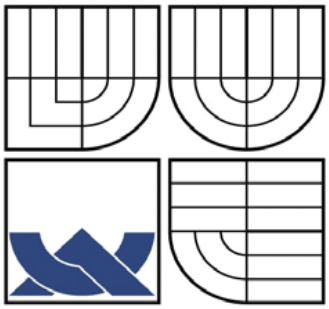
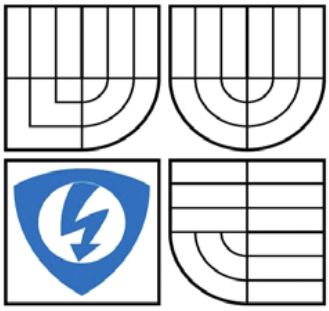


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKACNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

SPRÁVA KONCOVÝCH UZLŮ DATOVÝCH SÍTÍ

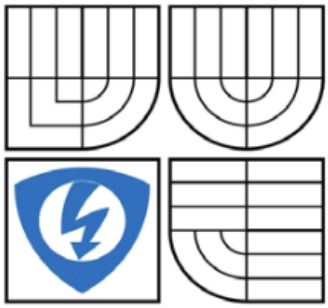
MANAGEMENT OF TERMINAL NODES OF DATA NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Radek Knol
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Vít Novotný, Ph.D.
SUPERVISOR

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Radek Knol ***ID:*** 125153
Ročník: 3 ***Akademický rok:*** 2011/2012
NÁZEV TÉMATU:

SPRÁVA KONCOVÝCH UZLŮ DATOVÝCH SÍTÍ

Pokyny pro vypracování:
Prostudujte možnosti centralizace správy koncových uzlů podnikových datových IP sítí. Navrhněte systém obsahující databázi koncových uzlů rozdělených dle typů, jako server, osobní počítač, IP telefon, IP kamera a podobně s webovým rozhraním pro možnost rychlého vzdáleného přístupu k těmto zařízením, ať už prostřednictvím www služby či vzdálené konzoly. Pro možnost upgradu firmware či nastavení konfigurace do systému zakomponujte i ftp server. Navrhněte řešení pro aktualizaci operačního systému a dat mimo dobu výuky v laboratoři.

DOPORUČENÁ LITERATURA:

[1] SOSINSKY B.: Mistrovství - počítačové sítě. Computer Press, ISBN 978-80-251-3363-7, ČR, 2010
[2] C. SIECHERT, C. STINSON, E. BOTT: Mistrovství v Microsoft Windows 7. Computer Press, ISBN 978-80-251-2817-6, ČR, 2010

Termín zadání: 6.2.2012 **Termín odevzdání:** 31.5.2012

Vedoucí práce: doc. Ing. Vít Novotný, Ph.D.

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

ANOTACE

Tato bakalářská práce má za cíl analyzovat možnosti správy koncových uzlů datových sítí. Na základě této analýzy vznikla aplikace pro operační systémy Microsoft Windows, která má za úkol efektivně spravovat a usnadňovat správu a konfiguraci koncových prvků sítě jakými jsou počítače, servery, přepínače, rozbočovače, IP telefony, IP kamery a další zařízení. Tato aplikace umí pracovat se skupinami zařízení, umí je třídit podle zadaných kritérií a na výslednou skupinu či jednotlivé prvky umí aplikovat různé funkce. Aplikace poskytuje v jednom přehledném rozhraní všechny základní operace pro správu sítě a koncových prvků, včetně synchronizačních scénářů pro aktualizaci dat na osobních počítačích. Dostupnost funkcí a přístup do jednotlivých skupin zařízení lze definovat pomocí uživatelských práv. Součástí této práce je také návrh systému pro automatickou aktualizaci operačních systému MS Windows a dalších programů společnosti Microsoft.

Klíčová slova: Správa síťových prvků, třídění prvků sítě, WSUS, Synchronizace, Microsoft, Delphi.

ABSTRACT

The aim of this Bachelor Thesis is to analyze different possibilities of administration of external nodes of data networks. On the basis of this thesis an application for the operating system Microsoft Windows has been created which is intended to enable and facilitate the administration and configuration of individual network components, such as computers, servers, network switches, hubs, IP phones, IP cameras and other devices. This application can work with groups of devices, it can sort them according to set point criteria, and it can apply different functions to the individual components or to the whole target group. This application provides all essential operations for the administration of the network and of the individual components in a well-arranged interface, including synchronization rules for data updates on personal computers. The availability of different functions and access to the individual groups of devices can be defined by means of user rights. Another part of this thesis is a proposal of a system for automatic updates of the operating systems MS Windows and other programs of the company Microsoft.

Keywords: Administration of network components, classification of network components, WSUS, synchronization, Microsoft, Delphi.

Knol R. *Správa koncových uzlů datových sítí*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2012. 45 s. Vedoucí bakalářské práce doc. Ing. Vít Novotný, Ph.D.

Prohlášení

Prohlašuji, že svoji bakalářskou práci na téma Správa koncových uzlů datových sítí jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

podpis autora

Poděkování

Chtěl bych tímto velmi poděkovat svému vedoucímu bakalářské práce doc. Ing. Vítovi Novotnému, Ph.D., za vedení, dohled a za poskytnutí informačních zdrojů potřebných k vypracování práce. Také bych chtěl poděkovat své rodině za morální podporu.

V Brně dne ....

Obsah

1 ÚVOD

Fenoménem dnešní doby je všudypřítomnost výpočetní techniky a jiných, obdobných elektronických zařízení usnadňujících naši práci. Pro co možná největší efektivitu bývají tato zařízení propojena datovou sítí, výrazně usnadňující přenos informace mezi těmito zařízeními. Funkcionalita některých zařízení je na připojení k síti přímo závislá (např. IP telefon, IP kamera) nebo tvoří přímo její nezbytnou součást (směrovače, přepínače). S rostoucím počtem těchto zařízení začal růst i počet potřebných správců s vysoce odbornou znalostí těchto technologií, což mělo za následek zvýšené náklady na provoz a údržbu těchto zařízení. Také složitost zařízení a nároky na jeho využití se stále zvyšují. Z důvodu zvýšení efektivity správy nad těmito prvky začaly vznikat počítačové programy, které usnadňují dohled a správu velkého počtu různorodých síťových zařízení. Implementace takovéhoto software má potom za následek výrazné zjednodušení a zefektivnění správy a tedy i lepší využití lidských zdrojů při správě IT zařízení.

Tato bakalářská práce se zabývá možnostmi centralizované správy síťových prvků a koncových zařízení, které se vyskytují v běžných podnikových sítích LAN. Práce má tři základní části. V první části je rozebrána obecná problematika správy prvků v počítačové síti, jsou zde popsány možné prvky takovéto sítě, problematika správy hardware, software a monitoring provozu zařízení a sítě. V druhé části jsou potom popsána již některá existující softwarová řešení pro centralizaci správy prvků sítě. Třetí část se zabývá analýzou a návrhem vlastního programu pro centralizovanou správu koncových prvků sítě.

Jelikož jsem zaměstnán jako správce informačních technologií a využívám různorodý software pro centralizovanou správu IT zařízení, tak při psaní této práce čerpám mnohé zkušenosti z technické praxe.

2 PROBLEMATIKA SPRÁVY PRVKŮ POČÍTAČOVÉ SÍTĚ

2.1 HISTORIE

První počítače vypadaly úplně jinak než dnes. Byly to obrovské elektronické, případně elektromechanické stroje s obrovskými rozměry a obrovskými nároky na prostor, chlazení a hlavně údržbu. Obsluhu takového počítače mnohdy tvořilo více vysoce vyškolených odborníků případně celých odborných týmů. Propojení do okolního světa nějakou sítí prakticky neexistovalo a počítač pracoval pouze jako autonomní celek. Záznamová média byla na bázi děrných pásků, štítků nebo později magnetických pásků. Programy byly relativně jednoduché (hlavně z dnešního pohledu) a naprostá většina závad byla hardwarového charakteru.

S postupným vývojem elektroniky - nástupem tranzistoru a poté především integrovaných obvodů počítače dostávaly dnešní tvář. Stávaly se menšími a také levnějšími, a proto i dostupnějšími veřejnosti. Počítačové sítě však nebyly rozšířené a tak byl stále počítač samostatně fungujícím celkem. Data se přenášela na magnetických médiích, jako byla audiokazeta či později disketa. Jelikož ceny byly stále ještě pro masové rozšíření velmi vysoké, výkon a softwarová výbava nebyla na nijak vysoké úrovni tak nedošlo k masovému rozšíření těchto počítačů a neměly obvykle klíčovou funkci v žádné oblasti - používaly se spíše k usnadnění nějakých činností, především matematickým výpočtům jako řešení soustav rovnic, či pro jednoduché optimalizační úlohy. Pokud takový počítač přestal pracovat, tak nedošlo ke ztrátě dat, přerušení komunikace či jiné fatální chybě. V této době také začaly vznikat různé periferie využívající počítače - tiskárny, plotry, různé záznamové mechaniky, ukazovací zařízení (tablety, myši, joysticky atd.). Obsluhou takového počítače byl obvykle velmi zkušený člověk, který zvládal i částečnou správu hardware i software.

Průlomem v rozvoji výpočetní techniky a s tím souvisejících ostatních prvků bylo uvedení počítače s označením IBM PC. Tyto počítače již byly cenově výhodné, docela spolehlivé a výkonově dostatečné pro chod snadno ovladatelných aplikací. Dochází k masovému rozšiřování počítačů a s tím potřeba jejich propojení do počítačových sítí. Následkem toho se rozšiřují i další prvky, které jsou integrovány do těchto sítí. Počítače se stávají všudypřítomnými a nepostradatelnými pracovními nástroji. Standardním vybavením budov je již strukturovaná kabeláž, propojující počítače a ostatní prvky. Ta vytlačuje postupně ostatní druhy vedení (telefonní linky, televizní okruhy pro průmyslové kamery, koaxiální kabely apod.) a dochází k integraci zařízení do počítačových sítí. To má za následek mnohdy značnou složitost celé sítě a rozmanitost zařízení, jež jsou její součástí. Také narůstají na významu informace uložené v souborových systémech a databázových systémech výpočetních systémů. Správu takovéto sítě by potom muselo obstarávat velké množství specialistů, což je finančně velmi neefektivní. To vedlo ke snaze o zjednodušení správy všech prvků v síti a začalo vznikat spoustu nástrojů a metodik vedoucích k zjednodušení správy.

2.2 PRVKY POČÍTAČOVÉ SÍTĚ

Pro správné pochopení celé problematiky je třeba zmínit nejběžnější prvky dnešních počítačových sítí, seznámit se s jejich základní funkcionalitou, principy fungování a vlastnostmi důležitými pro jejich správu. Nejrozšířenější síť (více než 80%) je typu Ethernet. Pokud nebude uvedeno jinak, budu předpokládat tento typ sítě.

2.2.1 Osobní počítač (PC)

Osobní počítač, neboli PC (Personal Computer) je nejběžněji a nejhojněji užívané koncové zařízení datových sítí. Může být v provedení pro trvalé umístění (desktop, tower, mini tower…) nebo mobilní provedení (notebook, PDA, tablet…). Pro usnadnění práce PC obsahuje operační systém, v němž jsou potom instalovány specializované programy. Použití osobního počítače je natolik univerzální, že může s použitím periferií fungovat i jako jiné koncové zařízení - například jako IP telefon, směrovač, kamera a podobně. Vlastní rozhraní mezi hardware a software potom je firmware - u PC označováno jako BIOS (Basic Input-Output System).

2.2.2 Server

Je v podstatě osobní počítač, u kterého je kladen důraz na vysoký výkon, velkou spolehlivost, datovou propustnost a často i velkou úložní kapacitu pro data. Komfort uživatelského rozhraní je až na druhém místě. Server poskytuje své prostředky (výpočetní výkon, datové úložiště, jiné služby) ostatním počítačům v síti. Fenoménem dnešní doby jsou virtuální servery, kdy na jednom (či více) výkonném fyzickém serveru běží více virtuálních serverů. Toto řešení dokáže velmi efektivně využívat výkon serverů a usnadňuje i jejich správu.

2.2.3 Síťový přepínač (switch)

Je aktivní síťový prvek, který propojuje segmenty sítě. Je to základní komponenta každé sítě. Obsahuje více síťových portů a jeden konfigurační (konzolový) port. Pracuje s druhou (linkovou) nebo třetí (síťovou) vrstvou modelu OSI. Na rozdíl od svého předchůdce - hubu, disponuje určitou inteligencí, nerozesílá příchozí pakety na všechny ostatní porty, ale dokáže na základě naučené tabulky (CAM) přepínat data pouze na určené porty. Na připojených spojích navíc podporuje plně duplexní provoz. Tím výrazně zvyšuje propustnost sítě. Přepínače standardně podporují stromovou strukturu a při zapojení do smyčky se může zahltit i celá síť - to by znemožňovalo přítomnost redundantních linek. Proto jsou lepší přepínače vybaveny protokolem STP (Spanning Tree Protocol), v současnosti jeho rychlou verzí RSTP, který si dokáže zmapovat síť, vyhledat optimální strom a spoje, které jsou duplicitní, odstaví a nechá je jako záložní pro případ výpadku hlavních spojů. Inteligentnější přepínače kombinují funkcionalitu přepínače. Přepínače jsou schopny vytvářet tzv. Trunky (sdružit více portů do jednoho virtuálního a tím zvýšit propustnost a získat redundanci). Umí monitorovat jednotlivé porty včetně pokročilého nastavení rychlostí a různých omezení. Samozřejmostí spravovatelných typů přepínačů jsou virtuální sítě (VLAN), kdy v jednom fyzickém portu může komunikovat i několik stovek virtuálních, od sebe oddělených sítí. Konfigurace těchto prvků je možná vzdáleně přes webové rozhraní (HTTP, HTTPS), textovou konzolu (TELNET, SSH) anebo i hromadně specializovaným programem pro správu prvků. Lokálně bývá přístup pouze přes konzolový port a SSH či TELNET. Přepínač disponující 48 ethernetovými a jedním konzolovým portem je na Obr. 1.

Obr. 1: Přepínač firmy Enterasys umožňující lokální i vzdálený management

2.2.4 Směrovač (router)

Primární funkcí směrovače je oddělení/propojení sítí, kdy jednotlivé sítě mohou fungovat i na různých technologiích. Směrovač má alespoň dva porty (pro virtuální sítě může mít i jeden). Každá síť by měla být oddělena od okolního světa směrovačem. Směrovač pracuje na 3. vrstvě síťového modelu OSI. Disponuje logikou, která dokáže najít optimální cestu od bodu A k bodu B. To je možné díky směrovacím tabulkám, které mohou být definovány staticky (manuálně administrátorem) nebo častěji se dynamicky tvoří, směrovače si je mezi sebou vyměňují a tak získávají potřebné informace k určení topologie sítě a následnému určení optimální cesty. Jako směrovač může fungovat i běžný osobní počítač se dvěma síťovými kartami. Konfigurace směrovače je možná vzdáleně přes webové rozhraní, textovou konzolu nebo lokálně přes konzolový port [1].

Hlavně pro domácí použití nebo v menších společnostech se používají směrovače, které v sobě integrují funkci směrovače, síťového přepínače a bezdrátového přístupového bodu. Tato zařízení nedisponují vysokým výkonem ani pokročilými funkcemi, ale umožňují snadnou konfiguraci a vynikají vysokou univerzálností použití a příznivou cenou. Ukázka takového zařízení je na Obr. 2.

Obr. 2: Směrovač integrovaný s přístupovým bodem

2.2.5 IP kamera

IP kamera by se dala popsat jako kamera a mikropočítač v jednom. Kamera zajišťuje snímání obrazu a mikropočítač má na starostí vše od zpracování obrazu přes sofistikované funkce až po odeslání dat z kamery přes počítačovou síť ke klientovi. Aby IP kamera mohla fungovat v síti, jako to umí počítač, má svoji IP adresu, zná svou masku podsítě, IP adresu směrovače i aplikaci webového serveru, takže se v síti tváří jako PC. Moderní kamery mívají veliké rozlišení a proto i navzdory pokročilým kompresním algoritmům jsou náročné na datový tok. Pokud má být v síti více IP kamer, je nutno s touto skutečností počítat již při návrhu sítě, aby kamery neovlivňovaly provoz ostatních prvků sítě. Ke konfiguraci kamery se obvykle používá webové rozhraní (HTTP). V případě velkých kamerových systémů může být použito i sofistikovaných programů k administraci kamer, které integrují většinu funkcionalit do jednoho správcovského rozhraní.

2.2.6 IP Telefon

IP telefon je telefon s pokročilými funkcemi, který ke své funkcionalitě využívá nejčastěji síťové technologie ethernet, případně WLAN. Ve své podstatě je to jednoduchý počítač, který je hardwarově upraven pro hlasovou, případně i vizuální komunikaci (agent VoIP). To je umožněno speciálním SW implementovaným v přístroji. Mnoho IP telefonů také obsahuje malý switch (2-portový), díky kterému může využívat stávající síťové připojení k PC a není tak třeba budovat další přívod. IP telefon může v sobě sdružovat i další funkce jako např. ovládání dveřního vrátného, informace z internetu (bankovní kurzy, počasí) apod. Správa telefonu se uskutečňuje přes webové rozhraní, z vlastního přístroje nebo specializovaným programem.

