TECHNICKÁ UNIVERZITA V LIBERCI

Fakulta mechatroniky a mezioborových inženýrských studií

Studijní program: B2612 – Elektrotechnika a informatika

Studijní obor: 1802R022 – Informatika a logistika

Informační systém pro monitoring a evidenci počítačů v počítačové síti malé firmy

Information system for detection and monitoring computers inside small company computer network

Bakalářská práce

Autor: Tomáš Klaban

Vedoucí práce: RNDr. Klára Císařová Ph.D.

V Liberci 5.12.2008

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č.121/2000 o právu autorském, zejména § 60 (školní dílo).

Beru na vědomí, že TUL má právo na uzavření licenční smlouvy o užití mé BP a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

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

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Tomáš Klaban

V Liberci 5.12.2008

Poděkování

Na tomto místě bych rád poděkoval za vedení, cenné rady, připomínky a nápady vedoucí mé bakalářské práce RNDr. Kláře Císařové Ph.D.

Abstract

This work tries to comprehend the questions of local networks of smaller companies. Firstly it describes local network and its structure. It defines the reasons and particular modes of its supervision in daily working and points out the needs of evidence of client stations. The examples of available softwares, these questions can be solved with, are mentioned in the project. The work also designes own solution including the implementation of possible supervising together with the evidence of computers in a local network The functionality of the proposal is also described here. According to the fact that the designed application closely relates to the system register of Windows, one part of the work devotes to detailed description of Windows register The last part of the work analyzes the results of testing operation of designed application.

Abstrakt

Tato práce se snaží obsáhnout problematiku lokálních sítí menších firem. Nejprve definuje pojem lokální síť a popisuje její strukturu. Objasňuje důvody a možné způsoby jejího dohledování v běžném provozu a upozorňuje na potřeby evidence klientských stanic. Jsou zde zmíněny příklady dostupného software pomocí něhož se dá tato problematika řešit. Současně se zabývá i návrhem vlastního řešení, které v sobě implementuje možnost dohledu provozu společně s evidencí počítačů v lokální síti. Funkčnost tohoto návrhu je zde rovněž popsána. Z důvodu toho, že navržená aplikace přímo zasahuje i do systémového registru operačního systému Windows, je část této práce věnována i podrobnějšímu seznámení s registrem Windows. V závěru práce jsou zhodnoceny výsledky, kterých bylo dosaženo v průběhu zkušebního provozu aplikace.

Obsah

1 Úvod

V dnešní době každá firma, ať už se jedná o firmu větší či menší, vlastní jeden nebo více osobních počítačů.

V případě, že se jedná o malou firmu, například malého živnostníka, který používá pouze jeden počítač, který mu slouží povětšinou za účelem použití kancelářských aplikací, se jedná o záležitost poměrně jednoduchou. Takovýto počítač není součástí žádné lokální sítě a jeho případné připojení do veřejné sítě internetu je velice jednoduše řešeno pomocí nějakého veřejného poskytovatele připojení k internetu. Nevyskytují se zde tedy žádné síťové služby v rámci firmy, například nějaký server jako centrální úložiště dat, síťová tiskárna k centrálnímu tisku apod. Rovněž zde povětšinou není problém s administrací takovéhoto počítače. Menší poruchy se dají řešit uživatelskou svépomocí, případně servis zajistí autorizovaná firma.

Je-li však firma vlastníkem alespoň dvou počítačů a požaduje-li jejich vzájemné propojení nebo připojení těchto počítačů do jiné sítě, např. internetu, neobejde se již při řešení tohoto problému bez vzniku své lokální sítě. Takovéto lokální počítačové sítě se stávají stále běžnější a především nepostradatelnou součástí většiny firem a podniků, bez ohledu na jejich velikost a odvětví, ve kterém působí. Důvodem je především sdílení společných dat, kvalitnější a rychlejší komunikace mezi zaměstnanci, ochrana dat, připojení k internetu a mnoho dalších služeb, které jim lokální síť nabízí. Obecně by se dalo říci, že firma, která v současnosti nevyužívá síťové technologie pro svou podnikatelskou činnost, se značně znevýhodňuje na trhu mezi konkurenty.

Se stávajícím počtem uživatelských stanic a síťových zařízení v lokální síti je třeba také nějakým způsobem řešit její administraci. Jednou z možností pro firmu jak tento problém vyřešit je přenechat její veškerou administraci na nějaké jiné firmě, zabývající se takovouto činností , a která plně převezme veškerou odpovědnost za její zřízení i provoz na sebe, tzv. outsoursing. Pro firmu využívající takovouto lokální síť je tento stav ideální a v dnešní době je tento způsob i velice rozšířenou záležitostí.

Pokud se ale firma rozhodne administrovat svou vlastní síť sama, což je v dnešní době stále rozšířené jak u velkých tak i u malých firem a to z mnoha důvodů, je nucena sama řešit mnoho problémů, které přímo souvisí s jejím provozem.

2 Cíl

Cílem této práce je seznámit se se strukturou lokální sítě používané v praxi menší firmou a vytvořit lehce použitelnou aplikaci, která by dokázala současně monitorovat funkčnost koncových stanic v této síti a zároveň poskytovala databázi těchto zařízení. V této databázi by měla být uložena nejenom základní systémové informace o koncových zařízeních, ale měla by zde být i možnost zpětného dohledání provozu těchto stanic.

Pro získání relevantních informací o koncových zařízeních je předpoklad, že koncové stanice mají nainstalován operační systém Windows verze 2000 a výš a bude tedy možnost tyto informace získat vzdáleně z registrů Windows. Cílem této práce je také tyto registry Windows zmapovat.

3 Počítačová sít

3.1 Definice pojmu počítačová síť

Počítačová síť je distribuovaný výpočetní systém, který je tvořený soustavou vzájemně propojených počítačů a dalších síťových prvků. Mezi ně mohou patřit jednotlivé počítače a další prvky, z nichž se počítačová síť skládá, se nazývají uzly sítě a uzly jsou propojeny komunikační infrastrukturou. [6]

Existuje několik kritérií, podle kterých se nejčastěji počítačové sítě rozdělují.

- Jedním z nich je geografické pokrytí sítě, tedy rozsahu jaký zaujímají. Mezi ně patří například PAN, MAN, WAN a LAN. Z nichž právě LAN je ta, o kterou se jedná v případě firemních lokálních sítí.
- Dalším kritériem je dělení podle používaných přenosových médií. Přenosové médium je prostředí, ve kterém se šíří signál. Mezi ně patří metalická, optická a bezdrátová vedení.
- Síťová architektura je další kriterium. V dnešní době je jedním z nejpoužívanějších protokol TCP/IP.
- Podle přenosových technologii, z nichž nejrozšířenější, zhruba v 80%, je technologie Ethernet.

3.2 Sítě LAN

LAN (Local Area Network) označuje v oblasti informatiky malou datovou síť, která umožňuje komunikaci mezi propojenými počítači. Sítě LAN jsou dnes charakterizovány nejen vysokými přenosovými rychlostmi a malým dosahem, ale dnes již poměrně nízkými pořizovacími náklady a snadnou instalací. Najdeme je dnes již nejenom ve firmách, ale i v domácnostech. Nejpoužívanější technologií v oblasti LAN je ethernet a samotná komunikace je založena na protokolu TCP/IP. V dnešní době je již také většina firemních sítí LAN rovněž propojena do vnější internetové sítě, tedy do sítě typu WAN (Wide Area Network). [4] [6]

Topologie sítí LAN

Topologie sítí charakterizuje způsob, jakým jsou mezi sebou propojeny jednotlivé stanice. Je to vlastnost sítě, ke které se přihlíží hlavně ve fázi zavádění sítě, kdy se propojení stanice realizuje. Topologie sítě je plně určena použitým síťovým hardwarem, jimiž jsou samotné počítačové stanice, servery, síťové tiskárny a síťové přepínače. V oblasti sítí LAN jsou v současnosti běžné následující typy topologií.

- Topologie sběrnicová

  Topologie sběrnicová (Bus) je charakteristická tím, že jediné přenosové médium je sběrnice, ke které jsou postupně připojovány jednotlivé stanice. Zpráva vyslaná libovolnou stanicí se šíří po celé sběrnici, a tak ji může stanice, které je adresována, přímo přijmout. Problémem jsou zde však kolizní stavy, ke kterým dochází v případě souběžného pokusu o komunikaci

  Nejčastěji je tento princip využíván u Ethernetových sítí za použití koaxiálního kabelu.

- Topologie hvězdicová

  Pro lokální sítě typu LAN je tato topologie typická. Jednotlivé stanice v síti jsou vždy přímo propojeny na nějaký síťový prvek, jako je router nebo rozbočovač. Tyto prvky potom v síti působí jako jistá forma propojovacího centra. Velice často je pak tato koncepce používaná ve složitější podobě. Namísto jedné nebo více stanic, jsou do sítě připojeny další síťové prvky, jako např. HUB nebo Switch. Z nich je potom znovu rozvedena další hvězdicová struktura, čímž vznikne stromová architektura

vzájemně propojených stanic. I v této topologii se zpráva vyslaná jednou stanicí šíří po celé síti, aby ji mohla cílová stanice přijmout.

Této topologie se využívá při použití kroucené dvoulinky a je nejobvyklejší při použití ve firemních lokálních sítích.

- Topologie kruhová

  Topologie kruhová (Ring) označuje postupné propojení jednoho uzlu ke dvěma dalším uzlům tak, že je postupně vytvořen souvislý kruh. V takovéto síti je zpráva předávána postupně jedním směrem od stanice ke stanici až dospěje do stanice cílové. Tato metoda předávání informací je pomalejší a výpadek jakékoliv části sítě má bohužel za následek zkolabování sítě celé, nemohou však v takové síti vznikat kolizní situace.

3.3 Technické prostředky

V sítích LAN je fyzické propojení stanic v síti realizováno prostřednictvím síťových karet, které musejí být součástí všech počítačových stanic a ostatních zařízení v síti. Tato karta realizuje vlastní přenos informací ze stanice na vlastní vedení a naopak. Jako mezičlánky v lokálních firemních sítích potom slouží například další různé směrovače jako Switche nebo routry v případě připojení k sítím WAN.

Spojovací vedení

Spojovací vedení je v sítích LAN realizováno různými druhy propojovacích kabelů opatřených příslušnými konektory. V současnosti se používají následující druhy kabelů

- Koaxiální kabel

  Koaxiální kabel se vyznačuje velikou odolností proti rušení elektromagnetickým polem, jednoduchým způsobem konektorování a příznivou cenou. Významným parametrem je u něho impedance, pro různé typy sítí je totiž vyžadována různá přenosová rychlost u takovéhoto vedení je kolem 10 Mb/s na vzdálenost až 1 km. Tento typ vedení se však v menších firmách a domácnostech prakticky nevyskytuje a v současnosti je spíše historií.

- Kroucená dvoulinka

  Je to v současnosti nejoblíbenější a nejpoužívanější působ zajištění lokální sítě ve firmách a domácnostech. Jedná se o kabel, jehož jádrem jsou čtyři páry kroucené

dvoulinky. Samotný kabel může být potom v provedení stíněný (STP) nebo nestíněný (UTP). Maximální délka takovéhoto vedení může být 100m a přenosová rychlost se pohybuje do 250 Mb/s a s omezením vzdálenosti až 1Gb/s.

- Optický kabel

  Optický kabel je zatím nejmodernějším prostředkem pro propojení stanic v sítích LAN. Jeho významnou vlastností je naprostá odolnost proti rušení elektromagnetickým polem. Dále je charakteristický vysokou přenosovou rychlostí, vyšší cenou a náročným způsobem konektorování. Vlákna se dělí na jednovidová a vícevidová. Rychlost tohoto druhu přenosu se pohybuje okolo několika Gb/s a vzdálenost je omezena na 100 km. V lokálních firemních sítích se pro svou nákladnost a v podstatě nevyužití jeho předností téměř nevyužívá.

- Bezdrátové sítě Wi-Fi

  Wi-Fi je standartem pro lokální bezdrátové sítě LAN. Jedná se o bezdrátový digitální přenos na bezlicenčních pásmech 2,4 a 5 GHz, což má poměrně negativní důsledky ve formě zarušení a častých bezpečnostních incidentů. I přesto je v dnešní době čím dál více rozšířen v oblasti firemních sítí z důvodu jeho integrace do většiny přenosných zařízení.

3.4 Protokol TCP/IP

Protokol TCP/IP je dnes základní protokolovou architekturou, která se používá v rámci síťové komunikace. Je to sada komunikačních protokolů, kde hlavními jsou protokoly Transmission Control Protocol (TCP) a Internet Protocol (IP). Samotná architektura TCP/IP je členěna do čtyřech vrstev. Výměna informací mezi vrstvami je přesně definována. Každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší. Komunikace mezi stejnými vrstvami dvou různých systémů je řízena komunikačním protokolem za použití spojení vytvořeného sousední nižší vrstvou. [4] [6]

3.4.1 Vrstvy síťové komunikace

- Vrstva síťového rozhraní

  Jako nejnižší vrstva umožňuje přístup k fyzickému přenosovému médiu. Ve firemních sítích je většinou představována ethernetem.

- Síťová vrstva

  Tato vrstva zajišťuje především síťovou adresaci, směrování a předávání datagramů. Je implementována ve všech prvcích sítě jako směrovačích i koncových zařízeních a je představována v těchto firemních sítích právě protokolem IP.

- Transportní vrstva

  Transportní vrstva je implementována až v koncových zařízeních, tedy počítačích a umožňuje proto přizpůsobit chování sítě potřebám aplikace. Tato vrstva poskytuje spojované či nespojované transportní služby. Tyto služby jsou představovány protokolem TCP nebo UDP a používají 16 bitové číslo portu přidělené aplikaci.

- Aplikační vrstva

  Jedná se o samotnou vrstvu aplikací. Jsou to samotné programy nebo procesy, které využívají přenosu dat po síti ke konkrétním službám pro uživatele.

3.4.2 IP Protokol

IP (Internet Protokol) je protokol, pomocí kterého spolu komunikují všechna zařízení v Internetu. Dnes nejčastěji používaná je jeho čtvrtá verze (označovaná jako IPv4), postupně se však začíná rozšiřovat také novější verze 6 (IPv6).

