.4 Výhody řešení

Hlavní výhodou standardního řešení je použití oficiálně doporučeného postupu společnosti Microsoft (přizpůsobeného pro server běžící na operačním systému GNU/Linux) a snížení velikosti přenášených souborů na minimum.

7.5.5 Nevýhody řešení

Mezi hlavní nevýhody tohoto řešení patří problematické nastavení linuxového serveru a napevno stanovená adresářová struktura ve složce `"/tftpboot"`, která prakticky znemožňuje jakoukoliv změnu. V případě, že není dodržen postup zmíněný výše, skončí bootování chybou.

7.6 Bootování přes PXE (stažení ISO obrazu)

Ze serveru se stáhne image, který do operační paměti pracovní stanice stáhne ISO obraz a následně jej připojí jako lokální jednotku. Z jednotky je následně zaveden operační systém. [42]

7.6.1 Obsah ISO obrazu

Nezávisle na zavedení ze sítě, ISO soubor je obraz disku CD založený na jednotlivých sektorech a jeho primární účel je být vypálen na CD. Obraz disku se může vytvořit ve dvou verzích. Buď systém běží přímo z CD a do RAM jsou ukládány pouze změny oproti CD, nebo se celý obsah CD nejdříve zkopíruje do RAM a teprve potom se provede zavedení.

Disk vytvořený prvním způsobem pro svůj běh vyžaduje méně operační paměti, protože systém je umístěn na CD a veškeré potřebné informace jsou načítány přímo z CD, do RAM jsou ukládány pouze změny dat oproti CD a uživatelská data. Nevýhoda řešení je v tom, že systém potřebuje, aby bylo CD neustále vloženo v mechanice. Takto vytvořený ISO soubor obsahuje přímo jednotlivé soubory, celková velikost vytvořeného ISO obrazu je kolem 310 MiB. Po rozbalení ISO souboru do složky je ve složce 703 MiB dat. [43]

Disk vytvořený druhým způsobem potřebuje pro běh více operační paměti, protože se do operační paměti zkopíruje celý systém a následně se zruší závislost na CD. CD se tedy může vyjmout z mechaniky a do mechaniky se může vložit jiný disk. Takto vytvořený ISO

soubor obsahuje pouze komprimovaný *wim* soubor a soubory nutné pro zavedení systému. Takto vytvořené ISO má velikost okolo 132 MiB [34].

V případě bootování ze sítě nebude ISO obraz uložen na fyzickém CD (žádné CD nebude potřeba). Místo toho bude ISO soubor uložen na serveru, z něž se jako celek stáhne do operační paměti bootujícího počítače, v níž bude následně použit k zavedení systému.

Ačkoliv se pro zavedení ze sítě zdá být vhodnější první způsob, kdy je ISO soubor po zkopírování ze serveru do operační paměti cílového počítače už v RAM počítače obsažen, a tedy systém může naběhnout přímo z něj, čímž se ušetří místo v operační paměti (není potřeba, aby se Windows ještě jednou zkopírovala do RAM), bude z důvodu velikosti stahovaného ISO obrazu zvolen způsob dva.

Tento způsob bootování bude sice neefektivně využívat operační paměť cílového počítače, protože se do ní nejdříve stáhne ISO obraz CD a po nabooteování z něj si Windows vytvoří svůj vlastní ramdisk, do kterého nakopírují data a nabooteují z něj (zruší se závislost na původním ISO obrazu, soubory budou v RAM duplicitně), ale na druhou stranu mnohem méně zatíží síť, protože místo stahování 310 MiB dat se bude stahovat pouze 132 MiB dat. Předpoklad zde je, že pracovní stanice mají dostatek RAM, ale přenosové kapacity sítě jsou omezeny. Za dostatek operační paměti je považován 1 GiB RAM.

7.6.2 Vytváření ISO obrazu

Provedou se všechny body v kapitole 7.3 - Vytvoření spustitelného image se systémem.

Spustí se "**Příkazový řádek nástrojů pro nasazení**" [34]. Nyní se musí odstranit hláška "*Libovolnou klávesou spustíte systém s disku CD nebo DVD...*", která se objevuje před zavedením systému.

Provede se to tak, že se odstraní soubor "*c:\winpe_x86\ISO\boot\bootfix.bin*".

```
del c:\winpe_x86\ISO\boot\bootfix.bin
```

Nyní se soubor "*winpe.wim*" zkopíruje do adresáře "*ISO\sources*" a přejmenuje na "*boot.wim*".

```
copy c:\winpe_x86\winpe.wim c:\winpe_x86\ISO\sources\boot.wim
```

Smaže se složka "*c:\winpe_x86\ISO\EFI*", protože je zbytečná.

```
rmdir /s /q c:\winpe_x86\iso\efi
```

Nakonec se vytvoří ISO soubor.

```
oscdimg -n -bC:\winpe_x86\etfsboot.com C:\winpe_x86\ISO  
C:\winpe_x86\winpe_x86.iso
```

Výsledný soubor "*c:\winpe_x86\winpe_x86.iso*" se přesune na server.

7.6.3 Nastavení serveru

V adresáři "*/tftpboot*" je nutno vytvořit tuto strukturu (soubory je možno získat z balíku popsaného v kapitole 6.1.5):

```
/tftpboot/gpxelinux.0  
/tftpboot/memdisk  
/tftpboot/pxelinux.cfg/default
```

Nyní se zkopíruje soubor "*winpe_x86.iso*" do adresáře "*/tftpboot*", tak aby platila cesta:

```
/tftpboot/winpe_x86.iso
```

zkontroluje se, zda soubor ***/etc/dhcp/dhcpd.conf*** obsahuje:

```
next-server <IP adresa TFTP serveru>;  
filename "gpxelinux.0";
```

a do ***/tftpboot/pxelinux.cfg/default*** se vloží [42]:

```
default Win_PE  
label Win_PE  
linux /memdisk  
initrd /winpe_x86.iso  
append iso raw
```

7.6.4 Postup při bootování

Popis založen na [42].

- 1) Klient si z PXE serveru stáhne soubor "*gpxelinux.0*" (NBP) a spustí jej (umožňuje zobrazit menu s výběrem operačního systému, automaticky vybrán Windows PE)
- 2) "*gpxelinux.0*" stáhne přes protokol TFTP soubory "*memdisk*" a "*winpe_x86.iso*"
- 3) "*memdisk*" po spuštění připojí "*winpe_x86.iso*" jako CD disk
- 4) Bootování proběhne, jako by probíhalo standardně z CD
- 5) "*Bootmgr.exe*" připojí image systému "*boot.wim*"
- 6) Systém z image "*boot.wim*" naboootuje a provede přednastavené skripty

7.6.5 Výhody řešení

Hlavní výhodou tohoto řešení je možnost zavést jakýkoliv bootovatelný ISO obraz (je možné, že v jednotlivých případech budou nutné dílčí úpravy). Řešení je tedy univerzálně použitelné pro bootování jakéhokoliv Windows PE, případně live distribuce operačního systému Linux.

7.6.6 Nevýhody řešení

Mezi hlavní nevýhody tohoto řešení patří větší přenos dat po síti. Při použití standardního řešení (kapitola 7.5) se přenáší okolo 119 MiB dat, při použití tohoto řešení (za předpokladu, že je image systému stejný) se přenáší přibližně 132 MiB dat.

7.7 Bootování přes HTTP (stažení ISO obrazu)

Tento postup se velmi podobá předchozímu. Stejně jako v předchozím bodě se stáhne ISO obraz se systémem, který se nahraje do operační paměti lokálního počítače a následně se z něj zavede systém. Ke stahování je ovšem použit protokol HTTP.

7.7.1 ISO obraz

Obsah i vytváření ISO obrazu jsou shodné s postupem uvedeným v kapitole 7.6 - Bootování přes PXE (stažení ISO obrazu). K zavedení přes HTTP může být využit stejný ISO soubor nebo vytvořen nový. Jedinou změnou by bylo přidání podpory pro stahování balíčků s aplikacemi přes protokol HTTP, toto je řešeno v kapitole 7.4.