2.2.7 Ostatní zařízení

Se stále větším rozšíření počítačových sítí i v domácím prostředí vzniká nově spoustu zařízení, která využívají tuto technologii. Výhodou těchto zařízení je vzájemná síťová konektivita, snadná konfigurace přes velkou obrazovku osobního počítače, možnost vzdáleného sledování např. mobilním zařízením a jiné. Jsou to např. síťové tiskárny, bezdrátové přístupové body, disková úložiště, alarmy, AV systémy, inteligentní elektroinstalace, domácí spotřebiče atd. Ačkoliv i tyto prvky lze považovat za koncová zařízení sítí, nejsou v podnikovém prostředí nijak rozšířeny nebo vyžadují speciální aplikace pro správu, a proto jejich správu nebudu dále uvažovat.

2.3 SPRÁVA HW

Od zavedení prvních sálových počítačů udělala technika velký skok dopředu, elektronické součástky, ze kterých jsou počítače vyráběny jsou na vysoké kvalitativní úrovni. Při dodržení doporučených provozních podmínek se není nutno o hardware počítačů ani ostatních síťových prvků nijak obzvláště starat. Doporučenými optimálními podmínkami rozumíme optimální teplotu vzduchu, minimální prašnost a nízkou vlhkost prostředí. Okolní teplota má velký vliv na chlazení součástek přístrojů. Vysoká teplota výrazně snižuje životnost součástek nebo je může i poškodit. Prach ucpává chladicí otvory a snižuje tak chlazení přístrojů a v případě vniknutí do přístroje potom mění dieletrické vlastnosti součástek. Vysoká vlhkost může způsobit korozi spojů a konektorů a tím nespolehlivou funkci přístroje. Pokud okolní prostředí nedovoluje splnit požadavky pro provoz zařízení, lze

je umístit do speciálních skříní - racků, a ty vybavit klimatizačními jednotkami. Případně zařízení umístit do speciálních místností - serveroven, kde je prostředí optimalizované pro provoz počítačů a podobných zařízení.

I v případě ideálních podmínek mívají prvky počítačových sítí součásti, na něž je třeba dbát zvýšené pozornosti a třeba je i preventivně vyměňovat. Jsou to točivé mechanické součásti, jako jsou chladící ventilátory či pevné disky. Ty mají právě kvůli přítomnosti mechanických součástí mnohem menší životnost než ostatní části.

Pro správu hardware existují programy, které umí zařízení monitorovat po hardwarové stránce a upozorní uživatele či správce, pokud se vyskytne nějaký problém. Většina takovýchto nástrojů dokáže i predikovat závadu na základě různých technologií a ukazatelů. Například pevné disky disponují technologií S.M.A.R.T. (self-monitoring, analysis and reporting technology), kdy jsou sledovány ukazatele jako počet vadných sektorů, doba roztočení disku, opakované pokusy čtení, vibrace, zvýšená teplota a hluk. Pokud hodnoty překročí určitou mez, tak systém vyhodnotí, že brzo může dojít k poškození disku, a dá nám o tom informaci. U ventilátorů lze sledovat počet otáček, hlučnost a odběr proudu.

Časté poruchy bývají také způsobeny krátkodobými výpadky napájení - kolísání napájení. Přepětí může celý prvek úplně zničit, zatímco podpětí nemívá destruktivní účinek, nicméně vlivem krátkodobého výpadku napájení může dojít k jakémusi neúplnému restartu zařízení a to se dostane do nefunkčního stavu. Je potom nutné prvek odpojit od napájení a znovu nastartovat - někdy je i nutné obnovit SW. To je častý případ hlavně u síťových prvků (přepínače, směrovače). Proto je dobré všechny tyto prvky napájet ze zdrojů nepřetržitého napájení (UPS - Uninterruptible Power Source).

Pro sběr dat za účelem správy prvků se nejčastěji používá SNMP protokol (simple network management protocol). Na klientech jsou nainstalování agenti, s nimiž potom komunikuje server. Existuje již ve třech verzích, které se od sebe liší hlavně zabezpečením. Verze jedna je prakticky nezabezpečená, verze dva umí autentizaci a verze tři šifrování [1].

2.4 SPRÁVA SW

Instalace počítače, konfigurace směrovače nebo přepínače je časově nejnáročnější činností v přípravě zařízení k provozu. Není proto divu, že se programátoři snaží vyvíjet software pro zjednodušení těchto činností. Softwarové vybavení většiny prvků sítě je dáno výrobcem a na administrátorovi je obvykle „jen“ nastavení. V těchto prvcích je obvykle nahrán tzv. firmware a konfigurace se provádí přímo v tomto firmware nebo pomocí konfiguračního souboru. Mnohem složitější situace je u osobních počítačů a serverů, kde je prakticky nekonečně mnoho řešení konfigurace. Software počítačů se dají rozdělit do tří základních úrovní:

- **BIOS (Basic Input Output System):** nezbytný software pro chod jakéhokoli sofistikovaného elektronického zařízení. Je obvykle uložen na základní desce daného zařízení v přepisovatelné paměti z důvodu možné aktualizace. Nebývá příliš veliký (max. jednotky MB) a jeho nahrání trvá krátkou dobu - maximálně v řádu několika minut. V případě poškození není zařízení plně funkční nebo není funkční vůbec. Termín BIOS se používá převážně u počítačů. U ostatních zařízení se více užívá termín firmware. Ten může být více či méně složitý, ve většině případů bývá možnost aktualizace firmware nebo jen jeho konfigurace.
- **Operační systém (pouze PC):** je základní programové vybavení každého počítače či serveru. Do paměti je zaveden ihned po zavedení BIOSu. Hlavním úkolem je zajistit uživateli pohodlné ovládání počítače a vytvořit rozhraní pro chod ostatních aplikací. Instaluje se na pevný disk, je obvykle velmi složitý

a zabírá až několik GB kapacity disku. Porucha operačního systému může a nemusí mít za následek nefunkčnost celého systému. Díky složitosti bývá nejčastější příčinou nefunkčnosti PC právě závada na operačním systému.

- **Uživatelské programy (pouze PC):** Existuje jich nepřeberné množství, mají různou funkcionalitu a složitost. V případě poruchy jednoho programu obvykle nefunguje pouze jen on, ostatní fungují bez problému. Chyba v programu tedy není obvykle fatální pro celý systém. Špatně nevržený software však může způsobit i nefunkčnost systému či výrazně zpomalit jeho činnost.

Jak již bylo zmíněno na začátku této kapitoly, existuje mnoho programů pro správu. Obvykle je problém, aby jeden program uměl spravovat všechna zařízení s plnou funkcionalitou k danému zařízení. Obvykle jsou tedy programy rozděleny podle funkcionality nebo obsahují různé moduly pro různé činnosti:

- **Management sítě:** programy pro správu sítě a síťových prvků. Monitorují stav sítě a stav klíčových prvků sítě (směrovače, rozbočovače, opakovače atd.). Dokáží zálohovat a upgradovat firmware a konfiguraci prvků, hromadně měnit parametry a konfigurace. V případě poruchy prvku dokáží ze zálohy obnovit konfiguraci na nový prvek. Umí zobrazit topologii sítě a chovat se dle zadaných scénářů. Pomáhají při hledání poruch nebo je sami dokáží detekovat a proaktivně odhalují chybové stavy.
- **Instalace počítačů:** instalace mohou probíhat dvěma způsoby:
  - Prvním způsobem je distribuce instalační image. Ze vzorově nainstalovaného stroje se udělá pomocí nějakého programu (Symantec Ghost, Acronis True Image…) bitový obraz disku a ten se potom klonuje na jiné počítače. Je to velmi rychlá (jednotky minut) a spolehlivá metoda. Nevýhodou je to, že zdrojový a cílový hardware musí být stejný (nebo hodně podobný) a také že při jakékoli změně se musí udělat znovu nový zdrojový image. Tato metoda je funkční pro více operačních systémů (MS Windows, různé distribuce Linuxu, Novell).
  - Druhou metodou je automatická instalace pomocí odpovědního souboru. Při spuštění instalace (ručně nebo automaticky) se instalátor chová podle předložené šablony (odpovědní soubor). Instalace tak probíhá podobným způsobem jako by ji dělal uživatel s tím rozdílem, že veškerá customizace se automaticky doplní z šablony. Tento způsob instalace je velmi univerzální - nezáleží až tolik na typu hardware, ale časově je poměrně zdlouhavý (desítky minut). Navíc tato metoda řeší pouze instalaci operačních systémů MS Windows.

Výše uvedené metody jsou vhodné pro instalaci operačních systémů, nikoliv však pro instalaci aplikací (i když první metoda to zvládne). Aplikace se obvykle instalují pomocí tzv. instalačních balíčků. Ty lze vytvořit z klasického instalátoru, který prakticky každý program určený k instalaci obsahuje. Přesná tvorba instalačních balíčků je závislá na použitém správcovském software a je velmi individuální. Jednoduchý, spolehlivý a poměrně univerzální způsob je spuštění instalátoru vzdáleně z příkazové řádky (spousta programů toto umí, nebo lze použít dávku v tzv. logon scriptu).

Příkaz, který by zajistil instalaci na vzdáleném PC by mohl vypadat asi následovně:

```
\\192.168.1.2\installDir\sp3.exe /quiet.
```

Tímto se spustí tichá, bezobslužná instalace bez interaktivity uživatele. Parametry spuštění lze obvykle zjistit tak, že napíšeme do příkazového řádku jméno instalačního souboru /? - např:

Sp3.exe /?

```
---------------------------------------------------------------------------------------------------
Instalace aktualizace Service Pack 3
---------------------------
Dostupné přepínače:
[/help] [/quiet] [/passive] [/norestart] [/forcerestart] [/warnrestart] [/promptrestart] [/overwriteoem]
[/nobackup] [/forceappsclose] [/integrate:<úplná_cesta>] [/d:<cesta>] [/log:<úplná_cesta>]

        /help                           Zobrazí tuto zprávu

Režimy instalace

        /quiet                          Tichý režim (bez zobrazování informací a interakce s
uživatelem)
        /passive                        Bezobslužný režim (zobrazeny informace o průběhu)

Možnosti restartování

        /norestart                      Po dokončení nerestartovat
        /forcerestart                   Po dokončení vynutit restartování
        /warnrestart[:<sekundy>]        Zobrazit upozornění a v případě nutnosti restartovat počítač
                                        (Výchozí doba: 30 sekund)
        /promptrestart                  Zobrazí žádost o restartování počítače

Zvláštní nastavení

        /overwriteoem                   Automaticky přepíše soubory OEM
        /nobackup                       Nevytvoří záložní soubory pro odinstalaci
        /forceappsclose                 Při vypínání systému vynutí ukončení programů
        /integrate:<úplná_cesta>        Integruje aktualizaci softwaru do umístění <úplná_cesta>
        /d:<cesta>                      Zazálohuje soubory do umístění <cesta>
        /log:<úplná_cesta>              Do umístění <úplná_cesta> uloží protokol

---------------------------
OK
```

Výhoda této metody je ta, že není závislá na verzi operačního systému MS Windows (funguje na Win 2000,XP,Vista,Win7).

Pokud instalátor neumožňuje bezobslužnou vzdálenou instalaci, tak existuje další princip tvorby instalačních balíčků. Jedná se o tzv. rozdílový obraz. Princip spočívá v tom, že si program, který takto umí tvořit balíčky (Symantec GhostAI Snapshot, CA DSM Unicenter Packager) vytvoří obraz konfigurace počítače. Ten si uloží. Potom se instaluje aplikace (jedna nebo i více) určena k tvorbě balíčku, případně se provedou jiné změny v systému. Potom si program opět vytvoří obraz konfigurace. Rozdíl mezi těmito dvěma konfiguracemi potom tvoří instalační balíček. Například v programu Symantec Ghost AISnapshot je to jediný *.exe soubor, který lze distribuovat vzdáleně nebo instalovat lokálně. Nevýhoda tohoto řešení je ta, že výsledný balíček nemusí fungovat na všech systémech MS Windows vůbec nebo nemusí fungovat korektně. Distribucí nekorektně vyrobeného balíčku lze snadno poškodit i celou instalaci operačního systému!

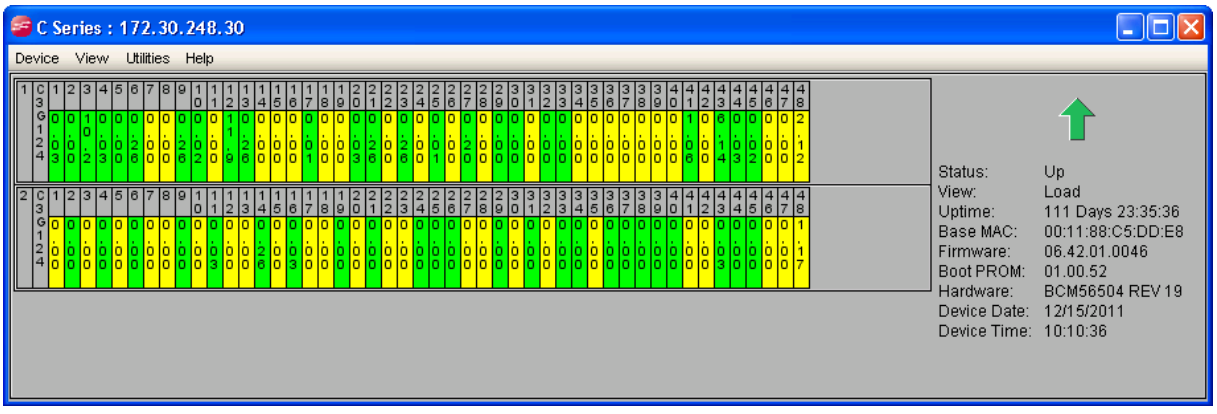
Výše zmíněné instalační metody se dají i kombinovat. To znamená, že například lze operační systém instalovat metodou instalační image a po jeho rychlém nainstalování se

použijí instalační balíčky, u kterých již trvá instalace déle, ale lze takto optimálně customizovat výslednou softwarovou konfiguraci. Nevýhodou této metody je potřebná znalost více metod, obvykle složitější konfigurace správcovského programu, případně paralelní použití více takových programů. A také nutnost dvojího licencování a tím vyšší náklady na správu.

2.5 MONITORING

Monitorovat, neboli sledovat můžeme v počítačové síti velmi mnoho parametrů. Některé parametry jsou společné většině prvků (dostupnost, teplota), jiné jsou specifické pro dané zařízení (switch-vytížení portů, UPS-kapacita baterie, počítač-počet kliků myši). Můžeme monitorovat jak hardware, tak i software. Každá síť se bez monitoringu může obejít, nicméně s rostoucí velikostí a složitostí sítě se stává nutností. Díky monitorování si může správce snadno udělat přehled o využití a stavu prvků, využití software i aktivitách uživatelů. Lze tak efektivně nastavovat parametry sítě, nastavovat konfigurace počítačů a do jisté míry předcházet poruchám. Nejčastěji monitorované parametry sítě jsou:

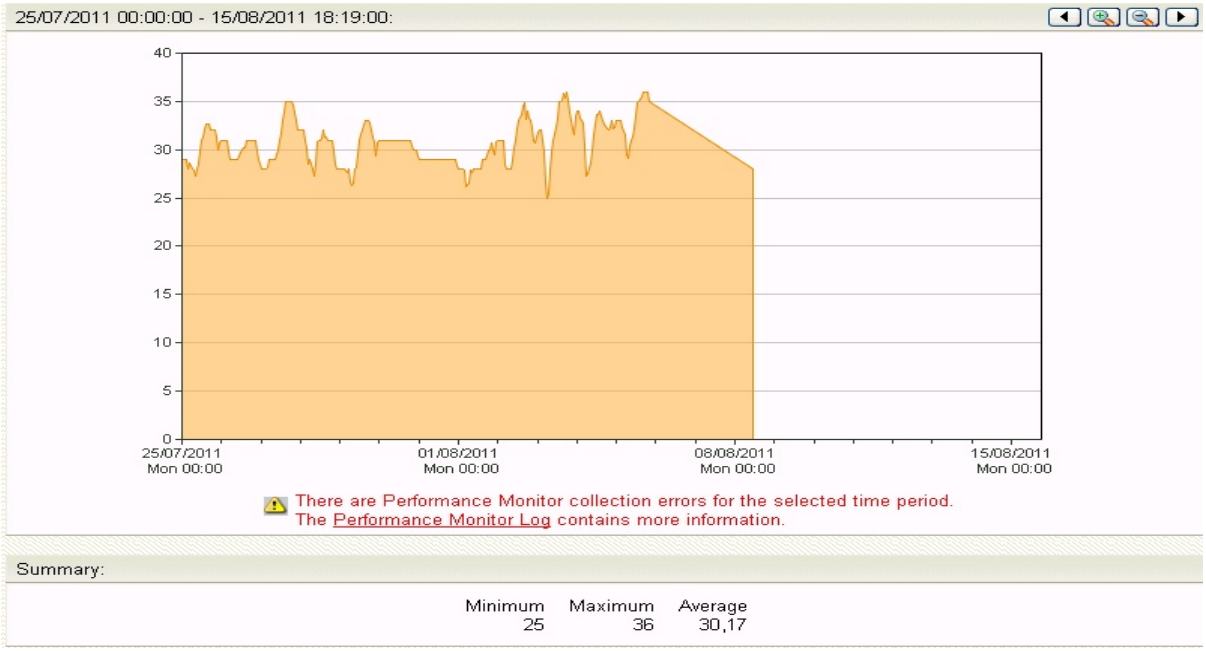
- **Dostupnost prvku:** je kontrolováno, zdali je prvek v provozu. Pokud se prvek neohlásí za daný časový interval (například na příkaz ping) tak je prohlášen za nefunkční.
- **Zatížení portů:** sledování zatížení portů může pomoci k optimalizaci nastavení sítě. Jeden přetížený port lze potom třeba rozdělit do více portů (LOAD BALANCING). Ukázka zatížení portů na dvou spřažených přepínačích Enterasys C3-48 je na Obr. 3.
- **Teplota zařízení, funkčnost ventilátorů:** tento monitoring je důležitý jako prevence před zničením prvku. Tyto jsou často umístěny v odlehlých částech areálu a uzavřeny ve speciálních skříních (Racky) a správce k nim fyzicky nepřijde často i několik měsíců. Vzdálený monitoring je tak jediná cesta jak lze zjistit závadu na chlazení. V případě přehřátí prvku může dojít k jeho poškození, výrazně klesá jeho životnost a také spolehlivost.