3.4.3 IP Adresa

IP adresa je logická adresa zařízení a tedy jednoznačná identifikace konkrétního zařízení v prostředí jakékoliv počítačové sítě, tedy i v případě firemní sítě. Skládá se ze 4 částí zvaných octety (ve verzi IPv4), každá část je veliká 8 bitů, a zapisuje se oddělená tečkou. Adresa se většinou zapisuje v dekadické formě, ale pro výpočet je jasnější binární zápis. Teoreticky je tedy adresní rozsah od 0.0.0.0 do 255.255.255.255. Příkladem IP adresy může být tedy např. 178.71.62.180.

Adresa se v IPv4 dělí na tři základní části. První část nám určuje adresu sítě, druhá adresu podsítě a třetí konkrétní adresu počítače.

3.4.5 Maska podsítě

Maska podsítě nám pomáhá určit rozdělení sítě na podsítě. Určuje, která část IP adresy je síťová, a která pro hosty. Zápis je stejný jako u IP adresy, ale platné hodnoty jsou pouze ty, které mají v binárním tvaru zleva jedničky a zprava nuly (pokud se zleva na některé pozici

objeví nula, dále již musí následovat pouze nuly). Jedničky v masce jsou tzv. *network ID* a je to část, která je pro daný subnet stále stejná. Nuly jsou tzv. *host ID* a tedy část, která je proměnná a určuje adresu hosta v daném subnetu. Příkladem jednoduché masky je 255.255.255.0.

Maska podsítě se může zapisovat také ve zkrácené formě, které se říká CIDR notace. Ta se zapisuje jako IP adresa následovaná lomítkem (/) a číslem, které reprezentuje počet jedničkových bitů v masce podsítě v binární formě například 10.0.5.2/20, což představuje masku 255.255.240.0

3.4.6 Adresace lokálních sítí

Některé síťové rozsahy mají speciální vlastnosti. Tou hlavní je, že se neroutují, tzn. neprochází do dalšího subnetu. To se využívá u privátních subnetů, které neprochází do internetu. V praxi je využívá většina firem v lokální síti a do internetu přistupují přes veřejnou adresu za pomoci NATu.

tabulka 1: Adresace lokálních sítí

síť	adresa sítě	adresy hostů
10.0.0.0/8	10.0.0.0	10.0.0.1 - 10.255.255.254
192.168.0.0/16	192.168.0.0	192.168.0.1 - 192.168.255.254
172.16.0.0/12	172.16.0.0	172.16.0.1 - 172.31.255.254

3.5 Výhody lokální sítě

Výhod, které firma získá vznikem své lokální počítačové sítě je mnoho. Do jejího vzniku se vždy musí investovat mnohdy nemalé prostředky, ale vynaložené investice se povětšinou vždy vyplatí.

- Sdílení souborů
- Konverzace mezi uživateli sítě
- Tisk na sdílených tiskárnách
- Spojení s jinými sítěmi
- Práce na vzdálené stanici
- Ochrana dat
- Distribuované aplikace
- IP telefonie

4 Struktura sítě v malé firmě

4.1 Použité technologie

4.1.1 Klientská stanice

V drtivé většině případů lokálních firemních sítí klientskou stanici zastupuje osobní počítač, jehož síťové rozhraní představuje ethernetový adaptér. Jedná se o síťovou kartu, která je v dnešní době nezřídka integrována přímo na základní desce počítače. V případě, že není integrována, je propojena nejčastěji přes PCI slot na desce. Rychlostním standardem je v dnešní době 100 Mb/s, ale používají se dnes i karty s rychlostí 1Gb/s. Každá klientská stanice potom pracuje s protokolem TCP/IP a má tedy přidělenu jedinečnou IP adresu v rámci lokální sítě.

4.1.2 Ostatní síťová zařízení

Nejčastějším síťovým zařízením, kromě klientských stanic, jsou v dnešní době síťové tiskárny a síťové disky.

Lokálně připojené tiskárny jsou v dnešní době stále častěji nahrazovány multifunkčním zařízením, které je za pomoci vlastního ethernetového adaptéru schopno samostatného tisku.

Síťové disky jsou sdílená úložiště, která jsou v rámci sítě využívána více uživateli. V dnešní době se již tyto disky vyrábějí jako samostatné prvky s vlastním síťovým rozhraním a nemusí tak být součástí jiného počítačového systému.

Dalšími síťovými prvky jsou switche a routery. Switch, neboli přepínač je aktivní síťový prvek, který propojuje jednotlivé segmenty sítě. Switch většinou obsahuje od čtyřech až do několika desítek ethernetových portů, na něž se připojují síťová zařízení nebo části sítě. Pojem switch se používá pro různá zařízení v celé řadě síťových technologií. V dnešní době již switche téměř vytlačily dříve používané huby, které datagramy jednoduše rozesílaly do všech svých rozhraní. Oproti tomu switch datagram zašle pouze určenému adresátovi v síti na základě vlastní směrovací tabulky, kterou si sledováním sítě sám vytvoří.

Router je také síťový směrovač, v lokální síti má však na rozdíl od switche zcela jiný význam. Hlavním rozdílem mezi nimi je to, že router odděluje lokální síť od sítě vnější, např. internetem. Jako router lze společně s vhodným softwarem používat i osobní počítač.

Ve většině menších lokálních sítích se však používá účelových zařízení, kterých je v dnešní době na trhu nepřeberné množství. Většina takovýchto zařízení již také obsahuje DHCP (Dynamic Host Configuration Protocol) server a překlad síťových adres NAT (Network Address Translation). Mnohdy také bývají routery v kombinaci se Switchem a počet LAN portů je jedním z hlavních kritérií výběru. Dalším plusem bývá implementace Firewallu nebo logových záznamů, kterých se dá využít ke sledování provozu routeru.

Mezi další síťová zařízení, která se v dnešní době stále více vyskytují i v lokálních sítích jsou různé síťové kamery a v poslední době i stále se rozšířenější IP telefony.

4.1.3 Strukturovaná kabeláž

Základním prvkem infrastruktury moderní počítačové sítě je bezesporu strukturovaná kabeláž. V dnešní době se již prakticky vůbec nevyužívá koaxiálního nebo telefonního kabelu. Základem strukturované kabeláže je rozdělení celé kabeláže na úrovně a oddělené řešení jednotlivých úrovní. Jako základní médium se pro připojení zásuvek uvnitř budov používá ve strukturovaných kabelážích čtyřpárová kroucená dvoulinka. Vyrábí se v několika kvalitativních třídách, které se liší maximální přenosovou rychlostí. Podle požadovaných přenosových rychlostí se kromě kabelu volí také ostatní prvky sítě (zásuvky, propojovací panely, opakovače, atd.).

5 Administrace lokální sítě

5.1 Činnosti administrace

Se stále větším počtem a dostupností osobních počítačů, úměrně narůstá počet stanic v lokálních sítích. V důsledku toho také začínají mít místní administrátoři podnikových sítí nemalé problémy s jejich správou. Některé činnosti, které jsou součástí správy stanic v síti lze s pomocí různých postupů, software a technologií zjednodušit, některé však nikoliv. Součástí zjednodušení administrace může být správné nastavení sítě a stanic. Také použití vhodného software řeší mnoho operací za administrátora.

Počet lidí, kteří se zabývají administrací sítě se liší jednak podle velikosti firmy, ale podle nutné a požadované kvality správy. V řadě menších firem je administrace řešena povětšinou nekvalifikovaně, případně externě. Některé menší firmy mají případně jednoho administrátora, který je nucen řešit celou problematiku sám. Od vytváření strukturovaných

kabeláží, přes instalace a údržbu klientských stanic až po případné programování firemních aplikací.

Údržba hardware

Jedná se o fyzickou úpravu sítě, instalaci hardware nebo výměnu jednotlivých prvků v případě poruchy nebo plánované výměny. Výměnu z důvodu poruchy lze minimalizovat použitím kvalitního a ověřeného hardwaru s možností rychlé výměny jednotlivých komponentů nebo zamezením velkého namáhání v podobě vysoké teploty, nadměrné prašnosti, případně hrubým zacházením uživatelů.

Instalace operačního systému

Instalace operačního systému na klientské stanice se dá v případě multilicencí OS provádět za pomoci tzv. image (obrazů systému). Menší firmy však těchto multilicencí nevyužívají a instalace OS je nutno provádět jednotlivě.

Instalace software a jeho aktualizace

Jednou možností jak provádět instalaci programového vybavení stanic, je jednak provádět instalaci místně nebo to lze provádět vzdáleně za pomocí .msi balíčků daného software, které lze vytvářet pomocí programu Windows Installer. Aktualizace samotného operačního systému je povětšinou sama aktualizována pomocí služby Microsoft Update, který lze na místním serveru podpořit vzdálenou správou Windows Software Update Services.

Sledování funkčnosti sítě

V lepším případě by Administrátor lokální sítě měl mít možnost neustálé kontroly provozu v místní síti. Existují specializované firmy, které se zabývají jejich vývojem a implementací. Pro nejmenší a malé firmy se však mnohdy nevyplatí z různých důvodů jejich zakoupení a nasazení. O některých těchto prostředcích se zmíním později.

Sledování uživatelů a nastavení restrikcí

Uživatelé se na firemních počítačích mnohdy zabývají činnostmi, které nejsou zcela v souladu s přáním firmy. Takovouto činnost lze částečně omezit restrikcemi, případně činnost uživatelů sledovat za pomoci specielních software. Takovýto software by však měl být využíván vždy s ohledem na omezení soukromí uživatelů a nemělo by zde být ani

opomíjeno morální hledisko věci. Do této oblasti spadá také důležitá činnost a to zajištění bezpečnosti sítě, ať už z důvodu narušení jejího chodu nebo vynesení citlivých informací.

5.2 Software pro správu stanic

Požadavky pro správu stanic se nijak výrazně neliší od požadavků na ostatní software. Očekává se od něj především, že bude plnit úlohy, které administrátorům usnadní práci, případně zvýší schopnosti sítě. Požadavky administrátorů se mohou na tento druh softwaru výrazně lišit, proto jich existuje velké množství, které je stavěno takříkajíc na míru, aby co nejvíce vyhovovalo specifickým problémům a potřebám. Důvodem proč některé software jsou pro daný provoz nepoužitelné je nejenom případný nedostatek funkcí, ale i naopak jejich překombinovanost. Takovéto prostředí by mělo poskytnout jasný přehled o síti, stanicích v ní a situaci, v níž se síť a stanice nacházejí a nikoliv administrátora zaměstnávat mnoha nepotřebnými informacemi. Takovéto funkce mohou naopak nepříznivě ovlivnit ovladatelnost, složitost a nákladnost jejich uvedení do provozu. Takovýto software by měl především urychlit často potřebné, opakované nebo časově náročné operace.

Některá řešení těchto programů nabízejí například provádět hromadné operace, automaticky řešit nastalé situace v síti, získávat z počítačů potřebná data a vytvářet z nich různé analýzy a propojovat různé systémy dohromady. Pomáhají s instalacemi a úpravami operačních systémů, updaty software a nastavování chování celého systému. Někdy lze i nastavovat zasílání zpráv o problémech administrátorovi a následné reakce systému na vzniklou situaci.

V řadě případů menších lokálních sítí mnohdy postačí k řešení administrace pouze sada menších programů, mnohdy i volně dostupných bez nutnosti zakoupení licence nebo administrátorova šikovnost a znalost síťových služeb, které poskytuje vlastní operační systém. Proto je třeba výběr software pro správu sítě vždy důkladně zvážit a porovnat vynaložené náklady se skutečnými potřebami. Jejich cena, nabízené služby i použitelnost se totiž může výrazně lišit.

Jiný software budeme pořizovat, pokud se bude jednat o lokální síť čítající několik desítek až stovek počítačových stanic rozmístěných v několika objektech. Zde asi není třeba pochybovat o jeho potřebě. Naopak lokální sít čítající jen několik málo stanic rozmístěných na poměrně malém prostoru několika kanceláří bude mít zcela jiné požadavky. V takovémto

případě nám zcela jistě postačí nějaký freeware program, který bude poskytovat pouze prvotní informaci o provozním stavu.

5.2.1 Příklady software

Nagios

Nagios je program pro centrální správu a řízení systémů a sítí a je nejspíše jedním z nejznámějších. Je pod open source licencí GPL2 (General Publick Licence) a byl původně vytvořen výhradně pro operační systém Linux, přistupovat k němu lze však i z jiných operačních systémů. Pracuje s pomocí protokolu SNMP a umožňuje sledovat vybrané stanice a síťové služby. V případě odhalení nějakého problému v síti je schopen například přes web nebo email informovat administrátora. Neexistuje zde však žádná možnost evidence zařízení v síti.

Správce IT, Aktivity

Program Správce IT je především určen k evidenci výpočetní techniky a k provádění hardwarových a softwarových auditů. Jeho tvůrcem je firma MiCoS Software. Program vzdáleně scanuje hardware i software stanic a síťových prvků a získaná data a informace o stanicích ukládá na SQL server.

Program Aktivity je také od firmy MiCoS Software a narozdíl od Správce IT sleduje efektivitu využití softwarového a hardwarového vybavení stanic a licenční politiku.

Pro komplexní použití je možné oba zmiňované programy navzájem propojit, lze je však využívat pouze pro operační systém Windows. [12]

OptimAccess

Optim Access je vytvořen firmou Sodatsw. Při použití všech osmi nabízených modulů poskytuje velké množství administrátorských služeb, jako například ochranu operačního systému, restrikce, monitoring aktivit, audity a licenční politiku, vzdálené přístupy a centrální vyhodnocení získaných dat. Při používání tohoto systému je na jednotlivé stanice nejprve nainstalován klient, který posléze spolupracuje s administračním rozhraním na serveru. I zde je jeho použití omezeno výhradně na operační systém Windows. [19]

AuditPro

AuditPro je jeden z dalších nástrojů pro automatizovanou správu stanic a jeho výrobcem je firma TruconneXion. Automaticky scanuje PC v síti, sbírá reálné informace o jejich provozu a software. Jeho součástí je i schopnost snadného reportování vytvořených statistik ze získaných dat nebo možnost zabránění nežádoucích aktivit ze strany uživatele.