7.7.2 Nastavení serveru

Na PXE serveru v adresáři `"/tftpboot"` musí být vytvořena tato struktura (viz. kapitola 6.1.5):

```
/tftpboot/gpxelinux.0  
/tftpboot/pxelinux.cfg/default
```

Nyní je nutno nastavit webový server. Předpokládá se, že je kořenová složka webového (http) serveru dostupná na adrese `"http://192.168.1.100"` přes port 80.

V kořenové složce webového serveru je nutno vytvořit adresář `"win_pe"` a do něj vložit dříve vytvořený soubor `"winpe_x86.iso"`. Dále je nutno vytvořit adresář `"memdisk"` a do něj zkopírovat soubor `"memdisk"` (součást SYSLINUX).

Platí tedy cesty:

```
http://192.168.1.100/win_pe/winpe_x86.iso  
http://192.168.1.100/memdisk/memdisk
```

zkontroluje se, zda soubor `/etc/dhcp/dhcpd.conf` obsahuje:

```
next-server <IP adresa TFTP serveru>;  
filename "gpxelinux.0";
```

a do `/tftpboot/pxelinux.cfg/default` se vloží [42]:

```
default Win_PE
label Win_PE
linux http://192.168.1.100/memdisk/memdisk
initrd http://192.168.1.100/win_pe/winpe_x86.iso
append iso raw
```

V případě, že je http server provozován na jiném než výchozím portu, např. 85, provede se standardní doplnění portu do adresy.

```
http://192.168.1.100:85/memdisk/memdisk
http://192.168.1.100:85/win_pe/winpe_x86.iso
```

Místo IP adresy lze použít i doménové jméno (FQDN).

7.7.3 Postup při bootování

Popis založen na [42].

- 1) Klient si z PXE serveru stáhne soubor "*gpxelinux.0*" (NBP) a spustí jej (umožňuje zobrazit menu s výběrem operačního systému, automaticky vybrán Windows PE)
- 2) "*gpxelinux.0*" stáhne přes protokol HTTP soubory "*memdisk*" a "*winpe_x86.iso*"
- 3) "*memdisk*" po spuštění připojí "*winpe_x86.iso*" jako CD disk
- 4) Bootování proběhne, jako by probíhalo standardně z CD
- 5) "*Bootmgr.exe*" připojí image systému "*boot.wim*"
- 6) Systém z image "*boot.wim*" nabootuje a provede přednastavené skripty

7.7.4 Výhody řešení

Hlavní výhoda tohoto řešení spočívá v možnosti nabootovat jakýkoliv bootovatelný ISO obraz. K bootování se navíc používá protokol HTTP, tudíž odpadají problémy s velkou odezvou sítě.

V případě stahování souboru přes protokol TFTP musí být každý paket potvrzen příjemcem a teprve po doručení potvrzení o doručení předchozího paketu (ACK) se vysílá další paket (běžně 512 B). V daném okamžiku je v síti mezi odesílatelem a příjemcem vždy

maximálně jeden paket. Tento jev výrazně zpomaluje přenos dat na lince s vysokou odezvou, protože následující paket může být odeslán až v okamžiku, kdy se od druhé strany vrátí ACK předchozího paketu. TFTP používá pro přenos protokol UDP.

Při použití protokolu HTTP problém s vysokou odezvou sítě odpadá, protože se pro přenos používá metoda okénka (protokol TCP). V tomto případě se vždy potvrzuje až určité větší množství doručených paketů jako jeden celek. Na lince se tedy v jednom okamžiku může objevit více paketů, protože vysílací strana nemusí čekat na potvrzení jednotlivých paketů. Pokud dojde k chybě, jsou znovu vyslány pouze pakety, které přišly po posledním správně doručeném paketu.

7.7.5 Nevýhody řešení

Mezi hlavní nevýhody tohoto řešení patří nutnost provozovat webový server. Množství přenesených dat po síti je téměř shodné s případem, kdy je ISO obraz stahován pomocí protokolu TFTP.

7.8 Bootování přes protokol iSCSI (stažení do RAM)

V tomto případě se pro naboootování Windows PE využije síťový disk sdílený přes protokol iSCSI. Nebude sice využito možnosti OS streamingu, kdy by se data přenášela po jednotlivých souborech, jako by se četla z lokálního pevného disku, ale alespoň bude ukázáno, že lze Windows PE zavést i tímto způsobem.

7.8.1 Příprava

Nejdříve se na serveru vytvoří disk (o velikosti nejméně 150 MiB) a zpřístupní se přes protokol iSCSI (např. *192.168.1.199:::WindowsPE*). Následně se tento disk připojí ve Windows a vytvoří se na něm primární oddíl. Tento oddíl se dále zformátuje na souborový systém FAT32, nastaví se jako aktivní a připojí se jako lokální jednotka (zde "*M:*").

7.8.2 Přesun souborů na disk

Nejdříve se podle postupu 7.3.1 vytvoří image ("c:\winpe_x86\winpe.wim").

Nyní se v nabídce "**Start** → **Všechny programy** → **Microsoft Windows AIK**" spustí "**Příkazový řádek nástrojů pro nasazení**" a provedou se příkazy [44]:

```
copy c:\winpe_x86\winpe.wim c:\winpe_x86\ISO\sources\boot.wim
rmdir /s /q c:\winpe_x86\iso\efi
xcopy c:\winpe_x86\iso\*. * /e m:\
```

Nyní se iSCSI disk ve Windows odpojí.

7.8.3 Nastavení serveru

K nabotování tímto způsobem je nutné, aby adresář **"/tftpboot"** obsahoval (viz. kapitola 6.1.5):

```
/tftpboot/gpxelinux.0
/tftpboot/sanboot.c32
/tftpboot/pxelinux.cfg/default
```

Do souboru **/tftpboot/pxelinux.cfg/default** je nutno doplnit:

```
default Win_PE_iSCSI
label Win_PE_iSCSI
kernel sanboot.c32
append iscsi:192.168.1.199:::WindowsPE
```

Nyní stačí klientský počítač restartovat.

7.8.4 Výhody a nevýhody řešení

Teoreticky by se měla projevit výhoda ve vyšší přenosové rychlosti oproti protokolu TFTP, měření bohužel ukázala opak. Nejde ani tak o samotný přenos dat, jako spíše o celkové prodloužení doby zavedení systému (viz. kapitola 7.10). Mezi další nevýhodu patří nutnost provozovat disk sdílený přes protokol iSCSI.

7.9 Výběr operačního systému při spuštění počítače

7.9.1 Nutné podmínky pro vytvoření menu

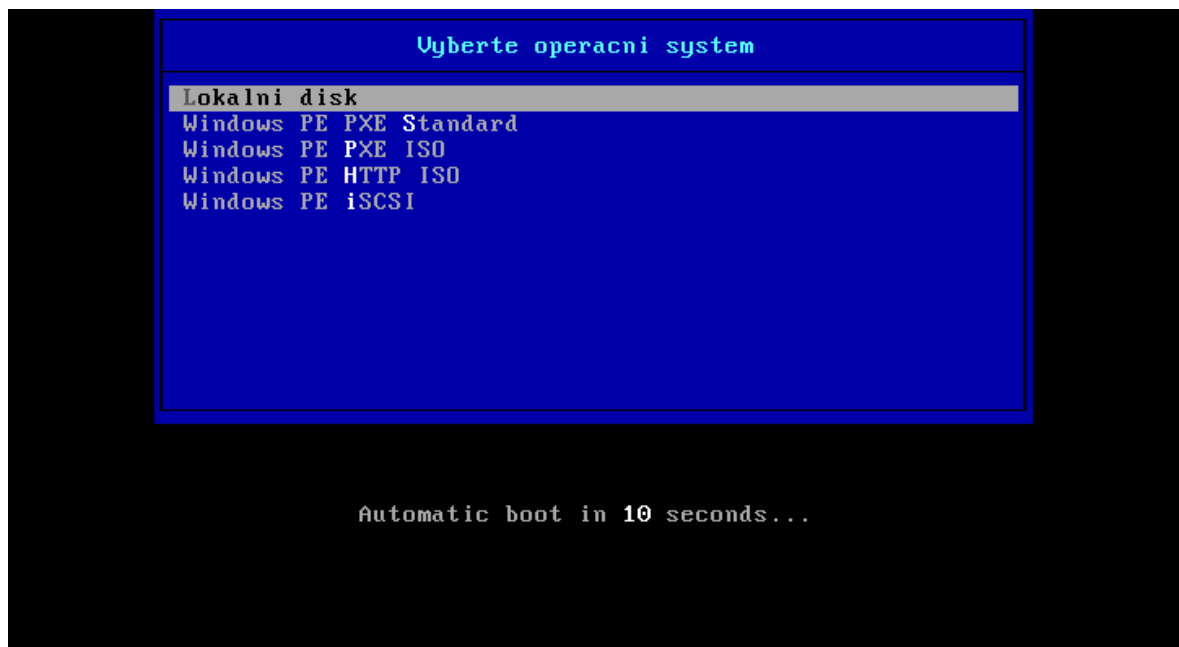
Aby bylo možné při spuštění počítače vybrat z více operačních systémů je nutno mít v adresáři **"/tftpbboot"** všechny potřebné soubory (viz. kapitola 6.1.5). Pro jednoduchý příklad menu uvedený zde je potřeba toto rozmístění:

```
/tftpbboot/gpxelinux.0  
/tftpbboot/menu.c32  
/tftpbboot/pxelinux.cfg/default
```

Pozn.: Soubory zde uvedené jsou nutné pro zobrazení samotného menu. Pro úspěšné zavedení systému je nutno přidat další soubory, které jsou popsány u jednotlivých způsobů zavádění.