Obr. 3: Ukázka procentuálního zatížení jednotlivých portů síťového přepínače Enterasys C3-48

Monitoring počítačů/serverů skýtá mnohem větší možnosti. Zde lze kromě hardware sledovat i využití programů a poměrně přesně sledovat i činnost uživatele. Monitoring PC má tedy tři hlavní významy:

- **Technická analýza:** podobně jako u síťových prvků sledování dostupnosti, vytížení hardware, chybovost a zaplněnost disků, teplotu skříně apod. Vyhodnocením těchto parametrů můžeme optimalizovat chod a správu PC (přetěžované či nevyužívané PC). Monitoring teploty počítače je zobrazen na Obr. 4.
- **Inventarizace:** v rozsáhlých sítích bývá problémem mít přehled o hardware a software ve společnosti. Manuálně udržovat databázi všeho HW a SW může být poměrně složité. K částečné automatizaci lze využít právě monitoringu. Monitorovací software umí zjistit sériová čísla počítačů, výrobce a typ (informace uložené v BIOSu), připojená příslušenství (tiskárna, skener) a je schopen detekovat nainstalovaný software. Z těchto informací lze poměrně aktuálně a přesně vytvářet inventární přehledy.
- **Sledování uživatelů:** je na hraně zákona, nicméně za dodržení jistých pravidel (vnitropodnikové směrnice apod.) má na to zaměstnavatel právo. Počítače se staly neodmyslitelnou pracovní součástí většiny THP pracovníků. Ne vždy jsou však využity pouze k pracovním účelům. Pomocí monitoringu lze tedy sledovat využití počítače uživatelem, využití jednotlivých programů během pracovní doby, navštívené webové stránky, připojená periferní zařízení, multimediální obsah disků atd. Mnohdy lze restrikcemi některé chování zakázat - typickým příkladem je omezení některého obsahu webu nebo připojení jen schválených periferií (např. USB disků).



Obr. 4: Ukázka monitoringu vnitřní teploty počítače

2.6 ZÁKLADNÍ POŽADAVKY NA SOFTWARE URČENÝ PRO SPRÁVU PRVKŮ V SÍTI

Požadavky na správu zařízení se mohou lišit dle nároků jednotlivých správců od pouhého monitoringu až po úplnou konfiguraci prvků, aktivní mapou sítě, instalací, dohledem SW i HW a jiných požadavků. V této kapitole budou rozebrány základní požadavky, které by měl splňovat každý software určený pro správu koncových zařízení.

2.6.1 Funkcionalita

Funkcionalita je nejdůležitější parametr při výběru vhodného programu pro správu - právě kvůli funkcionalitě si ho správce hodlá pořídit. Jinými slovy by program měl umět minimálně to, co správce vyžaduje. Je důležité, aby měl správce přehled o jiných produktech a jejich funkcích, aby mohl dobře porovnat a posoudit, co vlastně potřebuje. Dnešní programy totiž umí i mnoho užitečných věcí, o kterých nemusí mít správce ani tušení. Dobrý program pro správu by měl správci usnadnit práci, zrychlit konfiguraci a správu a měl by umožnit správci získat dobrý a srozumitelný přehled nad zařízeními v síti. Měl by umět alespoň do jisté míry konfigurovat zařízení - ideálně i hromadně. Základní funkce jsou samozřejmě různé podle typu spravovaného hardware - jiné budou u síťových prvků, jiné u počítače.

U síťového prvku (přepínač, směrovač, opakovač) je důležitá informace o dostupnosti v sítí - to v podstatě znamená informaci o tom, zda prvek je funkční či nikoli. Je dobré mít rychlý přístup ke konfiguraci, například kliknutím na prvek se zavolá výchozí webový prohlížeč, kde je možné prvek konfigurovat. Další možností konfigurace je přístup přes SSH a TFTP klienta. Software může posílat i různé notifikace, například při nefunkčnosti nějakého přepínače, serveru či IP kamery pošle SMS nebo email na předvolené osoby. Vestavěný scheduler zase může automaticky spustit předvolené akce mimo pracovní dobu, typickým příkladem může být záloha či update firmware prvků.

Správa počítačů je od správy síťových prvků odlišná - proto většina management software je určená buď pro správu PC, nebo pro správu síťových prvků a zřídka kdy jsou tyto dva odlišné programy sloučeny do jednoho. Primárními funkcemi software pro správu počítačů je automatická instalace operačních systémů a programů, případně synchronizace datových adresářů. Pokud je SW určen pro rozsáhlejší podnikové sítě, tak je nezbytnou nutností uživatelská podpora - což z velké části znamená vidět obrazovku uživatele. To umožňuje funkce k přebírání vzdálených obrazovek. Také zde je dobré mít podporu probuzení PC po sítí (WOL - WAKE ON LAN). Často bývá integrován nástroj asset managementu pro tvorbu auditů a přehled instalovaných či používaných produktů.

2.6.2 Přehlednost a ovladatelnost

Pokud má být software efektivně používán, tak musí být uživatelské rozhraní správně navrženo. Na přístupných místech musí být umístěny nejčastěji používané prvky. Správce by měl mít přehled o všech důležitých prvcích v síti a rychlý přístup k informacím a hlavním ovládacím prvkům. Ovládací prvky či skupiny prvků musí být členěny do logických celků, které si může správce navolit a pojmenovat dle svých zvyklostí nebo zavedených standardů firmy. Prostředí programu musí být intuitivní přehledné a ovládací prvky musí být umístěny na místech, kde jsou očekávány.

2.6.3 Spolehlivost a kompatibilita

Při návrhu programu je třeba počítat s tím, že aktuální verze operačního systému bude brzo nahrazena novější verzí. Vývoj programového vybavení jde tak rychle kupředu, že verze

je kolikrát aktuální pouze několik měsíců. Program by tedy měl být navržen tak, aby neměl problémy s přechodem na vyšší verze operačních systémů - alespoň po nějakou dobu. Neměl by využívat žádné nestandardní komponenty systému či chyby v systému nebo jeho důležité součásti (např. firewallu). Program nesmí negativně ovlivnit chod operačního systému či firmware, nadměrně zatěžovat hardware nebo samotnou síť. Pokud jsou využíváni klienti, tak je třeba počítat s nehomogenním prostředím, různými operačními systémy či různými výrobci hardware a různými typy a druhy hardware. Program pro správu by měl umět pracovat s co možná největším portfoliem těchto zařízení, byť s některými třeba jen omezeně.

2.6.4 Podpora a údržba

Neméně důležitými aspekty při výběru management softwaru je podpora při implementaci a provozu a také nároky na rutinní údržbu software. Obzvláště sofistikovaný software určené pro správu velkých sítí vyžaduje vysokou odbornost při instalaci a zavedení do provozu. Může se stát, že správce při implementaci narazí na problém, který sám nedokáže řešit - v takovém případě je dobré mít možnost konzultace s odborníkem, který má znalost programu. Tato možnost bývá standardem u produktů komerčních výrobců, kteří disponují vývojovými týmy a oddělením uživatelské podpory. Nekomerční produkty nebývají tak složité a podpora jim obvykle chybí, nebo je velmi omezená.

Údržbou je zamýšlena hlavně údržba případné databáze, kontrola chyb a zálohování. Tyto úkony by měly co nejméně zatěžovat správce, měly by se nastavit při implementaci a dále se provádět na pozadí. Správce by měl dostat pouze informaci o případné chybě. Veškeré udržovací činnosti nesmí narušit činnost koncových zařízení.

2.6.5 Náklady na pořízení a provoz

Cena je často nejdůležitější atribut při výběru software pro správu sítě. Produkty se dají rozdělit do dvou základních kategorií:

- **Komerční produkty:** obvykle velké balíky nebo modulární systém s nadstandardní funkcionalitou. U modulárního typu je výhoda, že zákazník zaplatí pouze moduly, které využije. Nicméně ceny se dle typu, rozsahu a počtu spravovaných stanic pohybují od několika desítek tisíc až po stovky tisíc korun. Velkou výhodou je podpora dodavatele buď v ceně, nebo dodatečně placená. Pro středně velké a velké společnosti, které disponují více než desítkami prvků v síti je tento software prakticky nezbytný, neboť na síťovém provozu obvykle stojí vnitřní i vnější komunikace firmy. Při větším počtu PC se stává problematická i manuální instalace PC. Naproti tomu existují produkty, které jsou „předplaceny“ nákupem jiného software. Například systém pro updatovaní operačních systémů MS Windows je možné provozovat zdarma.
- **Nekomerční produkty:** zpravidla menší programy, tvořené často jednotlivcem. Mají malý počet funkcí, jsou levné nebo úplně zdarma. Systémová podpora programu obvykle žádná nebo velmi omezená. Hodí se pro malé sítě a to spíše jako podpůrné nástroje.

Je na každém, pro jaký model se při výběru rozhodne. Při rozhodování je třeba vzít v potaz velikost síťového prostředí, důležitost bezchybného chodu a rychlost opravy případné havárie či instalaci software.

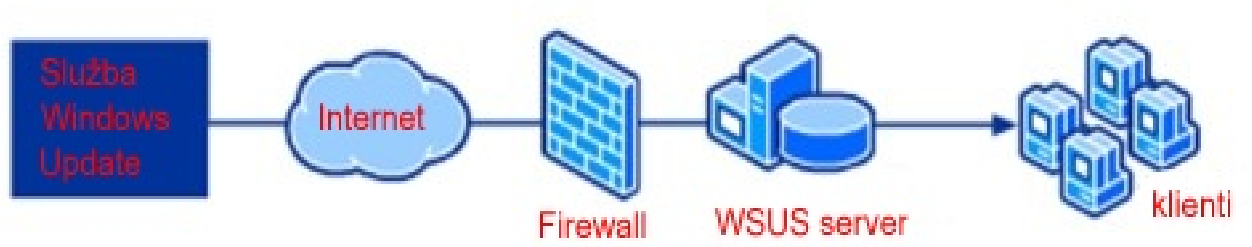
3 POPIS A FUNKCIONALITA EXISTUJÍCÍCH SYSTÉMŮ

Tato kapitola je zaměřena na popis některých již existujících systémů pro správu prvků v počítačové síti. V podstatě žádný produkt nedokáže splnit zadání této práce beze zbytku. Je to dáno tím, že produkty jsou specializovány buď na správu sítě - přepínače, směrovače, opakovače, přístupové body nebo na správu stanic. Například aktualizaci stanic - uvažuji systém MS Windows, který je naprosto převažující, lze řešit mnoha způsoby. Nicméně existuje efektivní nástroj, který je přímo k tomuto účelu určen, a není důvod ho nepoužít. V praxi je tedy nutno použít minimálně tři systémy pro úplnou správu rozsáhlé sítě. Tím bude systém pro aktualizaci operačního systému (MS WSUS), systém pro správu síťových prvků a systém pro správu počítačů, případně serverů.

Budu se zabývat převážně komerčními produkty renomovaných výrobců, neboť nekomerční software obvykle neposkytuje dostatečnou funkcionalitu, nebo není garantována a pro správu podnikové IT infrastruktury považuji za nutné použít spolehlivý produkt s dostatečnou technickou podporou.

3.1 WSUS(WINDOWS SERVER UPDATE SERVICES)

Tento software je určen k instalaci aktualizačních balíčků a bezpečnostních záplat operačních systémů MS Windows, balíku MS Office, Internet Exploreru, Systém Management Serveru a dalších produktů z rodiny Microsoft. Poskytuje v rámci lokálních sítí Microsoft úplné řešení správy aktualizací. Společnost Microsoft vydává každé druhé úterý v měsíci nové opravy a aktualizace pro své produkty. Výjimečně, případě kritických aktualizací i v jiné termíny. Operační systémy MS Windows mají v sobě integrovánu službu Windows Update, která je schopna se buď automaticky, nebo manuálně připojit pomocí sítě Internet k aktualizačnímu serveru Windows Update a stáhnout si výše zmíněné aktualizace. Tento proces je ve firemním prostředí velmi neefektivní, neboť by každý počítač v síti potřeboval přístup do sítě Internet, každý počítač by si stahoval stejné aktualizace jako ostatní počítače a tím nadměrně zatěžoval jak internetovou přípojku, tak síťové prvky a koneckonců i aktualizační servery. Navíc, v tomto případě nemá správce žádnou kontrolu nad provedenými či neprovedenými



Obr. 5: Princip služby WSUS

aktualizacemi. Tuto situaci lze řešit právě službou WSUS. Velmi důležitým faktem je to, že tento produkt je zcela **zdarma**, a je ke stažení na webových stránkách Microsoftu. Princip služby je zobrazen na **Chyba! Nenalezen zdroj odkazů.**.

Vzhledem k tomu, že vyřešení automatických aktualizací systémů jsou jedním z požadavků na tuto bakalářskou práci, tak níže rozeberu instalaci této služby podrobněji.

3.1.1 Požadavky pro fungování služby WSUS (v.3.0)

Hardwarové nároky na provoz WSUS serveru nejsou nijak vysoké. Zhruba pro 500 klientů je dostačující PC s dvoujádrovým procesorem, 4GB paměti RAM a dvěma diskovými oddíly. Na jeden bude instalován operační systém a samostatná služba, zde je třeba minimálně 2GB prostoru. Druhý potom bude sloužit jako datové úložiště - doporučeno je cca 30GB prostoru. Samozřejmostí je připojení k síti internet.

Služba WSUS může být provozována pouze na operačních systémech Windows Server 2003(SP1) a novějších. Konkrétní softwarové požadavky, závislé na použitém operačním systému jsou:

MS Windows Server 2003 SP1:

- Internetová Informační služba IIS 6.0 - součást operačního systému
- Microsoft .NET Framework 2.0 (ke stažení z webu Windows Update)
- Microsoft Report Viewer Redistributable 2005 (ke stažení z webu Windows Update)
- Microsoft Management Console 3.0 (ke stažení z webu Windows Update anebo je součást Service Packu 2 pro windows 2003)
- Databázový server - například MS SQL express (ke stažení zdarma)

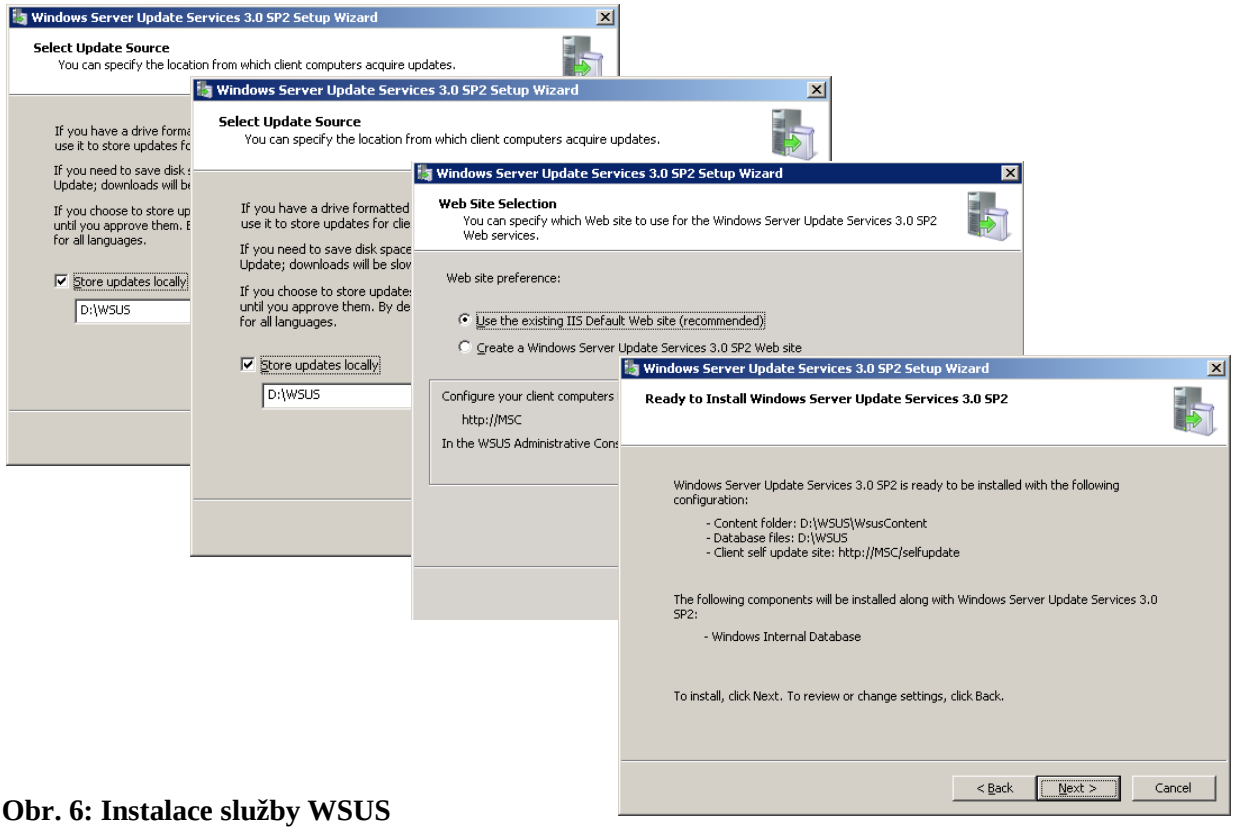
MS Windows Server 2008:

- Internetová Informační služba IIS 7.0, kde je třeba povolit tyto komponenty:
  - ASP.NET,
  - Windows autentizace,
  - 6.0 Management Compatibility,
  - IIS Metabase Compatibility,
- Microsoft Report Viewer Redistributable 2005 (ke stažení z webu Windows Update),
- Databázový server - například MS SQL express (ke stažení zdarma).