Lze jej rovněž rozšířit pomocí různých modulů, jako je například Správa Majetku nebo Čárové kódy. Pro provoz je třeba mít na stanicích nainstalovaného klienta pro sběr dat a funkčnost AuditPro je omezena na operační systémy Windows. [21]

Freeware

V dnešní době se dá pořídit také mnoho nástrojů, které jsou od různých autorů, jsou jednoduché a hlavně na jejich pořízení není třeba vydávat žádné náklady. Mezi ně patří například softwary jako je IPscan, Check nebo Look LAN. Jsou to však povětšinou programy sloužící pouze pro jeden daný účel. Mnohdy mohou velice dobře posloužit k orientaci o stanicích v síti, k ucelenější administraci sítě se však pro omezené možnosti povětšinou příliš nehodí. Jedním z mála poměrně povedených freewarových nástrojů je program Steel Inventory od firmy SteellSonic. Tento program dokáže řešit vzdáleně audit software a správu licencí, z mého pohledu mu však schází trochu větší přehlednost.

6 Návrh řešení

Navržený systém vznikl na základě požadavku jedné středně velké firmy, která využívá vlastní lokální počítačovou síť a čítá zhruba 80 osobních počítačů. Administraci této sítě firma řeší svépomocí a tak při této činnosti neustále naráží na problémy spojené s absencí jakési ucelené evidence, která by poskytovala větší přehled o koncových stanicích a jejich provozu. Mnohdy je nutné nově instalované stanice umisťovat u uživatelů dříve, než mají přidělena inventární čísla, nebo jsou z důvodu různých změn přemisťovány mezi jednotlivá oddělení. Při servisní činnosti tak dochází k nepřehledné situaci. Administrátor ztrácí nejenom přehled o konkrétním umístění PC, ale také postrádá jakékoliv reálné informace týkající se jejich základní konfigurace. Jejich fyzická kontrola je většinou velice zdlouhavá a používání vzdálené plochy je také velice často neefektivní.

Zmiňovaná firma nejprve zvažovala použití některého specializovaného software pro vzdálenou správu, narážela však neustále na několik aspektů, které vylučovali jejich použití.

Jedním z nich byli poměrně vysoké pořizovací náklady u nabízených produktů a ne vždy zcela jednoduchá implementace do vlastní sítě. U open source aplikací zase naopak mnohdy chyběla potřebná funkcionalita.

Danou firmou tedy bylo požadováno navržení jednoduchého systému, který by pro ně znamenal zjednodušení administrátorské činnosti a splnil jejich požadavky. Jedním požadavkem bylo získání ucelené evidence počítačů v síti, zahrnující základní poznatky o počítačích. Představa firmy byla taková, aby Administrátor v případě poruchy jakékoliv koncové stanice o ní věděl podstatné informace již při zjištění závady. Tím je myšleno, jaká verze OS je na počítači nainstalována, jaký je jeho typ, evidenční číslo i popis fyzického umístění. Stejně tak i jaký software a tiskárny jsou na daném počítači používány.

Druhým požadavkem byla možnost sledování provozu stanic. Firemní administrátor požadoval mít alespoň základní představu o provozu a dostupnosti počítačů v síti. Současně s tím i možnost zpětné informace o provozu jednotlivých počítačů.

Firma svou síť specifikovala jako síť LAN založenou na protokolu TCP/IP, která je zcela oddělena od vnější internetové sítě a tím i bez možnosti většího rizika napadení sítě z venku. Veškeré počítače v síti pracují s operačním systémem Windows 2000 nebo Windows XP. Nejnižší konfigurace počítače v síti je 800MHz s 256 MB RAM. Většina počítačů je využívána pouze jako kancelářské stroje a v síti se nenachází žádný databázový server.

7 Registry Windows

Před samotnou realizací a tvorbou software jsem byl nucen prostudovat nejdříve Registr systému Windows. Zejména tu část, ze které jsem se rozhodl získávat potřebné systémové informace o klientských stanicích. Ve firemní síti jsou totiž veškeré klientské stanice na platformě operačního systému Windows 2000 a Windows XP a Registr Windows jsem považoval za zdroj relevantních informací.

Registry (přesněji Windows Registry) jsou jakousi databází, do které si Windows (95/98/Me/NT/2000/XP/Vista) ukládají všechna svá nastavení. V registrech se dají najít veškerá nastavení týkající se používaného hardwaru a softwaru, dále pak nastavení týkající se vzhledu plochy, konkrétních uživatelů atd. Jakmile uživatel provede jakoukoliv změnu v systému prostřednictvím Ovládacích panelů, změnu v asociování souborů, systémových

politikách nebo v instalovaném softwaru, tak všechny tyto změny se promítnou zpětně do registrů. Windows Registry mají tedy pro chod systému zcela zásadní význam. [9] [13] [14]

7.1 INI soubory systému Windows

Soubory INI se velice často označují jako předchůdce systémového registru, který známe z operačních systému řady Windows. Tyto soubory byly zavedeny z důvodu požadavku na uchování důležitých informací o systémových, aplikačních a uživatelských nastaveních a poprvé se objevily s příchodem operačního systému Microsoft Windows 3.1x. Byli to textové soubory, které byli umístěny v kořenovém adresáři.

Hlavní rozdělení INI souborů bylo na tři základní typy

První typ

Prvním typem bylo šest inicializačních souborů. V těch bylo ukládáno především nastavení systému.

- *Win.ini*
  obsahoval základní informace o konfiguraci sytému a nově instalovaných programech
- *Systém.ini*
  obsahoval informace o hardwarovém nastavení
- *Control.ini*
  obsahoval seznam instalovaných ovladačů a nastavení pracovního prostředí
- *Progman.ini* a *Winfile.ini*
  obsahovaly nastavení pomocných aplikací pro práci s OS a nebyly zásadní pro běh samotného systému
- *Protocol.ini*
  obsahoval inicializační nastavení sítě

Druhý typ

Druhým typem byli samostatné inicializační soubory INI, které byli přidávány aplikacemi instalovanými do systému. V nich se ukládali konkrétní informace o instalovaných aplikacích.

Třetí typ

Třetím typem byl soubor Reg.dat, který byl již přímým předchůdcem v současnosti používaných registrů. Jednalo se o hierarchickou databázi, která obsahovala strukturu s názvem *HKEY_CLASSES_ROOT*. Tato databáze umožňovala uživatelům Windows 3.1x upravovat chování propojených nebo vložených objektů a nabízela možnost zobrazení seznamu aplikací registrovaných v prostředí Windows.

Soubory INI byly v podstatě textové soubory, které byly snadno upravitelné v jakémkoliv textovém editoru. Oproti tomu soubor Reg.dat byl binárním souborem a jeho úprava byla možná pouze pomocí aplikace Registry Editor, jakýmsi předchůdcem dnešního Regedit.exe.

Soubory INI měli však mnoho nevýhod a nedostatků. Jednak nebyla dána přesná pravidla pro jejich ukládání. Mohli být uloženy v jakémkoliv adresáři čímž bylo stíženo jejich nalezení, špatná ochrana proti zápisu a jejich nechtěnému smazání. Neposkytovaly žádnou podporu pro prostředí více uživatelů a více konfigurací hardwaru. Z tohoto důvodu nebyla ve Windows 3.1x také podpora Plug and Play. A hlavně každá aplikace ukládala své nastavení ve vlastních inicializačních souborech. Nebyla zde tedy ani možnost, na rozdíl od moderních operačních systémů, snadné implementce možností odinstalování.

7.2 Dnešní Registr Windows

Prvním operačním systémem řady Windows, který měl registry podobné těm dnešním byl Windows NT 3.5. Jeho registr obsahoval čtyři hlavní klíče.

HKEY_LOCAL_MACHINE, HKEY_CURENT_USER, HKEY_CLASSES_ROOT a HKEY_USERS. Díky tomu byla zajištěna mnohem efektivnější možnost správy systémového prostředí. U novějších verzí operačního systému k těmto čtyřem přibyl ještě klíč jeden a to HKEY_CURENT_CONFIG. Tyto kořenové klíče se velice často uvádí pod zkratkami HKLM, HKCU, HKCR, HKU a HKCC.

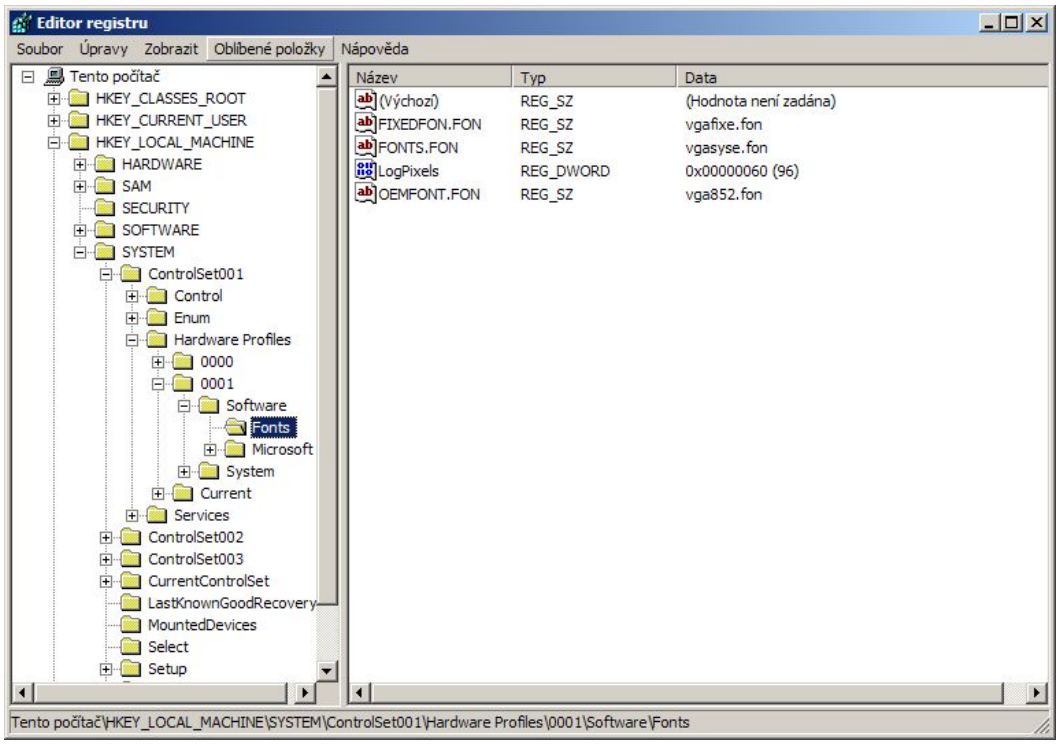
Mezi ty části systému, které nejčastěji používají registr Windows od verze NT patří hlavně

- Instalační programy
- Rozpoznáváni hardwaru
- Profily uživatelů

- Jádro Windows
- Hardwarové profily
- PnP manager
- Ovladače zařízení
- Nástroje pro správu

7.2.1 Struktura registru

Struktura registru se dá popsat stejně jako je popsána struktura jednotlivých souborů na disku. Registr obsahuje jednotlivé klíče, začínající vždy řetězcem HKEY_ , které se podobají složkám na disku. V nejvyšší úrovni této struktury je nazýváme kořenové klíče. A dále obsahuje hodnoty, které můžeme přirovnat k jednotlivým souborům. Jednotlivé klíče registru mohou obsahovat jak samotné hodnoty, tak ale i další podklíče. Samotné hodnoty registru pak obsahují data.



Obrázek 1: Hierarchická struktura registru zobrazená pomocí Regedit.exe

7.2.2 Popis jednotlivých kořenových klíčů

HKEY_LOCAL_MACHINE

Tento klíč je jedním z nejdůležitějších a nejzajímavějších kořenových klíčů registru. Obsahuje informace o hardwaru počítače, data operačního systému jako je typ sběrnice, údaje o spouštěcím procesu systému, údaje o paměti a ovladačích zařízení. Informace o tomto klíči jsou k dispozici pro všechny uživatele, kteří se přihlásí k místnímu systému.

Tento klíč obsahuje pět pro systém nejdůležitějších podklíčů, o kterých se zmíním později podrobně, neboť tento klíč je rozhodující pro získávání systémových informací.

HKEY_CLASSES_ROOT

Tento Klíč obsahuje informace týkající se asociací názvů souborů, informací OLE (Object Linking and Embedding) přiřazené objektům COM a asociací tříd souborů. Klíč s HKEY_CLASSES_ROOT je tedy odkazem na podklíč s příponou _Classes právě přihlášeného uživatele. Tento podklíč je umístěn v HKEY__USERS. V dřívějších verzích Windows, mimo Windows ME, je toto nastavení sdíleno všemi uživateli, což může mít jisté nevýhody. Například přepsání asociace souborů jedním uživatelem má vliv i na ostatní uživatele systému.

HKEY_CURENT_CONFIG

Poprvé se objevil ve verzi Windows NT 4.0. Zahrnuje konfigurační data pro aktuálně používaný hardwarový profil. Fyzicky jsou zde umístěna však pouze změněná data profilu. Ve skutečnosti jsou všechny klíče jen odkazem na klíč registru HKEY_ _LOCAL_MACHINE\Systém\CurentControlSet\HardwareProfiles\Curent, čímž je usnadněn přístup ke konfiguraci hardwarového profilu.

HKEY_CURENT_USER

Jsou zde uložena data popisující uživatelský profil uživatele, který je právě přihlášen do systému. Profil obsahuje informace definující individuelní nastavení pro pracovní plochu, síťová připojení a proměnné prostředí. Tento klíč je odkazem na klíč HKEY_USER\ \user_SID, kde user_SID je Security ID uživatele. který je přihlášen. Secuity ID je řetězec, který je používán k jednoznačné identifikaci uživatelů. Ve Windows 3.1 byli tyto údaje uloženy v souboru Win.ini.

HKEY_USERS

Zahrnuje všechny aktivně zavedené uživatelské profily. Podklíč DEFAULT je použit jako výchozí profil v případě prvního přihlášení uživatele do systému. Ostatní podklíče tvoří názvy uživatelů u systémů Windows 9x/ME. V případě Windows NT/2000/XP/Server 2003 jsou zde uvedena Security ID uživatele.

HKEY_DYN_DATA

Tento klíč obsahuje dynamické informace o zařízeních Plug and Play připojených k počítači. Vyskytuje se pouze ve verzích Windows 9x/ME. V betaverzích Windows 2000 vyvolávala editace tohoto klíče chybová hlášení, proto již od této verze není v Editoru registru zobrazován.

7.2.3 Datové typy registru

Data registru jsou parametry ukládané v jednotlivých klíčích registru. Každý parametr má svůj název, datový typ a hodnotu. Název je vždy textový řetězec. Samotná hodnota je potom uložena v jednom ze čtrnácti datových typů.