7.9.2 Vytváření jednoduchého menu

Menu s operačními systémy může vypadat například takto:



Obr. 15: Výběr operačního systému při zavádění ze sítě

Aby bylo dosaženo menu výše, musí být soubor `/tftpboot/pxelinux.cfg/default` upraven do tvaru [25][26]:

```
default menu.c32
```

```
prompt 0
noescape 1
nocomplete 1
allowoptions 0
timeout 100
totaltimeout 300
```

```
menu title Vyberte operacni system
```

```
label Local
menu label ^Lokalni pevny disk
menu default
localboot 0
```

```
label Win_PE_STD
menu label Windows PE PXE ^Standard
kernel Boot/pxeboot.0
```

```
label Win_PE_ISO
menu label Windows PE ^PXE ISO
linux /memdisk
initrd /winpe_x86.iso
append iso raw
```

```
label Win_PE_HTTP
menu label Windows PE ^HTTP ISO
linux http://192.168.1.100/memdisk/memdisk
initrd http://192.168.1.100/win_pe/winpe_x86.iso
append iso raw
```

```
label Win_PE_SCSI
menu label Windows PE ^iSCSI
kernel sanboot.c32
append iscsi:192.168.1.199:::WindowsPE
```

7.9.3 Význam jednotlivých položek skriptu

Zde je popsáno, co jednotlivé volby ve skriptu znamenají. Z důvodu přehlednosti jsou volby seskupeny podle významu, který ve skriptu mají.

Nastavení týkající se výběru podoby menu:

`default menu.c32` na menu se použije modul "menu.c32"

Nastavení týkající se zvýšení bezpečnosti:

`prompt 0` nezobrazí příkazový řádek pro napsání vlastních parametrů, nutí uživatele vybrat pouze z nabízených voleb

`noescape 1` příkazový řádek nejde vyvolat ani stiskem kláves

`nocomplete 1` uživatel nemůže zobrazit parametry bootování na příkazové řádce

`allowoptions 0` uživatel nemůže dopsat vlastní parametry bootování

Nastavení délky čekání při výběru operačního systému:

`timeout 100` jak dlouho se má čekat než se automaticky nabojuje výchozí volba, hodnota v 1/10 s, odpočet lze přerušit stiskem libovolné klávesy, zde 10 s

`totaltimeout 300` za jak dlouho se má nabojet výchozí volba, pokud uživatel nevybere jinak před zadaným časem, čas udán v 1/10 s, zde 30 s

Nastavení titulku menu:

`menu title` titulek menu

Nastavení jednotlivých položek v menu:

`label` interní označení položky menu

`menu label` název volby zobrazený uživateli (např. název operačního systému), `te^xt` - stiskem písmene *x* vybereme danou volbu

`menu default` volba obsahující tento text je vybrána jako výchozí

`localboot 0` nabojuje z lokálního pevného disku, pokud dochází k neočekávanému chování (zatumnutí počítače, restart počítače), je možné zkusit volbu `localboot -1`

`kernel` parametrem je NBP konkrétního operačního systému

`linux` parametrem je jméno souboru s linuxovým jádrem, které se má zavést

`initrd` parametrem je jméno souboru s ramdiskem

`append` parametry předávané linuxovému jádru

7.10 Srovnání řešení z hlediska rychlosti bootování

Pro zjištění, která z možností zavádění Windows PE je nejvhodnější, byl proveden jednoduchý test rychlosti zavádění systému jednotlivými způsoby.

Měření probíhalo na 100 Mbit/s síti, která v okamžiku měření vykazovala nízké zatížení a minimální latence (~1ms). Ve všech případech se stahoval stejný image se systémem, někdy přímo, někdy jako součást ISO obrazu. TFTP i HTTP server běžel na *Debian 6*, iSCSI disk zabezpečoval *Openfiler 2.3*, oba servery byly virtualizovány programem *VirtualBox* na NB se procesorem Core i3 2.4 Ghz, 3 GiB RAM, 1 Gbit/s síťové rozhraní. Bootujícím počítačem byl Asus EEE 1000H, který byl připojen přes 100 Mbit/s switch.

Z důvodu metodiky měření jsou tyto hodnoty pouze orientační.

Způsob zavádění	Velikost stahovaného image [MiB]	Doba stahování image do RAM [min:sek]	Průměrná rychlost stahování [MiB/s]	Celková doba zavádění systému [min:sek]
Standardní PXE	116,7	1:12	1,62	2:29
ISO obraz PXE	128,3	1:08	1,88	2:27
ISO obraz HTTP	128,3	0:13	9,86	1:32
iSCSI disk	128,2	0:22	5,82	3:47

Tab. 7: Srovnání různých metod zavádění Windows PE z hlediska času

Z měření vyplývá, že jako nejvhodnější řešení se jeví stažení ISO obrazu přes protokol HTTP (kapitola 7.7). Při použití tohoto protokolu trvá stažení image systému do RAM bootujícího počítače pouze 13 sekund, což je oproti stahování protokolem TFTP více jak pětinasobné zrychlení. Po stažení image následuje samotné zavádění systému, které trvá přibližně 1 minutu a 19 sekund.

Zajímavý jev vykazuje bootování přes protokol iSCSI (kapitola 7.8), kdy je image systému stažen do RAM za 22 sekund, ale potom následuje zdlouhavé zavádění systému, což v konečném důsledku způsobí delší dobu zavádění, než při použití standardních PXE (TFTP) metod. Tento jev je pravděpodobně způsoben čekáním na splnění určité podmínky.

Z hlediska úspory přenosové kapacity je nejvhodnější použít standardní PXE řešení (kapitola 7.5), kde se oproti jiným metodám přenáší přibližně o 11,6 MiB dat méně.

Z praktického hlediska je ovšem z důvodu režie přenášeno větší množství dat, než je velikost stahovaného souboru. Skutečné množství přenášených dat je dáno velikostí stahovaného souboru a režii jednotlivých protokolů. Režie jednotlivých protokolů závisí na nastavení přenosu a kvalitě sítě (velikost potvrzovaných dat u TFTP, velikost paketu a okénka u HTTP a iSCSI, nutná znovu vyslání nedoručených dat a podobně).

7.11 Alternativní způsob vytvoření image se systémem

Zde bude ukázáno, jak vytvořit image pomocí programu **WinBuilder**. Vytvářeným systémem bude **Win7PE_SE**. Dále bude ukázáno, jak instalovat programy přímo do image se systémem.

Pozn.: zde vytvářený image se systémem nemá nic společného s hlavním řešením - *Windows PE 3.0* a zaváděním programů ze síťového disku - je to zcela nezávislý alternativní postup, který má ukázat další způsob vytvoření "Windows PE". Přestože se jedná o odlišný systém, formát vytvořeného image je shodný s *Windows PE 3.0* a je jej tedy možné zavádět stejnými způsoby, jako oficiální *Windows PE* (stažení ISO obrazu přes PXE, stažení ISO obrazu přes HTTP, boot přes protokol iSCSI).

