Komfortní správa počítačové sítě

Comfortable computer network administration

Jan Bartoň

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan BARTOŇ**
Osobní číslo:	**A08845**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Komfortní správa počítačové sítě**

Zásady pro vypracování:

1. **Proveďte literární rešerši na dané téma.**
2. **Popište používaný HW v počítačových sítích (servery, stanice, síťové prvky).**
3. **Analyzujte používaný SW (serveru, stanic, aplikací pro správu, uživatelských aplikací).**
4. **Navrhněte doménové politiky a nakonfigurujte doménu.**
5. **Popište používané nástroje správce (vzdálené procesy, registry, plocha, zálohování).**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SIMMONS, Curt; CAUSEY, James F. Mistrovství v sítích Microsoft Windows XP. Vyd. 1. Brno : CP Books, 2005. 620 s. ISBN 8025105830.**
2. **KABELOVÁ, Alena; DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno : Computer Press, 2008. 488 s. ISBN 978-80-251-2236-5.**
3. **ALLEN, Robbie; LIŠKA, Alois; LOWE-NORRIS, Alistair G. Active Directory : implementace a správa Microsoft Active Directory. 1. vyd. Praha : Grada, 2005. 644 s. ISBN 8024709732.**
4. **PRICE, Brad. Active Directory : optimální postupy a řešení problémů. Vyd. 1. Brno : CP Books, 2005. 381 s. ISBN 80-251-0602-0.**
5. **HORÁK, Jaroslav; KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. 4., aktualiz. a rozš. vyd. Brno : Computer Press, 2008. 327 s. ISBN 978-80-251-2073-6.**

Vedoucí bakalářské práce: **Ing. Jiří Korbel**
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

Zaměstnání správce sítě vyžaduje diametrálně odlišný přístup než například správa domácích stanic. Principy jsou podobné, ale rizika mnohem větší. Jednou z důležitých oblastí správy větších sítí jsou také metody jak práci usnadnit, automatizovat, zpřehlednit. Důvodem zde není lenost správce, ale v prvé řadě systémovost, bezpečnost, rychlost. Přestože počítače někdy dělají chyby, je statisticky prokázáno, že je jich daleko méně než těch, které napáchá sám správce z nepozornosti či neznalosti. Tato práce je stručným průvodcem několika oblastí správy sítě s operačními systémy z rodiny Windows se zaměřením na vzdálenou správu stanic na středně velké základní škole.

Klíčová slova: RDP, VNC, doména, GPO , hromadná tvorba uživatelských účtů.

ABSTRACT

A position of a network administrator requires a completely different approach than, for example, administration of home computers. The principals are similar, but the risk is much higher. Methods of simplifying and automating work are also important fields of network management. The reason is not laziness of an administrator, but systematism, safety and speed in the first place. Although computers make mistakes from time to time, it is statistically proven that more mistakes are caused because of carelessness or unacquaintanceby by the administrator himself. The thesis is a brief guide through the field of computer administration in operating systems of the Windows family, focused on a distant administration of computers at a medium-sized elementary school.

Keywords: RDP, VNC, domain, GPO, mass creation of user accounts

Poděkování:

Rád bych poděkoval všem, kteří přispěli k vytvoření této práce svými podněty a radami, především pak panu Ing. Jiřímu Korbelovi za odborné a konstruktivní připomínky.

Motto:

Plus ratio quam vis caeca valere solet.

„Rozum platívá víc než slepá síla“

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 …….……

podpis diplomanta

OBSAH

ÚVOD

Problematika správy počítačových sítí je dána především použitým hardware a software. V současných počítačových sítích se nachází stanice, síťové prvky a servery, jejichž výkon (hardware) se neustále zlepšuje, stejně tak jako software, který tuto techniku umožňuje konfigurovat a využívat. Skutečným problémem správce sítě je kromě hardwarových a softwarových kolizí především neustálá a nikdy nekončící nutnost dalšího vzdělávání se.

S každou novou implementovanou technologií se rozšiřuje oblast nutných znalostí vzhledem k potřebě predikce všech představitelných rizik. Málokterý obor se vyznačuje takovou dynamikou vývoje jako právě informatika, přesto se budu v této práci snažit vystihnout nejen obecné principy, ale i momentální nasazená a funkční řešení.

Výsledkem komfortní správy sítě nemá být pouhé šetření času správce a jeho pohodlí, ale především dlouhodobá a spolehlivá funkčnost celého podnikového ekosystému. Tato práce se také pokusí vymýtit představu o správci sítě jako o opraváři. Primárním úkolem administrátora sítě je nastavit systém tak, aby k opravám docházelo pouze v případě selhání hardwaru. I tehdy ale musí být systém natolik robustní, aby prostoje uživatelů byly minimální.

Noční můrou každého správce je pak fatální selhání v podobě nenapravitelné ztráty či kompromitace důležitých dat. Zodpovědnost správce sítě tak může šplhat i k astronomickým částkám. Řešení takovýchto problémů spočívá v pravidle být vždy krok před útočníkem. Bohužel z praxe je známo, že někdy ani to nestačí a stoprocentně bezpečný systém je pouhou iluzí. Leckdy by však byla vhodná alespoň základní snaha o eliminaci těch nejzjevnějších bezpečnostních rizik. Přesto některé domácnosti i firmy nezálohují a nezabezpečují, ba ani nekonzultují své postupy s žádným odborníkem. Stejně tak se najdou zaměstnavatelé schopní kritizovat správce sítě za to, že si „v pracovní době čte články na internetu“, aniž by tušili, že právě aktuální a neustále tříbené know-how jejich informatika je tou nejmocnější zbraní proti neustále číhajícím IT katastrofám.

I. TEORETICKÁ ČÁST

1 TEORIE SÍTÍ, SÍŤOVÉ PROTOKOLY A SLUŽBY

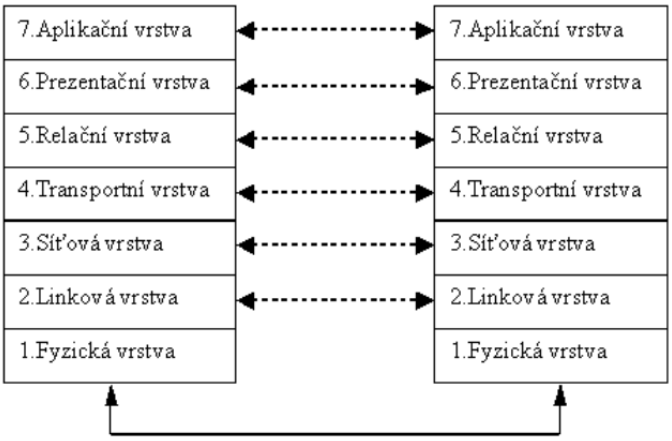
1.1 Síťové protokoly

„Podobně jako diplomaté při svých jednáních používají diplomatický protokol, tak i počítače v počítačových sítích používají pro vzájemnou komunikaci síťové protokoly. Síťových protokolů existuje celá řada. V Internetu se používají síťové protokoly TCP/IP.

Síťový protokol je norma napsaná na papíře (resp. textovým editorem na počítači). V Internetu se používají normy nazývané Request For Comments – zkratkou RFC, které se číslují průběžně od jedničky. V současné době jich jsou necelé tři tisíce. Mnohé však postupem času zastaraly, takže z první tisícovky jich je aktuálních jen několik.“ [1]

1.2 ISO OSI

„Referenční model ISO/OSI byl definován jako standard pro návrh komunikačních systémů (ISO 7498, 1984), protože bylo potřeba sjednotit schématický popis komunikačního systému.“ [6]



Obr. 1: Komunikace mezi dvěma počítači podle modelu OSI/ISO

ISO/OSI je normalizovaný referenční model vrstvové architektury. Cílem bylo vytvořit zvláštní vrstvy pro odlišné funkce, ale zároveň soustředit příbuzné funkce do společné vrstvy a tím počet vrstev minimalizovat. Dále potom byla snaha zabezpečit snadnou výměnu protokolů a funkcí v rámci jedné vrstvy bez dopadu na vrstvy ostatní.

Mezi dvěma sousedními vrstvami je pak přesně definováno rozhraní – to znamená jaké operace a služby nabízí nižší vrstva vrstvě vyšší s tím, že vyšší vrstva není zatěžována podrobnostmi o vlastní realizaci služby nižší vrstvy.

1.2.1 Fyzická vrstva

Popisuje elektrické či optické signály používané při komunikaci. Je na ní vytvořen tzv. fyzický okruh, na který mohou být vkládána další zařízení typu modem apod., schopná signál modulovat.

1.2.2 Linková vrstva

Zajišťuje v případě sériových linek výměnu dat mezi sousedními počítači a v případě lokálních sítí výměnu dat v rámci lokální sítě. Základní jednotkou pro přenos dat je zde datový rámec**.** Datový rámec se skládá ze záhlaví (Header), přenášených dat (Payload) a zápatí (Trailer)**.** Záhlaví je tvořeno linkovou adresu příjemce, linkovou adresu odesílatele a dalšími řídícími informacemi. V zápatí je obvykle kontrolní součet z přenášených dat. V přenášených datech je pak zabalen paket síťové vrstvy.

1.2.3 Síťová vrstva

Síťová vrstva zabezpečuje přenos dat mezi počítači na velké vzdálenosti – což nemusí být nutně fyzicky velká vzdálenost, ale propojení např. přes velký počet uzlů. Základní jednotkou přenosu je síťový paket (datagram), který se balí do datového rámce (z linkové vrstvy). Síťový paket se skládá ze záhlaví a datového pole. Se zápatím se u síťových protokolů setkáváme jen málo. Síťová vrstva zná skutečnou topologii sítě a zajišťuje doručení paketů až k cílovému uzlu.

1.2.4 Transportní vrstva

Síťová vrstva zabezpečí spojení mezi vzdálenými počítači, takže transportní vrstva už vůbec neřeší přítomnost modemů, opakovačů, mostů, směrovačů… Předpokládá, že spojení mezi počítači je zajištěno, proto se může věnovat pouze spojení mezi aplikacemi na vzdálených počítačích. Jejím úkolem je zajišťovat efektivní spojení pro nadřízenou vrstvu relační.

„Transportní vrstva může měnit nespolehlivý charakter přenosu na spolehlivý, může zvyšovat spolehlivost přenosu a měnit nespojovaný přenos na spojovaný. Slaďuje nabídku nižších a požadavky vyšších vrstev, zajišťuje komunikaci mezi koncovými uživateli. Zvyšuje zabezpečení samoopravnými cykly. Mezi dvěma počítači může být několik transportních spojení současně. Jednotkou přenosu je transportní paket, který se opět skládá ze záhlaví a datové části.“ [5]

1.2.5 Relační vrstva

Relační vrstva zabezpečuje výměnu dat mezi aplikacemi. Provádí tzv. checkpoint, synchronizaci transakcí (commit) a korektní uzavírání souborů. Relace (session) se dá nejlépe přirovnat k telefonnímu hovoru. Ten se sice vytáčí a spojuje (transportní vrstva), ale poté již můžeme vést rozhovor (relaci). V ISO/OSI lze relaci zřizovat a rušit, existují i situace, kdy transportní spojení zajišťuje i více po sobě jdoucích relací. Obvykle se rozlišují tři způsoby vedení relace - plně duplexní (Two Way Simultaneous), poloduplexní (Two Way Alternate) a simplexní (One Way).

1.2.6 Prezentační vrstva

Prezentační vrstva je zodpovědná za reprezentaci a zabezpečení dat. Reprezentace dat může být na různých počítačích různá. Pět nejnižších vrstev referenčního modelu ISO/OSI zabezpečuje, aby přenášená data vždy dorazila ke svému příjemci přesně v takové podobě, v jaké byla vyslána. Prezentační vrstva pak zajistí nezbytné konverze přenášených dat. Může však řešit také zabezpečení přenášených dat pomocí šifrování, zabezpečení integrity dat, digitální podepisování atd. Pro minimalizaci objemu přenášených dat pak může být na úrovni prezentační vrstvy zajišťována i jejich komprimace.

1.2.7 Aplikační vrstva

Počítačové sítě jsou využívány prostřednictvím nejrůznějších aplikací. Do aplikační vrstvy se zahrnují jen části těchto aplikací, které realizují obecně použitelné mechanismy. Aplikační vrstva pak předepisuje, v jakém formátu a jak mají být data přebírána/předávána od aplikačních programů. Např. protokol odesílání elektronické pošty bude v různých aplikacích stejný, přestože budou existovat nejrůznější metody pro čtení a vytváření zpráv. Tyto metody však už do aplikační vrstvy nepatří.

1.3 TCP/IP

Rodina protokolů TCP/IP se nezabývá (až na výjimky) fyzickou a linkovou vrstvou. V praxi se i v Internetu používají pro fyzickou a linkovou vrstvu často protokoly vyhovující normám ISO/OSI.

„Protokoly ISO OSI a TCP/IP jsou obecně nesouměřitelné. Každá skupina má vlastní definici svých vrstev i protokolů jednotlivých vrstev. V praxi však je třeba využívat

komunikační zařízení vyhovující ISO OSI pro přenos IP-paketů nebo např. naopak realizovat služby podle ISO OSI přes Internet.“ [3]

1.3.1 Internet Protokol

Internet Protokol (IP protokol) odpovídá síťové vrstvě. IP protokol přenáší tzv. IP datagramy mezi vzdálenými počítači. Každý IP datagram ve svém záhlaví nese adresu příjemce, což je úplná směrovací informace pro dopravu IP datagramu k příjemci. IP datagramy však mohou k adresátovi dorazit v jiném pořadí, než byly odeslány. Každé síťové rozhraní v Internetu má svou jedinečnou IP adresu. Internet samotný je tvořen jednotlivými sítěmi, které jsou propojeny pomocí směrovačů. Momentálně používané adresování (IPv4) je již na hranici vyčerpanosti všech dostupných adres, proto je přistupováno k adresování pomocí IPv6.