REG_BINARY

Jsou to nezpracovaná binární data a nejčastěji se jimi popisuje nastavení hardwarových součástí. Editory registrů tyto data zobrazují v hexadecimálním formátu.

REG_DWORD

Tento datový typ nejčastěji využívají položky služeb a ovladačů zařízení. Informace jsou zobrazována v hexadecimálním, binárním nebo decimálním formátu a je to číslo o délce 4 bajtů.

REG_DWORD_LITTLE_ENDIAN

Číslo o délce 32 bitů. Při uvádění této hodnoty se nejdříve objevuje nejnižší bit.

REG_DWORD_BIG_ENDIAN

Číslo o délce 32 bitů. Oproti předchozímu datovému typu se nejprve při zobrazování objevuje nejvyšší bit.

REG_EXPAND_SZ

Rozložitelný datový řetězec s různou délkou dat. Obsahuje název proměnné, který může být nahrazen hodnotou při vyvolání aplikací.

REG_MULTI_SZ

Představuje pole s více řetězci. Používá se pro seznamy textových řetězců. Znak NULL je zde použit jako oddělovač.

REG_SZ

Je to textový řetězec s pevnou délkou. Nejčastěji je tento typ používán pro popisy součástí.

REG_LINK

Je to řetězec znaků Unicode. Tento datový typ je určen pouze pro interní použití a umožňuje, aby proměnná s touto hodnotou odkazovala na jiný klíč nebo proměnnou v registru. Windows NT/200/XP tuto metodu aktivně používají (např. v HKEY_ _CLASSES_ROOT, který odkazuje na podklíče HKEY_USER).

REG_NONE

Je to nedefinovaný datový typ a zobrazuje se v hexadecimálním formátu.

REG_QWORD

64 bitové celé číslo a používá se pouze ve Windows 2000/XP/Server 2003/Vista.

REG_RESOURCE_LIST

Data tohoto typu jsou použita pouze v klíči HKEY_LOCAL_MACHINE \HARDWARE\RESOURCEMAP a je to seznam hardwarových prostředků používaných ovladačem hardwarových zařízení nebo některým z fyzických zařízení, které tento ovladač ovládá.

REG_RESOURCE_DESCRIPTION

Zpracováné hardwarové prostředky použité fyzickým zařízením, uložené v registru pod klíčem HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION.

REG_RESOURCE_REQUIREMENTS_LIST

Seznam možných hardwarových prostředků, který je používán pouze v klíči HKEY _LOCAL_MACHINE\HARDWARE\DESCRIPTION.

7.2.5 Registr v 64 bitových Windows

64bitové verze systému Windows XP a Windows Server 2003 mají většinu registru rozdělenou do 32bitových a 64bitových klíčů, jejichž obsah v podobě názvů klíčů je podobný. 32bitová část je v případě 64bitového EDITORU registru zobrazena pod klíčem HKEY_LOCAL_MACHINE\WOW6432. Do této části je také směřován veškerý přístup 32bitových aplikací. Tato služba je v 64bitových Windows označována jako WOW64.

7.3 Fyzické umístění registru

Přestože se zdá, že registr je jediné datové úložiště, ve skutečnosti se registr Windows skládá z více souborů. Umístění a počet souborů se vždy liší podle verze systému.

7.3.1 Windows 3.x

Ve Windows 3.x se konfigurační soubory s příponou .INI vyskytují v kořenovém adresáři systému.

7.3.2 Windows 9x

Tento OS ukládá registr do třech souborů, které se nacházejí v kořenovém adresáři systému.

- *USER.DAT*

  Informace o uživatelských profilech. V případě, že je použito více profilů, vyskytuje se tento soubor také v podsložkách adresáře %Složka systému%\Profiles.

- *SYSTEM.DAT*

  Zde je uloženo nastavení počítače a hardwaru.

- *CONFIG.POL*

  Umožňuje správcům sítě konfigurovat síťovou bezpečnost. Není však povinnou součástí instalace.

7.3.3 Windows ME

Používá stejné soubory jako Windows 9X, navíc však používá soubor *CLASSES.DAT*.

7.3.4 Windows NT/2000/XP/Vista

Tyto verze systému Windows ukládají položky registru v atomické struktuře. Registr je rozdělen do součástí nazývaných podregistry. Jedná se o části registru, které jsou stálé. Nejsou vytvářeny dynamicky při spuštění systému a nejsou odstraněny, když je systém vypnut (např. klíč HKEY_LOCAL_MACHINE\HARDWARE, který je vytvářen dynamicky rozpoznáním hardwaru při spuštění systému, tedy není považován za podregistr). Všechny soubory podregistrů, kromě některých podklíčů HKEY_USERS jsou ukládány ve složce %Složka systému%\System32\Config. Podklíče HKEY_USERS, které obsahují profily uživatelů jsou u Windows NT uloženy v podadresářích %Složka systému%\Profiles a v případě Windows 2000/XP ve složkách %Systémový disk%\Documents and Settings\%User%.

Každý podregistr je spojen se sadou standartních podpůrných souborů.

- HKEY_LOCAL_MACHINE\Sam - *Sam, Sam.log, Sam.sav*
- HKEY_LOCAL_MACHINE\Security – *Security, Security.log, Security.sav*
- HKEY_LOCAL_MACHINE\Software – *Software, Software.log, Software.sav*
- HKEY_LOCAL_MACHINE\Systém –*Systém, Systém.alt, Systém.log, Systém.sav*
- HKEY_CURENT_CONFIG – *Systém, Systém.alt, Systém.log, Systém.sav*
- HKEY_USERS\.DEFAULT – *Default, Default.log, Default.sav*
- HKEY_CURENT_USER – *Ntuser.dat, Ntuser.dat.log*
- Soubory, které nejsou spojeny s klíči – *Userdiff, Userdiff.log, Userdifr, Userdifr.log*

Jak je zřejmé, existují čtyři typy souborů, které souvisejí s podregistry. Bez přípony a s příponou .alt, .log a .sav.

- Bez přípony

  Obsahuje kopii podregistru.
- ALT

  Ve Windows NT/2000 obsahují záložní kopii podregistru HKEY_LOCAL_ _MACHINE. Ve Windows XP však byly tyto soubory zrušeny z důvodu přepracování algoritmů pro rychlejší dotazy, zvětšení registrů a jejich spolehlivost.
- LOG

  Tyto soubory uchovávají poslední změny, které byly provedeny v klíčích a hodnotách registru.

- SAV

  Soubory s touto příponou představují kopie podregistru z doby, kdy probíhala textová část instalace systému.

Registr zajišťuje atomicitu jednotlivých operací. To znamená, že veškeré úpravy v hodnotách registru se provádějí najednou a nemohou být přerušeny a odloženy na později. To vylučuje kombinace porušených starých a nových hodnot registru, například při výpadku proudu, potížích se softwarem nebo nefunkčnosti hardwaru. Díky tomu se nemůže v registru objevit nesmyslný záznam. Po restartu systému je položka registru buď nastavena na svou předchozí hodnotu nebo na hodnotu novou.

7.4 Velikost registru

Velikost inicializačních souborů win.ini u systému Windows 3.1x byla 64KB. Tento soubor mohl být i větší, veškerá data za touto hranicí však byla ignorována.

Systém Windows 2000/NT měl velikost registru omezenou přibližně na 80 procent velikosti stránkovacího souboru. Toto mělo zabránit situaci, kdy registr využije veškerý prostor potřebný pro jiné procesy. Existují totiž zařízení, jako jsou například terminálové služby využívající velkou část prostoru pro samotný registr a pro další součásti je ponecháno jen málo paměti.

V systému Windows XP bylo omezení velikosti odebráno. Je zde použit správce mezipaměti k provádění správy mapovaných zobrazení registru. Je zde také využíváno zdokonaleného algoritmu, který uchovává související paměťová místa ve větší blízkosti, což zvyšuje celkový výkon systému a rychlost prováděných dotazů. Velikost registru je zde tedy omezena pouze dostupným prostorem na disku.

7.5 Klíč HKEY_LOCAL_MACHINE

Jak jsem se již zmínil, tento klíč je jedním z nejdůležitějších a nejzajímavějších kořenových klíčů registrů, protože obsahuje konfigurační data pro místní počítač. Je využíván prakticky všemi aplikacemi a operačním systémem.

Tento kořenový klíč obsahuje pět podklíčů a jsou jimi

- HARDWARE
- SAM

- SECURITY
- SOFTWARE
- SYSTEM

Každý z těchto podklíčů potom obsahuje řadu dalších podklíčů. Tato struktura se zdá být velice nepřehledná, každá hodnota klíče má však v této struktuře pevné místo a jakákoliv neuvážená změna v hodnotách klíčů by mohla znamenat kolaps systému.

7.5.1 HKLM\ HARDWARE

Tento klíč obsahuje databázi, která popisuje všechna hardwarová zařízení nainstalovaná na počítači a vzájemnou spojitost mezi ovladači zařízení. Důležité je zde zmínit, že veškerá data v tomto podklíči jsou nestálá a systém tato data vytváří při každém spuštění. Téměř každá aplikace a ovladač používá tento podstrom k získání informací o systémových součástech a pro ukládání dat. Všechny sady důležitých dat jsou rozděleny mezi tři další podklíče. Pokud však jako uživatel potřebujete zjistit systémové informace, je přímá editace registrů obtížná. Většina informací je uložena v binárním formátu a je tedy výhodnější, použít k získání těchto informací okno Systémové informace.

DESCRIPTION

Zde se nachází popis veškerého hardware, který je fyzicky přítomný v počítači, zjištěný službou rozpoznání hardwaru, tedy Ntdetect.com a Ntoskrnl.exe. Ntdetect.com je standardní program stylu DOS, který používá volání BIOS pro výběr hardwarových informací a konfiguraci hardwarových zařízení. Během spuštění systému jsou ze získaných informací vytvořeny datové struktury, které Ntoskrnl.exe uloží pod tento klíč. U verzí Windows 2000/XP je však detekce zařízení Plug and Play přenechána ovladačům těchto zařízení. Ntdetect.com zjišťuje následující hardwarové zařízení.

- Typ sběrnice
- Klávesnice
- Adaptéry SCSI
- ID počítače
- Grafický adaptér
- Porty COM
- Aritmetický koprocesor

- Myš
- Disketová jednotka
- Paralelní porty

Každá takto zjištěná hardwarová součást je uložena do podklíče *MultifunkctionAdapte*r a obsahuje většinou alespoň tři parametry – *Component Information* (binární data o jejich součásti), *Configuration Data* (konfiguraci) a *Identifier* (název součásti).

DEVICEMAP

Tento klíč obsahuje řadu dalších podklíčů. Zde jsou potom uloženy data ve tvaru REG_RZ řetězců a která odkazují na jednotlivé ovladače a nastavení jednotlivých zařízení. Tyto informace jsou posléze uloženy do klíče HKM\SYSTEM\CurentControlSet\Services.

RESOURCEMAP

Jsou zde zmapovány prostředky ovladačů zařízení a hardwaru přiřazeného k těmto ovladačům. Uložená data se týkají ovladačů zařízení, IRQ a kanálů DMA. U Systémů Windows NT/2000/XP je RESOURCEMAP vytvářen při každém spuštění systému. Konkrétně tento klíč se značně liší v počtu podklíčů u jednotlivých verzí sytému Windows. Je to dáno úplností podpory Plug and Play. U verze 2000 a XP je zde například zřízen další klíč pojmenovaný PnP Manager.

7.5.2 Klíč HKLM\ SAM

Přístup ke klíči SAM (Security Account Manager) je implicitně zakázán a obsahuje informace o zabezpečení uživatelských a skupinových účtů uložených v databázi adresářů na místním počítači.

U systému Windows 9x a ME neexistuje a u verzí NT a 2000 obsahuje také data zabezpečení pro doménu, ke které místní počítač patří.

Tento klíč je zároveň odkazem na klíč HKLM\ SECURITY\ SAM a všechny změny, které se provedou v některém z jeho klíčů se zároveň projeví i v klíči HKML_SECURITY.

7.5.3 Klíč HKML\ SECURITY

Tento klíč je odpovědný za veškerá uživatelská práva a oprávnění uživatelů, zásady hesel a členství v místních skupinách.

Všechny tyto informace jsou definovány pomocí nástrojů pro správu a jsou tedy pro běžného uživatele skryté. Také jako u klíče SAM se jakákoliv změna projeví v klíči druhém.

Ve verzích Windows 9x/ ME tento klíč neexistuje.

7.5.4 Klíč HKML\ SOFTWARE

Nastavení, která jsou umístěna pod tímto klíčem, jsou platná pro každého uživatele přihlášeného k místnímu systému a obsahují konfigurační data týkající se softwaru nainstalovaného na místním počítači. Tento klíč obsahuje kromě spousty jiných, několik důležitých podklíčů.

Classes

V tomto podklíči se objevují data spojující aplikace nainstalované na místních počítačích s typy souborů podle přípony. Tyto podklíče obsahují data, která můžeme přidat pomocí karty Typy souborů.

Description

Zde jsou obsaženy názvy a čísla verzí softwaru, které jsou nainstalovány na místním počítači.

Microsoft

V tomto klíči jsou uložena konfigurační nastavení pro softwarové produkty Microsoft nainstalované na místním počítači.

Jedním z jeho nejdůležitějších podklíčů je HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion. Jsou zde uvedeny informace o softwaru, který podporuje vestavěné služby Windows a typ a číslo verze aktuální instalace Windows NT/2000/XP.

Policies

Zde se dá nalézt nastavení zabezpečení pracovních skupin.

7.5.5 Klíč HKLM\ Systém

V tomto klíči jsou uloženy informace o řízení spouštění systému. Sady zavedení ovladačů zařízení a služeb jsou uloženy v podklíčích ControlSet00x a CurrentControlSet.

Tato část registru hraje klíčovou roli při spuštění systému. Všechna data potřebná k řízení procesu spouštění jsou uspořádána v těchto podklíčích. Každý z nich potom obsahuje následující čtyři podklíče

- *Control* – obsahuje konfigurační nastavení použité pro správu systému, včetně síťového názvu místního počítače.
- *Enum* – obsahuje hardwarová data, včetně dat hardwarových zařízení a ovladačů, které mají být zavedeny.
- *Hardware Profiles* – obsahuje hardwarová nastavení a konfigurace ovladačů souvisejících s jednotlivými hardwarovými profily.
- *Services* – obsahuje seznam ovladačů, programy služeb a systémy souborů, které běží v uživatelském režimu.