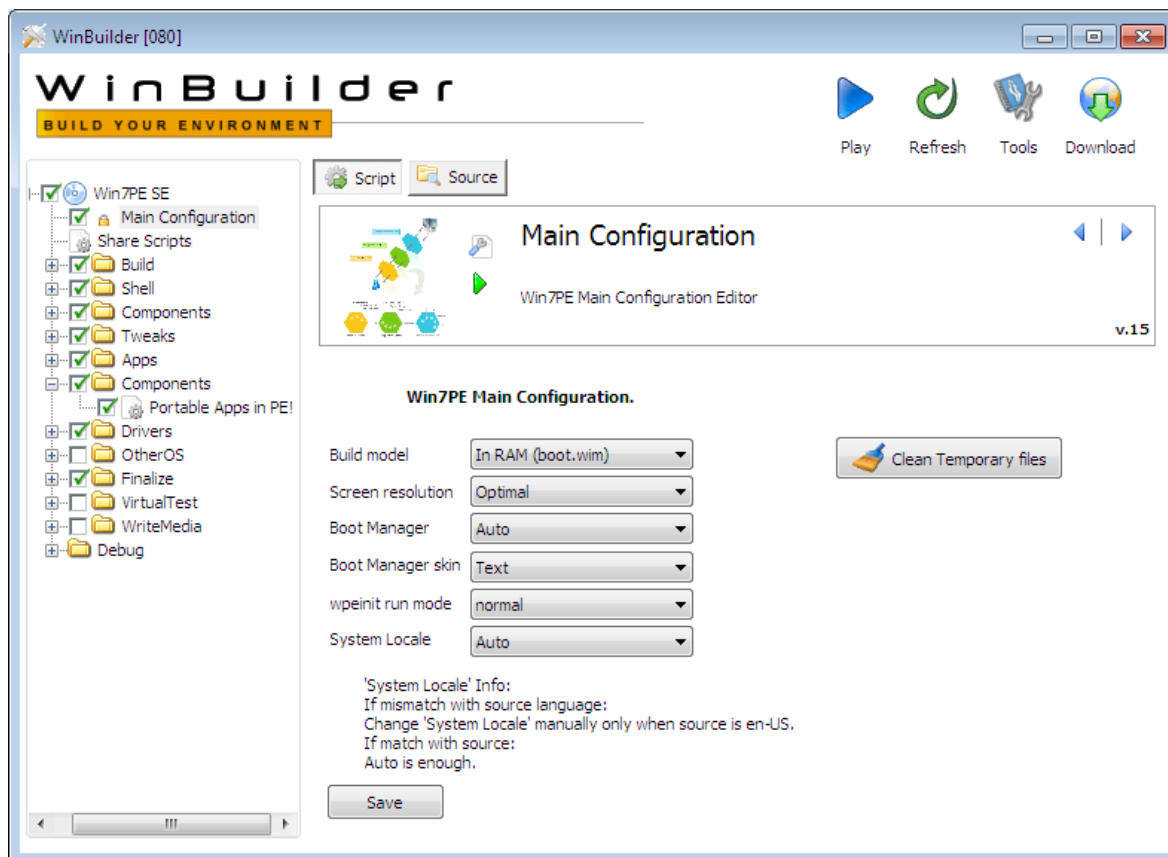
Tento postup se podařilo zprovoznit, pouze pokud byl program *WinBuilder* nainstalován ve *Windows 7* (anglická verze, volume license), v systému byl nainstalován *Windows AIK 3.0* v anglické verzi a jako instalační médium (soubory) bylo vloženo *Windows 7* (anglická verze, volume licence). Pokud byl *Windows 7* nebo *AIK* v české jazykové mutaci, příp. verze *Windows 7* z MSDNAA, skript v programu *WinBuilder* vygeneroval chybu.

7.11.1 Stažení projektu Win7PE_SE

Nejdříve se musí z internetu stáhnout soubory projektu. Ty se dají sehnat např. zde [47]. Pro vytvoření popisu zde byla použita verze *Win7PE_SE_2011_02_10*, daná verze je součástí příloh. Stažený soubor se může rozbalit např. na disk "C:\\" (odstraní se tím problémy, které by mohly vzniknout tím, že cesta k souboru "*WinBuilder.exe*" obsahuje mezery mezi slovy). Pro potřeby instalace programů je potřeba stáhnout plugin "*ppAppsGen*"[48], rozbalit jej a zkopírovat jej do rozbalené složky s projektem. Pokud je složka s projektem `C:\Win7PE_SE`, zkopíruje se rozbalený soubor "*ppAppsGen.script*" do `C:\Win7PE_SE\Projects\Win7PE_SE\Components`.

7.11.2 Prostředí programu WinBuilder

Program WinBuilder se spustí poklepnutím na soubor "*WinBuilder.exe*" v kořenové složce projektu.



Obr. 16: Okno programu WinBuilder

Okno se skládá ze dvou hlavních částí, v levé jsou zaškrťovací políčka - zde je možné zvolit jednotlivé komponenty systému a položky nastavení. V pravé části okna se nachází samotné nastavení dané komponenty. Zde je možné provést různá nastavení dle libosti, důležitá jsou ovšem pouze tato:

- V "**Main Configuration**" nutno zvolit položky "**Build model**" na "**InRAM**" (menší velikost výsledného souboru) a "**Boot Manager**" na "**Auto**" (nezobrazí výběr operačních systémů).
- V "**Build**" (levý panel) vybrat "**2 - Shell & Config**" a nastavit "**FBWF cache size**" na 512 MB.
- Odškrtnout volbu "**OtherOS**" (levý panel).

7.11.3 Nepřipojení lokálních disků při startu Windows

Pro automatické nepřipojování lokálních disků pracovní stanice lze použít úprava registru [36][50].

V adresáři "C:\Win7PE_SE\Projects\Win7PE_SE\Tweaks" je nutno vytvořit soubor

"**DontMountHDD.script**", který obsahuje text:

```
[main]
Title=Don't mount local hard drives
Type=Script
Selected=True
Level=7

[Process]
RegHiveLoad,Tmp_System,%RegSystem%
RegWrite,HKLM,0x4,Tmp_System\ControlSet001\services\mountmgr,NoAutoMount,1
RegWrite,HKLM,0x4,Tmp_System\ControlSet001\services\partmgr\Parameters,SanPolicy,3
RegHiveUnLoad,Tmp_System
```

Soubor je nutno uložit, restartovat program *WinBuilder* a ujistit se, že je v nabídce "**Tweaks**" zaškrtnuta volba "**Don't mount local hard drives**".

Pozn.: Novější verze Win7PE_SE obsahuje v nabídce "Finalize → Optimizations" volbu "Don't mount local harddrives", tato volba byla do programu přidána z podnětu dotazu, který byl formulován na diskusním fóru v rámci vytváření této práce. [36]

7.11.4 Instalace programu přímo do Windows PE

Pro instalaci programu přímo do Windows PE je buď nutno manuálně upravit registry a nahrát potřebné soubory už při vytváření systému, nebo je možno použít skript *ppAppsGen* (návod založen na [48]), který se při spuštění systému automaticky postará o přidání potřebných informací do registru a vytvoření zástupců. Zde je uvedeno, jak instalovat programy za pomoci daného skriptu.

V první řadě je potřeba se ujistit, že je v programu *WinBuilder* zaškrtnuta volba "**Components**" a podvolba "**Portable Apps in PE!**". Dále je nutno v nabídce "**Finalize**" odškrtnout volbu "**4 - Create ISO**".

Nyní je potřeba přepnout se v levém menu na "**Finalize**", vybrat "**PostConfig**", zvolit "**Compression: maximum**" a kliknout na ikonu velkého modrého "**Play**" v hlavním okně programu. Proběhne vytvoření souboru "*boot.wim*".

Jako ukázkový instalovaný program bude použit multimediální přehrávač "**VLC player**".

Instalace se skládá ze dvou fází, nejdříve se program nainstaluje do lokálního počítače a zachytí se zápisy do registrů při instalaci programu, následně se tyto zápisy vyexportují do "**.reg*" souboru a spolu se soubory nainstalovaného programu se uloží do struktury vytvářeného Win7PE.

Zachycení zápisů do registru se provede např. pomocí programu "**Advanced Registry Tracer**"[49] společnosti *Elcomsoft*, který se nainstaluje do referenčního počítače.