3.1.2 Instalace služby WSUS

Pokud jsou splněny všechny požadavky pro provoz služby, je možné přistoupit k samotné instalaci. Instalaci je nutno provádět pomocí účtu, který je v místní skupině Administrators. Aktuální verzi WSUS je možné stáhnout na adrese: *http://go.microsoft.com/fwlink/?LinkId=47374*.
Instalační soubor se má název „*WSUSSetup.exe*“. Po spuštění a odsouhlasení licenčního ujednání je nutno vybrat cíl instalace. Zároveň si můžeme zvolit, zdali chceme aktualizace ukládat na místní disk nebo je použít ze vzdáleného serveru. Doporučuji ukládat místně. Dalším oknem průvodce instalační služby je výběr databáze, která bude pro chod služby využita. Výchozím nastavením je instalace WMSDE, který je volitelnou součástí Windows 2003. Osobně doporučuji použít volně šiřitelný databázový stroj SQL Express, který skýtá při případných problémech širší možnosti správy a diagnostiky. V případě použití externí databáze, je tuto nutno vybrat právě v tomto okně. Třetí možností je použití databáze instalované na úplně jiném serveru. Třetím a velmi důležitým oknem instalátoru je výběr webového serveru, na kterém služba WSUS poběží a na který budou směrováni klienti. Výchozím nastavením je port 80. Pokud již na tomto serveru a portu již provozován nějaký webový server tak se vytvoří nový web server s portem 8530. Na adresu a tento port potom

budou směrování klienti služby. Potom instalátor zobrazí rekapitulaci nastavení a po potvrzení proběhne instalace služby.[2]



Obr. 6: Instalace služby WSUS

3.1.3 Průvodce nastavení WSUS

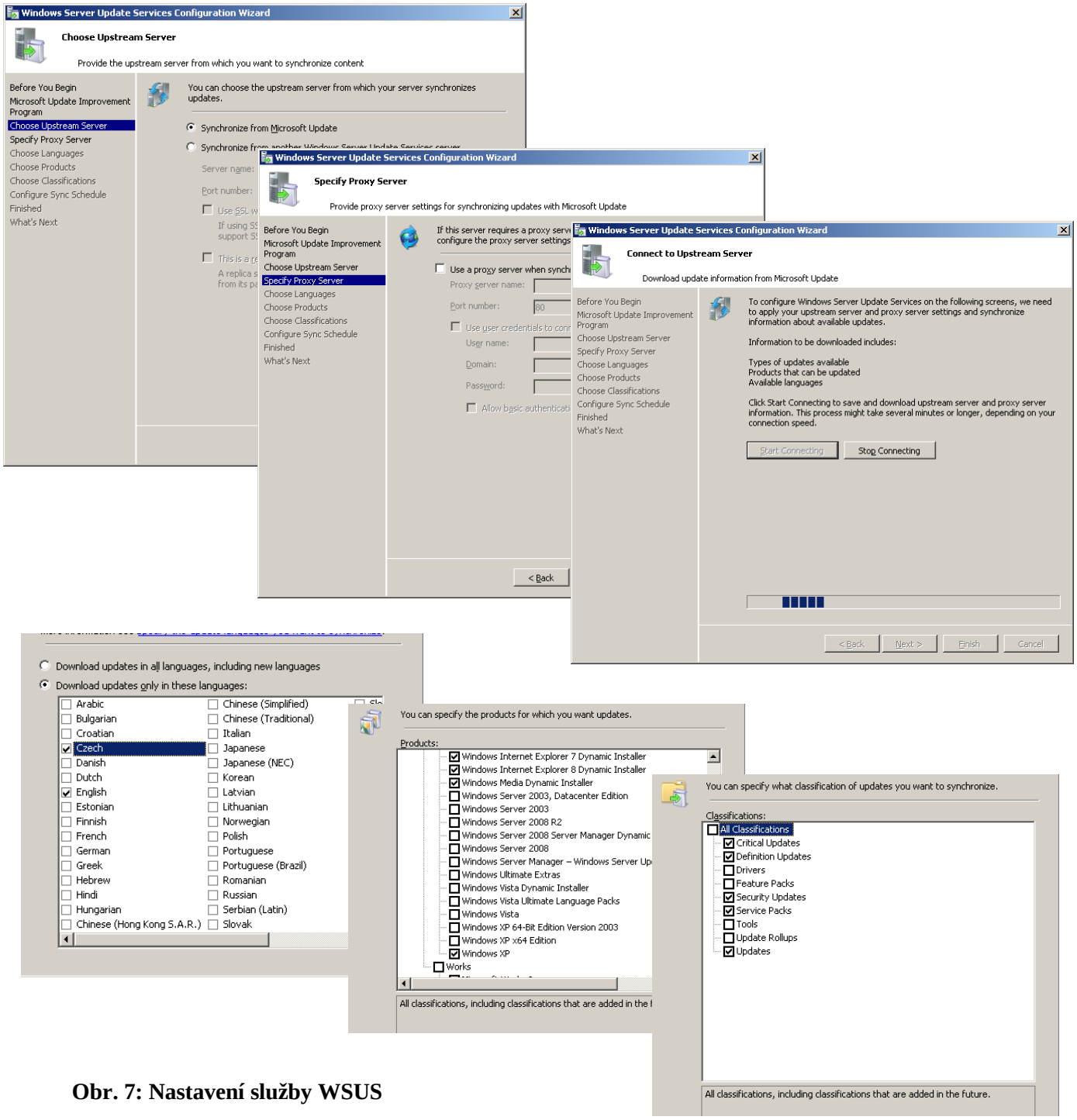
Po úspěšné instalaci ihned instalátor nabídne průvodce prvotním nastavení systému. Prvním oknem je nepodstatné nastavení zapojení či nezapojení se do programu vedoucímu ke zlepšování služeb a software. Další stránka průvodce umožní nastavení zdroje instalačních a opravných balíčků. Je vhodné ponechat výchozí nastavení a stahovat tyto aktualizace ze serveru Microsoft Update. Pouze v případě složitější struktury a velkého počtu klientů je vhodné provozovat v jedné síti více WSUS serverů a jeden použít jako „mateční“ a stahovat aktualizace z tohoto nadřazeného serveru. Na další stránce průvodce je možné nastavit proxy server pro připojení k internetu. Toto nastavení je individuální dle parametrů sítě. Toto nastavení kontroluje další stránka, která ověří, jestli se lze anebo nelze připojit k Windows Update serveru. Pokud spojení na server Microsoft Update proběhne úspěšně, tak se zobrazí aktuální seznamy jazyků, balíčků a produktů, které je možno pomocí služby WSUS stahovat a ukládat na lokální úložiště. Toto lze provádět manuálně anebo automaticky v zadaných časových intervalech. Doporučuji vybrat pouze produkty a verze, které jsou v aktuálním používání, neboť výběrem mnoha produktů a jazykových verzí se výrazně zvyšují nároky na lokální datové úložiště.[2]

3.1.4 Konfigurace klientů

Způsob nastavení klientů záleží na nastavení konkrétní síťové infrastruktury. V podstatě jsou

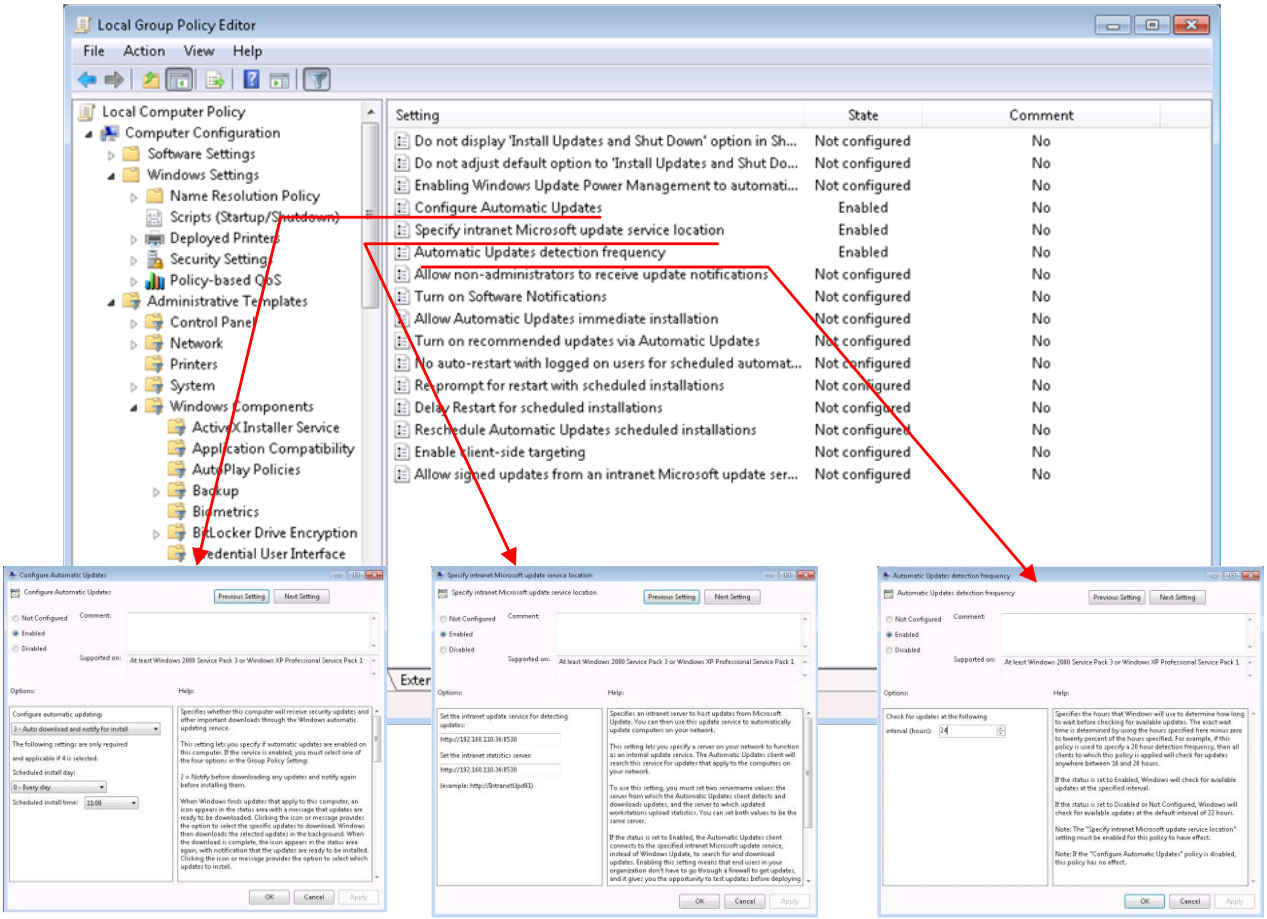
dva možné způsoby nastavení:

- Pokud je v síťovém prostředí nastavena služba Active Directory (s řadičem domény), tak je ideální použít hromadnou konfiguraci pomocí zásad skupiny (GPO). Zde se nakonfiguruje politika skupiny a ta je potom aplikována automaticky při přihlášení počítače do dané organizační jednotky.
- Jestliže jsou klienti v prostředí bez řadiče domény, je nutno konfigurovat Zásady místní skupiny. Toto je nutné udělat na všech klientských počítačích manuálně. Editor místních zásad se spustí příkazem gpedit.msc z nabídky: „*Start - Spustit*“v systému MS Windows XP anebo „*Start - Všechny programy - Příslušenství - Spustit*“ v systému MS Windows 7.



Obr. 7: Nastavení služby WSUS

V obou výše uvedených případech je nutné na klientských stanicích povolit službu automatických aktualizací a nasměrovat je na ten správný aktualizační server. Cesta k nastavení služby WSUS je v Editoru místních zásad následující: *Konfigurace počítače - Šablony pro správu - Součásti systému Windows - Windows Update* (Obr. 8). Ostatní nastavení umožňují upravit další vlastnosti a chování klienta, jako je například způsob instalace, restartování systému a podobně. Jejich význam je velmi dobře patrný z popisu.[2]



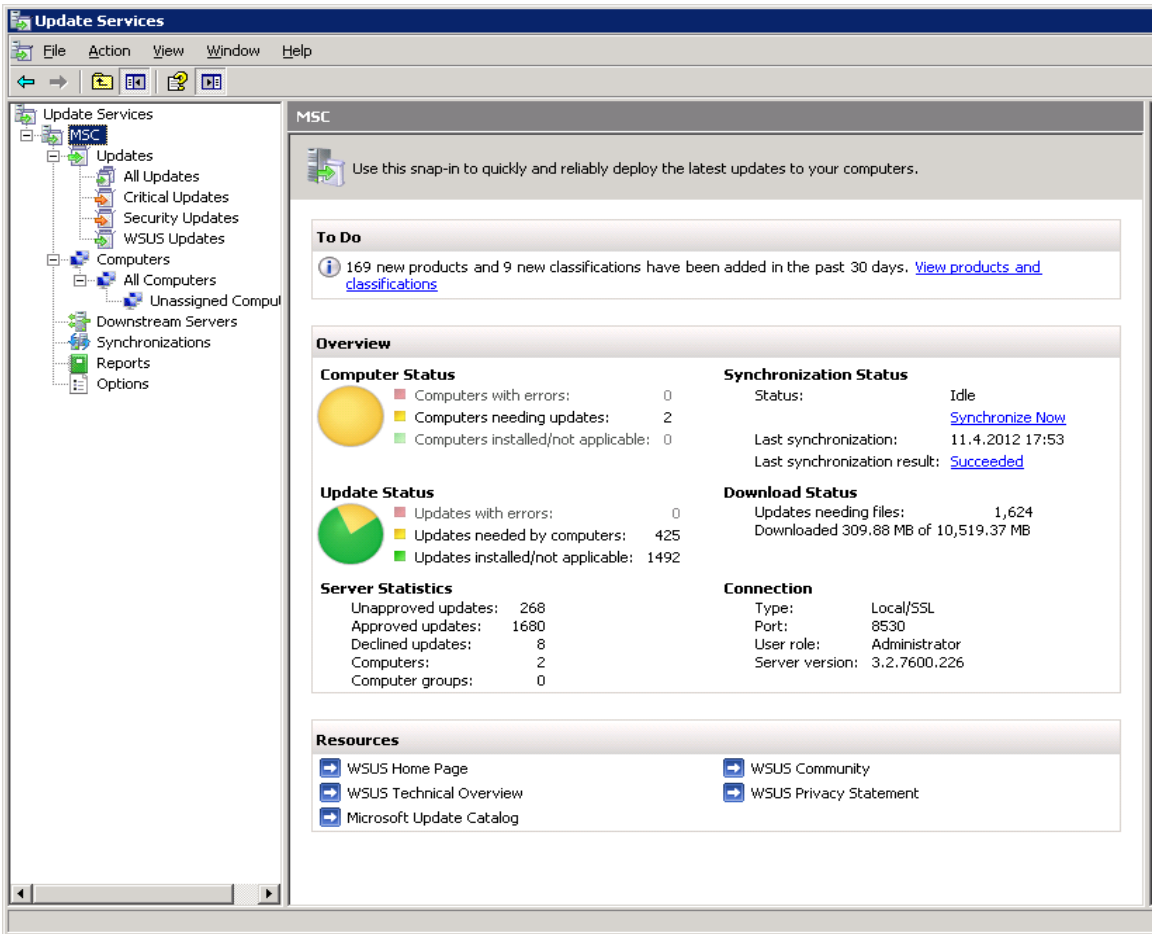
Obr. 8: Konfigurace lokálních politik pro službu WSUS

3.1.5 Správa služby WSUS

Správcovská konzole se spouští z nabídky „*Start*“. Po spuštění se zobrazí výchozí okno služby - Obr. 9. Jsou zde zobrazeny případné úkoly, na které je třeba reagovat. Je to například počet aktualizací, které je třeba schválit/neschválit. Další informace zobrazují přehled o službě :

- **Stav počítače** - informace o tom, kolik počítačů je zaktualizovaných a kolik z nějakého důvodu zaktualizovaných není

- **Stav aktualizací** - informace o počtu nainstalovaných aktualizací a o počtu aktualizací, které se mají ještě nainstalovat
- **Stav synchronizace** - stav poslední synchronizace se serverem Microsoft Update.
- **Stav stahování** - informace o počtu a velikosti aktualizačních balíčků, které jsou schváleny k instalaci, ale ještě nejsou staženy ze serveru Microsoft Update do lokálního úložiště.