1.3.2 Protokoly TCP a UDP

Protokoly TCP a UDP odpovídají transportní vrstvě. Protokol TCP dopravuje data pomocí TCP segmentů, které jsou adresovány jednotlivým aplikacím. Protokol UDP dopravuje data takzvanými UDP datagramy. Rozdíl mezi protokoly TCP a UDP spočívá v tom, že protokol TCP je tzv. spojovanou službou (příjemce potvrzuje přijímaná data) a v případě ztráty dat si příjemce vyžádá zopakování přenosu. Protokol UDP se už nezajímá o to, zdali byl datagram doručen.

Adresou pro TCP i UDP je tzv. port. Ten představuje další upřesnění celkové IP adresy. (která může mít tvar IP:PORT – např.: 192.168.1.1:1234) Porty rozdělujeme jako:

- známé porty – v rozsahu 0 až 1023 (jsou vyhrazené pro nejběžnější služby)
- registrované porty – v rozsahu 1024 až 49151
- dynamické a soukromé porty – v rozsahu 49152 až 65535

1.3.3 Aplikační protokoly

Relační, prezentační a aplikační vrstva ISO/OSI jsou zredukovány do jedné aplikační vrstvy TCP/IP. Podle užití je lze dělit na:

- Uživatelské protokoly, které využívají uživatelské aplikace (např. pro vyhledávání informací v Internetu). Příkladem jsou: HTTP, SMTP, Telnet, FTP, IMAP, POP3 atd.

- Služební protokoly, např. směrovací protokoly, které používají směrovače, aby si správně nastavily směrovací tabulky nebo SNMP, který slouží ke správě sítí.

1.4 Síťové protokoly a služby

1.4.1 DNS (Domain Name System)

Protokol DNS nelze snadno zařadit ani mezi služební protokoly, ani mezi uživatelské. Přesto je používán takřka neustále. Je to hierarchický systém doménových jmen, který je realizován servery DNS a stejnojmenným protokolem. Hlavním úkolem jsou vzájemné obousměrné převody doménových jmen a IP adres. Dnes slouží jako distribuovaná databáze síťových informací. Protokol používá porty 53 TCP i UDP. Hierarchicky uspořádaná jména domén jsou orientační pomůckou pro člověka, IP adresace pak může být 32bitová (IPv4) nebo 128bitová (IPv6). Větší množství DNS serverů pak umožňuje udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy.

1.4.2 DHCP

Zkratka DHCP znamená Dynamic Host Configuration Protocol. Jeho využití je velmi běžné a v sítích s množstvím klientských stanic a jejich fluktuací (např. fyzické zapojování notebooků do různých sítí) se stává takřka nutností. Požadavek různé konfigurace připojení pro jedno zařízení lze jistě vyplnit i ručně. Přesto automatická konfigurace šetří čas a umožňuje i připojení lidem, kteří jej neumějí nebo nemohou nastavit. DHCP protokol umožňuje prostřednictvím DHCP serveru nastavit všem stanicím celou sadu parametrů nutných pro komunikaci protokoly TCP/IP. Serverů může být sdruženo i více, decentralizace pak vede ke zvýšení odolnosti vůči výpadkům. Parametry nastavitelné pomocí DHCP jsou IP adresa, maska sítě, brána, další DNS servery a další údaje, např. servery pro NTP, WINS, atd…

Klienti (stanice) vždy žádají server o IP adresu. Ten adresy eviduje a zapůjčuje, přičemž doba zápůjčky je nastavitelná. Komunikace klienta probíhá na UDP portu 68, server naslouchá na UDP portu 67. IP adresa může být stanici přidělena ručně (DHCP server není využit), staticky (DHCP server na základě evidovaných MAC adres přiděluje vždy stejnou IP adresu) a dynamicky (IP adresy jsou přidělovány z vymezeného rozsahu a jejich pronájem je časově omezen).

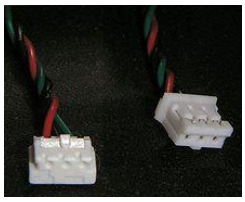
1.4.3 Síťové tunelování

Tato technika zapouzdřuje jedno nebo více síťových spojení do spojení jiného. Většinou souvisí se snahou zajistit zabezpečené spojení počítačů při připojení nedůvěryhodnými prostředky (Internet). Jedním z využití může být zapouzdření jiných než aktuálně povolených protokolů, další může spočívat např. v šifrování protokolů, které toto nativně neumožňují (velmi časté je použití SSH spojení). Tunel samotný je budován pomocí konfigurace koncových síťových prvků. Zde se nastaví typ přenášeného i přenosového (tunelovacího) protokolu, mechanismus tunelování a adresy koncových uzlů.

1.4.4 Magic packet a WoL (wake on LAN)

Wake on LAN je způsob probuzení (zapnutí) počítače vysláním speciálního signálu po síťovém kabelu. Běžně se používá u počítačů, ke kterým nemáme fyzický přístup, ale přesto je potřebujeme zapnout. Znamená to ovšem nechat PC s napájenou síťovou kartou. Toto je možno nastavit v BIOSu u naprosté většiny současných počítačů. Předchůdcem tohoto způsobu probouzení byla metoda Wake on Ring, která probouzela počítač přes faxmodem. Vzhledem k ústupu modemového připojení k internetu je tato možnost již dnes téměř nevyužívaná. Obě tyto funkce bývají nejčastěji nastavitelné v části BIOSu, která řeší energetický management - „Power Management“.

Starší základní desky musely být vybaveny konektorem WAKEUP-LINK, kterým byla propojena deska se síťovou kartou. Již dlouhou dobu síťové karty a základní desky takový kabel nepotřebují, protože oživovací signál i nezbytné napájení se šíří přímo po sběrnici PCI. Síťová karta je tedy i při vypnutém PC pod napětím a reaguje na speciální posloupnost bajtů (paket), která se nazývá Magický packet (Magic Packet). Magický paket je speciální rámec odeslaný protokolem UDP na port 7 nebo 9. Obsahuje šest konstantních bajtů hexadecimálně zapsaných jako FF:FF:FF:FF:FF:FF následovaných MAC adresou (16x opakovanou). Tento paket je odesílán broadcastem do celé LAN. Konkrétní síťová karta tento paket přijme, ale probouzení spustí, jen pokud se jedná o Magický paket s její MAC adresou.



Obr. 2: WAKEUP-LINK

Nevýhodou použití WOL technologie je nutnost udržovat zařízení pod napětím. To představuje konstantní spotřebu elektrické energie a zároveň riziko poškození v případě výkyvů napětí v elektrické síti (například při zásahu bleskem). Dále je to nemožnost zabezpečení před útokem (probouzením) zevnitř LAN a jen slabé možnosti zabezpečení při útoku zvnějšku. Toto je dáno podstatou broadcast vysílání a problém se dá řešit pouze omezením konkrétních vnějších adres, ze kterých se signál směruje na lokální síť. Existují snahy výrobců zabezpečovat reakce stanic na magic packet (např. Intel AMT), ale nejsou příliš rozšířené.

2 SÍŤOVÝ HARDWARE

Zařízení umožňující síťovou komunikaci jsou dělena do dvou základních kategorií. Obecně platí, že jakýkoliv napájený síťový prvek, tedy takový, který ovlivňuje výsledný signál, nazýváme aktivní. Patří sem například brány, modemy, opakovače, přístupové body, routery, switche, síťové karty. Prvky, které nijak výsledný signál neovlivňují, jsou pasivní. Řadíme sem např. huby, zásuvky, patch panely a racky (datové rozvaděče).

2.1 Bridge

Dnes již nepoužívané řešení. Sloužil k propojení nebo oddělení segmentů sítě. Pracoval na druhé vrstvě OSI modelu (rozhodoval podle MAC adresy, propouštěl všechny boadcasty a multicasty)

Obr. 3: Bridge od firmy Planet

2.2 Brána (gateway)

Spojuje dvě sítě nebo dva segmenty sítě, které používají různé komunikační protokoly. Funguje také jakou router. Typické využití je například GSM brána napojená na lokální síť nebo internet. Často bývá tento pojem zaměňován s tzv. „default gateway“, což je způsob označení routeru, který v lokální síti umožňuje připojení do sítě internet.

Obr. 4: GSM/VoIP brána od firmy Planet

2.3 Hub

Hub (neboli rozbočovač) je zařízení, které fyzicky spojuje jednotlivé uzly v síti. V jeden okamžik může vysílat pouze jeden uzel a ostatní musí čekat. S tím je spjata největší nevýhoda HUBů - nadměrné zatěžování sítě. Dnes se proto již téměř nepoužívají, je jich využíváno především v nepříliš rozsáhlých sítích

Obr. 5: 16 a 24 portový HUB firmy Linksys

2.4 Modem

Název modem pochází z výrazu „modulátor demodulátor“. Používá se pro převod mezi analogovým a digitálním signálem. Dnes se modemy používají především pro přenos

digitálních dat pomocí analogové přenosové trasy (telefonní linka, radiový přenos apod.). Většina telefonních modemů, ISDN, GSM, GPRS a UMTS modemů podporuje také přenos faxů. Dnes jsou nejčastěji používány právě ISDN (pro pevné telefonní linky) a UMTS (HSDPA, HSUPA) pro mobilní zařízení (např. tzv. „chytré“ telefony, notebooky, čtečky elektronických knih…)

Obr. 6: Modem pro připojení k tel. síti

2.5 Opakovač (repeater)

Dnes již nepoužívané zařízení, sloužilo k prodloužení dosahu signálu především u sběrnicových topologií. Mívalo většinou pouze dva porty a pracovalo na první vrstvě modelu OSI.

Obr. 7: Repeater firmy Matrox

2.6 Přístupový bod (access point)

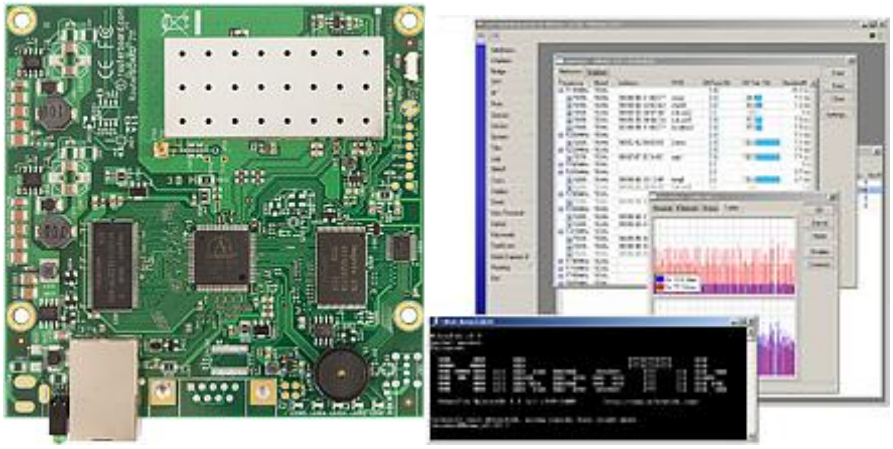
Přístupový bod je zařízení používáno v souvislosti s bezdrátovými sítěmi. Klienti bezdrátové sítě (např. Wi-Fi) spolu nekomunikují přímo, ale prostřednictvím přístupového bodu. Nemusí tedy být ve vzájemném rádiovém spojení. Tento centralizovaný způsob

komunikace umožňuje jednoduché nastavení bezpečnostních politik. Typ uspořádání takové sítě je nazýván infrastrukturní. AP je s rozvojem domácích bezdrátových sítí velmi levné a často používané zařízení. Často se jedná o malá víceúčelová zařízení, která kombinují funkcionalitu AP a routeru a bývají vybavena uživatelsky přívětivým firmware (založeným např. na OS Linux).

Obr. 8: AP firmy D-link

2.7 Router (směrovač)

Router funguje na vyšší úrovni než hub nebo switch. Shromažďuje informace o připojených sítích a vybírá nejvýhodnější cestu pro posílaný paket. K tomu slouží routovací tabulka. Setkáváme se také s bezdrátovými routery, které slouží zároveň jako přístupové body (AP). Pro účely běžné sítě LAN se příliš nepoužívá, setkáváme se s ním při připojování sítí k Internetu.



Obr. 9: Mikrotik Router board a náhled obslužného rozhraní

Zařízení MikroTik Router board je v podstatě malým počítačem, který disponuje několika síťovými rozhraními a je osazený upravenou linuxovou distribucí. Díky tomu nabízí velmi

rozsáhlá nastavení při zachování značného uživatelského komfortu. Na tomto zařízení běží také Firewall, DHCP a DNS server. Správa je prováděna dálkově prostřednictvím WinboxLoaderu, případně přes webové rozhraní. Veškerá nastavení se dají snadno zálohovat, importovat a exportovat. Veškeré úkony provedené na tomto zařízení se pak ihned projevují v celé síti.

2.8 Switch

Switch (přepínač) je zařízení, které propojuje jednotlivé části sítě. V dnešních sítích s hvězdicovou topologií tvoří důležitý centrální prvek. Pracuje obvykle na 2. vrstvě modelu ISO/OSI a přepíná mezi jednotlivými porty. Princip práce spočívá v kontrole paketu (adresa příjemce a odesílatele) a následném přepnutí paketu na port, na kterém se nachází cílový uzel s cílovou adresou příjemce. Switch na rozdíl od HUBu nezatěžuje síť zbytečným přeposíláním veškerého provozu, šetří tím kapacitu sítě a je v konečném výsledku mnohem rychlejší.