Postup je následující:

- Spustí se "**Advanced Registry Tracer**" a klikne se na ikonu "**Scan Registry**".
- Do referenčního počítače se nainstaluje program, který bude vyexportován do PE.
- V "**Advanced Registry Tracer**" se klikne na ikonu "**Compare**". V zobrazeném okně se vybere záložka "**Distinction in data**" a následně se klikne na ikonu "**Save to Redo files**" a uloží se soubor "*nazev.reg*" obsahující změny registru oproti předchozímu scanu.

Nyní je potřeba soubor "**.reg*" manuálně prohlédnout, upravit cesty k souborům a smazat zbytečná data. Tento postup se u různých programů liší.

V případě programu VLC je nutné v souboru "*vlc.reg*" nahradit řetězec:

```
C:\\Program Files\\VideoLAN\\VLC za Y:\\ppApps\\VLC,
```

čímž se změní cesta ke složce s programem tak, aby odpovídala umístění složky ve Windows PE, dále je nutné provést dílčí vyčištění souboru od zbytečných informací.

Dále je potřeba vytvořit složku "*ppApps*", například na disku "C:\\" a zkopírovat do ní programové soubory. Vytvořená složka zde je C:\ppApps.

V případě přehrávače VLC se v souladu s nahrazovanou cestou v registru zkopíruje složka C:\Program Files\VideoLAN\VLC do C:\ppApps\VLC.

Nyní je nutno přejmenovat daný "*.reg" soubor na "**setups.reg**" a umístit jej do složky s programem, v případě přehrávače VLC tedy platí cesta: C:\ppApps\VLC\setups.reg.

Do složky s programem (C:\ppApps\VLC) je dále nutno (vedle "*setups.reg*") přidat konfigurační soubor s informacemi pro vytváření zástupců. Daný soubor se jmenuje "**ppApp.ini**" a jeho syntaxe pro VLC přehrávač je následující:

```
<Title>
VLC player           ;Titulek programu

<Flags>
MakeInRoot = 0       ;Nevytvářet "připnutého" zástupce ve Start
MakeStart = 1        ;Vytvořit zástupce ve Start
MakeSendTo = 0       ;Nevytvářet kontextový odkaz "Send To"
MakeDesktop = 1      ;Vytvořit zástupce na ploše
MakeQuickLaunch = 0 ;Nevytvářet na panelu rychlého spuštění

<StartMenuSourcePath>
VLC player           ;Umístění zástupce v nabídce Start

<ppApp>
CommandLine = "vlc.exe"           ;Jméno spustitelného souboru
ShortcutName = "VLC player"       ;Titulek zástupce
Description = "Plays everything"   ;Popis zástupce

<End>
```

Nyní se v programu *WinBuilder* v nabídce "**Debug**" vybere volba "**Mount**". Zde je potřeba se ujistit, že volba "**Mount Point**" je nastavena na "%BaseDir%\Mount" a následně v oblasti "*Mount PE (Target)*" kliknout na tlačítko "**Mount**".

Po úspěšném připojení souboru "*boot.wim*" je nutno zkopírovat složku "*C:\ppApps*" do složky "*C:\Win7PE_SE\Mount*", tak aby platila cesta *C:\Win7PE_SE\Mount\ppApps* a v programu *WinBuilder* kliknout na tlačítko "**UnMount**".

7.11.5 Vytvoření image se systémem

Před vytvářením ISO souboru se systémem je zapotřebí přepnout se v levém menu na "**Finalize**", vybrat "**Create ISO**" a odznačit volbu "**Enable press any key to boot option**". Dále pravým tlačítkem myši kliknout na "**4 - Create ISO**" a z kontextové nabídky zvolit "**Run this script**".

Na konci tohoto procesu je ve složce "*C:\Win7PE_SE\ISO*" ISO soubor, který může být buď přímo nakopírován na server, nebo vyextrahován do složky. V této složce se pak nachází soubor "*boot.wim*", který může být naboootován po síti.

7.12 Přínos pro administraci počítačů na FAI UTB

Zavádění Windows PE ze sítě popsané zde může být efektivně využito ke správě počítačů v budově FAI UTB ve Zlíně. V případě použití technologie stažení ISO obrazu do RAM počítače a jeho následného spuštění (kapitola 7.6) je možno zavést systém startující z CD/DVD přes síť a na cílovém počítači jej spustit. Na serveru může být předpřipraveno několik ISO souborů různých operačních systémů - např. Windows PE určené pro běžné použití, Windows PE obsahující antivirové a systémové nástroje na diagnostiku počítače a záchranu dat, live verze Linuxu pro běžné použití, live verze Linuxu obsahující diagnostické nástroje, nebo například ISO obraz média pro obnovení poškozeného obrazu disku na lokální stanici (jednotlivé systémy musí být speciálně upraveny, aby byly schopny číst z takto zavedeného ISO souboru).

Administrátor pouze v BIOSu počítače nastaví zavádění systému ze sítě, načež se mu po restartu počítače zobrazí menu (kapitola 7.9) s výběrem operačních systémů, z nabídky vybere operační systém dle svých potřeb a volbu potvrdí. Po dokončení práce s vybraným operačním systémem jednoduše v BIOSu počítače vypne zavádění systému ze sítě a počítač může dál bootovat z lokálního pevného disku.

Řešení zavádění ISO obrazu není z hlediska využití přenosové kapacity sítě a operační paměti zaváděného počítače ideální a navíc vyžaduje speciální úpravu zaváděného operačního systému, ale v konečném důsledku poskytuje unifikovanou platformu pro zavedení téměř jakéhokoliv upraveného ISO obrazu ze sítě. Pro stahování může být použit protokol HTTP (kapitola 7.7), který efektivně využije dostupnou propustnost sítě, všechny operační systémy mohou být přístupné přes jedno společné menu (kapitola 7.9) při startu počítače.

Z hlediska momentálního stavu sítě v budově FAI UTB, kdy je celá budova U5 připojena optickými vlákny s propustností 1 Gbit/s k hlavnímu L3 switchi v budově U13, mezi jednotlivými IDF rozvodnami je zapojen 1 UTP kabel CAT6 s propustností 1 Gbit/s a většina koncových počítačů je zapojena tak, že 23 počítačů sdílí jednu 100 Mbit/s linku, se zdá být stažení ISO obrazu do RAM počítače a následné odstranění závislosti zaváděného operačního systému na síti nejvhodnějším řešením. Popis sítě vychází z [51].

Využití Windows PE jako náhrada plné verze Windows se nezdá být optimálním řešením. Windows PE lze sice použít pro nejběžnější úkony, jako je prohlížení webových stránek nebo psaní jednoduché práce v textovém editoru, ale z hlediska bezpečnosti a nižší uživatelské přívětivosti je tento systém vhodný pouze pro případy nouzového nasazení na stanici bez lokálního pevného disku, nebo jako mocný nástroj určený pro administraci lokálně instalovaných Windows.

ZÁVĚR

Proces zavádění operačního systému Windows ze sítě není až tak jednoduchý, jak se na první pohled mohlo zdát. V cestě stojí hlavně technické překážky, které komplikují, případně přímo zabraňují, zavést systém tímto způsobem.

V teoretické části práce byly popsány možné způsoby zavedení systému Windows ze síťového serveru, u každého způsobu byly zmíněny možné problémy, výhody a nevýhody. Podrobně byl rozebrán způsob, jak systém zavést přes protokol iSCSI za pomoci serveru s operačním systémem GNU/Linux. Dále bylo popsáno komerční řešení CCBoot a zmíněny výhody a nevýhody systému Windows PE.

V praktické části byla zpočátku realizována možnost zavedení plné verze systému přes protokol iSCSI, kterou se ovšem přes veškerou snahu a úsilí nepodařilo z důvodu technického vybavení počítačů v budově FAI UTB realizovat. Dalším prakticky realizovaným způsobem bylo zavedení Windows PE ze sítě. Toto se podařilo plně realizovat přes několik protokolů - PXE, HTTP a iSCSI. Zřetel byl brán rovněž na zabezpečení a správu Windows, kde byly popsány základní principy instalace programů do Windows PE a nepřipojení lokálních disků pracovní stanice po naboťování Windows. Všechny postupy jsou podrobně zdokumentovány a popsány.