7.6 Práce s registry

Pokud chceme pracovat s registry a upravovat je, existuje několik způsobů jak to udělat. Samotný systém Windows nám nabízí způsobů několik.

7.6.1 Nástroje pro správu

Pokud budeme chtít zasahovat do registrů jako běžný uživatel, postačí nám k tomu bohatě samotné prostředí Systému Windows. Většina změn se dá provést pomocí ovládacích panelů a nástrojů pro správu systému. Toto nastavení je vždy uživatelsky velice jednoduché a hlavně bezpečné. Nemělo by se tak stát, že dojde k takovému zásahu do registru, které povede k nestabilitě či úplné nefunkčnosti systému.

7.6.2 Editory registru

Dalším způsobem jak registr Windows editovat, je použít jeden z editorů, které nám Windows nabízí. Tento způsob je ale vhodný jen pro uživatele, kteří již o registr Windows něco vědí, znají alespoň trochu jeho strukturu a jsou si vědomi co mohou změnou registru vyvolat.

Regedit

Prvním takovým způsobem je použít editor registru Regedit. Tento editor je automaticky zkopírován během instalace OS do *%SystemRoot%* a spustit se dá zadáním

příkazu *Regedit.ex*e. Tento silný nástroj se dá používat k zobrazování, přidávání, odstraňování a upravování prvků registru a má uživatelské rozhraní Průzkumníka Windows.

Po spuštění se nám zobrazí okno editoru, které je rozděleno na dvě hlavní podokna. V horní části je potom zobrazen panel nabídek a ve spodní části stavový řádek.

V levém podokně se nám zobrazuje hierarchická struktura klíčů a jejich podklíčů. Hodnotové položky registru jsou zobrazeny v pravém okně editoru. Tyto hodnoty mají vždy tři parametry

- Název hodnoty
- Datový typ hodnoty
- Data hodnoty

Stavový řádek ve spodní části okna nám indikuje cestu vybrané položky registru, což je nezbytné pro orientaci v jeho velmi složité stromové struktuře.

Pomocí panelu nabídek můžeme jednotlivé hodnoty klíčů měnit, kopírovat, exportovat či importovat. Je-li počítač součástí sítě, která obsahuje servery Windows NT/2000 nebo Novell NetWare, můžeme pomocí regedit upravovat registry i na vzdáleném počítači.

Regedt32

Editor Regedt32.exe je jakýmsi předchůdcem Regedit.exe a byl původně vytvořen pro možnost úprav registru Windows 95/98, kde není jinak jejich úprava podporována. Oproti Regedit nemá uživatelské rozhraní podobné Průzkumníku Windows.

7.6.3 Zálohování registru

Většina nástrojů pro přímou editaci registru nedokáže vrátit provedené změny zpět. Proto by před jakoukoliv úpravou registru měla být provedena jeho záloha. Zálohování však může být užitečné i při nepřímém zásahu do registru, jako je například přidání nového zařízení nebo změna konfigurace pomocí konfiguračních nástrojů.

Bod obnovení

V dnešní době je nejčastějším způsobem vytvoření bodu obnovení.

Tento nástroj byl poprvé představen ve Windows ME a umožňuje zálohování systému do tzv. bodu obnovení. Obsahuje komponentu pro sledování souborů, která zajišťuje sledování změn v souborech systému a aplikací (nejedná se však o uživatelská data jako jsou

dokumenty a obrázky). Jednotlivé body jsou ukládány na základě plánu nebo při instalaci nové aplikace či ovladače, jejichž součástí je samozřejmě i registr systému. Obnovení systému však požaduje minimálně 200MB volného místa na pevném disku.

Čištění registru

S rostoucím používáním registru aplikacemi a systémem vzniká v jeho struktuře množství již neplatných odkazů. I když nejsou tyto údaje používané, systém je musí při svém startu načíst. Proto odstraněním takovýchto odkazů může dojít k mnohdy značnému zrychlení systému.

Nástroj RegCleaner poskytuje možnost manuálního výběru neplatných položek v daných místech registru nebo automatické vyhledávání neplatných položek. Tyto položky jsou následně z registru odstraněny. V případě nestability systému však mohou být vráceny nazpět ze zálohy. Takovýchto nástrojů pro odstranění nebo opravení neplatných položek je nepřeberné množství a většina z nich je freewarových.

8 Vlastní aplikace

Aplikace, kterou jsem nazval Monitor je vytvořena ve vývojovém prostředí Delphi. Toto vývojové prostředí je založeno na programovacím jazyce Object Pascal a je kompletně postaveno na objektově orientované architektuře, což umožňuje využívat řadu výhod objektového přístupu

Delphi je vývojovým nástrojem, jehož první verze byla vypuštěna firmou Borland v roce 1995. V té době bylo toto vývojové prostředí považováno za jakousi revoluci v oblasti programování pod Windows. Do dnešní doby bylo vydáno mnoho verzí a i přes to, že jsou dnes na trhu i jiná prostředí pro objektové programování pod Windows, mnohdy i více prosazovaných, stále patří mezi ty používanější. Je to dáno i tím, že jeho různé verze, většinou však s podstatnými omezeními, jsou volně dostupné pro všechny zájemce o programování v prostředí Windows. Neopomenutelnou výhodou tohoto prostředí je rovněž i velká podpora databází.

V mém případě jsem volil pro tento nástroj také z důvodu, že poskytuje snadné použití vlastních metod pro přímý přístup do Registru Windows. Snadný přístup k registru je možný jak na lokální stanici, tak obsahuje i metody umožňující snadný přístup do Registru okolních

stanic. A právě tato možnost byla pro mne podstatná z toho důvodu, že jsem se rozhodl Registr Windows použít jako zdroj k získání potřebných systémových informací o vzdálených počítačích.

8.1 Delphi a práce s registry

V Delphi má Knihovna VCL (knihovna vizuálních komponent) dvě třídy pro práci s registry systému Windows. Jednou je třída TRegistry a druhou třída TRegistryIniFile. Druhá jmenovaná je třída, která umožňuje pracovat s registrem a zároveň vytvářet přenositelné informace.

Pro účely prohledávání registrů je podstatná třída prvně jmenovaná a to TRegistry. Pomocí této třídy můžeme velice jednoduše otvírat, zavírat, ukládat, přesouvat, kopírovat a mazat jednotlivé klíče registru. [5] [8]

8.1.1 TRegistry

Pokud chceme pracovat s Registry Windows nejprve musíme do sekce *Uses* přidat jednotku Registry, protože jednotka TRegistry je definována právě zde. Tato třída nám umožní přístup, čtení, zápis i editaci registru. Základní vlastností této třídy je, že dokáže pracovat pouze s jedním klíčem, je tedy nutné, abychom před otevřením dalšího tento klíč uzavřeli.

8.1.2 Otevření a uzavření klíče

K otevření klíče nám slouží metoda *OpenKey,* která má dva parametry. Jeden obsahuje název klíče a je typu string a druhý je typu boolean a udává, zda se má klíč vytvořit, pokud neexistuje. Pokud takto otevřeme klíč, je pro nás přístupný až do doby, než použijeme metodu *CloseKey* a klíč uzavřeme. Žádný klíč bychom neměli nechávat otevřený déle, než je bezpodmínečně nutné!

8.1.3 RootKey

Pokud nezvolíme jinak, klíč bude otevřen, popřípadě vytvořen v kořenovém klíči *HKEY_CURRENT_USER*. Podle potřeby tento klíč můžeme změnit pomocí vlastnosti RootKey.

8.1.4 Metody pro práci s registry

Pro práci s registry nám Delphi nabízí mnoho metod. Já zde uvedu jen ty podstatnější.

- *CloseKey* - uzavře aktuální klíč
- *CreateKey* - vytvoří nový klíč v registru
- *DeleteKey* - smaže zadaný klíč včetně všech dat, která klíč obsahuje
- *DeleteValue* - smaže zadanou hodnotu v aktuálním klíči
- *GetKeyNames* - zjistí jména všech podklíčů v aktuálním klíči
- *GetValueNames* - zjistí jména všech hodnot v aktuálním klíči
- *HasSubKeys* - zjistí, zda aktuální klíč obsahuje nějaké vnořené klíče
- *KeyExists* - zjistí, zda zadaný klíč v registru existuje
- *LoadKey* - vytvoří nový klíč v kořenovém klíči a načte do něj data ze souboru
- *MoveKey* - přesune klíč včetně obsahu na nové místo Registru
- *OpenKey* - otevře, popř. vytvoří zadaný klíč
- *OpenKeyReadOnly* - otevře zadaný klíč pouze pro čtení
- *ReadBinaryData* - načte binární data z aktuálního klíče
- *ReadCurrency* - načte z aktuálního klíče hodnotu typu Currency
- *RegistryConnect* - vytvoří spojení s registrem na vzdáleném počítači
- *RenameValue* - přejmenuje zadanou hodnotu
- *ValueExists* - zjistí, zda zadaná hodnota existuje v aktuálním klíči
- *WriteBinaryData* - zapíše do aktuálního klíče binární data
- *WriteCurrency* - zapíše do aktuálního klíče hodnotu typu Currency

8.2 Systémové informace

V následující tabulce pro názornost uvádím některé příklady, kde přesně se dají v systémovém registru nalézt potřebné informace o systému. V aplikaci jsem využil z těchto informací jen některé, neboť mnohé z nich byly pro účely aplikace nadbytečné.

tabulka 2: Umístění konkrétních informací v registru

Druh informace	Umístění v Registru
Jméno počítače	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
Uživatelské jm.	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
Organizace	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
Operační systém	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
Verze OS	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
Druh procesoru	HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0
IP adresa	HKLM\SYSTEM\CurrentContr...\Services\Tcpip\Parameters\Interfaces
Zařízení IDE	HKLM\HARDWARE\DEVICEMAP\Scsi
Instal. software	HKLM\ SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
Instal. tiskárny	HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers

Jako ukázku, jakým způsobem v Delphi přistupujeme k systémovému registru, zde uvádím i část zdrojového kódu.

```
uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,Dialogs,Registry, StdCtrls, Menus, ComCtrls;
                                        // Přidání jednotky Registry do
                                        // sekce Uses
 private
  Reg: TRegistry; // Vytvoření objektu


procedure TForm1.Read;
  begin
     Reg := TRegistry.Create(KEY_READ);   // parametrem konstruktoru je
TRegistry.Create                        // přístupové právo, s jakým bude objekt
                                        // přistupovat do systémového registru.
```

```
                                        // KEY_READ znamená přístup pro čtení
                                        // objekt tedy nemůže data v registru měnit

Reg.RootKey := HKEY_LOCAL_MACHINE   //stanovení kořenového klíče registru,
                                        //  k němuž se budou vztahovat všechny
                                        // další cesty.
Reg.RegistryConnect('\\'+ (Address)) ;      // určení PC, ke kterému je přistupováno

if Reg.OpenKeyReadOnly
      ('\HARDWARE\DESCRIPTION\System\CentralProcessor\0') then // kontrola zda
                                                               // existuje daný klíč

begin
      PromenaA := Reg.ReadString('Identifier') // přečtení uvedené hodnoty klíče
      PromenaB := Reg.ReadString('ProcessorNameString');

 end;
   Reg.Free;          //  uvolnění registru z paměti
     end;
```

8.2 Instalace programu

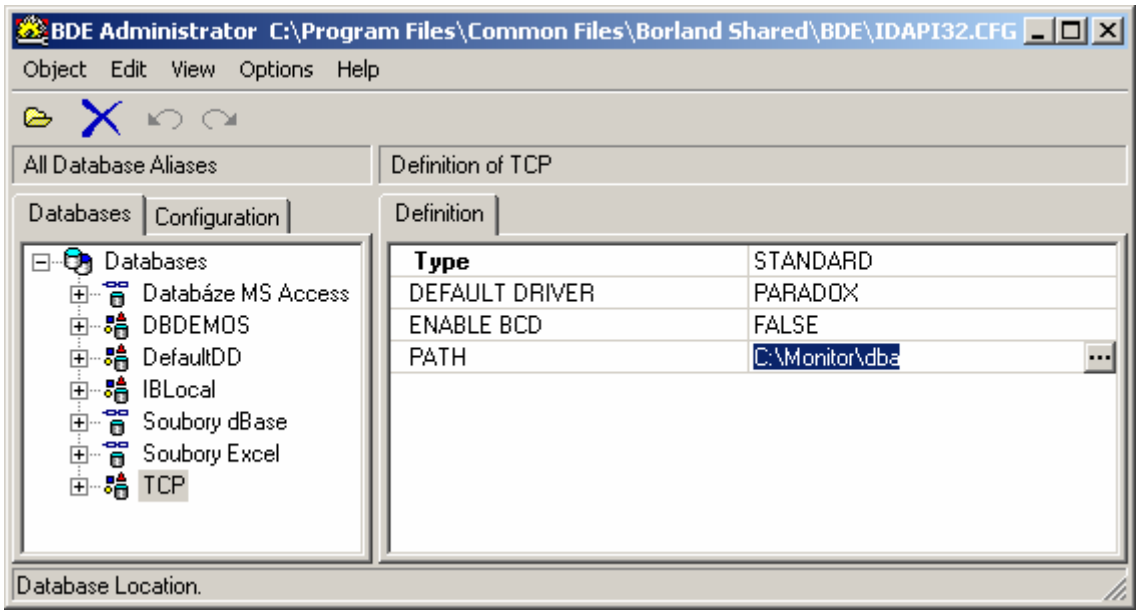
Aplikace Monitor je databázová aplikace, která pracuje s lokální databází typu Paradox. Je proto nutné mít na pracovní stanici, kde aplikace poběží, nejprve nainstalován Borland Database Engine (BDE). Je to Engine, který firma Borland využívá pro přístup k celé řadě databází a je volně ke stažení například přímo na jejich stránkách. Instalace je povětšinou bez další uživatelské specifikace a tak nepředstavuje většinou žádný problém.

Před dalším potřebným nastavením BDE je potřeba nainstalovat vlastní aplikaci. To spočívá v překopírování adresáře Monitor s jeho celým obsahem na místní disk stanice, kde bude aplikace spuštěna. Umístění tohoto adresáře na disku je libovolné. Já jsem volil jeho umístění do samotného kořene disku C:.