Obr. 10: 24 portový switch firmy CISCO.

2.9 Síťová karta (network interface card – NIC)

Je základním aktivním prvkem nutným pro připojení k počítačové síti. Bývá umístěna ve slotu (PCI) nebo integrovaná na základní desce. Každá síťová karta má od výrobce stanovenou tzv. MAC adresu, která by měla v počítačové síti představovat její jedinečný identifikátor. Dnešní běžné síťové karty již mají jen jeden typ konektoru (RJ45), kterým lze připojovat různě rychlé síťové prvky (10/100/1000Mbit/s), v serverech pak můžeme nalézt síťové karty disponující optickým konektorem, viz obrázek:

Obr. 11: Síťová karta s optickým konektorem D-link

II. PRAKTICKÁ ČÁST

3 KONFIGURACE DOMÉNY

Tato část je zaměřena na praktické aspekty správy sítě na základní škole, která je mým zaměstnavatelem. Konfigurace i nasazení jednotlivého SW bude ilustrováno na konkrétních příkladech jeho využití.

3.1 Situace školy

Po skončení účasti základní školy v programu INDOŠ měla tato organizace na výběr z několika možných řešení správy školní sítě:

- Správa externí firmou. Pozitivem je zde jistota přítomnosti dostatečného know-how i technického zázemí. Výrazným záporem je cena a neschopnost firem řešit drobné problémy flexibilně.
- Vlastní správce sítě. Ten je mnohem flexibilnější, nicméně finančně také nevýhodný.

Velké množství škol tuto situaci řeší tím, že správu sítě předá učiteli informatiky a finanční záležitosti kompenzuje snížením pracovního úvazku. Toto řešení je praktikováno i v tomto případě. Jeho výhodou je násobně menší finanční zátěž pro zaměstnavatele a flexibilita a neustálá přítomnost informatika na pracovišti.

3.2 Důvody nasazování doménového serveru

Situace ZŠ vyžadovala splnění těchto úkolů:

- Zachovat pokud možno stávající výukové i kancelářské prostředí
- Zajistit kontinuitu výuky na stejném HW a stejném nebo velmi obdobném SW
- Zajistit bezpečnost dat na těchto úrovních:
    - Zálohování
    - Archivace
    - Oprávněné a neoprávněné manipulace s uživatelskými daty
    - Publikování na veřejně dostupném kanále (WWW)

Majoritně používané operační systémy byly v té době Windows 2000 a XP. Jako dědictví po INDOŠi jsme dále obdrželi licence na provoz Windows 2000 serveru, multilicenci na

kancelářský balík MS Office 2000 a velké množství výukového SW pro operační systémy z rodiny Windows.

V této době však došlo i k velkému rozšíření počtu stanic, a proto bylo přistoupeno také k nákupu nového serveru. Bylo rozhodnuto nasadit opět OS z rodiny Windows, a to Windows 2003 server.

Obr. 12: Dell 2900 Poweredge

Použité OS:

Doménový server: virtuální stroj s nainstalovaným systémem Windows 2003 server.

Klientské stanice: Windows 2000, Windows XP, Windows Vista, Windows 7, Linux CentOS (experimentálně jako dualboot)

Pro všechny stanice a OS s výjimkou Linuxu bylo třeba vytvořit přenosné uživatelské prostředí. Proto padla volba na řešení pomocí domény a cestovních uživatelských profilů.

3.3 Doménový řadič

Tuto nejdůležitější součást domény bylo rozhodnuto virtualizovat z důvodu snadné zálohy i obnovení. Pomocí průvodce byl na této virtuální stanici vytvořen první řadič domény. Spolu s ním tak vznikla první (a jediná) doména a v ní běžící služba Active Directory. V tomto adresáři jsou publikována další sdílená zařízení. V době těchto změn byly školní prázdniny, a tak bylo možno vyzkoušet celou řadu různých nastavení GPO. Po konzultaci s ředitelkou školy a lokální firmou zabývající se implementacemi síťových řešení v podnikové sféře byla určena definitivní sada pravidel GPO.

3.4 Přidávání uživatelů do domény

Vytvořit jednoho nového uživatele domény není problém. Grafické i textové nástroje systému jsou pro jednorázové vytvoření účtu i jeho další konfiguraci vhodným řešením. Problém nastává v situaci, kdy je třeba vytvořit velké množství účtů s předem nadefinovanou konfigurací. Každým rokem ve škole jednorázově přibývá velké množství žáků, kteří potřebují vytvořit doménové účty. Zde je naštěstí možnost používat nejrůznější skripty, viz **Příloha I: Hromadný import uživatelů do domény**.

Jako zdroj slouží list MS Excel, na kterém je několik úprav v souladu s metodikou tvorby uživatelských jmen v doméně (uvedena zkrácená forma):

username	Jmeno	Prijmeni	heslo	Skupina
andrja	Jana	Andrášková	5602940559	ZacharZAK
andrma	Marek	Andrýsek	6616891133	ZacharZAK
bakaad	Adam	Bakala	7885353501	ZacharZAK
baliad	Adrián	Balica	3582852410	ZacharZAK
baroni	Nikol	Barošová	3202960768	ZacharZAK
bartma	Martin	Bartoněk	1917812166	ZacharZAK
bartra	Radek	Bartoš	5260597420	ZacharZAK
bartvi	Viktorie	Bartošková	6024841056	ZacharZAK
bartan	Andrea	Bartošová	8174222604	ZacharZAK
bartde	Denisa	Bartošová	9716672215	ZacharZAK
barifi	Filip	Bařinka	6380311396	ZacharZAK
bastve	Vendula	Baštincová	4243331732	ZacharZAK

Tabulka 1: Metodika tvorby uživatelských účtů

Uživatelské jméno je tvořeno prvními 4 znaky z příjmení žáka a 2 znaky z křestního jména. Seznam žáků je centrálně tvořen sekretářkou školy při nástupu žáků, proto stačí z tohoto seznamu zkopírovat jména a příjmení nově příchozích. List je dále doplněn o jednoduše generovaná výchozí hesla (žák je při prvním příchodu do učebny nucen vyhledat správce, se kterým si heslo přenastaví). Pro větší automatizaci jsou i uživatelská jména další VBA funkcí upravena tak, aby neobsahovala znaky s diakritikou, viz **Příloha II: Odstranění diakritiky z uživatelských jmen.**

Vlastnosti takto koncipovaných uživatelských jmen:

- Přehlednost, snadná identifikace uživatele podle uživatelského jména
- Snadná zapamatovatelnost

- Minimální šance na výskyt stejných uživatelských jmen dvou různých žáků (je řešena individuálně přidáváním dalších znaků)
- Minimální šance na výskyt kratších příjmení, než 4 znaky (řešeno individuálně)
- Téměř stoprocentní automatizace tvorby velkého množství uživatelských účtů

Zejména poslední vlastnost je velmi důležitá. V množství cca 500 uživatelských účtů dochází k velmi malému množství situací, které vyžadují zásah správce. Duplicita účtů je detekována přímo při jejich tvorbě a zodpovědný VBS skript v takovém případě končí svou činnost s odpovídajícím chybovým hlášením. Časová náročnost pro správce tak klesla z původních 2 minut na 1 účet při manuální tvorbě na necelou 1 minutu na 500 účtů při tvorbě skriptem.

Důležitým detailem je, že existuje sada skriptů, pro každou skupinu uživatelů jeden. Rozdělení do uživatelských skupin (OU) totiž umožní delegování rozdílných práv globálně, čímž např. diametrálně mění chování žákovského a učitelského účtu. Skupinám se mapují různé síťové prostředky a mají také různě definovaná práva pro používání zařízení a čtení/zápis do síťových složek.

3.5 Logon script

Jak již bylo naznačeno, různé skupiny uživatelů potřebují ke své práci různé prostředky. Tyto kategorie jsou v našem případě: Administrátoři, Učitelé, Žáci, Správní zaměstnanci.

Každá skupina je detekovaná v logon skriptu. Na základě příslušnosti ke skupině jsou uživatelům mapovány tiskárny, síťové jednotky apod., viz **Příloha III: Logon script (zkrácený).**

Přihlašovací skript zároveň detekuje problémy s připojením síťových disků. Pokud proběhne s chybou, je uživatel uvědomen prostřednictvím chybového hlášení. Stejně tak vykonání celého skriptu je zakončeno „uvítací zprávou“, která je zároveň potvrzením, že by pro uživatele měly být na dané stanici přístupné všechny očekávané funkce.

Nikdy nelze zcela potlačit lidský faktor a pokrýt všechny situace, kdy se uživatel může projevit v systému destruktivně. Zodpovědnost však v naprosté většině případů nese administrátor, protože je to on, kdo vytváří uživatelům jejich pracovní prostor. Pro ilustraci uvádím dva subjektivně zabarvené popisy příkladů z vlastní praxe:

Metodické materiály pro interaktivní tabule bývají datově objemné. Tvůrce takového materiálu chce kolegům pomoci a začne několik svých 100MB souborů rozesílat hromadně vnitřní mailovou poštou. Poštovní server má vyhrazený omezený prostor (5GB) na virtuálním stroji. Jakmile je tento prostor vyčerpán, nikdo další neobdrží jediný e-mail. Ze strany správce je možné maximální velikost odchozí zprávy omezit, ale řešením s přidanou hodnotou je za tímto „hříšníkem“ také zajít a vysvětlit mu používání sdíleného síťového úložiště. Teprve druhým krokem bylo preventivní omezení velikosti e-mailů na přijatelných 20MB.

Příklad druhý: Uživatel přijde ke stanici, zadá své údaje a místo uvítání vidí chybové hlášení. Je překvapen, proč se nedostane ke svým dokumentům na síťovém disku. Po přivolání správce a krátkém zjišťování je příčina jasná – uživatel si natáhl nohy pod stůl a vykopl tak nechtě síťový konektor RJ 45 ze zásuvky. V rámci projektu INDOŠ byly všechny ethernetové zásuvky v jedné PC učebně umístěny do výše cca 30 cm nad úroveň podlahy a tím byl popisovaný problém způsoben. Všechny nové zásuvky na základě těchto zkušeností již umisťujeme dostatečně vysoko. Od té doby navíc tento uživatel ví, že pokud ho potká stejné chybové hlášení, podívá se pod stůl a problém si tak často vyřeší sám.

Obr. 13: Umístění ethernetových zásuvek

3.6 GPO management:

„Nastavení zabezpečení, která budou vynucována pro uživatele a systémy, ke kterým se uživatelé připojují, je nutné určit mezi prvními. Je-li systém Windows Server 2003 nakonfigurován jako řadič domény, zásady zabezpečení domény požadují, aby uživatelé používali silná hesla.“ [4]

Prostředí školy má svá specifika, a proto i některá nastavení GPO jsou oproti podnikové sféře jiná. Patří mezi ně například heslo.

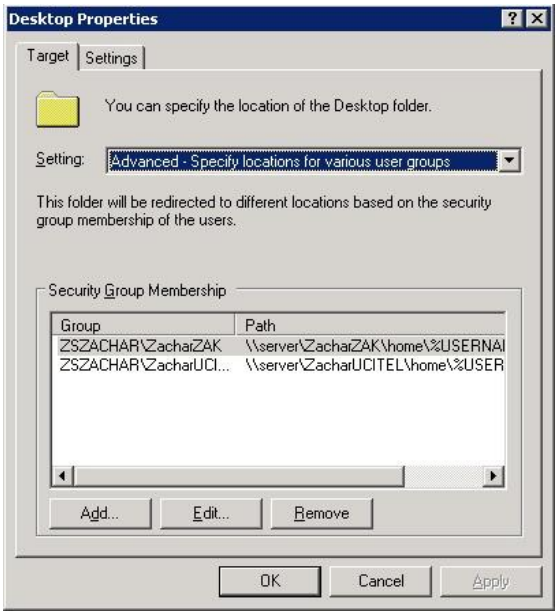
- Složitost ani expirace není omezena s ohledem na to, že stanice využívají i žáci prvního stupně, kteří by měli s měnícími se složitými hesly problém
- Je zakázáno pouze prázdné heslo
- Počet pokusů nesprávného uvedení hesla vedoucí k zamčení účtu je neomezený (někteří žáci cíleně zamykali účty svým spolužákům)

Dokumenty a plocha

- Obě složky jsou přesměrovány na síťový disk H: (dříve byla přesměrována pouze složka Dokumenty, ale velké soubory kopírované na Plochu způsobovaly fatálně pomalé načítání cestovních profilů)

Cestovní profily

- Nejsou po odhlášení ze stanice mazány, což vede k rychlejšímu opětovnému přihlašování na stejnou stanici. (Mazání je prováděno v rámci údržby stanic.)
- Jsou ukládány zvlášť pro žáky a ostatní uživatele. Žákovské cestovní profily jsou zálohovány s delší periodou než ostatní
- Jsou přístupné pouze konkrétnímu uživateli a správci.