Největší překážkou pro zavedení plné verze systému Windows přes síť je fakt, že Windows při bootování na síťový disk zapisují, což bez dalších úprav na straně serveru znemožňuje spouštět více počítačů současně z jednoho sdíleného image se systémem. Dalším problémem jsou rozdílné hardwarové konfigurace klientských počítačů. Pokud je změna hardwaru počítače, na němž je systém zaváděn, minimální oproti počítači, skrze nějž byl systém na síťový disk nainstalován, je systém zaveden bez problému. Při větších změnách v hardwaru, jako je například změna výrobce čipové sady nebo změna výrobce síťové karty, systém havaruje s chybou STOP.

Teoretické poznatky a praktické postupy uvedené zde mohou posloužit pro praktické nasazení Windows PE v síti FAI UTB, případně pro zvážení dalších způsobů zavádění Windows ze sítě.

ZÁVĚR V ANGLIČTINĚ

Boot up process of Windows operating system over a network is not as easy as it at first look seemed to be. There are many technical obstacles which complicate or directly prevents boot up system in this way.

In theoretical part, there is a description of possible ways how to boot up system Windows from a network server. Each method has mentioned eventual problems, advantages and disadvantages. There is in-depth description of the way how to boot up system over protocol iSCSI using server running operating system GNU/Linux. Furthermore, there is description of commercial solution called CCBoot and there are mentioned advantages and disadvantages of system Windows PE.

In practical part, there was initially realized method using protocol iSCSI to boot up full version of system Windows. This method was despite great effort which was put in it unrealized due to technical limitations of computers in FAI TBU building. Another practically realized method was boot up of system Windows PE over a network. Realization of this method was fully accomplished via several protocols - PXE, HTTP and iSCSI. Special care was dedicated to security and management of Windows, in this part there were described basic principles which apply to installation of programs directly into Windows PE and unmounting hard drives of local workstation after Windows boot up. All steps are in-depth documented and described.

The biggest obstacle which occurs when full version of system Windows have to be booted over a network is that Windows during startup stage write to network shared hard drive. This demands special adjustments on server side which will allow booting more than one computer at a time from one shared image with the system. Another big problem is different hardware configuration on each booted machine. If there is a very small change in hardware configuration between computer, through which Windows were installed to shared drive and computer which is booting Windows, the boot up process will end up successfully, otherwise it could crash with an STOP error.

Theoretical knowledge and practical steps mentioned here could help to facilitate practical deployment of Windows PE in FAI TBU network or be used to consider another ways of booting Windows over a network.

SEZNAM POUŽITÉ LITERATURY

- [1] BOTT, Ed; SIECHERT, Carl; STINSON, Craig. Windows 7 Inside Out. 1st edition. Redmond (Washington) : Microsoft Press, 2009. 1056 s. ISBN 0735626650, 978-0735626652.
- [2] MUELLER, Scott. Osobní počítač: hardware, upgrade, opravy. Přeložil Milan Daněk. 1. vyd. Brno: Computer Press, 2003, 862 s. ISBN 80-7226-796-5.
- [3] Etherboot Project [online]. 2006/04/21, 2011/03/26 [cit. 2011-04-17]. Etherboot/gPXE Wiki. Dostupné z WWW: <<http://etherboot.org/wiki/start>>.
- [4] IPXE - open source boot firmware [online]. 2011/03/29 [cit. 2011-04-17]. Frequently asked questions. Dostupné z WWW: <<http://ipxe.org/faq>>.
- [5] Intel Corporation. Preboot Execution Environment (PXE) Specification : Version 2.1 [online]. S.l. : S.n., September 20, 1999 [cit. 2011-04-16]. Dostupné z WWW: <<http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf>>.
- [6] GoogleTechTalks. gPXE: Modern FOSS Network Booting. In Youtube. [online video] 14.08.2008 [cit. 2011-04-16]. Dostupné z WWW: <<http://www.youtube.com/watch?v=GofOqhO6VVM>>.
- [7] POELKER, Christopher; NIKITIN, Alex. Storage Area Networks For Dummies. 2nd edition. Hoboken (New Jersey): Wiley Publishing, Inc., 2009. 456 s. ISBN 978-0-470-38513-5.
- [8] Network Working Group. The RFC Archive [online]. September 2nd, 2005 [cit. 2011-04-17]. RFC 4173 - Bootstrapping Clients using the Internet Small Computer System Interface (iSCSI) Protocol. Dostupné z WWW: <<http://www.rfc-archive.org/getrfc.php?rfc=4173>>.
- [9] OREMAN, Joshua. Introduction to Network Booting. In Vimeo. [online video] May 22, 2010 [cit. 2011-04-17]. Dostupné z WWW: <<http://vimeo.com/11948216>>.
- [10] Microsoft Corporation. Windows [online]. August 21, 2009 [cit. 2011-04-17]. iSCSI Boot Firmware Table (iBFT). Dostupné z WWW: <<http://msdn.microsoft.com/cs-cz/windows/hardware/gg463105>>.

- [11] HAVRÁNEK, Michal. Problematika bootování operačního systému Microsoft Windows. Zlín, 2009. 89 s. Bakalářská práce. UTB ve Zlíně.
- [12] Microsoft Corporation. Windows may fail to boot from an iSCSI drive [online]. September 24, 2009 [cit. 2011-04-17]. Dostupné z WWW: <<http://support.microsoft.com/kb/976042>>.
- [13] Etherboot Project [online]. 2008/07/17, 2011/01/22 [cit. 2011-05-07]. Installing Windows Server 2008 to an iSCSI target. Dostupné z WWW: <http://etherboot.org/wiki/sanboot/win2k8_iscsi_install>.
- [14] CCBoot - iSCSI Boot Windows XP, 2003, Vista, Windows7 and 2008 [online]. © 2011 [cit. 2011-03-20]. Home. Dostupné z WWW: <<http://www.ccboot.com>>.
- [15] CCBoot - iSCSI Boot Windows XP, 2003, Vista, Windows7 and 2008 [online]. © 2011 [cit. 2011-03-20]. Features. Dostupné z WWW: <<http://www.ccboot.com/features.htm>>.
- [16] CCBoot - iSCSI Boot Windows XP, 2003, Vista, Windows7 and 2008 [online]. © 2011 [cit. 2011-03-20]. Purchase. Dostupné z WWW: <<http://www.ccboot.com/purchase.htm>>.
- [17] CCBoot - iSCSI Boot Windows XP, 2003, Vista, Windows7 and 2008 [online]. © 2011 [cit. 2011-03-20]. Downloads. Dostupné z WWW: <<http://www.ccboot.com/download.htm>>.
- [18] TULLOCH, Mitch; NORTHRUP, Tony; HONEYCUTT, Jerry. Windows 7 Resource Kit. 1st edition. Redmond (Washington) : Microsoft Press, 2009. 1760 s. ISBN 0735627002, 978-0735627000.
- [19] Microsoft TechNet [online]. May 8, 2008 [cit. 2011-03-02]. How Booting into a Boot Image Works. Dostupný z WWW: <[http://technet.microsoft.com/en-us/library/cc771845\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc771845(WS.10).aspx)>.
- [20] KOHOUT, Petr. Nasazení bezdiskových pracovních stanic s OS Linux v síti FAI UTB. Zlín, 2008. 70 s. Bakalářská práce. UTB ve Zlíně.
- [21] SANDeploy iSCSI SAN Server [online]. © 2010 [cit. 2011-05-10]. SANDeploy Boot Server. Dostupné z WWW: <<http://www.sandeploy.com/SANDeploy-Boot-Server.php>>.