Tento adresář obsahuje spustitelný exe soubor aplikace *monitor.exe*, monitor.ini a dále potom podadresář *dba*, v němž jsou umístěny databázové tabulky „Connect.db a *TCP.db*. V těchto databázových tabulkách jsou při běhu aplikace ukládány data o klientských stanicích lokální sítě a o jejich síťové dostupnosti v danou dobu.

Před prvním spuštěním aplikace je ještě nezbytné pro funkčnost programu registrovat databázový alias v BDE, se kterým aplikace Monitor pracuje.

Nejprve spustíme BDE Administrator. Vybereme Object -> New a zvolíme typ Standard. Poté musíme napsat název aliasu, který je „TCP“. V dalším kroku je ještě potřeba vyplnit cestu k databázovému souboru. Soubor je uložen v kořeni disku C:, cesta k souboru je tedy „C:\Monitor\dba“ (viz. obr.1). V tomto okamžiku je aplikace připravena k prvnímu spuštění.



Obrázek 2: Registrace aliasu databáze

8.3 Spuštění a činnost programu

Jak je již z instalace patrné, aplikace se spouští pomocí exe souboru *monitor.exe*, který je umístěn v adresáři *Monitor*.

Po spuštění aplikace se otevře okno programu, které je rozděleno do čtyřech záložek. První z nich je záložka DBA, dále pak záložka DATA of PC, CONNECT a záložka CONFIG.

8.3.1 Config

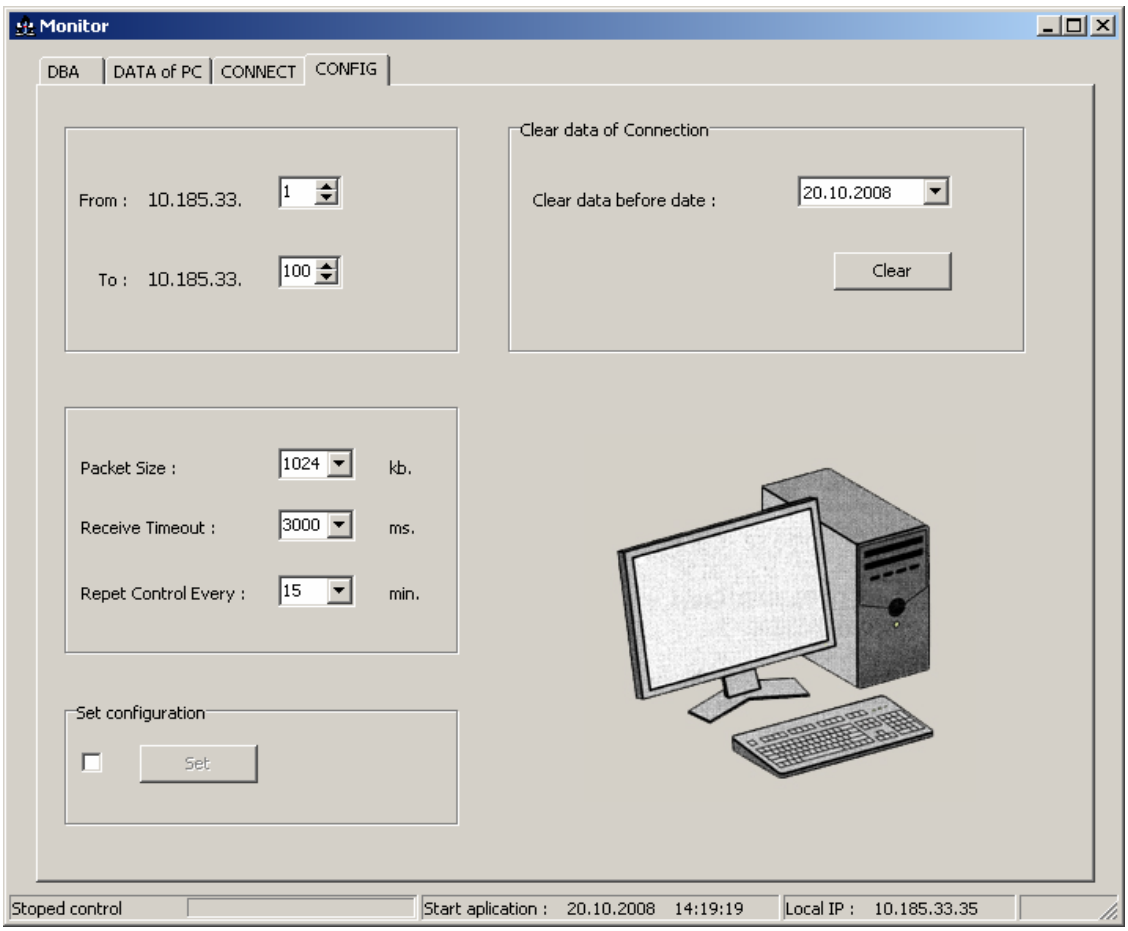
Po prvním spuštění je důležitá záložka CONFIG, kde je třeba prvotně nastavit rozsah IP adresace lokální sítě, ve které bude aplikace monitorovat provoz stanic. To provedeme v rámečku, který se nachází v levém horním rohu této záložky pomocí dvou komponent SpinEdit. Při spuštění aplikace je automaticky zjištěn prefix na prvních třech pozicích IP adresy. Stačí tedy nastavit pouze poslední octet první a poslední IP adresy počítačů v lokální síti. Standartně je rozsah nastaven od 1 do 254. V případě, že je v síti připojeno podstatně méně počítačů nežli 254, je lepší nastavit skutečný rozsah počítačů. Budeme tím šetřit nejenom čas potřebný k vlastní kontrole a prostředky procesoru, ale i velikost databáze.

Dostupnost počítačů v síti je kontrolována pomocí komponenty *Indy*, konkrétně *IdIcmpClient.* Jedná se v podstatě o běžně používaný příkaz *ping* v příkazové řádce Windows. Tato komponenta nám také umožňuje nastavení velikosti odesílaného paketu a velikosti timeoutu. Tyto hodnoty se dají nastavit v druhém rámečku této záložky. Přednastavené hodnoty velikosti paketu jsou 1024 kb a timeoutu 3000 ms. Zde je také třeba určit, v jakých intervalech požadujeme provádět kontrolu síťových stanic. Na výběr máme hodnoty 15, 30, 45 a 60 minut. Je to čas, v jakém započne následná kontrola počítačů, po ukončení předešlé kontroly.

Následně po změně popsaných parametrů musíme nastavení uložit, což provedeme tlačítkem SET a následným potvrzením dotazu, zda opravdu chceme nastavení uložit. Tímto je také vytvořena čistá databáze pro daný rozsah IP adres.

Na této záložce máme také možnost odmazání starších záznamů databázové tabulky, ve které jsou uloženy informace o dostupnosti jednotlivých počítačů v síti. To provedeme výběrem datumu v komponentě *DataTimePicker*, před kterým mají být data vymazána a následným potvrzením tlačítka *Clear*.

V tento okamžik je aplikace schopna začít monitorovat dostupnost počítačů v lokální síti a vzdáleně z nich získávat podstatné informace.

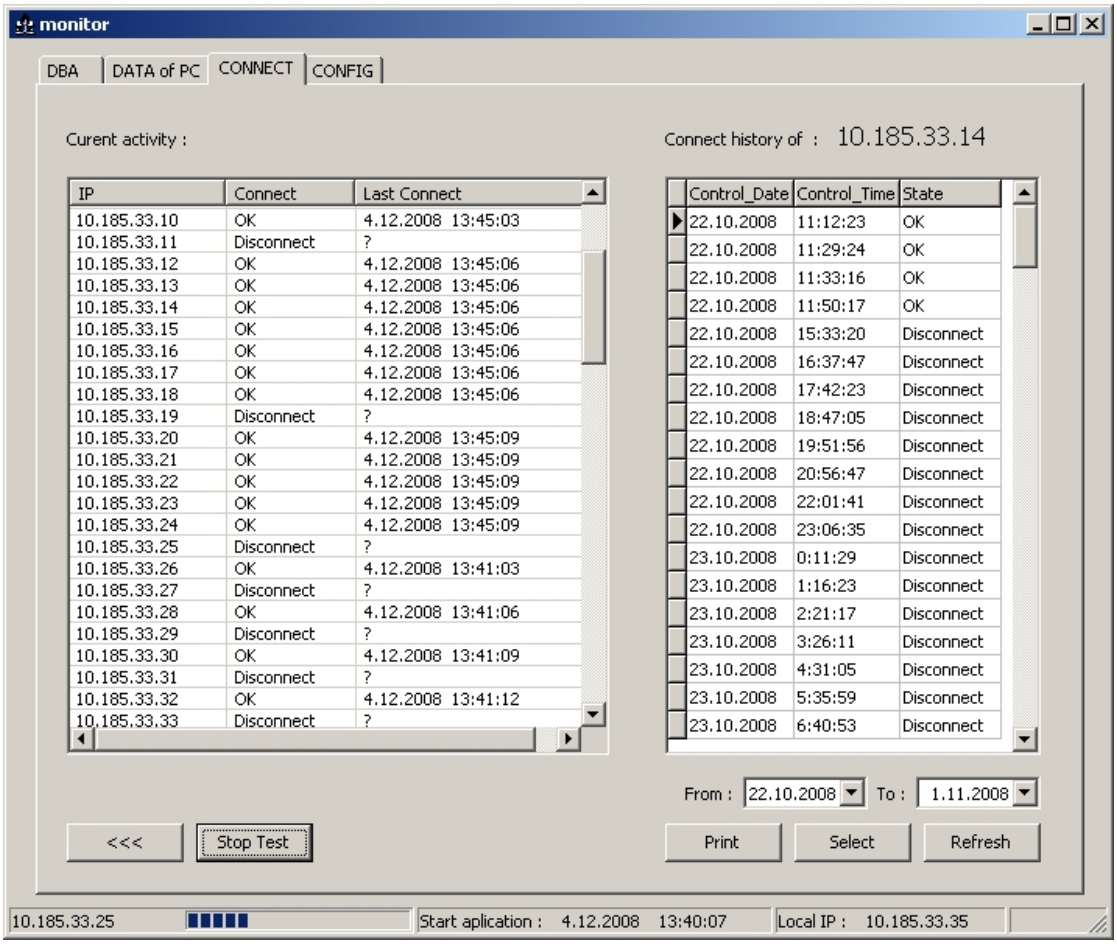


Obrázek 3 : Záložka CONFIG

8.3.2 Connect

Na této záložce jsou umístěny dvě tabulky. První tabulka nás informuje zda je spuštěna kontrola sítě. Pokud ano, jsou zde prezentovány informace, kdy byl který koncový počítač naposledy dostupný od spuštění aplikace a kontroly. Jedná se o komponentu *ListWiew*, která je rozdělena na tři sloupce. V prvním je vždy uvedena IP adresa koncového počítače, ve druhém slovně „OK“ pokud je počítač připojen nebo „Disconnect“ v případě nedostupnosti. Pokud je v tomto sloupci zobrazen symbol „?“, znamená to, že počítač nebyl od spuštění aplikace a kontroly ještě ani jednou dostupný. Ve třetím sloupci je uveden datum a čas poslední kontroly, vyhodnocené jako „OK“.

Kontrolu dostupnosti koncových počítačů spustíme případně zastavíme tlačítkem *Run Test* případně *Stop Test.* Ta je spuštěna v samostatném vlákně programu a neovlivňuje tím ostatní ovládání aplikace a práci s databází.



Obrázek 4: Záložka CONNECT

To, zda je spuštěna kontrola dostupnosti stanic je také zřejmé z komponenty *StatusBar*, kde je v levé části zobrazeno, která stanice je momentálně kontrolována, případně zda je kontrola zastavena nebo je zde uveden čas zbývající do další kontroly. Je zde také umístěna komponenta *ProgressBar*, která graficky znázorňuje stav právě probíhající kontroly. Ve *StatusBaru* je také uvedena informace, kdy byla aplikace spuštěna.

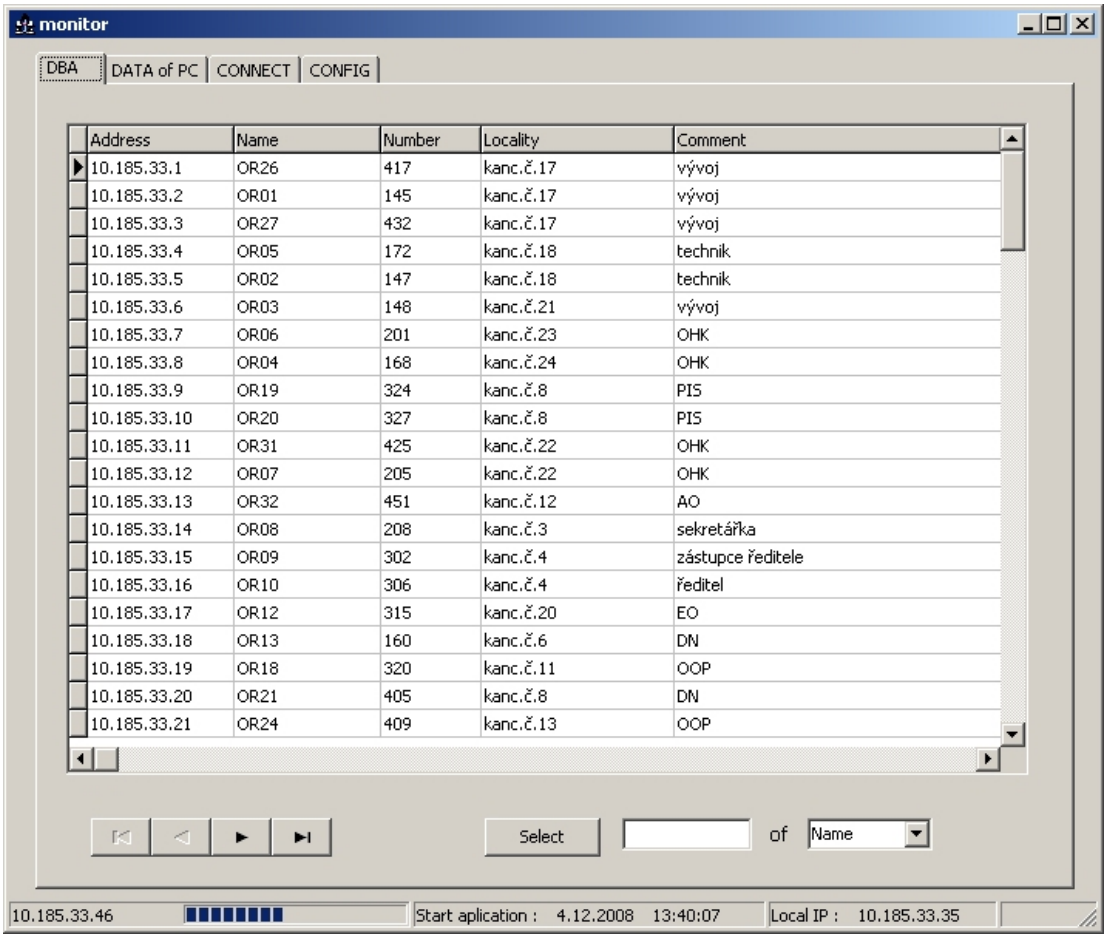
Druhá tabulka je tvořena databázovou komponentou *DBGrid*, která pomocí další databázové komponenty *Query* a dotazů jazyka SQL do databáze, zobrazuje historii kontrol počítačů.