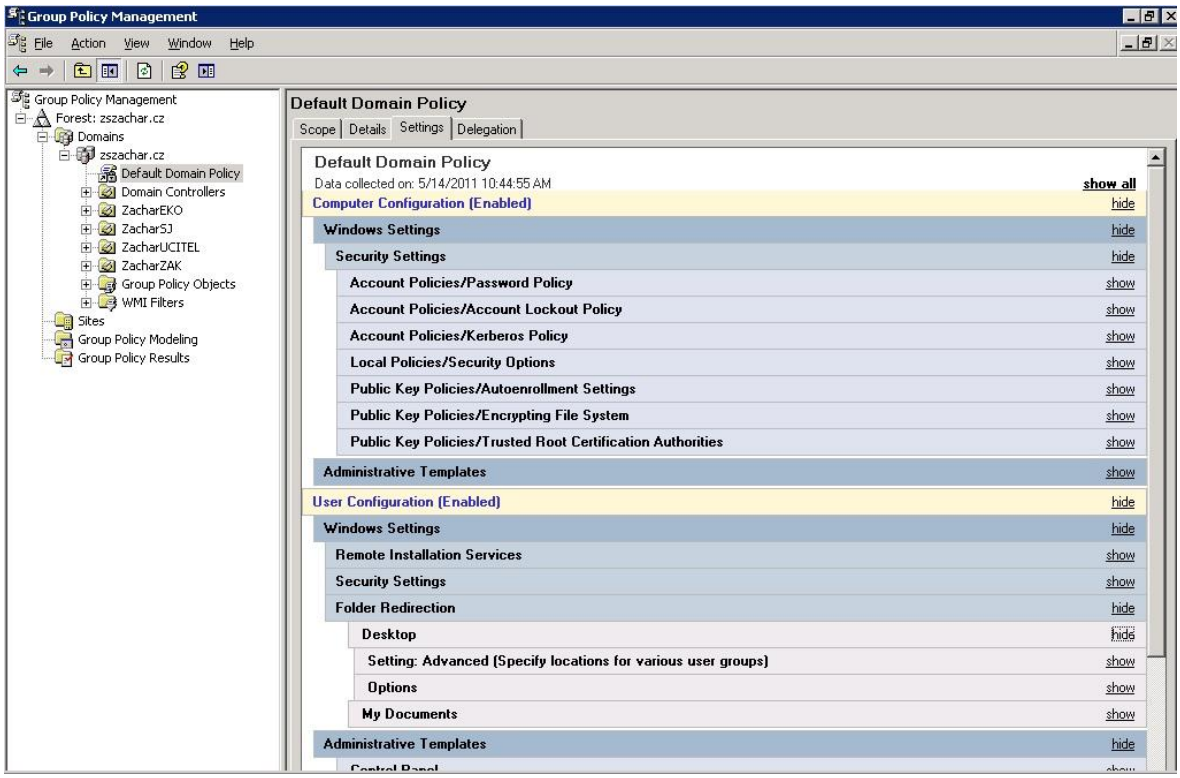
Obr. 14: Přesměrování plochy z lokálního do síťového umístění

Nastavení výchozích aplikací

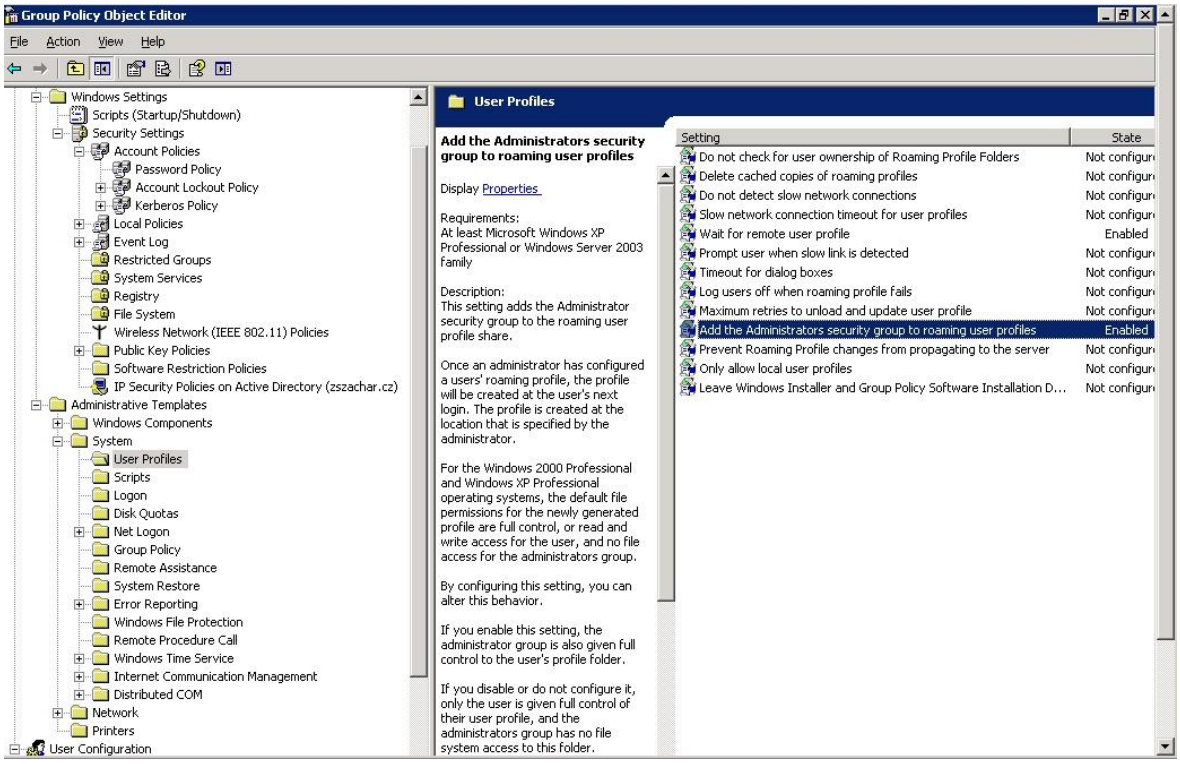
- Internet Explorer není výchozím prohlížečem (používáme jednotně Mozillu Firefox)
- Poštovním klientem je Mozilla Thunderbird, protože podporuje umístění databázového souboru s poštou v síti (Outlook Express toto neumí)
- Výchozím přehrávačem audio a video obsahu je GOM Player (interní podpora většiny kodeků umožňuje přehrávání valné většiny formátů bez nutnosti instalace externích balíků kodeků)

Ovládací panely

- Nejsou běžným uživatelům přístupné. Ti mohou měnit pouze velikost písem, schéma a pozadí plochy Windows



Obr. 15: GPO management – přehledové zobrazení



Obr. 16: GPO management – nastavování pravidel v GPO editoru

3.7 Konfigurace stanic, vzdálené instalace

V prostředí různorodých stanic se systémy MS Windows jsou kromě pravidel domény zapotřebí i další zákroky. Aby byla stanice na dálku plně kontrolovatelná, je hned při začlenění do domény ještě dále nastaveno:

- Sdílení systémového disku
- Instalace PS Tools
- VNC server

Od chvíle začlenění do domény se dané stanice týkají i instalace pomocí GPO a také všechna další pravidla v GPO definovaná.

3.8 Sdílení systémového disku

Ke sdílenému systémovému disku stanic má právo přístupu pouze administrátor. Promazávání i kopírování nejrůznějších dat je takto velmi usnadněno a může být prováděno i skriptem nebo dávkovým souborem. V příloze je uveden dávkový soubor, který řeší kopírovaní ikon a položek plochy a nabídky „Start“.

Příloha IV: Dávkové kopírování zástupců

Na jediné kliknutí je takto možno převést upravený obsah daných složek na všechny stanice v učebně, případně kabinety atp. Komplikací je zde používání systémů Windows Vista a Seven, které mají rozdílně koncipovanou strukturu složek a položky nabídky start a plochy:

„\Documents and Settings\All Users\“

jsou nahrazeny cestou:

„\ProgramData\Microsoft\Windows\Start Menu\“ a „\Users\Public\Desktop\“.

Toto je vyřešeno několika různými dávkovými soubory.

3.9 Zprovoznění PStools

PS Tools Marka Russinoviche je sada těchto užitečných nástrojů:

- *PsExec* - spustí proces vzdáleně
- *PsFile* - zobrazí seznam vzdáleně otevřených souborů
- *PsGetSid* - zobrazí SID počítače nebo uživatele
- *PsKill* - ukončí procesy podle názvu nebo ID procesu
- *PsInfo* - seznam informací o systému
- *PsList* - detailní seznam informací o procesech
- *PsLoggedOn* – ukáže, kdo je přihlášen
- *PsLogList* - zobrazí záznamy z výpisu (logu) událostí
- *PsPasswd* - změní heslo uživatelského účtu
- *PsService* - zobrazení a ovládání služeb
- *PsShutdown* - vypne nebo restartuje počítač
- *PsSuspend* - pozastaví procesy

Využití nalezne především program PSEXEC.EXE, který umožňuje dálkové spuštění libovolného programu včetně parametrů příkazové řádky. Toto lze využít pro dávkové instalace/odinstalace/konfigurace prakticky kteréhokoliv programu, který podporuje parametry příkazové řádky, např. takto:

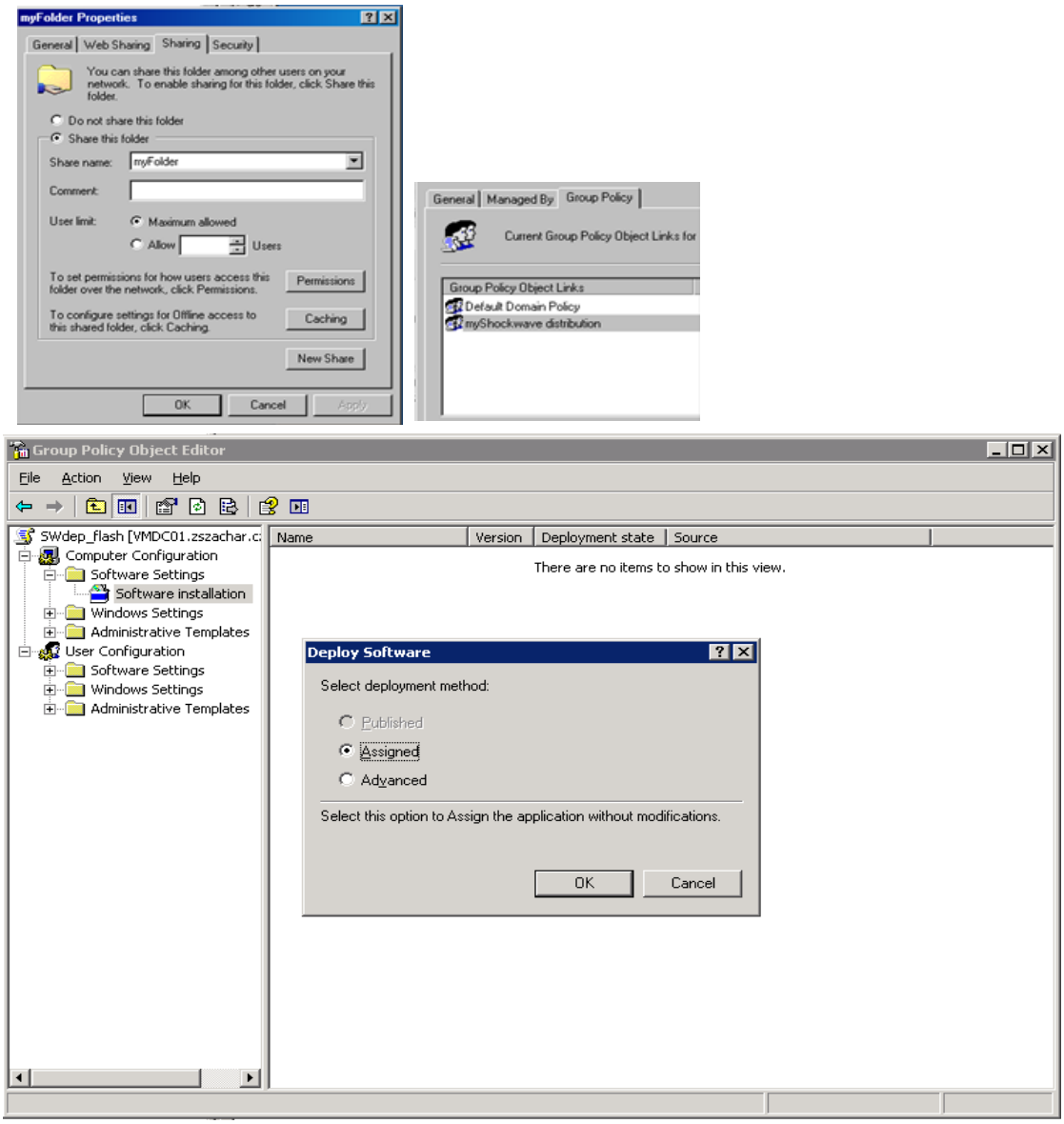
```
echo off
echo Pozor, operace trva dlouho
```

```
SET PC=\\PC
FOR %%a IN (01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18) DO %windir%\psexec -c -s %PC%%%a%
"\\server\_install\firefox4.exe /s /v" -q
echo konec operace **************************************************
pause
```

Pokud již existuje sada dávkových souborů, je tento způsob výhodnější než instalace pomocí GPO, protože nevyžaduje instalační balíčky MSI a je provedena okamžitě po spuštění dávkového souboru.

3.10 Instalace pomocí GPO

Instalace pomocí GPO je dalším způsobem hromadného nasazování softwaru uvnitř domény. Je to standard používaný jak pro instalaci aktualizací, tak pro instalaci SW třetích stran. Instalace pomocí MSI balíčku je možná pouze do počítačů s operačním systémem, které podporují technologii MSI, tedy Windows 2000, NT, XP a novější (viz návody ze stránek MS - http://support.microsoft.com/?kbid=314934).



Obr. 17: Fáze nastavení instalace pomocí GPO

Nejprve je nutné vytvořit distribuční místo, ze kterého bude MSI balíček instalován do klientských počítačů. Toto distribuční místo musí být viditelné z každého klientského počítače. Např. \\server\myFolder

Následuje vytvoření nového GPO (např. na obrázku uvedený myShockwave distribution). Tomuto objektu je nutné přiřadit skupiny nebo jednotlivce, pro které bude platit. Podle vybraného schématu je pak SW nainstalován automaticky, nebo připraven k instalaci při přihlášení uživatele.