Obr. 9: Správcovská konzole WSUS

Jednou z nejdůležitějších činností administrátora WSUS serveru je schvalování aktualizací k instalaci na vybranou skupinu počítačů. Doporučením je odzkoušet si plánované aktualizace na menší skupině PC a po ověření funkčnosti povolit tyto aktualizace na větší skupinu. Schválení se provádí tak, že se zobrazí neschválené aktualizace a pomocí pravého tlačítka myši se schvalují aktualizace pro jednotlivé skupiny. Po schválení služba vypíše informaci o výsledku schvalovacího procesu.[2]

3.1.6 Přehled ovládacích panelů WSUS

Levou stranu správcovské konzole tvoří řada ovládacích panelů. Jejich funkci se pokusím v následujících řádcích stručně popsat.

- **Aktualizace:** tento pohled obsahuje informaci o všech dostupných aktualizacích. Zobrazení je rozděleno podle kategorií: aktualizace zabezpečení, kritické aktualizace a aktualizace vlastní služby WSUS. Zároveň je zde zobrazen přehled o tom, kolik aktualizací je již nainstalováno (úspěšně, neúspěšně), kolik jich bude instalováno. Také je zde informace o jednotlivých aktualizacích - datum vydání, co aktualizace obsahuje, zdali vyžaduje restart PC, pro který produkt je určena atd. Kliknutím na aktualizaci lze získat její kompletní report.
- **Počítače:** zde je zobrazen přehled klientských počítačů, které službu WSUS využívají. Je možné je rozdělit do skupin a podle nich potom přiřazovat různé aktualizace. Přehledně je zde vidět kdy se počítač službě naposledy nahlásil, zda má nainstalovány všechny schválené aktualizace nebo jestli se nějaké nezdařily.
- **Synchronizace:** panel synchronizace zobrazuje výsledky jednotlivých synchronizací s aktualizačním serverem Microsoft Update.
- **Sestavy:** tento panel slouží ke generování různých reportů o klientských počítačích a statistiky o úspěšně či neúspěšně nainstalovaných balíčcích a aktualizací. Reporty lze potom tisknout v různých sestavách.

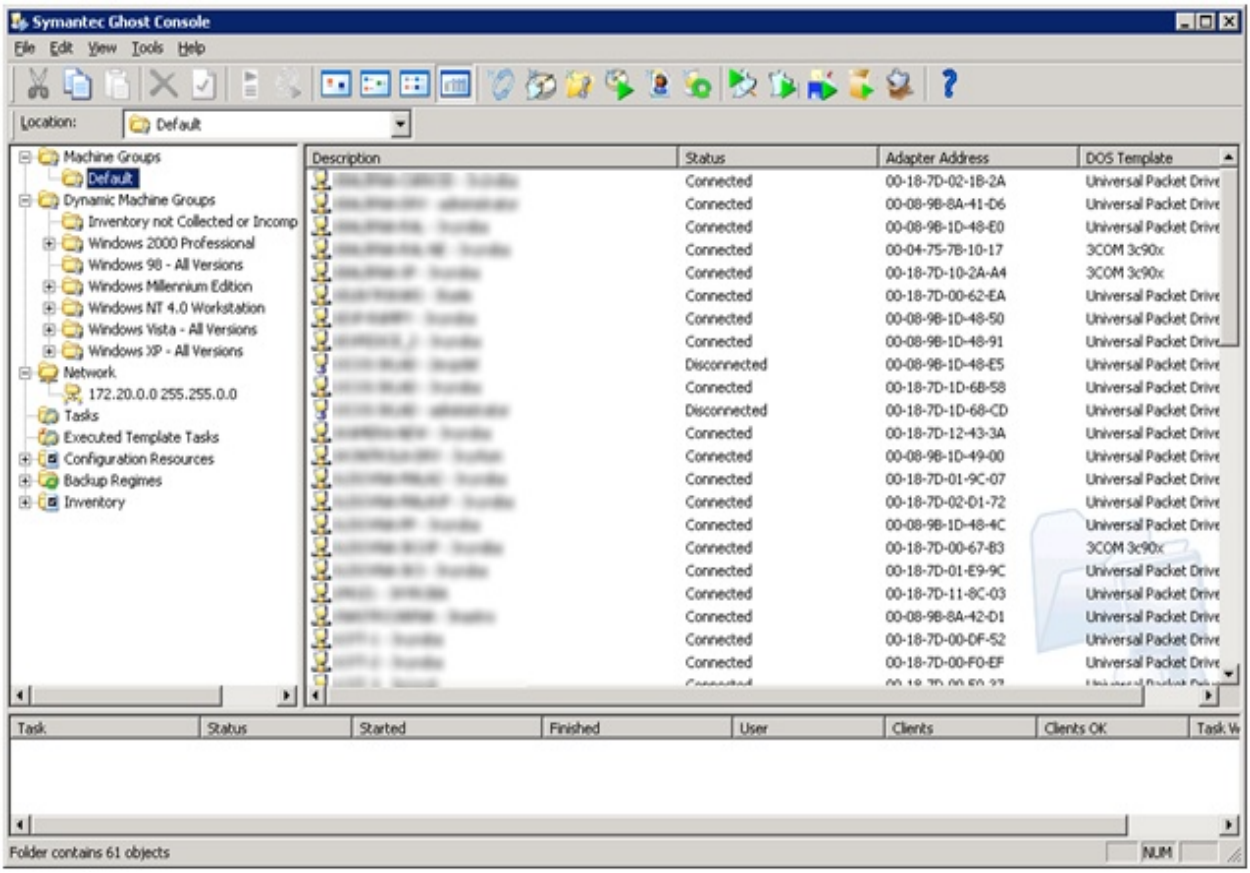
Aktualizace software, především potom operačních systémů je v době globální sítě Internet prakticky nutností. Počítače, jež nejsou součástí počítačových sítí, řeší tyto aktualizace přímo ze sítě Internet. Toto řešení je pro správu středních a větších sítí velmi neefektivní a řešením je právě služba WSUS. Aktualizační služba WSUS přináší zvýšení bezpečnosti a spolehlivosti provozu celé sítě i jednotlivých stanic. Zároveň správce získá informaci o stavu jednotlivých PC a může tyto informace snadno prezentovat. Vzhledem k tomu, že cena tohoto systému je prakticky nulová a implementaci lze realizovat v řádu hodin, výrazně doporučuji využívat v každé počítačové síti obsahující více počítačů s operačním systémem MS Windows.[2]

3.2 SYMANTEC GHOST SOLUTION SUITE

Symantec Ghost je určen k distribuci operačních systémů a softwarových balíčků. Lze ho také využít k zálohování a inventarizaci. Zde se zaměřím na deployment operačního systému a instalačních balíčků. Symantec Ghost používá k distribuci zejména bitové image disků, případně rozdílové image - pokud chceme např. obnovit dříve zálohovaný systém, který má vytvořenu kompletní záložní image a pak pouze přírůstkové zálohy. Přednostně je určen pro operační systémy MS Windows, kam si instaluje klienta a dokáže tak spravovat PC dálkově. Lokálně dokáže pracovat i s jinými systémy, zde v podstatě není důležité jaký systém je nainstalován, ale na jakém je souborovém systému. Podporuje souborové systémy FAT,FAT32,NTFS,EXT2,EXT3. Nainstalován může být na jakémkoliv počítači s operačním systémem MS Windows. Poslední verze podporují i práci s virtuálními stroji VMWare.

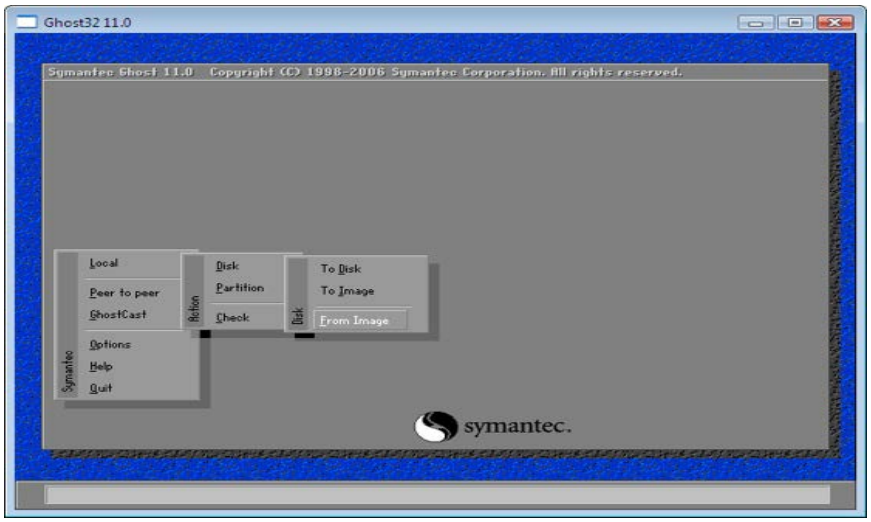
Výchozí obrazovkou programu je Symantec Ghost Console (Obr. 10). Ta nabízí přehled o počítačích v síti, je zde vidět, zda počítač je aktivní, či nikoli. Počítače lze dynamicky dělit podle různých parametrů (aplikované hotfixy, velikost disku, velikost paměti, USB, verze BIOSu apod.). Samozřejmostí je i manuální dělení do složek.

Z menu programu (serverová část) lze také spouštět ostatní podpůrné programy - Ghost Explorer, Ghost CastServer, Ghost Boot Wizard, AI Builder a Migration Package Explorer. Klient nemá žádné uživatelské prostředí, nicméně obsahuje mimo jiné program s názvem AISnapshot, který je důležitý k tvorbě instalačních balíčků. Vysvětlit kompletní funkcionalitu je poměrně složité a zdlouhavé, uvedu tedy alespoň základní funkce programu.



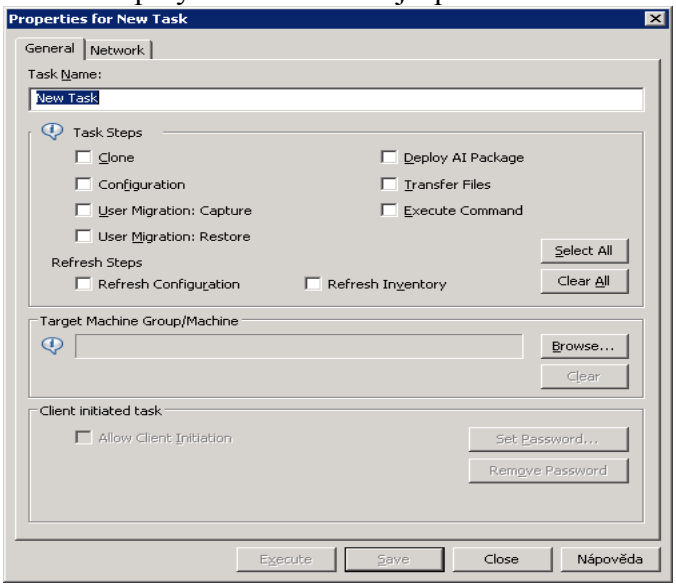
Obr. 10: Základní konzolové okno programu Symantec Ghost

Obrazy disků (Images) se vytváří ze vzorového PC. Na ten je nainstalován vzorový operační systém, včetně všech základních programů a provedení Windows Update. Potom startuje počítač z CD nebo flash disku, který lze vytvořit v programu Ghost Boot Wizard. Spustí se DOS a v něm grafický klient GHOST.exe, pomocí něhož lze klonovat pevné disky. Na serverové straně je spuštěn Ghost CastServer, který se spojí se spuštěným DOS klientem. Po té co se klient spojí se serverem, je možné vytvořit obraz disku klienta a uložit ho na disk serveru, kde je instalována Ghost Console. Nyní je na serveru uložena vzorová image. Pomocí klienta lze disky klonovat nebo vytvořené obrazy ukládat na jiná disková úložiště jako CD, DVD, Flash disky.



Obr. 11: DOS okno programu Symantec Ghost

Druhým krokem je nastavení uživatelské konfigurace. To se děje ve složce Configuration Resources-Configuration. Zde se pouze zadají údaje o novém PC, jako je jméno PC, doména, nastavení sítě atd. Tyto dva kroky jsou základní a nelze je při instalaci nového PC obejít. Vlastní deployment se zde děje pomocí tzv. Tasků. Menu-New Task, kde je opět několik nastavení (Obr. 12). Základní zatržítko je Clone, kde se vybere po zatrhnutí výchozí image, připravená na začátku celého procesu a druhé zatržítko Configuration, kde se vybere naše připravená konfigurace. Ostatní tlačítka se mohou a nemusí použít. Umí z uživatelského počítače stáhnout uživatelská data, poslat na stanici softwarový balíček nebo nějaké soubory. Je možné vzdáleně spustit i nějaký příkaz, soubor či skript - to se dá využít k instalaci např *.msi balíčků (kapitola 2.4 Správa SW). Následným spuštěním definovaného Tasku proběhnou v něm zadané operace a to i včetně změny SID operačního systému. Operace probíhají ve stejném pořadí jak jsou uvedena v definici Tasku. Časová náročnost celého procesu je závislá na velikosti image a rychlosti sítě, je to však obvykle záložitost několika minut.



Obr. 12: Možnosti Tasku Symantec Ghost

Symantec Ghost je vhodný hlavně do homogenního prostředí, kde je velký počet stanic s podobnou HW konfigurací. Je výborný i pro zálohování stanic a serverů. Vyniká přehledností a jednoduchostí. Nevýhodou je složitější tvorba programových balíčků [4].

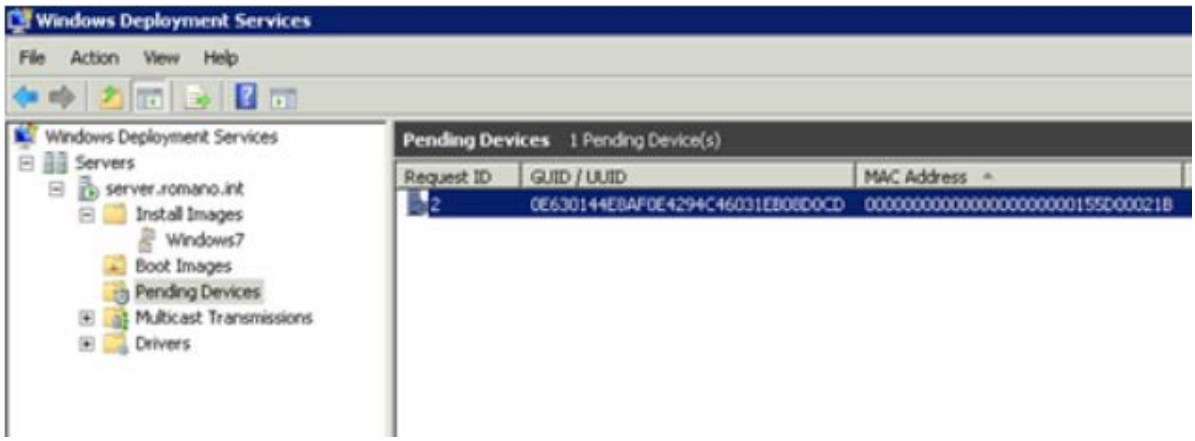
3.3 MICROSOFT DEPLOYMENT TOOLKIT

Microsoft Deployment Toolkit (MDT) je sada nástrojů, která slouží k instalacím jak operačních systémů, tak programových balíčků. Používá technologii tzv. souborových obrazů, WIM (Windows Imaging Format). Což je komprimovaná složka obsahující několik instalací

operačních systémů, ale každý soubor je v něm obsažen jenom jednou. Je použitelná pro operační systémy MS Windows Vista a Windows 7, verze 2010 podporuje i Windows XP. MDT umožňuje tzv. instalaci „Lite-touch“, což znamená téměř bezdotykovou instalaci - je nutná částečná účast uživatele. Instalaci „Zero-touch“ umožňuje nástroj, který se jmenuje System Center Configuration Manager, ale ten není na rozdíl od MDT zdarma. Nástroj Deployment Toolkit lze použít pro sítě s maximálním počtem cca 500 počítačů, což je pro většinu společností dostatečné. Systém a jeho nasazení je poměrně složitý, zaměřím se zde tedy pouze na základní body.