Výběr počítače, jehož historii kontroly chceme v komponentě zobrazit, provedeme dvojím kliknutím na odpovídající IP adresu v levé tabulce. Získaná data můžeme nadále třídit výběrem rozmezí datumů v komponentách *DateTimePicker* a potvrzením tlačítka *Select*. To je opět provedeno SQL dotazem do databázové tabulky Connect.db.

Tlačítkem *Refresh* dojde ke znovunačtení dat z databáze a doplnění nových dat do tabulky v případě, že v uplynulém čase došlo k získání nových informací o dostupnosti počítače.

Pomocí tlačítka *Print* se nám otevře dialogové okno tiskárny a námi vybraný výpis historie connectů si můžeme vytisknout.

8.3.3 DBA



Obrázek 5: Záložka DBA

Hlavní komponentou této záložky je komponenta *DBGrid*, která nám graficky znázorňuje data z databázové tabulky. Je zde uvedena většina informací, ať již vzdáleně získaných nebo námi doplněných, o tom kterém konkrétním koncovém počítači. Zde můžeme informace o počítačích pouze uceleně prohlížet, případně pro větší přehlednost třídit. K tomu nám slouží dole umístěné editační pole s komponentou *ComboBoxI*. Tlačítkem *Select*

následně výběr provedeme. Při výběru můžeme užít i hvězdičkové konvence pro nahrazení libovolného znaku.

Komponenta *DBNavigator* nám umožňuje zjednodušení pohybu po zobrazených datech.

8.3.4 Data of PC

Na tuto záložku můžeme přejít jednak kliknutím na její záhlaví nebo dvojím kliknutím v záložce DBA na řádek počítače, jehož data chceme editovat nebo jen zobrazit. Na této záložce se nám tak zobrazí ucelený výčet informací o tom daném počítači.

Část těchto informací je administrátorem libovolně editovatelná. Jsou to informace, které se netýkají systémových informací, ale jde spíše o informace evidenčního a informativního charakteru.

Jedná se o :

- *Numbe*r – zde se uvede čtyřmístné evidenční číslo počítače
- *Locality* – pro uvedení popisu umístění počítače (např. číslo kanceláře)
- *Coment* – libovolný komentář o velikosti 35 znaků
- *Type* – výrobce počítače, případně jiné typové označení

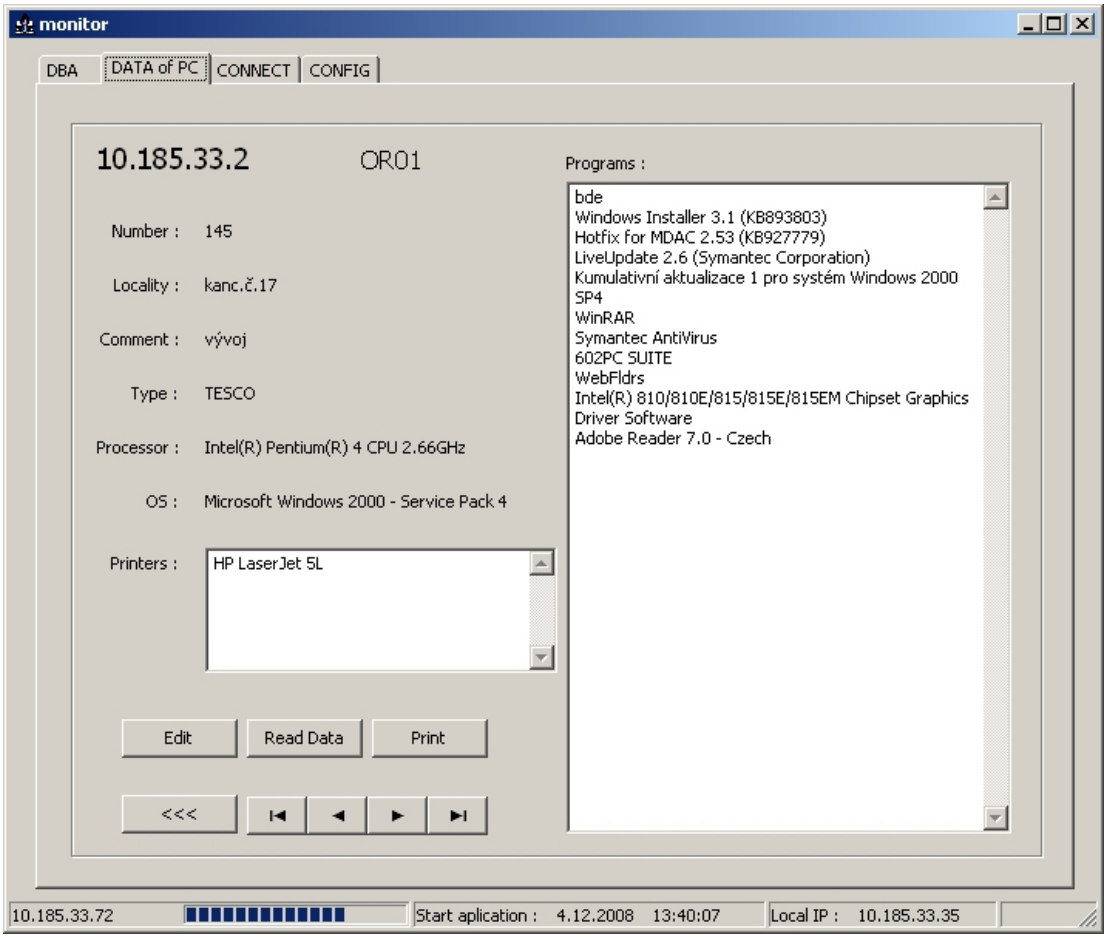
Po stisku tlačítka *Edit* se nám tyto kolonky změní v editační pole a poskytnou nám možnost doplnit pro nás potřebné údaje. Stiskem tlačítka *Save* tyto data uložíme do databáze.

Ostatní informace jsou získávány vzdáleně z koncového počítače z Registru Windows. K tomu je použito metod obsažených v Delphi, které pracují s třídou Tregistry. Jedná se o informace o jménu počítače, procesoru a jeho frekvenci, verzi operačního systému i s označením verze servis packu. Dále jsou to informace o tiskárnách a programech, které jsou instalované na daném počítači. Většina položek je z registru získávána jednoduchým načtením hodnoty hledaného klíče nebo několika klíčů. Oproti tomu, položky instalovaných programů se získávají rekurzívním procházením určité části kořenové struktury registru. Dále jsou potom ještě filtrovány, aby se odlišily od instalovaných programů aktualizační balíčky a bezpečnostní záplaty, jejichž popisy jsou v registru uloženy na stejném místě.

Tyto data jsou načtena po stisku tlačítka *Read Data*, kdy dojde nejprve k načtení IP adresy počítače a kontrole pomocí komponenty *Indy*, zda je počítač dostupný. Poté jsou vzdáleně načtena požadovaná data z registru a uložena do databáze.

Pomocí této záložky tak můžeme postupně jednak získat skutečné informace o kontrolovaných počítačích, doplnit je a uložit do databáze. Takto lze také kdykoliv zaktualizovat data a nahradit je skutečnými.

Na tomto listu je také ještě umístěn *DBNavigator,* opět pro snazší pohyb po zobrazovaných datech a tlačítko *Print*, pomocí něhož můžeme vytisknout sestavu právě zvoleného počítače.



Obrázek 6: Záložka DATA of PC

8.4. Funkčnost programu

Tento program je možné provozovat na operačních systémech Windows 2000, XP. Rovněž i koncové stanice, které jsou pomocí aplikace Monitor dohledovány, mohou mít libovolný z těchto uvedených operačních systémů.

Důležitou podmínkou pro funkčnost aplikace z pohledu vzdáleného přístupu k systémovým informacím je uživatelský účet. Program je nutné mít spuštěný z uživatelského

účtu, který je rovněž přítomný i na koncových stanicích a je pod stejným přístupovým heslem s administrátorskými právy. Pokud totiž není na koncovém počítači takovýto účet vytvořen, pokus o přístup do registru skončí výjimkou. Rovněž je důležité, aby klientské stanice měli přiděleny pevné IP adresy a nebyly jim přidělovány dynamicky pomocí DHCP serveru. Toto je důležité pro jejich jednoznačnou identifikaci při dohledování provozu a rovněž aby nemohlo docházet k záměně získaných dat.

Další podmínkou pro činnost aplikace je povolení činnosti protokolu ICMP (Internet Control Message Protocol) u systému Windows XP v nastavení Firewallu. Toho je využíváno při kontrole dostupnosti stanic příkazem PING a tato kontrola by jinak nebyla funkční.

V průběhu činnosti kontroly dochází ke stálému narůstání velikosti databázové tabulky Connect.db. Je tedy na místě, například vždy po uplynutí jednoho měsíce, tuto tabulku odzálohovat. Následně na záložce CONNECT k určitému datu odmazat staré záznamy a ponechat zde pro další potřebu pouze omezený počet dat, například z posledních několika týdnů.

8.5. Vyhodnocení provozu

Program byl nainstalován ve firmě na jednu stanici v síti a odzkoušen provozem v období jednoho měsíce. Rozsah IP adres zde byl nastaven v rozmezí od 1 do100 s ohledem na možné rozšíření o další stanice. Hodnota velikosti packetu byla nastavena na 1024 kb, timeoutu na 3000 ms a periodicita kontroly na 30 min.

Databáze počítačů byla postupně doplňována a vzdálené získávání informací, při dodržení podmínky existence administrátorského účtu na koncové stanici, nečinilo žádné potíže. Tyto informace byli rovněž průběžně využívány při servisních zásazích.

Zejména informace o instalovaných tiskárnách se v průběhu provozu projevily jako velice užitečné. Problémy s tiskem byli totiž ve sledovaném období jedním z nejčastějších problémů, s jakým se uživatelé obraceli na administrátora sítě. Ten tak již mohl efektivněji reagovat na vzniklý problém. Rovněž byla velice kladně hodnocena možnost získání aktuálních informací o instalovaném software.

Informací týkajících se dostupností stanic bylo používáno zejména k průběžné kontrole provozu jednotlivých počítačů. Velikost databázové tabulky Connect.db po 30 denním zkušebním provozu a periodicitě kontroly 30. min. byla cca. 2,5 MB.

Po ukončení zkušebního provozu byl vznesen provozovatelem sítě požadavek o zhodnocení provozu sítě, respektive celkové využitelnosti počítačů ve sledovaném období. Postupné získávání informací o provozu jednotlivých počítačů je pomocí aplikace Monitor samozřejmě možné. Pro získání celkového přehledu všech počítačů však není tato aplikace uzpůsobena z důvodu toho, že nebyl tento požadavek prvotně specifikován.

Ze získaných dat během provozu uložených v tabulce Connect.db se tyto informace vyzískat dala. Bylo však třeba pro tuto činnost použít nějaký databázový editor, spolupracující s tabulkami Paradox. Zvolil jsem pro tuto činnost editor databázových tabulek TbView5, který umožňuje pomocí příkazů SQL zpracovávat uložená data tabulek. Aplikaci TBView5 jsem zvolil jednak pro svoji jednoduchost bez nutnosti instalace a také proto, že se jedná o freeware software.

Pomocí tohoto editoru a dotazů SQL byla z tabulky Connect.db získána tabulka č.3. Jednotlivé hodnoty v tabulce znamenají vždy počet počítačů z celkového počtu 80, které byli v průběhu jednoho měsíce v jednotlivé dny v provozu. První řádek uvádí celkový počet spuštěných počítačů v dané dny. Druhý udává počet spuštěných počítačů v pracovní dobu, tedy v období od 7:00 hod. do 15:30 hod. Třetí řádek uvádí počet počítačů spuštěných mimo pracovní dobu, respektive mimo běžnou pracovní dobu. Část zaměstnanců firmy totiž nepracuje pouze v běžnou pracovní dobu a plní své úkoly v průběhu 24 hodin. Ze získané tabulky byl poté sestaven graf č.1.

Použité SQL dotazy do databáze

Pro získání celkového počtu spuštěných počítačů v daný den

```
SELECT  COUNT (Distinct ID_Address)  FROM  Connect
WHERE  Control_Date = '1.11.2008' and State = 'OK'
```

Pro získání počtu spuštěných počítačů v době od 7.00 do 15.30 hod.

```
SELECT  COUNT (Distinct ID_Address)  FROM Connect
WHERE  Control_Date = '1.11.2008' and State = 'OK' and (Control_Time  Between '07:00' and '15:30')
```

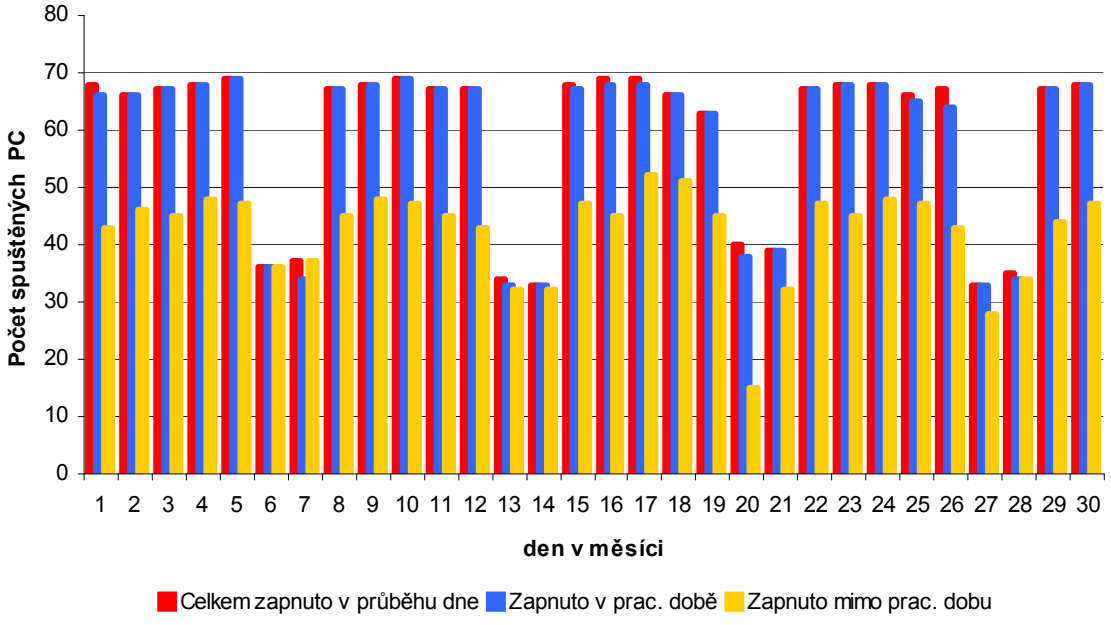
Pro získání počtu spuštěných počítačů mimo dobu od 7.00 do 15.30 hod.