3.11 RIS – vzdálené instalace ve velkém

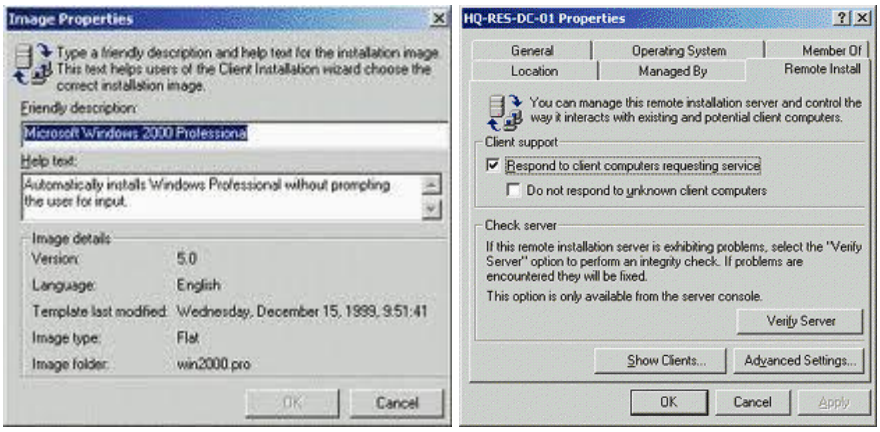
Služba vzdálené instalace (RIS) je volitelná součást zahrnutá v operačních systémech řady Microsoft Windows Server 2003 a vyšších. Existují i její opensourcové alternativy, např. Linux PXE server.

Službu RIS lze použít k vytvoření obrazů instalace operačních systémů nebo úplných konfigurací počítače včetně nastavení plochy a aplikací. Pak lze tyto systémy zpřístupnit uživatelům v klientských počítačích. Serverů RIS může být v síti několik.

Výhodou je, že při použití služby RIS není pro instalaci OS do klientského počítače požadován disk CD-ROM. Klientské počítače však musí podporovat vzdálené spuštění pomocí ROM PXE. V případě, že tato podmínka není splněna, lze RIS používat po nastartování služby z bootovací diskety, optické mechaniky nebo flash disku.

Pomocí služby RIS můžeme vytvořit bitové kopie automatické instalace operačních systémů řady Windows 2000 a vyšší. Na stránkách Microsoftu je k dispozici množství návodů, např.: http://technet.microsoft.com/en-us/library/bb742501.aspx

Pořízení bitových kopií všech OS je časově náročné a také vyžaduje dodatečnou investici do serverového hardware. Z tohoto důvodu je zatím školní RIS server pouze experimentální. S nutností reinstalace operačních systémů na stanicích se setkávám jen velmi sporadicky (1-2 případy ročně), a proto je využití RIS plánováno až v dlouhodobém horizontu.



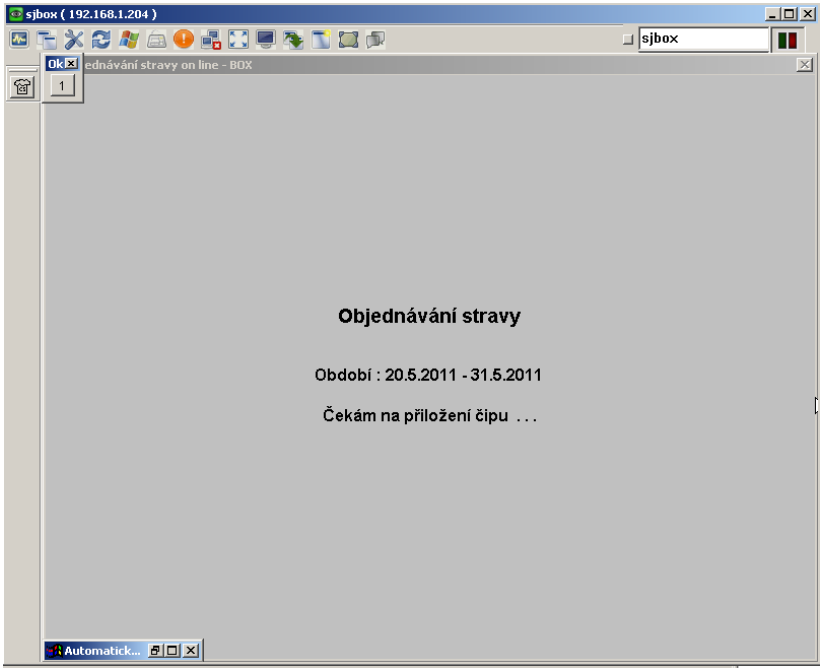
Obr. 18: Nastavení RIS

4 VZDÁLENÁ PLOCHA (RDP - MSTSC A VNC)

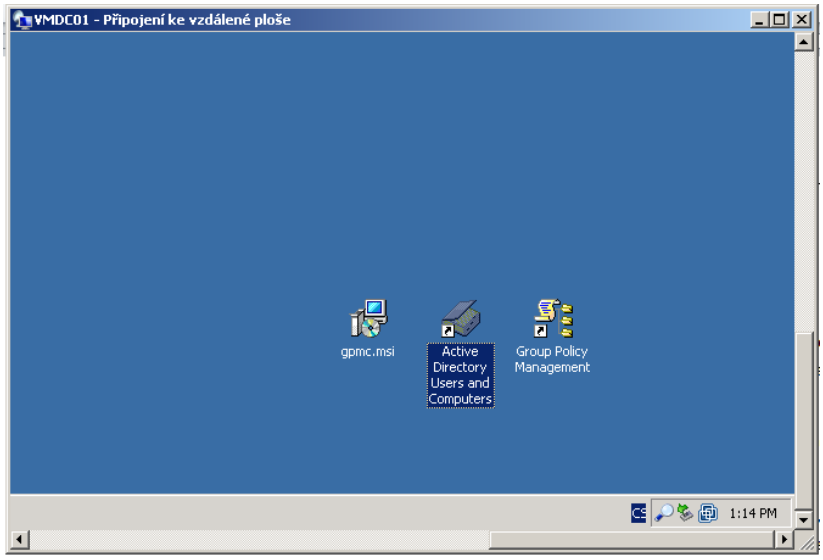
Prakticky všechny moderní systémy nějakým způsobem podporují připojení takzvané vzdálené plochy (remote desktop). Odpadá tak nutnost fyzické přítomnosti správce u počítače, který potřebuje ovládat. Vzdálená plocha je příjemná hlavně tím, že v okně (nebo na celé ploše) klientského počítače vidíme přímo plochu vzdáleného serveru a jsme schopni s ní pracovat stejně, jako bychom seděli přímo u něj. Navíc tuto funkci můžeme různě směrovat a tunelovat tak, že lze vytvořit bezpečné spojení i se serverem geograficky velmi vzdáleným.

Jedním z nativních programů OS Windows (od XP výše v každé distribuci) je mstsc.exe. Existuje také celá řada programů třetích stran. Mezi nejznámější patří VNC, který je vyvíjen v několika na sobě nezávislých verzích (Tight, Ultra, Real…).

Všechny tyto programy mají společnou důležitou vlastnost – schopnost zobrazit plochu vzdáleného počítače a posílat na tento počítač údaje o pohybu myši a stisknutých klávesách.



Obr. 19: Vzdálená plocha zobrazená v programu UltraVNC



Obr. 20: Vzdálená plocha zobrazená pomocí MSTSC.

4.1 Popis terminálových služeb a příslušného SW

Terminal Services (TS) tvoří serverovou část vzdáleného připojení k počítači, používají Remote Desktop Protocol (RDP) a Remote Procedure Call (RPC). Nachází se na serverovém i klientském operačním systému od Microsoftu. Jednotlivé verze se mezi sebou liší. Windows XP Professional povoluje jedno připojení na konzoli (console), což je přímé lokální připojení a jedno vzdálené připojení. Bohužel současně může běžet pouze jedno. Tato připojení jsou označována jako session 0 a 1. Windows Server 2003 a vyšší podporuje konzoli a dvakrát vzdálené připojení, pokud terminálové služby pracují v módu Remote Desktop for Administration. Větší počet vzdálených uživatelů lze připojit, když TS přepneme do módu terminálového serveru (Terminal Server). V tomto případě je nutné každé takové připojení licencovat.

Služba TS standardně naslouchá na portu 3389. Toto spojení je standardně šifrované. Od SP1 pro Windows Server 2003 umožňuje použít přihlášení a šifrování pomocí RDP over SSL a protokolu TLS 1.0.

Verze na Windows Serveru 2008 byla rozšířena o možnost připojit vzdáleně také pouze samotnou aplikaci.

Jako klient slouží Remote Desktop Connection (RDC), dříve Terminal Services Client, reprezentovaný souborem mstsc.exe (tse.exe). Ten umožňuje nastavit řadu parametrů připojení, včetně uložení tohoto nastavení do souboru s příponou .rdp. Mezi parametry patří kromě adresy vzdáleného stroje také přihlašovací údaje, rozlišení a další parametry

obrazovky, propojení zvukových zařízení, tiskáren, disků atd. Pokud chceme vzdálený systém spravovat, nesmíme zapomenout na přepínač /console u Windows XP starších, než SP3 a /admin u novějších. V příkazové řádce tento příkaz vypadá takto: mstsc.exe /v:{jméno serveru nebo IP} /console

Můžeme použít i další parametry:

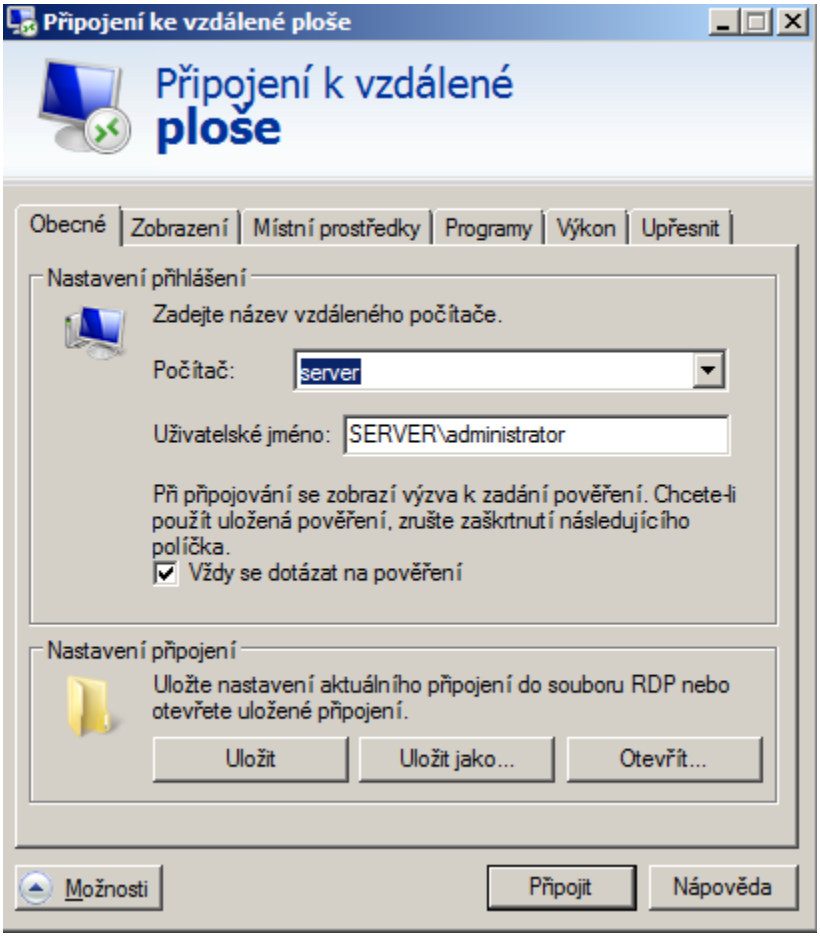
/f - full screen

/w:{width} - rozlišení RDP – šířka

/h:{height} - rozlišení RDP – výška

/v:{serverIP:port} - změna portu (pokud požíváte nestandardní port)

Další možností je použít nástroj "Remote Desktops", který je součástí Windows Server 2003 Administration Pack a lze jej nainstalovat i na Windows XP. Zde můžeme hromadně definovat připojení k RDP a také máme možnost zaškrtnout volbu "Connect to console"



Obr. 21: Konfigurační panel RDC

RDP existuje v řadě verzí, odpovídající verzi RDC je možno stáhnout pro různé verze operačního systému:

- Windows XP **5.1**
- Server 2003 **5.2** (mapování některých lokálních zdrojů)
- Vista **6.0** (možnost připojit se k aplikaci)
- Server 2008, Seven **6.1 – 7.0** (vylepšení tisku a připojení lokálních zařízení)

Bezpečnostní novinkou od verze 6.0 je Network Level Authentication (NLA), která umožňuje ověřit klienta ještě dříve, než se připojí. Připojení ke vzdálené ploše 7.0 umožňuje používat nové funkce služby Vzdálená plocha. Tyto funkce byly zavedeny v systému Windows 7 a Windows Server 2008 R2. Tyto funkce jsou k dispozici pro počítače se systémem Windows XP Service Pack 3 (SP3), Windows Vista Service Pack 1 (SP1) a Windows Vista Service Pack 2 (SP2).

Klienta RDC 7.0 lze používat pro připojení i ke starším terminálovým serverům a vzdáleným plochám. Nové funkce jsou však k dispozici pouze v případě, že se klient připojuje ke vzdálenému počítači, který používá systém

Windows 7 nebo Windows Server 2008 R2 .

Obr. 22: Různé verze RDC

Novinkou na Windows Server 2008 je také role Terminal Services Gateway. Klienti z internetu s ní komunikují na portu 443 tunelovaně protokolem HTTPS a ona předává komunikaci dovnitř sítě na port 3389.