- [22] Linux : Dokumentační projekt. [s.l.] : Computer Press, 2008. 1336 s. Dostupné z WWW: [http://ii.iinfo.cz/r/kd/LDP_4.pdf]. ISBN 978-80-251-1525-1.
- [23] Etherboot project [online]. 2011 [cit. 2011-05-08]. ROM-o-matic.net. Dostupné z WWW: <<http://rom-o-matic.net/gpxe/gpxe-git/gpxe.git/contrib/rom-o-matic>>.
- [24] Etherboot project [online]. 2007/08/12, 2010/07/14 [cit. 2011-05-08]. PXE chainloading. Dostupné z WWW: <<http://etherboot.org/wiki/pxechaining>>.
- [25] Syslinux [online]. 21 July 2006, 30 October 2010 [cit. 2011-03-06]. SYSLINUX. Dostupné z WWW: <<http://syslinux.zytor.com/wiki/index.php/SYSLINUX>>.
- [26] Syslinux [online]. 21 July 2006, 3 November 2010 [cit. 2011-03-06]. PXELINUX. Dostupné z WWW: <<http://syslinux.zytor.com/wiki/index.php/PXELINUX>>.
- [27] Syslinux [online]. 1 November 2007, 19 October 2010 [cit. 2011-05-08]. Download. Dostupné z WWW: <<http://syslinux.zytor.com/wiki/index.php/Download>>.
- [28] Openfiler [online]. © 2009 [cit. 2011-05-08]. Openfiler Community. Dostupné z WWW: <<http://www.openfiler.com/community>>.
- [29] Openfiler [online]. © 2009 [cit. 2011-05-08]. Administrator Guide. Dostupné z WWW: <<http://www.openfiler.com/buy/administrator-guide>>.
- [30] Gregory Strike [online]. 2010/08/01 [cit. 2011-05-09]. WinPE v3.0 and Microsoft iSCSI Initiator. Dostupné z WWW: <<http://www.gregorystrike.com/2010/01/08/winpe-v3-0-and-microsoft-iscsi-initiator>>.
- [31] iPXE - open source boot firmware [online]. 2011/04/07 [cit. 2011-05-09]. Home. Dostupné z WWW: <<http://ipxe.org>>.
- [32] PortableApps.com [online]. 2011-03-11 [cit. 2011-03-19]. Portable App Directory. Dostupné z WWW: <<http://portableapps.com/apps>>.
- [33] SS64 [online]. © 2011 [cit. 2011-02-28]. Create shortcut. Dostupné z WWW: <<http://ss64.com/nt/shortcut.html>>.
- [34] Microsoft TechNet [online]. October 22, 2009 [cit. 2011-03-03]. Walkthrough: Create a Bootable Windows PE RAM Disk on CD-ROM. Text v angličtině. Dostupný z WWW: <[http://technet.microsoft.com/en-us/library/dd799303\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd799303(WS.10).aspx)>.

- [35] 7-Zip [online]. © 2011 [cit. 2011-02-27]. Download. Dostupné z WWW: <<http://www.7-zip.org/download.html>>.
- [36] Reboot.pro [online]. 12 April 2011 [cit. 2011-05-10]. How to not attach local HDD. Dostupné z WWW: <<http://reboot.pro/14298/>>.
- [37] Explorer++ [online]. © 2011 [cit. 2011-02-27]. Home. Dostupné z WWW: <<http://www.explorerplusplus.com>>.
- [38] All About Windows PE 2.x [online]. June 4, 2008 [cit. 2011-03-03]. Change the Desktop Resolution. Dostupné z WWW: <<http://winpe2.blogspot.com/2008/06/change-desktop-resolution.html>>.
- [39] Microsoft TechNet [online]. October 22, 2009 [cit. 2011-03-02]. Walkthrough: Deploy an Image by Using PXE. Dostupný z WWW: <[http://technet.microsoft.com/en-us/library/dd744541\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd744541(WS.10).aspx)>.
- [40] Good to Know Database [online]. 27.11.2009 [cit. 2011-03-04]. WinPE 3.0: Windows PE 3.0 via PXE booten. Dostupné z WWW: <http://www.gtkdb.de/index_17_797.html>.
- [41] MSFN [online]. 29 November 2006 [cit. 2011-03-04]. PXELinux Boot WinPE 2.0 . Dostupné z WWW: <<http://www.msfm.org/board/topic/87664-pxelinux-boot-winpe-20>>.
- [42] Save Lono [online]. Mar 09 2010 [cit. 2011-03-05]. How to Install Windows 7 over a Network using Linux - PXE, DNSMasq, and Samba. Dostupné z WWW: <<http://www.savelono.com/linux/how-to-install-windows-7-over-a-network-using-linux-pxe-dnsmasq-and-samba.html>>.
- [43] Microsoft TechNet [online]. October 22, 2009 [cit. 2011-03-04]. Walkthrough: Boot Windows PE from CD-ROM. Dostupný z WWW: <[http://technet.microsoft.com/en-us/library/dd744537\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd744537(WS.10).aspx)>.
- [44] Microsoft TechNet [online]. October 22, 2009 [cit. 2011-03-06]. Walkthrough: Create a Bootable Windows PE RAM Disk on a USB Flash Disk. Dostupný z WWW: <[http://technet.microsoft.com/en-us/library/dd744530\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd744530(WS.10).aspx)>.
- [45] GNU Operating System [online]. 2010/11/23 [cit. 2011-03-05]. GNU Wget. Dostupné z WWW: <<http://www.gnu.org/software/wget>>.

[46] GnuWin32 (sourceforge.net) [online]. 2011 [cit. 2011-03-05]. Wget for Windows. Dostupné z WWW: <<http://gnuwin32.sourceforge.net/packages/wget.htm>>.

[47] ChrisR. Reboot.pro : Win7PE_SE Release [online]. 06 September 2010 [cit. 2011-04-15]. Dostupné z WWW: <<http://reboot.pro/12427/>>.

[48] Amalux. Reboot.pro : Newcomer's Tutorial - LiveXP, Win7PE & Portable Apps! [online]. 08 March 2008 [cit. 2011-04-15]. Dostupné z WWW: <<http://reboot.pro/4111/>>.

[49] Elcomsoft. Elcomsoft Productive Software : Advanced Registry Tracer [online]. © 2011 [cit. 2011-04-15]. Dostupné z WWW: <<http://www.elcomsoft.com/art.html>>.

[50] Paraglider BartPE Plugins [online]. © 2011 [cit. 2011-05-12]. Script syntax. Dostupné z WWW: <http://www.paraglidernc.com/winbuilder/Help/scripts/script_syntax.html>.

[51] KORBEL, Jiří. Struktura počítačové sítě budovy U5 a připojení k Internetu. Zlín, 2011. 1 s. Interní dokument. UTB ve Zlíně.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

- ACK** Acknowledgement - zpráva, kterou posílá přijímající zařízení odesílajícímu zařízení jako potvrzení o doručení / nedoručení dat. ACK pakety se využívají v protokolu TCP.
- BIOS** Basic Input/Output System - program, který je uložen na základní desce. Po spuštění počítače inicializuje a zkonfiguruje připojená hardwarová zařízení a následně předá řízení operačnímu systému.
- BSOD** Blue Screen Of Death - slangové označení pro chybové hlášení systému Windows. Chyba je tak závažná, že se z ní systém nedokáže sám zotavit. Hlášení mívá obvykle podobu modré obrazovky s bílým textem, obsahuje kód chyby a její symbolický název. V případě, že tato chyba nastane, není možné se systémem dále pracovat a počítač je nutno restartovat.
- CIFS** Common Internet File System - síťový komunikační protokol pro přístup ke sdíleným souborům a tiskárnám. Protokol je znám také pod jménem SMB.
- DHCP** Dynamic Host Configuration Protocol - protokol sloužící pro automatickou konfiguraci zařízení v sítích s protokolem IP. Klient pomocí všesměrového vysílání požádá server o přidělení údajů nutných pro připojení k síti, server následně tyto údaje klientovi poskytne.
- DNS** Domain Name System - je hierarchický jmenný systém postavený na distribuované databázi. Hlavní využití systému je v síti Internet, kde slouží k překladu snadno zapamatovatelných doménových jmen na IP adresu počítače.
- EEPROM** Electrically Erasable Programmable Read-Only Memory - elektricky mazatelná a programovatelná paměť, která se používá pro uchování malého množství dat. Data jsou zachována i při odpojení napájení. Tato paměť je často používána k uložení BIOSu, případně jiného firmwaru.