SELECT COUNT (Distinct ID_Address) FROM Connect

WHERE Control_Date = '1.11.2008' and State = 'OK' and (Control_Time NOT Between '07:00' and '15:30')

tabulka 3: Získaná data z databázové tabulky Connect.db v měsíci září 2008

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
celkem	68	66	67	68	69	36	37	67	68	69	67	67	34	33	33
v prac. dobu	66	66	67	68	69	36	34	67	68	69	67	67	33	33	33
mimo prac. dobu	43	46	45	48	47	36	37	45	48	47	45	43	32	32	32
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
celkem	69	69	66	63	40	39	67	68	68	66	67	33	35	67	68
v prac. dobu	68	68	66	63	38	39	67	68	68	65	64	33	34	67	68
mimo prac. dobu	45	52	51	45	15	32	47	45	48	47	43	28	34	44	47



Graf č. 1: Přehled použití počítačů ve firmě v měsíci září 2008

Z tohoto grafu je zřejmé, v jakém počtu a v jakou dobu jsou ve firmě využívaný pracovní stanice. Jsou například patrné značné výkyvy v počtech zapnutých stanic

o víkendech. Rovněž počet zapnutých počítačů v mimopracovní dobu zřejmě zcela neodpovídá počtu pracovníků, kteří jsou ve firmě v tu dobu přítomní. Oprávněnost činnosti počítačů je však zcela v kompetenci řešení firmy.

9 Závěr

Díky nasazení tohoto software v provozu jsem si ověřil jeho provozuschopnost. Nejen, že se aplikace osvědčila jako prostředek k evidenci počítačů. V praxi tato databáze administrátorovi sítě posloužila pro rychlou orientaci a získání informací o koncové stanici při její poruše. Průběžné informace o provozu v síti a jednotlivých stanicích se několikrát ukázaly jako potřebné a byly využívány při prvotních detekcích chyb v provozu.

I přesto, že aplikace splňuje požadavky, které byli na počátku firmou respektive jejich administrátorem specifikovány, provoz ukázal i několik nedostatků. Projevila se zde absence jednodušší a komplexnější možnosti vyhodnocení uložených dat. Při žádosti o vyhodnocení dat více stanic najednou, jsem byl nucen tento požadavek splnit za pomoci jiného software pro editaci databázových tabulek.

Proto musím uvažovat pro další vývoj této aplikace s jejím rozšířením. Zejména v oblasti vyhodnocování dostupných dat. Z nich lze získat mnoho cenných informací a jejich jednodušší způsob vyhodnocování by byl pro firmu velkým přínosem. Mohlo by tím dojít například i k ušetření nákladů při investicích do pořízení nového počítačového vybavení.

Rovněž by firma měla začít uvažovat o instalaci nějakého databázového serveru. Pokud by se data ukládala na takovýto server, mohlo by se k datům přistupovat vzdáleně z jakékoliv koncové stanice, například od samotného uživatele. I to by potom bylo velkým přínosem pro práci administrátora.

Literatura

[1] *About.com* [online]. Delphi Programing
URL: <delphi.about.com/od/delphitips2008/qt/listview_draw.htm>

[2] *Arlow, Jim. Neustadt, Ila*. UML a unifikovaný proces vývoje aplikací. Computer Press. 2003. ISBN: 80-7226-974-X. 387 stran

[3] *Cantú, Marco*. Myslíme v jazyku Delphi 6, 2.díl. Grada Publishing. 2002. ISBN: 80-247-0335-1. 511 stran

[4] *Enciklopedie Wikipedia* [online]. Local Area Network.
poslední aktualizace 12.3.2008.
URL: <cs.wikipedia.org/wiki/LAN>

[5] *Frank Eller*: Delphi 6, Grada Publishing. 2002,
ISBN: 80-247-0303-3. 272 stran

[6] *Horčica, Adam* [online]. Počítačové sítě. poslední aktualizace 25.11.2004
URL: <emp.wz.cz/net/main.php?side=obsah>

[7] *Kadlec, Václav.* Delphi, hotová řešení. Computer Press. 2005.
ISBN: 80-251-0017-0. 312 stran

[8] *Kadlec, Václav*. Učíme se programovat v Delphi, Computer Press. 2001,
ISBN: 80-7226-245-9, 288 stran

[9] *Kokoreva, Olga.* Registr Microsoft Windows XP. Computer Press. 2004.
ISBN-80-7226-783-3, 393 stran

[10] *Kretchmar, James. M. Dostálek, Libor.* Administrace a diagnostika sítí.
Computer Press 2005. 216 stran. ISBN: 80-251-0345-5

[11] *Lacko, Luboslav*. SQL, Kapesní přehled. Computer Press. 2005.
ISBN 80-251-0788-4, 96 stran

[12] *MicosSoftware* [online]. Správce IT
URL: www.micos-sw.cz/Produkty/Spravce-IT

[13] *Microsoft Corporation* [online]. Rozdíly mezi Regedit.exe a Regedt32.exe.
poslední aktualizace 3.12.2007.
URL: <support.microsoft.com/kb/141377/>

[14] *Microsoft Corporation* [online]. Informace pro pokročilé uživatele.
poslední aktualizace 4.2.2008.
URL: < support.microsoft.com/kb/256986>

[15] *Microsoft TechNet* [online]. Ping. poslední aktualizace 21.1.2005.
URL:< www.microsoft.com/technet/prodtechnol/windowsserver2003/cs/
/library/ServerHelp/9eaf7bdd-ee42-4358-9b60-66c8463dbdee.mspx?mfr=true

[16] *Molíková,Jana*. Molíkovy stránky[online], Registry Windows.
publikováno 18.11.2007.
URL: <www.molik.go.cz/pc/registry20.htm>

[17] *PJ Soft* [online]. Delphi, databáze. publikováno 20.3.2008.
URL: <www.volny.cz/pjsoft/tipy/Delphi/DBase.htm>

[18] *Ráb Jakub, Zita Jakub* [online]. Vše o počítačových sítích.
Poslední aktualizace 12.1.2003.
URL: <www.vda.cz/studenti/prace/rab/>

[19] *SodatSW [online]*.
URL: < www.sodatsw.cz/titulka.asp>

[20] *Svoboda, Luděk.Voneš,Petr. Konšal, Tomáš. Mareš, Miroslav*. 1001 tipů a triků pro Delphi. Computer Press. 2003, ISBN: 80-7226-488-5. 546 stran

[21] *TruconneXion*. AuditPro [online].
URL: www.auditpro.cz/cs/prehled-funkcionalit

[22] *Zive.cz* [online]. Fórum programování v Delphi.
URL: <forum.zive.cz/forum-922/
/Programovani.html?sid=bd43c3d9d643d4079cb77b18cb30c3c3 různá fóra>

Přílohy

Příloha A - Struktura přiloženého CD

Bde - adresář obsahující instalační soubor Borland Database Engine

Doc - textová část BP ve formátu doc a pdf

Monitor - adresář obsahující veškeré potřebné soubory aplikace Monitor

TbView5 - editor databázových tabulek

Zdrojový kód - adresář obsahující zdrojový kód aplikace Monitor

Příloha B - Výpis sestavy počítače

PC Name : OR01

IP Adress : 10.185.1.2

Number : 145

Locality : kanc.č.17

Comment : vývoj

Type : TESCO

Processor : Intel(R) Celeron(R) M processor 1.50GHz

OS : Microsoft Windows 2000 - Service Pack 4

Programs :
==========

bde
Windows Installer 3.1 (KB893803)
Hotfix for MDAC 2.53 (KB927779)
LiveUpdate 2.6 (Symantec Corporation)
Kumulativní aktualizace 1 pro systém Windows 2000 SP4
WinRAR
Symantec AntiVirus
602PC SUITE
WebFldrs
Intel(R) 810/810E/815/815E/815EM Chipset Graphics Driver Software
Adobe Reader 7.0 - Czech

Printers :
==========

HP LaserJet 5L

Příloha C - Výpis historie provozu

10.185.33.27

2. 11. 2008	0:29:07	Disconnect	3. 11. 2008	9:09:49	OK	4. 11. 2008	17:01:02	Disconnect
	1:02:31	Disconnect		9:41:38	OK		17:33:47	Disconnect
	1:35:56	Disconnect		10:13:23	OK		18:06:39	Disconnect
	2:09:20	Disconnect		10:45:09	OK		18:39:30	Disconnect
	2:42:44	Disconnect		11:16:51	OK		19:12:21	Disconnect
	3:16:08	Disconnect		11:48:36	OK		19:45:12	Disconnect
	3:49:32	Disconnect		12:20:19	OK		20:18:03	Disconnect
	4:22:57	Disconnect		12:52:04	OK		20:50:55	Disconnect
	4:56:21	Disconnect		13:23:59	OK		21:23:46	Disconnect
	5:29:45	Disconnect		13:55:53	OK		21:56:37	Disconnect
	6:03:09	Disconnect		14:27:44	OK		22:29:32	Disconnect
	6:36:33	Disconnect		14:59:36	OK		23:02:29	Disconnect
	7:09:57	Disconnect		15:31:30	OK		23:35:26	Disconnect
	7:43:21	Disconnect		16:03:51	Disconnect	5. 11. 2008	0:08:23	Disconnect
	8:16:46	Disconnect		16:36:40	Disconnect		0:41:21	Disconnect
	8:50:10	Disconnect		17:09:28	Disconnect		1:14:18	Disconnect
	9:23:34	Disconnect		17:42:16	Disconnect		1:47:15	Disconnect
	9:56:58	Disconnect		18:15:07	Disconnect		2:20:13	Disconnect
	10:30:19	Disconnect		18:47:59	Disconnect		2:53:10	Disconnect
	11:03:37	Disconnect		19:20:50	Disconnect		3:26:07	Disconnect
	11:36:56	Disconnect		19:53:41	Disconnect		3:59:04	Disconnect
	12:10:14	Disconnect		20:26:35	Disconnect		4:32:01	Disconnect
	12:43:32	Disconnect		20:59:33	Disconnect		5:04:59	Disconnect
	13:16:50	Disconnect		21:32:30	Disconnect		5:37:56	Disconnect
	13:50:08	Disconnect		22:05:27	Disconnect		6:10:53	Disconnect
	14:23:27	Disconnect		22:38:24	Disconnect		6:43:45	Disconnect
	14:56:45	Disconnect		23:11:24	Disconnect		7:16:24	OK
	15:30:06	Disconnect		23:44:25	Disconnect		7:48:21	OK
	16:03:27	Disconnect	4. 11. 2008	0:17:25	Disconnect		8:20:07	OK
	16:36:48	Disconnect		0:50:25	Disconnect		8:51:52	OK
	17:10:10	Disconnect		1:23:25	Disconnect		9:23:38	OK
	17:43:31	Disconnect		1:56:26	Disconnect		9:55:23	OK
	18:16:49	Disconnect		2:29:26	Disconnect		10:00:52	OK
	18:50:04	Disconnect		3:02:26	Disconnect		10:32:34	OK
	19:23:19	Disconnect		3:35:26	Disconnect		11:04:17	OK
	19:56:31	Disconnect		4:08:27	Disconnect		11:35:59	OK
	20:29:44	Disconnect		4:41:27	Disconnect		12:07:44	OK
	21:02:56	Disconnect		5:14:27	Disconnect		12:39:30	OK
	21:36:08	Disconnect		5:47:28	Disconnect		13:11:18	OK
	22:09:20	Disconnect		6:20:25	Disconnect		13:43:01	OK
	22:42:32	Disconnect		6:53:19	Disconnect		14:14:43	OK
	23:15:41	Disconnect		7:25:52	OK		14:46:28	OK
	23:48:57	Disconnect		7:57:50	OK		15:18:20	Disconnect
3. 11. 2008	0:22:12	Disconnect		8:29:44	OK		15:50:26	Disconnect
	0:55:27	Disconnect		9:01:39	OK		16:23:15	Disconnect
	1:28:42	Disconnect		9:33:33	OK		16:56:03	Disconnect
	2:01:57	Disconnect		10:05:21	OK		17:28:51	Disconnect
	2:35:13	Disconnect		10:37:07	OK		18:01:42	Disconnect
	3:08:28	Disconnect		11:08:55	OK		18:34:34	Disconnect
	3:41:43	Disconnect		11:40:43	OK		19:07:28	Disconnect
	4:14:58	Disconnect		12:12:35	OK		19:40:22	Disconnect
	4:48:13	Disconnect		12:44:20	OK		20:13:16	Disconnect
	5:21:28	Disconnect		13:16:09	OK		20:46:11	Disconnect
	5:54:43	Disconnect		13:47:57	OK		21:19:05	Disconnect
	6:27:56	Disconnect		14:19:45	OK		21:51:59	Disconnect
	7:01:08	Disconnect		14:51:34	OK		22:24:53	Disconnect
	7:33:48	OK		15:23:31	OK		22:57:48	Disconnect
	8:05:55	OK		15:55:40	Disconnect			
	8:37:55	OK		16:28:20	Disconnect			