Pro provoz MDT je nutné mít zprovozněnou doménu s Active Directory, Windows server, DHCP server, který bude nakonfigurován pro PXE boot (boot PC ze sítě) za pomocí služby WDS(Windows Deployment Services) a WAIK (Windows Automated Installation Kit). Princip instalace bych naznačil do několika fází:

- **Příprava image:** do image, která lze získat z instalačního media Windows 7 (obvykle soubor install.wim) je nutno dodat aktuální opravné balíčky, aktualizace a ovladače pro podporu používaného hardware.
- **Deployment image:** používá se WinPE (Windows Preinstallation Enviroment), je to náhrada DOSu, používá se pro nasazení systémů, je schopen „bootovat“ ze sítě. V této fázi je třeba vybrat instalaci, na základě které se vytvoří obraz WinPE instalace. Vytvořený obraz se použije pro „bootování“ do koncového PC. Po té se připraví disk na aplikaci image, nahraje se image a systém se připraví na boot.
- **Konfigurace:** provede se konfigurace komponent, systém nastartuje do základního operačního systému a aplikují se licenční soubory.
- **První start:** poprvé „bootuje“ nový operační systém, je nutno pomocí komponenty sysprep vytvořit jedinečný systém.
- **Uživatelská nastavení:** zde se doladí uživatelská nastavení, je nutno přijmout licenční ujednání, zadat jméno systému, vytvořit případné uživatele, nastavit regionální nastavení a případnou konektivitu. Tato fáze není automatizovaná.



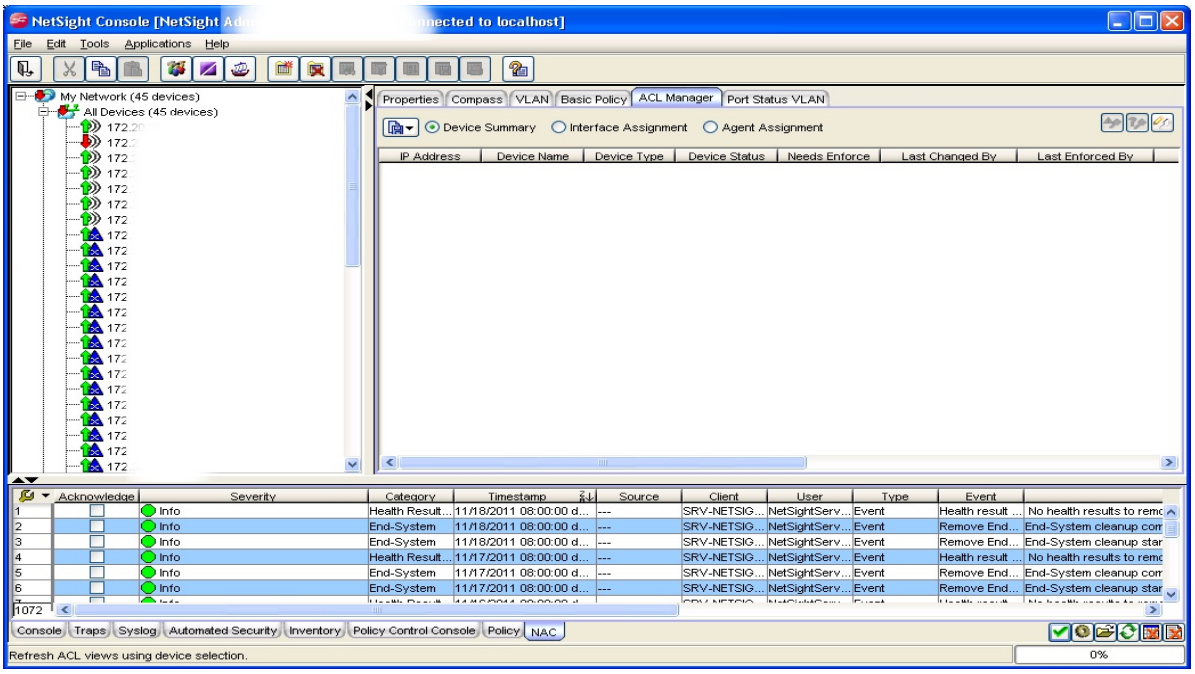
Obr. 13:Okno služby Microsoft Deployment Toolkit

Sada nástrojů Microsoft Deployment Toolkit je určena pouze pro prostředí Microsoft Windows. Výhodou je, že nepotřebuje homogenní prostředí a každá instalace může být na jiné hardwarové konfiguraci. Další výhodou je nulová cena. Nedisponuje však úplnou bezdotykovou instalací a dodatečnou instalací programových balíčků, a to není v podnikovém prostředí optimální. Ve spojení s nástrojem System Center Configuration Manager a ostatními nástroji pak System Center poskytuje kompletní správu koncových stanic i serverů a to i ve virtualizovaném prostředí.0

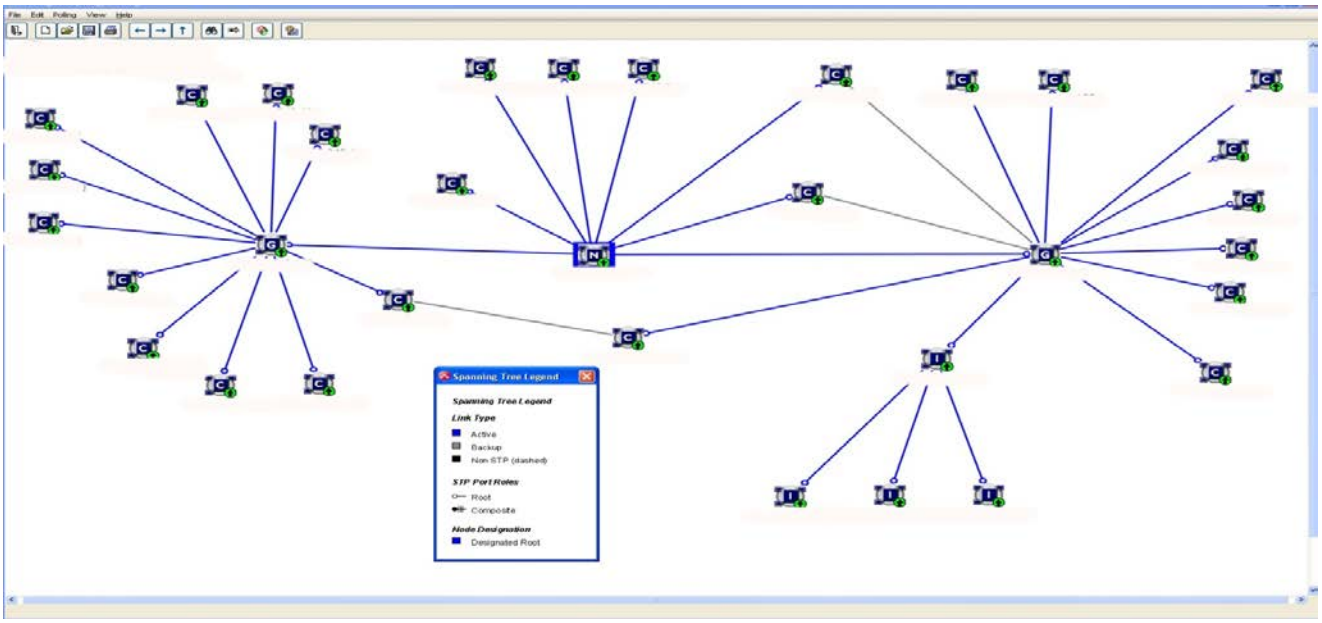
3.4 NETSIGHT SUITE

NetSight Suite je produkt od firmy Enterasys a je určen pro správu a dohled síťových prvků. Je optimalizován pro podporu prvků Enterasys, ale dokáže do svého prostředí integrovat i prvky jiných dodavatelů hardware. Umožňuje kontrolu na úrovni portů, aplikací i uživatelů. Díky jednotnému rozhraní umožňuje správci efektivně spravovat i rozsáhlé sítě, konfigurovat několik prvků najednou a poskytuje efektivní monitoring. To vše v grafickém prostředí. NetSight Suite tvoří několik modulů, z nichž každý má vlastní funkcionalitu:

- **NetSigh Console:** Obr. 14, základní prvek celého balíku. Používá se k monitorování a hlavně řízení všech prvků v síti. Umožňuje prvky organizovat do logických celků a těm přiřazovat práva jednotlivých administrátorů. Obsahuje například komponentu Compas, pomocí které lze vyhledat v celé síti jakýkoliv prvek na základě MAC adresy, IP adresy, vyhledá všechny prvky v podsíti apod. Umožňuje hromadné operace s virtuálními sítěmi - například vytvoření a nastavení VLAN na několika prvcích najednou. Obsahuje také tzv. FlexView, kde si správce může nastavit vlastní pohled, a to buď z předdefinovaných šablon nebo si vytvořit svůj.Ve spodní části je potom možné sledovat události systému. Součástí Console je i modul pro tvorbu mapa sítě - Topology Manager (Obr. 15). Ta se generuje automaticky a administrátor si ji může upravit dle skutečného rozmístění. Mapa dokáže i barevně rozlišit aktivní a záložní spoje, zobrazí virtuální propoje a spoustu dalších informací.



Obr. 14:Základní okno programu Netsight Suite



Obr. 15:Ukázka Topology Manageru programu Netsigh Suite (modré trasy jsou aktivní, šedé jsou záložní)

- **Policy Manager:** Správce uživatelských profilů spravuje profily uživatelů, protokoly, aplikace, virtuální sítě a porty. Pracuje s těmito profily v rámci celé sítě. Pomocí tohoto nástroje mohou administrátoři snadno definovat a prosazovat uživatelské profily. Tento nástroj zvyšuje bezpečnost celé sítě.
- **Automated Security Manager:** Automatický bezpečnostní správce, sleduje incidenty v síti v reálném čase, dokáže je vyhodnocovat, monitorovat a některé i řešit. Tím zabezpečuje bezpečnost a dostupnost dat v celé síti. ASM umí pracovat i s uživatelskými profily. V případě zjištění porušení nějakého pravidla dokáže uživatele například odpojit do sítě, připojit do karantény, snížit rychlost a podobně.
- **Network Acces Control Manager:** NAC je řešení pro řízení přístupu uživatelů, které zajišťuje, že daný uživatel má správná práva ze správného místa a ve správný čas. Ve spojení s jinými aplikacemi lze řídit přístup uživatele na základě dynamicky získaných dat - například, pokud má aktualizovaný antivirový program, tak může do lokální sítě. Pokud nemá může pouze do karantény...
- **Inventory Manager:** Je nástroj pro zpracování dokumentace a aktualizace detailů neustále se měnící sítě. Sleduje také změny v konfiguracích, které proběhly z jiného SW - např. z příkazové řádky nebo lokálně. Zajišťuje automatické zálohování prvků dle zadaných parametrů.

NetSight Suite je robustní a univerzální nástroj na správu sítě. Poskytuje správcům možnost efektivní správy a zvýšení zabezpečení celé sítě. Cena produktu je závislá na počtu spravovaných prvků a počtu modulů. Tento nebo podobný nástroj by měl mít k dispozici správce každé sítě, která má více síťových prvků tvořících funkční, a pro chod IT podstatný celek [5].

4 NÁVRH SOFTWARE PRO SPRÁVU PRVKŮ

Cílem této práce je i návrh vlastního programu pro správu některých koncových prvků v učebně. Program nedosahuje funkcionalit sofistikovaných nástrojů velkých výrobců, na kterých pracují celé vývojové týmy, ale jeho devizou je přehlednost a dostupnost základních požadovaných funkcí. Další vlastností, kterou většina programů nedisponuje, je sjednocení správy síťových prvků, osobních počítačů, serverů a ostatních zařízení do jednoho programu. Pro některé funkce program slouží jen jako prostředník a volá pouze příslušnou službu zajišťující danou funkcionalitu. Program má název IP Device Manager.

4.1 PROGRAMOVACÍ PROSTŘEDÍ

Vlastní program je napsán v programovacím prostředí Delphi v jazyce Object Pascal. Velikou výhodou tohoto programovacího jazyka je vizuální návrh grafické podoby programu a tím i značné zjednodušení a zrychlení celého programovacího procesu, kdy se programátor nemusí až tolik zabývat designem a může se soustředit na funkcionalitu programu. Další výhodou je integrace a dostupnost mnoha hotových komponent například tabulek, menu, editorů, které potom mohou sloužit jako základní stavební kameny aplikace. Jako úložiště dat je použita databáze Absolute Databaze, která je alternativou k vestavěné Borland databázi BDE. Výhodou je její kompaktnost, rychlost, jednoduchost a snadné použití - ve finále tvoří jediný soubor a stačí, když bude umístěna v jednom adresáři s výsledným .exe souborem. Instalovaná databáze obsahuje mimo jiné i editační nástroj „DBManager.exe“, kterým je možno přistupovat do databáze mimo program IP Device Manager a editovat takto její obsah. [6][7]

4.2 SYSTÉMOVÉ POŽADAVKY

Program IP Device Manager je určen pro operační systém MS Windows. Je otestován na standardních instalacích OS MS Windows XP,Windows 7 a Windows 2003 a 2008 server. Je koncipován jako portable a není nutno jej tedy instalovat. Veškeré podpůrné soubory potřebné pro chod programu jsou umístěné ve složce programu. Aby byla zaručena bezchybná funkčnost, tak je nutno v systémech, které pracují s uživatelskými účty spouštět pod uživatelem, který je přiřazen do skupiny „*Administrators*“. Obzvláště potom v operačním systému Windows 7 je nutné program spouštět „*jako správce*“. To lze jednoduše zajistit tak, že se vytvoří zástupce programu - IPDevMan.lnk a tomuto zástupci se v obecných vlastnostech přiřadí v záložce „kompatibilita“ úroveň oprávnění „Spustit tento program jako správce“. Hardwarové nároky jsou menší než požadavky na samotný operační systém, není nutno se jimi tedy zabývat. Samotný program zabere cca 10 MB volného prostoru na pevném disku.

4.3 FUNKCE PROGRAMU

Program IP Device Manager je software určený pro správu prvků sítě i koncových zařízení. Tvoří správcovské centrum obsahující základní funkce, které je možno využít při konfiguraci a dohledu nad síťovými zařízeními. Základní filozofií při návrhu programu byla přehlednost, jednoduchost použití, nenáročná implementace, spolehlivost, přehlednost

a možnost částečné customizace bez zásahu programátora. Některé funkce jsou realizovány komponentami operačního systému nebo externími programy. Výhodou tohoto řešení je snadná změna programu funkce v případě vydání nové verze nebo nefunkčnosti z důvodu zavedení například nových patchů do operačních systémů. Program disponuje následujícími funkcemi