FAT	File Allocation Table - souborový systém založený na alokační tabulce souborů. Systém byl původně využíván v operačním systému MS-DOS, nepodporuje transakční zpracování ani bezpečnostní prvky. Jedním z typů tohoto systému je FAT32.
FQDN	Fully Qualified Domain Name - doménové jméno, které specifikuje přesné umístění v hierarchii systému DNS. V jeho zápise se nacházejí všechny doménové stupně počínaje kořenovou doménou, pokračující všemi subdoménami až k názvu samotného prvku, který doména identifikuje.
GUID	Globally Unique Identifier - unikátní globální identifikátor. Unikátní 128-bitové číslo reprezentované 32 znakovým hexadecimálním řetězcem, které je v případě potřeby vygenerováno. Pravděpodobnost, že budou na světě vygenerována 2 stejná čísla, je zanedbatelná.
IP	Internet Protocol - komunikační protokol starající se o doručování a směrování paketů v síti Internet. Jednotlivá komunikující zařízení jsou označena IP adresou. Existuje ve verzi 4 (IPv4, 32-bitová adresa) a ve verzi 6 (IPv6, 128-bitová adresa).
IQN	iSCSI Qualified Name - řetězec, pomocí nějž je v síti adresován disk sdílený přes protokol iSCSI
iSCSI	Internet Small Computer System Interface - standard pro přenášení SCSI příkazů přes protokol IP. Protokol se skládá ze serveru (Target) a klienta (Initiator).
ISO	International Organization for Standardization - zkratka mezinárodní organizace pro standardy, v informatice je takto označován také formát souboru obsahující data každého zapsaného sektoru optického média.
LDAP	Lightweight Directory Access Protocol - aplikační protokol používaný pro práci s adresářovou službou. Umožňuje pracovat s objekty a jejich atributy.
LUN	Logical Unit Number - číslo sloužící k identifikaci logické jednotky adresované protokolem SCSI, případně iSCSI.

- MAC** Media Access Control - unikátní identifikátor přiřazený síťovému rozhraní na 2. vrstvě modelu OSI/ISO, je tvořen 48 bitovým číslem, které se skládá ze dvou částí - identifikátoru výrobce a čísla, které zařízení přiřadil samotný výrobce. Teoreticky by se na světě nemělo vyskytovat více jak jedno zařízení s daným jedním unikátním identifikátorem.
- MSDNAA** Microsoft Developer Network Academic Alliance - program společnosti Microsoft, umožňující školním zařízením za paušální poplatek využívat vývojářský software a operační systémy společnosti Microsoft. Podmínky používání softwaru jsou dány speciální MSDNAA licencí.
- NAS** Network Attached storage - úložné síťové zařízení určené pro ukládání a sdílení souborů. Pro přístup k souborům se často používají protokoly NFS a SMB.
- NBP** Network Bootstrap Program - program je ze serveru stažen bootujícím počítačem pomocí protokolu PXE, po stažení je mu předáno řízení a program se následně postará o zavedení samotného operačního systému.
- NFS** Network File System - síťový protokol umožňující přistupovat k souborům přes síť stejným způsobem, jakým je možno přistupovat k lokálním souborům. Tento protokol je využíván na UNIXových systémech.
- NIC** Network Interface Controller - počítačový hardware, který připojuje počítač k síti. Prakticky se jedná o síťovou kartu, případně integrovaný čip na základní desce.
- NTFS** New Technology File System - systém souborů využívaný operačním systémem Microsoft Windows řady NT, poskytuje lepší konzistenci a zabezpečení dat než systém souborů FAT.
- OS** Operating System (operační systém) - sada programů poskytující rozhraní mezi hardwarem počítače, uživatelem a dalšími uživatelskými programy. Operační systém přímo spravuje hardware počítače a současně poskytuje prostředí pro běh dalších programů využívajících funkce daného operačního systému.

POST	Power-On Self-Test - program, který se spouští ihned po zapnutí zařízení. Jeho úkolem je ověřit, zda všechny komponenty nezbytné pro správnou funkci zařízení pracují tak, jak mají. Po úspěšném provedení programu POST započne zavádění operačního systému.
PXE	Preboot Execution Environment - sada protokolů umožňující zavedení operačního systému ze sítě. Skládá se z protokolů DHCP a TFTP.
RAM	Random-Access Memory - rychlá paměť sloužící pro dočasné ukládání dat. V paměti RAM se nacházejí všechny momentálně běžící procesy a aktuálně zpracovávaná data. Po výpadku napájení se obsah paměti ztrácí.
ROM	Read-Only Memory - souhrnné označení pro skupinu pamětí. Data jsou jednorázově zapsána již při výrobě paměti a nemohou být následně měněna, čtení dat může probíhat opakovaně. Paměť si udrží obsah i při výpadku napájení. Označení ROM se také v přeneseném smyslu může vztahovat na bitovou kopii, která bývá v paměti ROM (příp. jiné paměti) uložena.
SAN	Storage Area Network - úložné síťové zařízení. S daty se pracuje po blocích, stejně jako na lokálním pevném disku. Pro přístup k datům se používá protokol iSCSI.
SCSI	Small Computer System Interface - standard pro fyzické propojení počítačů s periferními zařízení a přenos dat mezi nimi.
SMB	Server Message Block - síťový komunikační protokol pro přístup ke sdíleným souborům a tiskárnám. Tento protokol je používán v systému Windows.
TFTP	Trivial File Transfer Protocol - velmi jednoduchý protokol pro přenos souborů, neobsahuje žádnou autentizaci.
WDS	Windows Deployment Services - technologie společnosti Microsoft umožňující síťovou instalaci operačního systému Windows.
WDK	Windows Driver Kit - sada nástrojů od společnosti Microsoft umožňující vývoj ovladačů pro operační systém Windows.

SEZNAM OBRÁZKŮ

Obr. 1: Postup při zavádění operačního systému pomocí protokolu iSCSI.....	22
Obr. 2: Okno aplikace CCBoot - serverová část.....	25
Obr. 3: Okno aplikace CCBoot - klientská část.....	26
Obr. 4: Nastavení DHCP v programu CCBoot.....	30
Obr. 5: CCBoot - volba výchozího nastavení pro klienty.....	31
Obr. 6: CCBoot - nastavení vyrovnávací paměti serveru	32
Obr. 7: CCBoot - ostatní globální nastavení.....	33
Obr. 8: CCBoot - nastavení jednoho daného klienta	36
Obr. 9: Openfiler - seznam vytvořených svazků ve skupině "windows_images".....	57
Obr. 10: Openfiler - přidružení svazku k danému iSCSI targetu.....	58
Obr. 11: Instalace Windows 7 přímo na iSCSI disk, systém se nesnaží bootovat z druhého zařízení	60
Obr. 12: Chyba při instalaci Windows na iSCSI disk.....	62
Obr. 13: Jednoduchý image s Windows PE 3.0.....	74
Obr. 14: Složení ramdisku Windows PE	81
Obr. 15: Výběr operačního systému při zavádění ze sítě.....	90
Obr. 16: Okno programu WinBuilder.....	96

SEZNAM TABULEK

Tab. 1: Parametry adresování protokolu iSCSI	18
Tab. 2: Nastavení statické IP adresy PXE serveru	52
Tab. 3: Nastavení služby DHCP na PXE serveru	54
Tab. 4: Openfiler - nastavení parametrů pro iSCSI target	57
Tab. 5: Openfiler - nastavení parametrů pro iSCSI target (pokračování)	58
Tab. 6: Význam jednotlivých uživatelských adresářů ve Windows PE.....	68
Tab. 7: Srovnání různých metod zavádění Windows PE z hlediska času	93

SEZNAM PŘÍLOH

- P I DVD s textem BP, konfiguračními soubory DHCP serveru, nutným obsahem kořenového adresáře TFTP serveru pro jednotlivé způsoby zavádění systému ze sítě a soubory pro vytvoření obrazu s Windows PE.
- P II Označování násobků jednotek B (bajt) dle dodatku normy IEC 60027-2 (tabulka).

**PŘÍLOHA P II: OZNAČOVÁNÍ NÁSOBKŮ JEDNOTEK B (BAJT)
DLE DODATKU NORMY IEC 60027-2**

Mocnina	Jednotka	Značka	Velikost v B (bajtech)
2^{10}	Kibibyte	KiB	1 024
2^{20}	Mebibyte	MiB	1 048 576
2^{30}	Gibibyte	GiB	1 073 741 824
2^{40}	Tebibyte	TiB	1 099 511 627 776
2^{50}	Pebibyte	PiB	1 125 899 906 842 624
2^{60}	Exbibyte	EiB	1 152 921 504 606 846 976
2^{70}	Zebibyte	ZiB	1 180 591 620 717 411 303 424