Jako další řešení RD firmy Microsoft je třeba zmínit také Remote Desktop Web Connection, který umožňuje připojení k RD přes internetový prohlížeč pomocí komponenty ActiveX.

Holé řešení Microsoftu je samozřejmě výzvou pro tvorbu nadstavbových aplikací třetích stran. Většinou se vyznačují některými specifickými a užitečnými funkcemi. Jako zástupce mohu uvést např:

Visionapp Remote Desktop, RoyalTS 1.4.4, mRemote 1.35 beta, Remote Desktop Manager 3.0.0.2 (RDM), Terminals 1.6e, RDTabs 2.0.13.

Některé z těchto aplikací není nutno instalovat, jiné nabízejí například záložky nebo centrální správu přihlašovacích údajů.

Obr. 23: RDP programy třetích stran

4.2 VNC

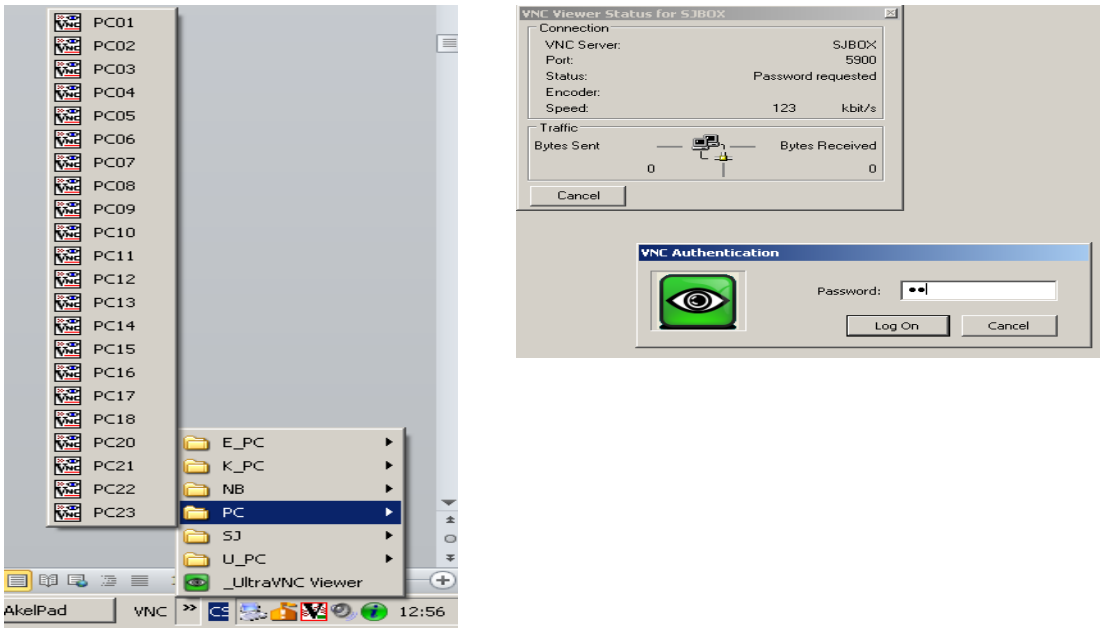
VNC (Virtual Network Computing) je program, který umožňuje vzdálené připojení ke grafickému uživatelskému rozhraní (GUI) pomocí počítačové sítě. VNC pracuje systémem klient-server. Server vytváří grafickou plochu v operační paměti počítače a ta je přenášena přes síť klientovi, který plochu zobrazuje (většinou na jiném počítači). Pro minimalizaci přenášených dat je použit protokol RFB (remote framebuffer). VNC se proto dá využít i v sítích s velmi pomalým připojením.

Původní zdrojový kód VNC i mnoho moderních odnoží je publikováno jako open source. Vývoj původního VNC byl ukončen v roce 2002, nové verze odnoží však stále vznikají a jsou dále vylepšovány.

VNC se skládá z klienta, serveru a komunikačního protokolu.

- Server je program, který sdílí obrazovku

- Klient (viewer) je program, který zobrazuje sdílenou plochu a ovládá server
- Protokol (RFB) používá bitmapu serveru, přenáší však pouze její změny a tím minimalizuje datový tok



Obr. 24: Panel zástupců VNC a přihlašovací obrazovka programu UltraVNC

Standardně VNC používá TCP porty 5900 - 5906. Porty odpovídají jednotlivým obrazovkám (0 až 6). Dají se měnit, je ovšem třeba nakonfigurovat server i klienta stejně. V některých klonech funguje ovládání i přes webový prohlížeč podporující Javu. Tam jsou standardně použity porty 5800 – 5806. Vícenásobné připojení k jednomu serveru je povoleno, ovládat lze však pouze z jednoho stroje. Ostatní klienti jsou v režimu prohlížení. Protože je VNC multiplatformní, setkáme se i se servery a klienty pro nejrůznější operační systémy včetně Linuxu, MAC OS. Jsou dostupné i aplikace pro chytré telefony s OS Windows Mobile, Symbian, Android a iPhony.

Nasazení VNC má také svá rizika. V naprosto uzavřené síti nejde o problém. Pokud však chceme využívat VNC pro přístup přes internet, případně pokud nejsme schopni kontrolovat všechna zařízení v naší síti, měli bychom jej rozhodně tunelovat, případně komunikaci šifrovat přes nějaký z doplňujících modulů. Komunikace mezi klientem a serverem standardně kromě samotné autentizace není zabezpečena. Nejvýhodnější způsob útoku na VNC komunikaci je tzv. Man in the middle – osoba sledující síťový provoz je v případě nezabezpečené komunikace schopná přesně zrekonstruovat všechna grafická data i stisky kláves a pohyby myši.

Při promyšleném a zabezpečeném nasazení je VNC vynikajícím nástrojem nejen pro dálkovou správu, ale také pro výuku, vzdálené prezentace a v neposlední řadě i jako prevence rizikového chování žáků na stanicích. V naší škole je VNC na všech stanicích mimo doménových serverů. Žáci nemají možnost tento proces ukončit a ani nevidí žádnou indikaci připojeného správce. Oproti tomu skupina učitelů má možnost s VNC serverem manipulovat a na svých počítačích také mají vizuální indikaci připojeného správce sítě.

Tato cesta se velmi osvědčila. Velmi časté jsou telefonické žádosti učitelů o vyřešení drobných problémů na jejich stanicích, případně o názorné naznačení a pomoc při práci v kancelářských aplikacích. Při výuce pak pomoc žákům nabývá mnohem konkrétnější a velmi účinné podoby. Učitel může převzít kontrolu nad plochou žáka a názorně ho vést krok za krokem. S těmito metodami jsou žáci seznamováni v prvních hodinách informatiky. Tam jsou podrobně rozebírány možnosti VNC, důvody jeho nasazení a také etický rozměr jeho používání.

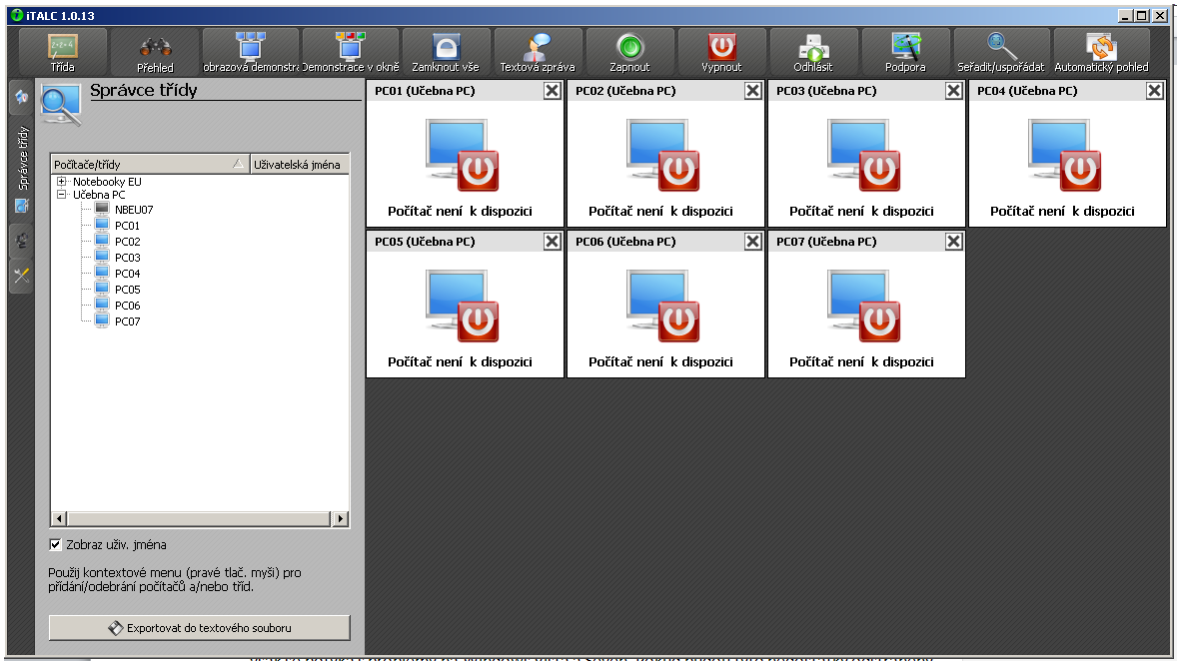
4.3 iTalc

Kromě VNC existuje celá řada aplikací pro kontrolu stanic, které jsou vybaveny centrálním kontrolním panelem, ve kterém jsou stanice seskupovány a některé příkazy jsou i hromadně vykonávány (restart, vypnutí, přihlášení, zamknutí…). Přestože je školství velmi specifickou oblastí, je na něj cílena celá řada komerčních aplikací:

- AB Tutor
- NetSupport
- Impero
- LanSchool

Rozdíly mezi nimi jsou ve funkčnosti i v ceně. Nulovou cenou si mne však získaly projekty VNCed a iTalc.

Kromě výše uvedených možností VNC nabízí iTalc velmi propracovanou centralizovanou správu počítačových učeben. Jeho nevýhodou je, že není příliš konfigurovatelný a především je v podstatě dílem jediného člověka, a proto je jeho vývoj velmi pomalý. V současné době testuji v běžném plném provozu verzi , která výborně pracuje na stanicích s Windows XP 2000, bohužel však se potýká s problémy na Windows Vista a Seven. Pokud budou tyto nedostatky odstraněny, vidím v tomto projektu velký potenciál, protože s nulovými pořizovacími náklady zajišťuje jednoduché a přehledné prostředí pro kompletní management počítačových učeben.



Obr. 25: Prostředí iTalc 1.0.13

5 KOMFORTNÍ SPRÁVA

Komfort správce sítě je z velké části závislý na používaném softwaru, nicméně nelze opomenout i některé zákonitosti fyzické manipulace s hardwarem, které mohou přispět k větší efektivitě práce

- Nálepky na zásuvce a na patchpanelu (např. s číslem místnosti) ušetří čas při dodatečném hledání v rozsáhlé kabeláži
- Databáze místností a rozmístění zásuvek
- Velká vytištěná „mapa sítě“

Obr. 26: Serverovna s patchpanelem a náhled, jak by patch panel měl vypadat

Postupem času je za cenu menších či větších kolizí přidáváno ke know-how každého správce mnoho dalších drobností. Nikdy nekončící nutností je zde ovšem neustálé získávání dalších vědomostí.

5.1 Komfort uživatelů stanic

Je zajištěn především bezproblémovým chodem hardware a co nejjednodušší údržbou software, nejlépe takovou, kterou uživatel vůbec neregistruje. U žádné ze skupin uživatelů nelze zajistit stoprocentní spolupráci, proto je nutné omezit všechny situace, které toto vyžadují na minimum, nejlépe však jim předcházet úplně. Snížení uživatelských práv na lokální stanici je z mnoha důvodů základním kamenem v prevenci většiny problémů. Uživatel by neměl mít možnost žádným ze svých zásahů učinit systém nefunkčním.

Po hardwarové stránce je dobré veškerou nutnou manipulaci také zjednodušit na minimum. Existuje jen málo způsobů, jak zabránit fyzické manipulaci se stanicí a většinou jsou velmi nákladné. Vycházejme ale z toho, že uživatel nemá v úmyslu techniku fyzicky ničit, nicméně neopatrnou manipulací i prostým užíváním může k poškození dojít. Fyzickému poškození stanic nelze vždy zcela zabránit, je však několik kroků, které mohou riziko omezit:

- Stanice umisťujeme pouze na stabilní stoly/podstavce/podlahy tak, aby nedocházelo k žádnému jejich pohybu
- Kabeláž svazujeme a zakrýváme tak, aby nebylo možno kabely „nechtěně“ přejíždět židlemi, přišlapávat, vytrhávat ze zásuvek a jinak poškozovat
- Prodlužovací kabely s vícenásobnými zásuvkami volíme nejlépe takové, které jsou vybaveny přepěťovou ochranou a možností vypínání
- Stanici vždy kompletně sešroubujeme, nenecháváme bočnice volně upadávat
- Veškeré příslušenství (dálkové ovladače, elektronická pera atd.) má vždy přesně určené místo, na kterém je skladováno
- Součástí komplikovanějších sestav výpočetní techniky je návod k použití (správnému vypnutí/zapnutí)

Obr. 27: Propojené PC, dataprojektor a sestava dvou videí. Návod k použití je na stole.

Zásad pro správnou manipulaci s výpočetní technikou je více. Ty nejpodstatnější (a zvláště nutné pro žáky) jsou vypsány formou řádů jednotlivých učeben.