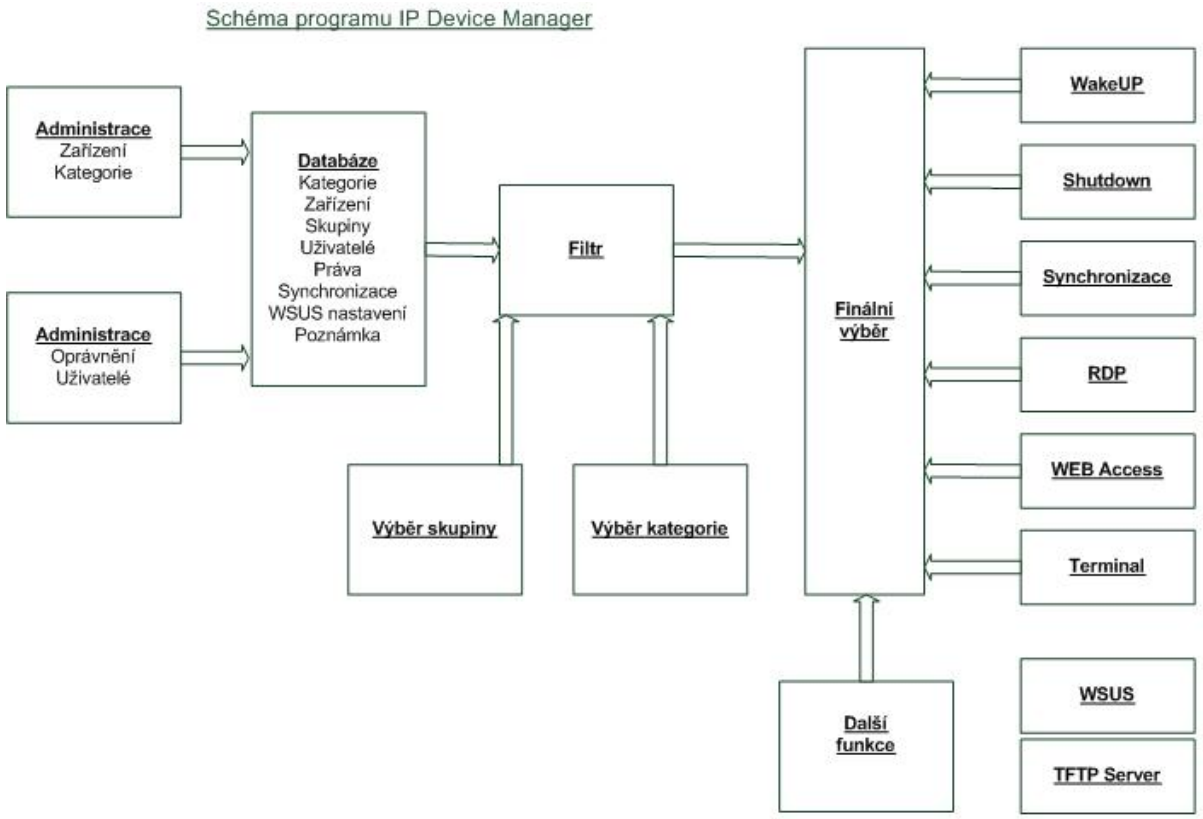
- **Zobrazení a třídění zařízení:** Program přehledně zobrazuje známá zařízení. Umí je třídit a zobrazit podle *Skupiny*, to může být například lokalita nebo jiné logické rozdělení. A podle *Kategorie*, což je obvykle typ zařízení (PC, notebook, tiskárna, router atd.). Pro lepší přehlednost jsou *Skupiny* i *Kategorie* rozlišeny ikonami. Ikony si může správce programu volit sám v sekci nastavení. Fyzicky jsou ikony umístěny ve složce programu v podsložce „*Ikony*“. Ikony lze do programu dodávat i vlastní. Musí být dodržen formát obrázku, což je bmp s rozlišením 16x16 pixelů. Obrázky splňující tyto požadavky lze nahrát do výše zmíněných složek a použít při vizualizaci v programu IP Device Manager.
- **Přehled o stavu zařízení:** vestavěnou funkcí *PING*, program testuje známá zařízení na dostupnost v síti. Graficky je potom zobrazeno zda je zařízení aktivní součástí sítě nebo je nedostupné. Zelená šipka nahoru značí dostupné zařízení a červená šipka směřující dolů potom zařízení nedostupné. Status bar v dolní části programu potom znázorňuje aktivitu této funkce.
- **Probuzení počítače:** dálkové probuzení počítače nebo serveru pomocí tzv. magic paketu vyslaného do segmentu sítě v které se probouzený počítač nachází. Tato funkce probudí všechny počítače, které jsou označeny zatržítkem. Podmínkou pro správnou funkčnost je vyplnění MAC adresy počítače v záložce nastavení a zapnutá podpora v BIOSu probouzeného počítače.
- **Vypnutí počítačů:** dálkové vypnutí počítačů pomocí příkazu *shutdown,* který je integrován v operačních systémech MS Windows. Tato funkce vypne najednou všechny počítače označené zatržítkem. K vypnutí dojde, i když jsou spuštěné další programy a nejsou uložená data!! Tuto funkci lze využít po hromadné aktualizace softwaru nebo třeba při odchodu studentů z učebny.
- **Webový přístup k zařízení:** pro konfiguraci síťových prvků jako jsou IP kamery, přístupové body, přepínače či směrovače je výhodné mnohdy využít přístupu přes webové rozhraní. Tato funkce umožňuje snadný přístup k takovémuto prvku pomocí jednoho tlačítka, které otevře výchozí webový prohlížeč a v něm konfigurační rozhraní daného prvku. Je otevřen vždy jen prvek který je v tabulce aktivní (je označen modrým pruhem).
- **Terminál:** zajišťuje konzolový přístup k zařízením jaké jsou především přepínače a směrovače. Tlačítko „terminál“ zavolá terminálové sezení pouze položky, která je v tabulce aktivní. K tomuto účelu je využit program Putty a program IP Device Manager zde funguje pouze jako zprostředkovatel spojení. Spojení je vždy zabezpečené - SSH.
- **Přístup na vzdálený počítač:** další funkcí v rámci systémové integrace je přístup na vzdálenou plochu počítače a převzetí jeho ovládání. Toto lze využít pro individuální nastavení konfigurace, kontrolu nastavení nebo nějaké činnosti bez nutnosti fyzické přítomnosti u daného PC. Tlačítko „*RDP*“ (Remote Desktop Protocol) otevře vzdálenou plochu počítače, který je v tabulce označen jako aktivní. Tato funkce je dostupná pro platformu Microsoft Windows 2000 a vyšší verze. Je využito systémové komponenty *mstsc.exe*. Program IP Device manager umožňuje také uživatelské nastavení tohoto spojení. Parametry jako je například rozlišení plochy převzatého počítače lze nastavit v „*Nastavení*“ a záložce „*Obecné*“. Zde je přímo umístěna nápověda k nastavení. Toto nastavení je potom stejné pro všechny přebírané počítače.

- **Aktualizace operačních systémů:** k aktualizaci operačních systémů MS Windows je použita služba od společnosti Microsoft - WSUS. Popis této služby je v kapitole 3.1. Tato služba je instalována nezávisle na programu IP Device Manager a doporučuji ji instalovat na jiném PC. V rámci integrace tento program umožní přístup k rozhraní WSUS pomocí RDP. V nastavení programu je nutno určit jakou má server s instalovanou službou WSUS IP adresu a jako v předchozím případě lze opět nastavit parametry zobrazení.
- **Synchronizace složek:** další vestavěnou funkcí programu IP Device Manager je synchronizace složek. Synchronizace složek bude probíhat mezi lokální složkou nebo složkou vybranou na připojeném serveru či diskovém poli a klientskými počítači. Těchto synchronizací - synchronizačních scénářů může v programu existovat libovolné množství. Je tak možno synchronizovat vždy jen vybraná data - například pouze dokumenty, pouze učební data, pouze virtual box - Linux, virtual box - Windows XP a podobně. Jednotlivé synchronizační scénáře jsou v „*Nastavení*“ a záložce „*Synchronizace*“. Zde je možné mimo nastavení zdrojových a cílových adresářů nastavit i parametry prováděcího příkazu *Robocopy*, kterého je při synchronizaci využito. Lze tak snadno customizovat synchronizační proces v závislosti na výkonu hardware sítě či počítačů nebo vytvářet logy. Syntaxe příkazu Robocopy je poměrně rozsáhlá a lze si ji zobrazit pomocí příkazu *robocopy /?* v příkazovém řádku systému MS Windows.
- **TFTP Server:** k aktualizaci a zálohování konfiguračních souborů síťových prvků je nutný TFTP server. Tento potom zpřístupňuje úložiště, na které se lze odkazovat při vlastní konfiguraci či zálohování prvků. Je použit externí program a IP Device Manager je pouze prostředníkem pro volání tohoto programu.
- **Autentizace přihlášení:** k přihlášení do programu je nutné zadat uživatelské jméno a heslo. Na základě těchto údajů může být omezen přístup jen na některé skupiny zařízení a některé funkce. Pokud uživatel nemá plný - administrátorský přístup, je mu také zakázáno zobrazení všech zařízení - může tedy vidět jen ty, na která má práva, a na ně aplikovat jen povolené funkce. První uživatel (výchozí jméno admin - dá se změnit) se nedá smazat a má vždy administrátorský přístup. Toto je ochrana proti nechtěnému smazání všech účtů s právem přístupu do nastavení programu.
- **Poznámka k zařízení:** pro lepší orientaci a přehled o zařízeních (použití například při inventarizaci) je možné ke každému zařízení přidat pětiřádkovou poznámku. Ta je vyvolána dvojklikem na řádku daného zařízení. Poznámku je možné vyplnit při zadávání zařízení do systému nebo i později v sekci *Nastavení/Zařízení*.
- **Uživatelská tlačítka:** z důvodu možné budoucí integrace jiné utility do programu IP Device Manager je naprogramováno několik tlačítek, ke kterým se dá přiřadit nějaký spustitelný soubor s parametry. Tuto funkci je potom možné použít v prostředí programu a aplikovat ji na několik označených zařízení nebo jen na jedno aktivní.

4.4 SCHÉMATICKÝ NÁVRH PROGRAMU

Obr. 16 ukazuje schematický návrh programu, tak aby splňoval zadanou funkcionalitu. Základem je databáze, která je plněna manuálně ze sekce „*Nastavení*“, údaji o zařízeních v síti. Je třeba zapsat do databáze informace o spravovaném zařízení (kategorie, skupina, IP adresa, oprávnění uživatelé, poznámky). Aby zde byla rozdělena přístupová oprávnění a zároveň byl program přehledný, tak je výstup z databáze filtrován dvěma parametry, které si volí správce programu. Jedním je rozdělení zařízení dle skupiny (například podle učeben) a druhým parametrem je rozdělení dle kategorie (PC, Server, IP kamera atd.). V praxi to bude

znamenat to, že danou skupinu zařízení bude moci spravovat pouze osoba k tomu pověřená administrátorem programu. Ve středovém okně se potom budou zobrazovat pouze filtrovaná zařízení, přičemž bude bráno v potaz oprávnění přihlášeného uživatele. Finální výběr zařízení bude zobrazovat i stav prvku v síti (je/není aktivní součástí sítě), bude možno řadit zařízení podle parametrů v jednotlivých sloupcích a hlavně bude možné zařízení hromadně nebo jednotlivě označovat. Na označená zařízení potom budou aplikovány funkce programu (vypnutí, zapnutí, synchronizace atd.).



Obr. 16: Schéma programu IP Device Manager

4.5 POPIS PROGRAMU

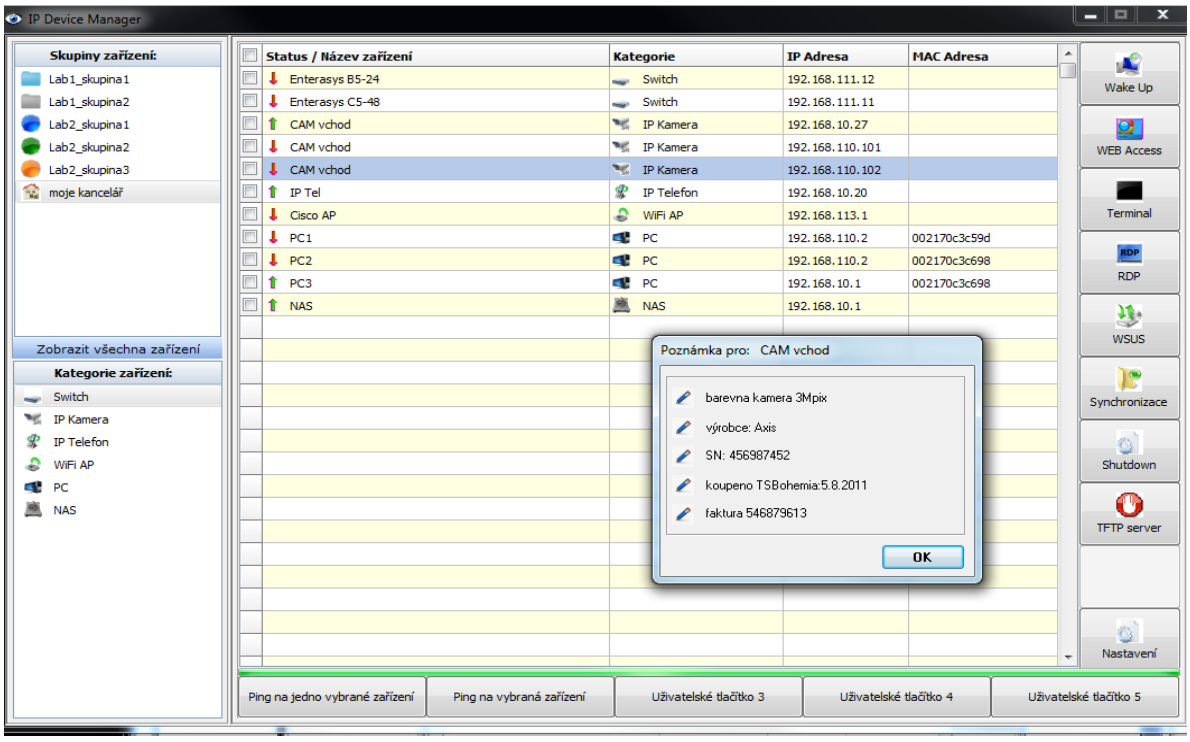
Výchozí okno programu je na Obr. 17. Program je rozdělen do několika částí:

- **Třídění:** v levé části programu jsou dvě podokna s názvy „*Skupiny zařízení*“ a „*Kategorie zařízení*“. Zde jsou zobrazeny všechny existující *Skupiny* a *Kategorie*, na které má přihlášený uživatel nastaveny práva. Pokud je přihlášen uživatel s právy administrátora, tak má zobrazeny všechny *Skupiny*, které program zná. Kliknutím na určitou *Skupinu* se filtrují všechna zařízení, která jsou v této *Skupině* zadána. V okně *Kategorie* zařízení jsou vypsána zařízení, která existují v označené *Skupině*. Kliknutím na nějakou položku v okně kategorie zařízení se potom filtrují pouze zařízení toho typu, na které bylo kliknuto - to znamená, že budou vypsána pouze určitá zařízení z určité skupiny. Tlačítko „*Zobrazit všechna zařízení*“ zobrazí všechna známá zařízení, která jsou zapsána v databázi programu. Toto tlačítko však může použít jenom uživatel, který má v programu nastaven administrátorský přístup.
- **Výběr:** prostřední hlavní okno finálního výběru zobrazuje vyfiltrovaná zařízení. Jsou zde zobrazeny názvy zařízení kategorie, IP adresa a případně MAC adresa. Také je zde indikováno, zda je zařízení v síti dostupné. Zelená šipka nahoru - zařízení je

dostupné, červená šipka dolů - zařízení je nedostupné. Dostupnost je testována funkcí ping na danou IP adresu s časem 200ms.

- Prvním sloupcem tohoto okna jsou tzv. checkboxy, které slouží k označení zařízení, na něž bude aplikována některá z funkcí. Označovat/odoznačovat se dá postupně po jednom zařízení nebo hromadně kliknutím na čtvereček checkboxu v záhlaví.
- Dvojklikem na řádek některého zařízení se otevře další malé okno, ve kterém mohou být poznámky k zařízení (výrobce, záruka, sériové číslo atd.). Tyto poznámky se zadávají v sekci *Nastavení* vždy k danému zařízení.

- **Funkce:** pravá řada tlačítek skrývá funkce programu, které se aplikují na vybraná nebo vybrané zařízení. Funkce *WSUS* a *TFTP* server nevyžadují žádný výběr. Dolní řada tlačítek slouží k nastavení vlastních funkcí.Tato tlačítka lze uživatelsky pojmenovat podle použité funkce. Indikátor nad uživatelskými tlačítky zobrazuje průběh funkce PING přes celou databázi zařízení. Tlačítko *Nastavení* slouží k přechodu do nastavení programu, kde je možné zadávat skupiny, kategorie, zadávat zařízení, definovat nové uživatele a jejich práva. Tyto funkce jsou podrobněji rozebrány níže v kapitole 4.6.



Obr. 17: Výchozí okno programu IP Device Manager

4.6 REALIZACE FUNKCÍ

4.6.1 Wake UP

Funkce Wake UP (označována též Wake on Lan,WOL) je funkce, která umí probudit zařízení v síti z vypnutého stavu, stavu spánku, či hibernace. Samozřejmě je to možné pouze, pokud toto zařízení takovouto funkci podporuje. Dnešní zařízení, především osobní počítače

touto funkcí obvykle disponují, je nutno ji však aktivovat v BIOSu či ovladači síťové karty - případně obojí. To, že je karta správně nastavena, lze obvykle rozpoznat tak, že indikátory na síťové kartě blikají, i když je zařízení vypnuté. Probuzení je realizováno speciální sekvencí dat, označovanou jako **„Magic packet“**. Jelikož je Magic packet obvykle posílán jako broadcast, tak je funkční pouze v rámci jedné broadcastové domény.

Magic Packet je rámec, který obsahuje zdrojovou MAC adresu stroje, z něhož je vyslán. Potom následuje inicializační sekvence FF:FF:FF:FF:FF:FF. A nakonec cílová MAC adresa stroje, který má být probuzen. Tato MAC adresa je šestnáctkrát zopakována. Tato sekvence je odeslána na adresu 255.255.255.255 - což je právě zmíněná lokální broadcastová adresa. V programu IP Device Manager je k probouzení použita komponenta ipwPingWol, která funguje na výše uvedeném principu. Funkce WakeUp je aplikována na všechna zařízení, která jsou označena checkboxem. Na Obr. 18 je část zdrojového kódu zajišťujicí funkci WOL.[7]

```
begin
  for x:= 1 to adsgZarizeni.RowCount do
    begin
      // kdyz je v Gridu adsgZarizeni checkbox zatrzen
      if adsgZarizeni.GetCheckBoxState(0,x,State) then //kdyz je checkbox zatrzen
        if State = True then
          if adsgZarizeni.Cells[4,x] <> '' then  //kdyz neni pole s MAC prazdny
            begin
              //WOL magic paket na broatcast IP a AMC adresu zarizeni
              try
                ipwPingWOL.WakeOnLAN('255.255.255.255',adsgZarizeni.Cells[4,x]);
              except
                ShowMessage('Probuzeni zařízení: '+adsgZarizeni.Cells[1,x]+'  se nezdařilo!');
              end;
            end
          else ShowMessage('Zařízení: '+adsgZarizeni.Cells[1,x]+'  nemá vyplněnou MAC adresu!')
        else
        else
    end;
end;
```

Obr. 18: Realizace Magic Packetu

4.6.2 Web Access

Mnoho zařízení se dá konfigurovat pomocí webového rozhraní nebo pomocí terminálového okna. Pro první možnost je v programu IP Device Manager implementována funkce, která zavolá výchozí webový prohlížeč s adresou zařízení na kterém je kurzor. Lze se tak velmi snadno a rychle dostat ke konfiguračnímu rozhraní ip kamer, switchů, routerů a dalších zařízení. Standardně je v operačních systémech MS Windows výchozím prohlížečem Microsoft Internet Explorer. Pokud bude nutno použít jiný prohlížeč, lze v systému Windows nastavit prohlížeč, který má být výchozí. Způsob tohoto nastavení se liší podle verze operačního systému. Například v systému Windows7 lze toto nastavení upravit v *Ovládací_panely/ Programy/ Výchozí_programy/ Nastavení_výchozích_programů*. Obvykle bývá výchozí ten prohlížeč, který je instalován jako poslední.

Při realizaci této funkce je využito funkce s názvem *ShellExecute*, která v podstatě simuluje v operačním systému příkaz *start*. Pokud je v systému MS Windows v příkazovém řádku zadáno například: „*start http://seznam.cz*“, tak je otevřen výchozí webový prohlížeč s webovou stránkou seznam.cz. Je zde tedy použita výše zmíněná funkce *ShellExecute*, která má přiřazenu funkci *open* a jako parametr je použito *http://[adresa zařízení]*. Pokud je aktivní

kurzor na prázdném řádku nebo není správně vyplněna IP adresa zařízení, tak na tuto skutečnost systém upozorní hláškou. Část zdrojového kódu, který řeší otevírání webové stránky s danou IP adresou je na Obr. 19.

Podmínkou funkčnosti je však podpora a zapnutí této funkce u spravovaného prvku. Velmi často prvek tuto funkci podporuje, ale ve výchozím stavu je vypnutá. Je tedy třeba povolit tuto funkci prostřednictvím jiného rozhraní - například SSH, Telnet.[8]

```
begin
  if adsgZarizeni.Cells[3,adsgZarizeni.Row] <> '' then
    begin
      Param:= 'http://'+adsgZarizeni.Cells[3,adsgZarizeni.Row];
      ShellExecute(self.WindowHandle,'open',PChar(Param),nil,nil, SW_SHOWNORMAL);
    end
  else ShowMessage('Vybraný řádek neobsahuje žádné zařízení nebo IP Adresu !');
end;
```

Obr. 19: Realizace spuštění webového rozhraní

4.6.3 Terminal

Druhou, výše zmiňovanou možností konfigurace některých prvků je terminálový přístup pomocí klienta. Obvykle se tímto způsobem konfigurují síťové prvky, jako jsou přepínače a směrovače. Ty mívají možnost zabezpečeného přístupu protokolem SSH a přístup nezabezpečeným protokolem Telnet. Telnet se z důvodu snadného odposlechnutí komunikace používá výhradně pro lokální přístup (například notebook - kabel - router). Pro vzdálený přístup (přístup přes síť) se prakticky výhradně používá pouze zabezpečený protokol SSH.

Na Internetu je mnoho volně šiřitelných SSH klientů. Rozhodl jsem se využít klienta Putty a programem IP Device Manager pouze volám program Putty s parametry, které zajistí spuštění SSH klienta na danou IP adresu. Principielně je volán Putty klient z adresáře, v němž je i vlastní program IP Device Manager. V počítači může být instalován i jiný Putty klient. Pokud by však došlo k potížím ve spolupráci s oběma programy, doporučuji obnovit výchozí nastavení programu Putty (ideálně v registru systému - *Počítač\Hkey_Users\aktuální uživatel\Software\SimonTatham\Putty*....smazat klíče).

Program Putty.exe je v programu volán funkcí *ShellExecute* s parametrem SSH, a je voláno zařízení, na němž je kurzor. Pokud je kurzor na prázdném řádku, tak vyskočí chybové hlášení „Vybraný řádek neobsahuje žádné zařízení nebo IP adresu“. Ukázka kódu je na Obr. **20**. Kód je velmi podobný kódu pro spuštění webové stránky, pouze je zde přidáno jméno spuštěného exe souboru (putty.exe). Pokud je třeba nastavit nějaké parametry programu Putty (barvy, font, počet zobrazených řádků atd), lze program pustit standardním způsobem a tyto parametry nastavit a uložit je jako výchozí. Po té již bude IP Device Manager spouštět terminálové okno s tímto nastavením.[9]

```
begin
  if adsgZarizeni.Cells[3,adsgZarizeni.Row] <> '' then
    begin
      Param:= '-ssh '+adsgZarizeni.Cells[3,adsgZarizeni.Row];
      ShellExecute(handle,'open',PChar('putty.exe'),PChar(Param),'',SW_SHOWNORMAL);
    end
  else ShowMessage('Vybraný řádek neobsahuje žádné zařízení nebo IP Adresu !');
end;
```

Obr. 20 Realizace spuštění PuTTy

4.6.4 RDP

Remote Desktop protokol je určen k ovládání vzdáleného počítače pomocí převzetí pracovní plochy na vlastní lokální počítač. Jak již bylo zmíněno výše v textu, je zde využito komponenty mstsc.exe, jež je standardní součástí operačních systémů MS Windows. Jelikož lze program mstsc.exe volat z příkazové řádky, podobně jako program Putty, využil jsem stejného principu, jaký je naznačen na Obr. 20.

Opět je voláno zařízení, na kterém se nachází kurzor. Podstatným rozdílem je to, že parametry spuštění se tentokrát modifikují v sekci *Nastavení/Obecné* v programu IP Device Manager. Za zásadní považuji úpravu parametrů, jež ovlivňují rozlišení pracovní plochu ovládaného počítače. Výchozím nastavením je */w:1024 /h:768*, což značí rozlišení 1024x768 pixelů a mělo by postačovat na většinu dnes používaných monitorů. Ostatní parametry nejsou natolik důležité a jsou pro přehlednost uvedeny v záložce „*Obecné*“, kde lze toto nastavení také modifikovat.[8]

Jelikož cílovou kategorií pro funkci RDP jsou osobní počítače a servery, je nutno pro správnou funkcionalitu dodržet několik pravidel:

- povolení protokolu RDP na vzdáleném počítači,
- přiřazení oprávnění pro uživatele,
- v případě použití firewallu povolit komunikaci RDP (TCP port 3389).

4.6.5 WSUS

Funkce WSUS je rozebrána v kapitole 3.1. Program IP Device Manager neřeší aktualizaci operačních systémů a k tomuto účelu je doporučen právě produkt Windows Server Update Services. Nicméně v rámci systémové integrace je do programu přidáno tlačítko, které otevře vzdálenou plochu serveru, na němž tato služba běží. K ovládání vzdálené plochy je využito protokolu RDP a proto i princip je shodný s principem popsaným v kapitole 4.6.4. Jediným rozdílem je vyplnění IP adresy serveru, na němž je služba WSUS instalována. To je možné provést v sekci *Nastavení/Obecné/Wsus Server*.

4.6.6 Synchronizace

Synchronizace dat je v programu IP Device Manager realizována pomocí tzv. synchronizačních scénářů. Je to z důvodu lepší přehlednosti a možnosti synchronizace jen části dat. Jednotlivé synchronizační scénáře jsou postupně aplikovány na **všechna** zařízení, které jsou zatrženy checkboxem. Každý synchronizační scénář má svůj název, svůj zdrojový adresář (z kterého se budou soubory kopírovat), cílový adresář na vzdáleném PC a parametry, které definují synchronizační proces.

Pro účel synchronizace je využita komponenta operačního systému MS Windows - *Robocopy.exe*, která je de facto rozšířením známých komponent *copy* a *xcopy*. Program IP Device Manager zde nechává otevřenou cestu pro použití i jiného programu, který by mohl být pro účely synchronizace využit. Lze dokonce pro každý jednotlivý scénář využit jiný synchronizační program.

Program *Robocopy.exe* (případně jiný) je volán funkcí *ExecAndWait*, která kontroluje, zdali proces ještě běží, nebo již skončil. Jakmile proces skončí, funkce jde na další položku v seznamu. Nejdříve je proveden první zatržený scénář nad všemi zatrženými zařízeními, potom druhý zatržený scénář nad všemi zatrženými zařízeními atd.

Pro synchronizaci je zapnuto logování, to slouží ke kontrole, zdali veškeré operace kopírování proběhly v pořádku či nikoliv. Logování je možno zapnout, vypnout, nebo jinak

nastavit parametry změnou parametrů synchronizačního programu. Ve výchozím nastavení je nastaveno logování do souboru (robocopy.log), přičemž se aktuální log připíše na konec souboru a zůstává tak historie o jednotlivých proběhnutých synchronizacích. Veškeré parametry lze zobrazit zadáním *robocopy.exe /?*, v příkazovém řádku systému MS Windows.[7]

```
//ulozeni potrebnych udaju a parametru pro SYNC do promennych
SyncProgram:= aqPomSync.FieldByName('SyncProgram').AsString;
SyncZdroj:= aqPomSync.FieldByName('SyncZdroj').AsString;
SyncCil:= aqPomSync.FieldByName('SyncCil').AsString;
SyncParam:= aqPomSync.FieldByName('SyncParam').AsString;

//Provedeni synchronizece pro vsechny vybrane zarizeni(checkbox zatrzen)
for x:= 1 to Form1.adsgZarizeni.RowCount do //pro vsechny zobrazeny polozky v GRIDu ZArizeni
  begin
    if Form1.adsgZarizeni.GetCheckBoxState(0,x,State) then //kdyz je checkbox zatrzen
      if State = True then //kdyz je checkbox zatrzenej
        if Form1.adsgZarizeni.Cells[3,x] <> '' then  //kdyz neni pole s IP prazdne
          begin
            try
              IPAdrCil:= Form1.adsgZarizeni.Cells[3,x];
              Param:= SyncZdroj+' \\'+IPAdrCil+SyncCil+' '+SyncParam;
              Form1.ExecAndWait(SyncProgram,Param,1);
            except

            end;
          end
        else ShowMessage('Zařízení: '+Form1.adsgZarizeni.Cells[1,x]+'  nemá vyplněnou IP adresu!')
      else

    else

  end;
```

Obr. 21 Realizace synchronizačních scénářů

4.6.7 Shutdown

Funkce *Shutdown* slouží k dálkovému vypnutí počítačů s operačním systémem MS Windows. Je zde opět využita funkce *ShellExecute*, a to velmi podobně jako například funkce *Wake UP*. Rozdíl je zde v tom, že na označená zařízení není posílán Magic Packet, ale příkaz Shutdown s parametry. Tyto parametry lze volit v sekci *Nastavení/Obecné/Parametry příkazu Shutdown*. Standardně jsou využity parametry -s (vypnutí počítače) a –f (vynucené vypnutí aplikací).[1]

4.6.8 TFTP Server

TFTP server slouží k zálohování a obnově konfigurace některých síťových prvků. Program IP Device Manager přímo tento TFTP server neobsahuje, pouze zprostředkovává přístup k tomuto programu. Jako program je zvolen Open TFTP server, který je volně šiřitelný a jeví se mi pro toto použití jako vhodný. Veškeré parametry se dají nastavit v souboru *OpenTFTPServer.ini* umístěném v adresáři programu.[10]

4.6.9 Uživatelská tlačítka

Pro budoucí snadnou integraci dalších funkcí je v programu IP Device Manager vytvořeno pět tlačítek, kterým je možno přiřadit externí spustitelný soubor s nějakými parametry a jeho funkce aplikovat na zařízení, které program IP Device Manager zná. Toto

lze aplikovat buď na zařízení, na kterém je kurzor, a nebo na zařízení, která jsou označena checkboxem.

Realizace těchto tlačítek je pomocí funkce *ExecAndWait,* v případě že je v nastavení zaškrtnuto, že program bude aplikován na vybraná (checked) zařízení nebo je využito funkce *ShellExecute* v případě, že je program použit pouze pro označenou položku. Výsledná syntaxe příkazu je potom: „[Program] [ip adresa zařízení] [Parametry]". Pro lepší orientaci je možné tlačítka pojmenovat vlastním názvem.

4.7 MOŽNÉ PROBLÉMY

Program je otestován na operačních systémech MS Windows ve verzích XP, 7 a 2003 Server a to na pěti různých počítačích ve čtyřech různých sítích. Všude fungoval bez problému. Podle verze OS Windows může dojít k rozdílům v některých grafických částech programu - například status bar indikující proces PING může být zelený a nebo modrý a složený ze segmentů.

Jelikož program používá některé systémové komponenty, tak doporučuji spuštění pod účtem patřícím do lokální skupiny *Administrators* - ideálně pokud takový uživatel bude přímo přihlášen (druhou cestou je "*spustit jako*"). Aby všechny funkce fungovaly korektně, měl by uživatelský účet, pod kterým je program IP Device manager existovat i na spravovaných počítačích a měl by být také ve skupině *Administrators*. Pokud tomu tak nebude, nebude fungovat například funkce *Shutdown*. Obdobně u funkce Synchronizace musí mít uživatel, který spustí IP Device Manager práva k zápisu do cílové složky a práva ke čtení ze zdrojové složky. Ideální je prostředí domény, kde se dají uživatelské účty řešit centrálně.

Další možnou příčinou je přítomnost firewallu a jeho špatné nastavení, které znemožňuje programu IP Device Manager kontaktovat přes uzavřený port klienta. V tomto případě je potom nutné nastavit ve firewallu povolené porty, programy nebo IP adresy - nastavení závisí na konkrétním druhu použitého firewallu.

Antivirové programy mohou způsobit dočasné zamknutí některého souboru (například databáze) a to může způsobovat problémy v tom, že program nebude moci tento soubor použít pro zápis. V takovém případě je nutno složku programu (nebo alespoň soubor IPDevMan.abs) vyjmout ze skenovaných souborů.

5 ZÁVĚR

Tato práce se v teoretické části zabývá problematikou správy prvků v počítačové síti. Jsou zde ukázány některé již existující systémy, které pracují na různých principech. Jednotným rysem všech těchto aplikací a koneckonců i většiny existujících aplikací této kategorie je obrovská funkcionalita. Daní za tuto vlastnost je ovšem složitost implementace a vysoké nároky na znalost programu. Pokud nebude mít správce znalost takovéhoto systému, může se nástroj pro hromadnou správu stát velmi nebezpečným nástrojem, kdy například reinstalace všech počítačů v sítí nebo smazání konfigurace páteřních síťových prvků může mít pro podnik fatální důsledky.

Program, který jsem se pokusil navrhnout v praktické části této práce, je poměrně jednoduchý jak na instalaci, tak na ovládání. Nedisponuje sice žádnými sofistikovanými funkcemi, ale jeho předností je integrace všech důležitých funkcí pro správu prvků v síti do jednoho okna. I když k některým funkcím využívá externích nástrojů, tak zprostředkovává jejich spuštění a je tedy vše dostupné z jednoho uživatelského prostředí.

Věřím, že program bude úspěšně nasazen do praxe a bude přínosem pro správce.

LITERATURA

[1] SOSINSKY B.: *Mistrovství - Počítačové sítě,* Computer Press a.s., ISBN 978-80-251-3363-7,ČR 2010.

[2] Microsoft.*Microsoft Technet, Instalace WSUS* [online]. © 2012 [cit.5.3.2012]. Dostupné z WWW: *http://technet.microsoft.com*

[3] Optimalizované IT. *Jak na přípravu instalací Windows 8 a Windows Server 8*[online]. © 2009 [cit.14.4.2012]. Dostupné z WWW: *http://www.optimalizovane-it.cz*

[4] Symantec Corporation, *Symantec Ghost Solution Suite* [online], ©1995-2012 [cit.17.4.2012]. Dostupné z WWW: *http://www.symantec.com/business/ghost-solution-suite*

[5] Enterasys Networks, Inc., *Enterasys NetSight*, [online]. ©2012 [cit.12.3.2012]. Dostupné z WWW: *http://www.enterasys.com/products/visibility-control/index.aspx*

[6] Kadlec Václav: *Učíme se programovat v Delphi a jazyce object pascal*,Computer Press a.s.,ISBN 80-7226-245-9,ČR 2001

[7] Kadlec Václav: *Delphi - Hotová řešení,*Computer Press a.s.,ISBN 80-251-0017-0,ČR 2003

[8] Grafika Publishing, s.r.o., *Otevírání externích programů* [online]. ©1997-2002 [cit.5.5.2012] .Dostupné z WWW: http://www.builder.cz/art/delphi/delphi_openextern.html

[9] *PuTTY: A Free Telnet/SSH Client* [online] Dostupné z WWW: http://www.chiark.greenend.org.uk/~sgtatham/putty/

[10] SOURCEFORGE.NET, *Open TFTP Server* [online]. ©1999-2009 - Geeknet, Inc., Dostupné z WWW: http://tftp-server.sourceforge.net/

SEZNAM ZKRATEK

PC	Personal Computer
BIOS	Basic Input - Output System
OSI	Open System Interconnection
STP	Spanning Tree Protocol
VLAN	Virtual Local Area Network
HTTP(S)	HyperText Transfer Protocol (Secure)
SSH	Secure SHell
Telnet	Telecommunication Network
IP	Internet Protocol
WLAN	Wireless Local Area Network
VoIP	Voice over Internet Protocol
S.M.A.R.T.	Self Monitoring Analysis and Reporting Technology
UPS	Uninterruptible Power Source
SNMP	Simple Network Management Protocol
HW	Hardware
SW	Software
USB	Universal Serial Bus
TFTP	Trivial File Transfer Protocol
SMS	Short Message Service
WOL	Wake On LAN
MS WSUS	MicroSoft Windows Server Update Services
GPO	Group POlicy
FAT	File Allocation Table
NTFS	New Technology File System
EXT2	EXTended filesystem
MDT	Microsoft Deployment Toolkit
WIM	Windows Imaging Format
DHCP	Dynamic Host Configuration Protocol
PXE	Preboot eXecution Environment
RDP	Remote Desktop Protocol