Obr. 28: Učebny vybavené počítači

5.2 Softwarové zabezpečení síťových prostředků

Rozdělení celé školy na učitele, žáky a správní zaměstnance je vhodné kopírovat i v systému přidělování uživatelských práv. Nejvýše stojí administrátor, který spravuje celou doménu a má lokální i doménová administrátorská oprávnění na všech stanicích. Nikdo z ostatních uživatelů nemá na žádné stanici lokální administrátorská práva s výjimkou učitelů, kteří vlastní notebooky, případně je mají školou zapůjčeny domů. Skupiny uživatelů pak mají přístup k rozdílným zdrojům:

	administrátor	**učitelé**	**žáci**	**správní zaměstnanci**
výuka	Ano (r/w)	Ano (r)	Ano (r)	Ne
úkoly	Ano (r/w)	Ano (r/w)	Ano (r)	Ne
trh	Ano (r/w)	Ano (r/w)	Ne	Ne
Foto a video archiv školy	Ano (r/w)	Ano (r/w)	Ne	Ne
účetnictví	Ano (r/w)	Ne	Ne	Ano (r/w)
zálohy	Ano (r/w)	Ne	Ne	Ano (r/w)

Tabulka 2: Síťové prostředky přidělené skupinám uživatelů

Sdílené složky

- Výuka (V:)
    - Obsahuje instalace výukového SW, celá složka je sdílená pro čtení, ale část podsložek bylo nutno z důvodu zajištění funkčnosti výukového SW i žákům zpřístupnit i pro zápis
- Úkoly (U:)
    - Je sdílená žákům pro čtení a učitelům pro čtení/zápis. Jejím prostřednictvím jsou žákům předávány i objemnější materiály a úkoly
- Trh (T:)
    - Přístupná pouze učitelům (čtení i zápis) jako úložiště výukových materiálů, prezentací, audio a videomateriálů
- Zálohy (Z:)
    - Dostupná pouze správním zaměstnancům a správcům sítě; Funguje jako prostor, kde jsou všechny dočasné i trvalé automaticky vytvářené zálohy
- Foto a video archiv školy (F:)

- Foto a video galerie všech školních akcí, přístupná pouze učitelům, do aktuálního roku lze zapisovat, všechny starší roky jsou pouze pro čtení

- Temp
  - Společné úložiště přístupné všem (r/w), promazáváno každodenně, není automaticky připojováno

Z cestovního profilu byla vyjmuta dvojice složek „Dokumenty“ a „Plocha“ a obě jsou mapovány skriptem až při přihlášení uživatele jako disk H:. Výchozí úložiště všech uživatelem tvořených dat je tak zabezpečeno přesměrováním do míst, kde se o zálohování stará server. Další výhodou je zkrácení doby načítání cestovního profilu na minimum.

Existuje také stálé úložiště pro archivaci, do kterého nemá přístup nikdo kromě administrátora. Jedná se fyzicky o jiný stroj sloužící pouze k tomuto účelu. Ve stavu nouze lze však na tomto stroji provozovat VMWare, a tak zajistit dočasný chod virtuálního doménového serveru a web/mail serveru.

5.3 Pracovní režim, Wake On LAN, magic packet

V pracovním procesu je počítač většinou využíván konstantně a s velmi malými prostoji. Ve většině prostředí je stanice se začátkem pracovní doby zapnuta a při jejím skončení vypnuta. Správce mezitím prakticky nemá prostor provádět žádné úkony, aniž by uživatele neomezoval. Většinou se samozřejmě jedná o rutinní úkony, nikoliv o naléhavé servisní zásahy. Ty časový odklad nesnesou. Pokud však chceme co nejvíce prodloužit MTBF (mean time between failures), neměli bychom rutinní servisní úkony nikdy podceňovat. V tomto ohledu je probuzení počítače správcem po ukončení běžné pracovní doby uživatele ideálním nástrojem. V kombinaci s automatizací servisních úkonů je možné zvládat nejen velké množství servisních operací, ale hlavně je možné tyto operace plánovat a vykonávat na velkém množství pracovních stanic zároveň.

Většina stanic je využívána přes den v rozmezí 07:00 - 17:00 hod. Pak bývají vypnuty. Aby tedy mohlo docházet k servisním zásahům, je BIOS stanic nastavený tak, aby reagoval na magic packet a stanici je možno na dálku zapnout. Existuje velké množství metod jak poté zjistit, jestli spouštění stanice proběhlo v pořádku. Od naprostého základu, jako je příkaz „ping“ až po software, který prověří celou síť i s dostupnými porty.

„Jedním z nejoblíbenějších a nejběžnějších testů konektivity je příkaz ping. Ping odesílá pomocí protokolu ICMP (Internet Control Message Protocol) datové pakety označované za

požadavky na echo vzdálenému počítači na síti. Požadavky na echo jsou pakety žádající odpověď, kterou vzdálený počítač odešle zpět vašemu počítači. Tímto způsobem lze určit, zda máte se vzdáleným počítačem základní propojení. Název testu ping je odvozen ze sonarové terminologie. Odesílání krátkých signálů aktivního sonaru při snaze o vyhledání objektu se označuje za pingování, protože zvuk podobný tomuto slovu vytvoří sonická vlna, jakmile narazí na kovový trup lodi nebo ponorky.“ [2]

Přehlednou grafickou reprezentací online a offline stavů se zabývá celá řada softwaru. Některé programy k této funkcionalitě přidávají ještě další možnosti. Jedním z takových je Wake On LAN.

5.4 Aplikace WoL – Wake On LAN

WoL je program, který už od roku 2000 vyvíjí německý programátor Marco Oette. Od jednoduchého „dálkového zapínače“ stanic se časem vyvinul v komplexnější nástroj. Autor jej dává k dispozici jako freeware. V posledním roce došlo k vytvoření zcela nové verze .net a také ke změně licence na GNU General Public License version 3.0 (GPLv3). Sám autor popisuje program takto:

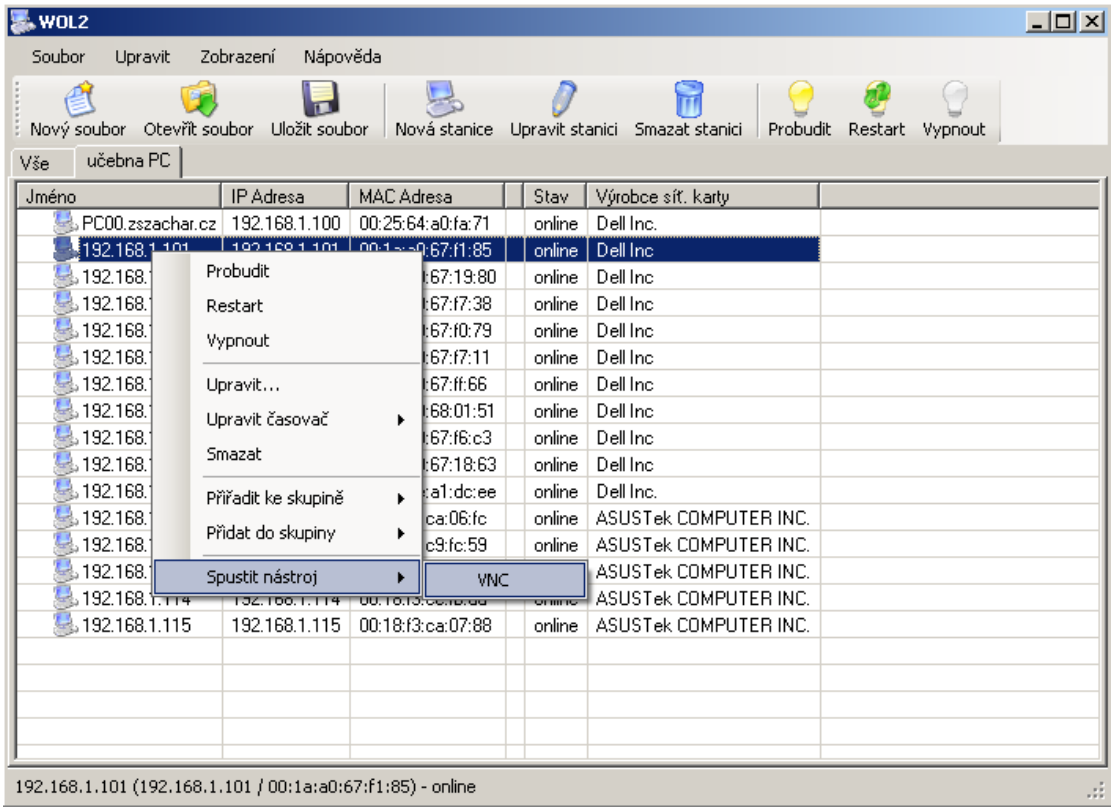
„The Wake On Lan Tool 2 allows you to power on, reboot or shut down computers / devices over LAN. You can organise your network into groups and set up timers for different tasks. WOL 2 can be configured to control VNC, Putty, MSTSC etc.“

Funkce programu:

- Zapnutí, restart, vypnutí vzdálených počítačů a zařízení v LAN
- Organizace zařízení a počítačů do skupin
- Nastavení časovače pro různé povely
- Asociace dalších programů (VNC, Putty, MSTSC atd.) a konfigurace příkazové řádky
- Vyhledávání zařízení v LAN

Program lze využívat jako nástroj správce sítě. Kombinuje sílu příkazové řádky s přehledným grafickým prostředím. Přehlednost je největším přínosem programu, protože se tak stává jakousi centrálou a rozcestníkem pro vykonání všech běžných úkonů síťové správy.

Vzhledem k tomu, že proces hledání optimální cesty správy sítě je dlouhodobý, dochází občas i k nutnosti komunikovat s autory některých SW a vznášet požadavky na funkcionalitu. Autor programu WoL Marco Oette (http://www.oette.info/) byl příznivě nakloněn všem reálným požadavkům (např. začlenění konfigurovatelné commandline přímo do menu jednotlivých zařízení) a výsledkem aktivní spolupráce byla verze WoL2 a realizace překladu jeho programu. K dnešnímu dni je přeložena stará i nová (.net) verze do češtiny.



Obr. 29: WoL2 – prostředí programu

V praxi, kdy správce sítě sedí u jednoho PC, je systém centralizovaného vizuálního přehledu nad sítí velmi užitečný. Takováto mapa sítě je neocenitelným pomocníkem zvláště z toho důvodu, že skýtá možnost konfigurovat i vlastní nástroje. Lze takto centralizovat i spouštění např. VNC, MSTSC, PSTOOLS a jiných z tohoto jednotného prostředí.

ZÁVĚR

Všechny typické úkony správy počítačové sítě je možné vykonávat i lokálně. Je však krajně nevýhodné obcházet stanice a tyto rutinní úkoly opakovat stále dokola. Důvodem je jak časová náročnost, tak i případná fyzická nepřístupnost stanic.

Komplexním řešením správy stanic se dnes často věnují až teprve firmy s „nadkritickým“ množstvím počítačů, kde by osobní přítomnost správce sítě nebyla ani vždy možná. U menších organizací je situace složitější. Nutnost řešení tohoto problému některé subjekty pochopí až v krajních situacích, nejčastěji tehdy, dojde-li ke ztrátě nebo ke kompromitaci citlivých dat.

Správa sítě ve školství znamená kromě velké zodpovědnosti také velmi omezené prostředky, kterými zaměstnavatelé disponují. Téma této práce je „komfortní správa sítě“, s ohledem na původní stav mého pracoviště bylo však potřeba se zaměřit na co nejlevnější software pro operační systémy rodiny Windows. Tyto programy přesto mohou být oprávněně považovány za standartní a bezpečné pracovní nástroje správce sítě. I ony však ke své správné funkci potřebují jeden další důležitý faktor. A tím ještě dlouho zůstane lidský mozek.

ZÁVĚR V ANGLIČTINĚ

All typical network administration tasks can be performed locally. However, it is extremely disadvantageous to walk around computers and repeat the routine tasks over and over again. The reason is time demandingness as well as the potential physical inaccessibility of machines.

The complex solution of the station administration is frequently being dealt with only by the companies with "supercritical" number of computers, where personal presence of the administrator would not be always possible. For smaller organizations, the situation is much more complicated. The need to solve this problem is often perceived only in extreme situations when sensitive data are lost or trespassed.

Working at school means at first very limited resources available to the employer. The theme of my thesis is "comfort network management", with regard to the context of my work it was necessary to focus on the cheapest software for the operating systems of the Windows family. These programs can still be justifiably considered to be a standard and safe working tool for administration. However, there is another important factor of their proper functioning. And this is going to remain the human brain.

SEZNAM POUŽITÉ LITERATURY

[1] KABELOVÁ, Alena; DOSTÁLEK, Libor - Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: CP, 2008. ISBN 978-80-251-2236-5

[2] SIMMONS, Curt; CAUSEY, James F. - Mistrovství v sítích Microsoft Windows XP. Vyd. 1. Brno : CP Books, 2005. 620 s. ISBN 8025105830.

[3] ALLEN, Robbie; LIŠKA, Alois; LOWE-NORRIS, Alistair G. - Active Directory : implementace a správa Microsoft Active Directory. 1. vyd. Praha : Grada, 2005. ISBN 8024709732.

[4] PRICE, Brad. - Active Directory : optimální postupy a řešení problému. Vyd. 1. Brno : CP Books, 2005. 381 s. ISBN 80-251-0602-0

[5] HORÁK, Jaroslav; KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. 4., aktualiz. a rozš. vyd. Brno :CP, 2008. 327 s. ISBN 978-80-251-2073-6.

[6] Peterka J.: Co je čím v počítačových sítích. COMPUTERWORLD 1993

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IT	Informační technologie, informatika.
IP	Internet Protocol, příp. Adresa IP – adresa v počítačové síti.
DNS	Domain Name System (Server) systém propojování IP adres a názvů.
NTP	Network Time Protocol - Protokol pro synchronizaci času v počítačové síti.
WINS	Windows Internet Names Service – služba Windows pro databázi síťových názvů.
PCI	Peripheral Component Interconnect - standard vysokorychlostní sběrnice.
UDP	User Datagram Protocol - Protokol druhé vrstvy TCP/IP.
MAC	Medium Access Control – Adresa MAC – identifikátor síťového hardware.
WOL	Wakeup On LAN Probuzení počítače (např. z hibernace) pomocí síťové aktivity.
GPO	Group Policy Objekt, Group Policy – zásady správy skupin a jejich objekty.
ICMP	Internet Control Message Protocol – obsluha chybových a řídících zpráv.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA I: HROMADNÝ IMPORT UŽIVATELŮ DO DOMÉNY

```
'    ---=== skript umoznující přidat do domény hromadně uzivatele z Excelové tabulky ===---
'-------------------------------------------------------------------------------------------------
' definice
Option Explicit
Dim oExcelApp, oWorkbook, oWorksheet
Dim iCounter, bEmpty, strUser
Dim sPath
sPath = WScript.ScriptFullName
sPath = Left(sPath,Len(sPath)-Len(WScript.ScriptName))
' vytvoreni objektu v Excelu
Set oExcelApp = CreateObject("Excel.Application")

' propojeni se souborem Users.xls
Set oWorkbook = oExcelApp.Workbooks.Open(sPath & "zaci.xls")

' propojeni s listem 1 a aktivace
Set oWorksheet = oWorkbook.Worksheets(1)
oWorksheet.Activate

' zviditelni zpracovavany list excelu
oExcelApp.Visible = True

' zacatek cteni dat posuneme na radek 2
iCounter = 2

' prochazeni vsech radku s vracenim hodnoty z prvniho sloupce(A)
Do Until bEmpty = True
   strUser = oWorksheet.Cells(iCounter, 1)                    ' radek, sloupec

   If strUser = "" Then                                       ' pokud je radek prazdny, je konec cyklu
      bEmpty = True
   Else
' pridavani uzivatele s predanim hodnot z dalsich bunek na radku (vola funkci addUser, ktera je nize)
            AddUser oWorksheet.Cells(iCounter, 1), oWorksheet.Cells(iCounter, 2), _
                     oWorksheet.Cells(iCounter, 3), oWorksheet.Cells(iCounter, 4), _
                     oWorksheet.Cells(iCounter, 5), oWorksheet.Cells(iCounter, 6), _
                     oWorksheet.Cells(iCounter, 7)

              iCounter = iCounter + 1
   End If
Loop
' zavira excel, ukoncuje skript
oExcelApp.Quit
WScript.Quit

' -------------------------------------------------------------------------------------------
' pridavaci procedura Adduser (je volana vzdy s hodnotami nactenymi po sobe z radku)
Sub AddUser(byVal sUserName, byVal sFirstName, byVal sLastName, _
            byVal sPhone, byVal sPassword, byVal sEMail, byVal sGroup)

            Dim oUSR, oOU, strUser, oGroup, oRoot
            Dim strUnitDrivePath                    ' cesta k sitovemu disku
            Dim strUnitDrive                        ' sitovy disk
```

```
	Dim	strExpdate		' Expiracni doba uctu
	Dim	strUserProfilePath	'cesta k profilu
	Dim	fldUserHomeDir		'pointer na složku home
	Dim	fldUserProfileDir	'pointer na složku s profilem
	Dim	strMsg,intMsg		' pro MsgBox
	Dim	curDate			'datum
	Dim	WshShell		'Pointer na script shell


	' nastaveni OU z LDAP
	Set oRoot = GetObject("LDAP://rootDSE")
	Set oOU = GetObject("LDAP://OU=ZacharZAK, " & oRoot.Get("defaultNamingContext"))
	Set oUSR = oOU.Create("User", "cn=" & cstr(sLastName)& " "& cstr(sFirstName)) ' zobrazovany tvar jmena v AD je "Prijmeni Jmeno"

	' nastaveni konkretnich hodnot pro daneho uzivatele
	oUSR.Put "sAMAccountName", cstr(sUserName)		' uzivatelske jmeno (pro systemy starsi, nez W2k)
	oUSR.Put "userPrincipalName", cstr(sUserName)		' prihlasovaci uzivatelske jmeno (stejne jako predchozi)
	oUSR.Put "sn", cstr(sLastName)				' prijmeni
	oUSR.Put "givenname", cstr(sFirstName)			' krestni jmeno
	' oUSR.Put "telephonenumber", cstr(sPhone)		' tel.
	' oUSR.Put "mail", cstr(sEMail)				' e-mail
	oUSR.Put "Description", "Ucet vytvoren scriptem v3.1"	' poznámka
	oUSR.Put "DisplayName", cstr(sLastName)& " "& cstr(sFirstName) ' zobrazované jméno

	oUSR.SetInfo


	oUSR.AccountDisabled = False				' zapnuti uctu
	oUSR.SetPassword cstr(sPassword)			' nastaveni hesla
	oUSR.SetInfo

	set oGroup = oOU.GetObject("Group","cn="& sGroup)	' nastaveni uzivatelske Skupiny
	oGroup.Add(oUSR.ADsPath)
	oGroup.SetInfo

	'mapovani slozky s profilem
	oUSR.Put "ProfilePath", "\\server\"& cstr(sGroup)& "\profily\"& cstr(sUserName)
	'mapovani domovske slozky
	oUSR.Put "HomeDirectory", "\\server\"& cstr(sGroup)& "\home\"& cstr(sUserName)
	oUSR.Put "homeDrive", "H:"
	oUSR.LoginScript = "logon.vbs"				' umisteni logon scriptu
	oUSR.SetInfo

	msgbox sFirstName& " "& sLastName& " ma uspesne vytvoreny ucet s nazvem "& sUserName& " patrici do skupiny "& sGroup	' zpráva o vytvoření uivatele

End Sub
```

PŘÍLOHA II: ODSTRANĚNÍ DIAKRITIKY Z UŽIVATELSKÝCH JMEN

```
Function nahraddiakritiku(source As Variant) As String

Const cz As String = "áÁčČďĎéÉěĚíÍňŇóÓřŘšŠťŤúÚůŮýÝžŽ"
Const en As String = "aAcCdDeEeEiInNoOrRsStTuUuUyYzZ"

Dim TmpS As String
Dim OutS As String

Dim I As Integer

OutS = ""
If IsNull(source) Or source = "" Then
 nahraddiakritiku = ""
Else
 For I = 1 To Len(source)
 TmpS = Mid(source, I, 1)
 If InStr(1, cz, TmpS, vbBinaryCompare) > 0 Then TmpS = Mid(en, InStr(1, cz, TmpS, vbBinaryCompare), 1)
 OutS = OutS & TmpS
 Next I
 nahraddiakritiku = OutS
End If

End Function
```

PŘÍLOHA III: LOGON SKRIPT (ZKRÁCENÝ)

```
Option Explicit
Dim objNetwork, objSysInfo, strUserDN, strUserName
Dim objGroupList, objUser, objFSO
Dim strComputerDN, objComputer

Set objNetwork = CreateObject("Wscript.Network")
strUserName = objNetwork.UserName
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objSysInfo = CreateObject("ADSystemInfo")
strUserDN = objSysInfo.userName
strComputerDN = objSysInfo.computerName

Set objUser = GetObject("LDAP://" & strUserDN)
Set objComputer = GetObject("LDAP://" & strComputerDN)

If (IsMember(objUser, "ZacharUCITEL") = True) Then

   If (MapDrive("S:", "\\Server\Sborovna") = False) Then
      MsgBox "Nemohu pripojit S: Sborovna"
' Kdyby nebylo namapovano pri zakladani tak tady se mapuje H Homedrive
'    End If
'             If (MapDrive("H:", "\\Server\ucitele\home\"& strUserName) = False) Then
'      MsgBox "Nemohu pripojit H: vase Dokumenty"
   End If
             If (MapDrive("T:", "\\Server\Trh") = False) Then
      MsgBox "Nemohu pripojit T:"
   End If
             If (MapDrive("U:", "\\Server\Ukoly") = False) Then
      MsgBox "Nemohu pripojit U: ukoly"
   End If
             If (MapDrive("V:", "\\Server\Vyuka") = False) Then
      MsgBox "Nemohu pripojit V: Vyuka"
   End If
             If (MapDrive("F:", "\\Server\foto a video archiv") = False) Then
      MsgBox "Nemohu pripojit F: Foto a video archiv"
   End If
             objNetwork.AddWindowsPrinterConnection "\\VMDC01\Ti01"
             objNetwork.AddWindowsPrinterConnection "\\VMDC01\Ti02"
             objNetwork.AddWindowsPrinterConnection "\\VMDC01\Ti03"
' Zprava
WScript.Echo "Vítejte, "& strUserDN & ". Přeji pěkný den!"
WScript.Quit
End If

If (IsMember(objUser, "ZacharZAK") = True) Then
             objNetwork.AddWindowsPrinterConnection "\\VMDC01\Ti01"
             objNetwork.SetDefaultPrinter "\\VMDC01\Ti01"
   If (MapDrive("V:", "\\Server\Vyuka") = False) Then
      MsgBox "Nemohu pripojit V: Vyuka"
   End If
             If (MapDrive("U:", "\\Server\Ukoly") = False) Then
      MsgBox "Nemohu pripojit U: ukoly"
   End If
```

```
' Zprava
WScript.Echo "Vítej, "& strUserDN & ". Přeji pěkný den!"
WScript.Quit
End If

Set objNetwork = Nothing
Set objFSO = Nothing
Set objSysInfo = Nothing
Set objGroupList = Nothing
Set objUser = Nothing
Set objComputer = Nothing

Function IsMember(ByVal objADObject, ByVal strGroup)
  ' test clenstvi ve skupine
  If (IsEmpty(objGroupList) = True) Then
    Set objGroupList = CreateObject("Scripting.Dictionary")
  End If
  If (objGroupList.Exists(objADObject.sAMAccountName & "\") = False) Then
    Call LoadGroups(objADObject, objADObject)
    objGroupList.Add objADObject.sAMAccountName & "\", True
  End If
  IsMember = objGroupList.Exists(objADObject.sAMAccountName & "\" _
    & strGroup)
End Function

Sub LoadGroups(ByVal objPriObject, ByVal objADSubObject)
  Dim colstrGroups, objGroup, j
  objGroupList.CompareMode = vbTextCompare
  colstrGroups = objADSubObject.memberOf
  If (IsEmpty(colstrGroups) = True) Then
    Exit Sub
  End If
  If (TypeName(colstrGroups) = "String") Then
    Set objGroup = GetObject("LDAP://" & colstrGroups)
    If (objGroupList.Exists(objPriObject.sAMAccountName & "\" _
        & objGroup.sAMAccountName) = False) Then
      objGroupList.Add objPriObject.sAMAccountName & "\" _
        & objGroup.sAMAccountName, True
      Call LoadGroups(objPriObject, objGroup)
    End If
    Set objGroup = Nothing
    Exit Sub
  End If
  For j = 0 To UBound(colstrGroups)
    Set objGroup = GetObject("LDAP://" & colstrGroups(j))
    If (objGroupList.Exists(objPriObject.sAMAccountName & "\" _
        & objGroup.sAMAccountName) = False) Then
      objGroupList.Add objPriObject.sAMAccountName & "\" _
        & objGroup.sAMAccountName, True
      Call LoadGroups(objPriObject, objGroup)
    End If
  Next
  Set objGroup = Nothing
End Sub
```

```
Function MapDrive(ByVal strDrive, ByVal strShare)
  Dim objDrive

  On Error Resume Next
  If (objFSO.DriveExists(strDrive) = True) Then
    Set objDrive = objFSO.GetDrive(strDrive)
    If (Err.Number <> 0) Then
      On Error GoTo 0
      MapDrive = False
      Exit Function
    End If
    If (objDrive.DriveType = 3) Then
      objNetwork.RemoveNetworkDrive strDrive, True, True
    Else
      MapDrive = False
      Exit Function
    End If
    Set objDrive = Nothing
  End If
  objNetwork.MapNetworkDrive strDrive, strShare
  If (Err.Number = 0) Then
    MapDrive = True
  Else
    Err.Clear
    MapDrive = False
  End If
  On Error GoTo 0
End Functin
```

PŘÍLOHA IV: DÁVKOVÉ KOPÍROVÁNÍ ZÁSTUPCŮ

```
echo off
echo Pozor, operace trvá cca 10minut **********
SET cesta1=\Documents and Settings\All Users\Plocha\
SET cesta2=\Documents and Settings\All Users
SET cesta3=\WINDOWS
SET cesta4=\WINNT
SET cesta5=\Documents and Settings\All Users\Nabˇdka Start
SET uvozovky="
SET lomitko=\

SET PC=\\192.168.1.1

FOR %%a IN (01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 20 21 22 23) DO del %uvozovky%%PC%%%a%lomitko%%%a%cesta1%%uvozovky% /F /S /Q
echo Vymazani starych zastupcu je hotovo **********
FOR %%a IN (01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 20 21 22 23) DO rmdir %uvozovky%%PC%%%a%lomitko%%%a%cesta5%%uvozovky% /S /Q
echo Vymazani polozek v menu Start je hotovo **********
FOR %%a IN (01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 20 21 22 23) DO xcopy "All Users" %uvozovky%%PC%%%a%lomitko%%%a%cesta2%%uvozovky% /S /Y
echo Prekopirovani novych zastupcu je hotovo **********
FOR %%a IN (01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 20 21 22 23) DO xcopy "WINDOWS" %uvozovky%%PC%%%a%lomitko%%%a%cesta3%%uvozovky% /S /Y
echo Prekopirovani do systemove slozky je hotovo **********
echo konec operace **********
pause
```