ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

PROVOZNĚ EKONOMICKÁ FAKULTA

OPERAČNÍ SYSTÉM WINDOWS 2000

DIPLOMOVÁ PRÁCE

AUTOR DIPLOMOVÉ PRÁCE: MAREK BREJNÍK
VEDOUCÍ DIPLOMOVÉ PRÁCE: ING. JIŘÍ VANĚK

V PRAZE 6. DUBNA 2001

1. OBSAH

2. ÚVOD

Vývoj v oblasti informačních technologií probíhá neuvěřitelně rychlým tempem. Žijeme na začátku 21. století a paradoxně i na začátku třetího tisíciletí. Moderní informatika vznikla teprve ve století dvacátém a za tak krátkou dobu se dostala do stavu, který známe. Stačí se podívat na jiné obory lidské činnosti a porovnat vývoj.

Tento vývoj se dotknul i mé diplomové práce. V rozpětí pouhých dvou let se toho na poli informačních technologií změnilo tolik, že při zadání tématu diplomové práce nebylo prakticky o čem psát, při prezentaci se na trh již připravuje nová verze Windows.

Jak se to mohlo stát ? Odpověď je jednoduchá. Při zadání tématu mé práce, tj. „Operační systém Windows 2000“, tento operační systém existoval pouze na počítačích vývojářů v Redmondu (sídlo firmy Microsoft Corp.). A nebylo to tak dlouho, co jeho název byl Windows NT 5.0. Neexistovaly žádné materiály ani žádná dokumentace přístupná zákazníkovi. Ta byla dostupná pouze specialistům, kteří si museli informace koupit prostřednictvím služby Microsoft Technet. V době, kdy předkládám a prezentuji tuto práci, by měl být ve fázi závěrečného testování následovník Windows 2000, Windows XP, původně známý pod kódovým označením Whistler. Naštěstí Windows XP mají stejné vlastnosti jako Windows 2000 a nabízejí jen kosmetické úpravy a opravy chyb předešlé verze.

Z tohoto názorného příkladu je vidět, do jak nelehkého úkolu jsem se pustil. Jelikož Windows 2000 je špičkový operační systém obsahující velké množství komponent, nebylo v mých silách během dvou let dokonale poznat všechny tyto komponenty natož je popsat.

Proto jsem svou práci rozdělil na dvě základní části. V první části se věnuji obecným informacím o Windows 2000, charakteristickým znakům tohoto operačního systému a jednotlivým součástem. Ve druhé jsem se soustředil na rozbor jedné ze služeb Windows 2000, a to terminálových služeb. Tato kapitola je pak dále rozdělena na teoretickou část, která popisuje jednotlivé složky terminálových služeb, použité protokoly apod. Druhá, praktická část, pak popisuje praktické nasazení a využití terminálových služeb jak v podnicích, tak ve školách.

V době psaní mé práce neexistovala dostupná kvalitní česká literatura. Proto jsem veškeré informace získal na internetových stránkách. Prvotním zdrojem byly stránky firmy Microsoft, která nabízí i část textů ze služby Microsoft Technet. Dalším zdrojem pak byly stránky jak oficiální (například firmy Citrix), tak neoficiální, tj. stránky firem, používající Windows 2000 a profesionálové, kteří se věnují praktickému nasazení Windows 2000.

Během práce se systémem Windows 2000 jsem samozřejmě přistoupil k vlastnímu studiu OS, právě z nedostatku literatury. A protože se řadím mezi nadšence, kteří nenechají kámen na kameni a věčné rýpaly, nechtěl jsem si svá zjištění a objevy nechat jen tak pro sebe. Proto jsem si zřídil vlastní internetové stránky, které jsou věnovány právě problematice Windows 2000. Tyto stránky je možno nalézt na internetové adrese *www.volny.cz/ferengi* (viz příloha C). Tyto stránky patří mezi nejlepší zdroje informací o Windows 2000 na českém internetu, o čemž svědčí jak dopisy od čtenářů mých stránek, tak recenze v odborných časopisech (např. PC World 9/2000).

Přílohou mé práce je disk CD, který obsahuje kompletní diplomovou práci ve formátu Microsoft Word 2000, ve formátu PDF, HTML a RTF. Dále je zde prezentace Microsoft PowerPoint, která obsahuje základní informace k mému tématu diplomové práce. Na CD je také kompletní web mých internetových stránek a obrazová dokumentace k páté části práce, věnované hodnocení možnosti implementace.

3. CÍL PRÁCE A METODIKA

Cílem této práce bude v první řadě popsat koncepci operačního systému Windows 2000. V této části bych se chtěl zaměřit na popis a charakteristiku jednotlivých verzí Windows 2000, na celkovou orientaci systému k využití sítě Internet, a to i z hlediska zabezpečení jak dat, tak systému jako celku. Dále se zaměřím na popis stability a dostupnosti systému na síti, možnosti dynamické správy, konfigurace a nastavení jak lokálně, tak vzdáleně. Na závěr této části uvedu výhody, které sníží náklady na vlastnictví (*TCO – Total Cost of Ownership*) a možnosti využití existujících investic do IT.

Ve druhé části se zaměřím na vlastní architekturu operačního systému. Rozeberu vrstvu *User mode* a vrstvu *Kernel mode* i všechny podsystémy těchto vrstev. V další části se pokusím popsat fungování práce procesů, jejich správu systémem, vysvětlím principy a fungování kooperace mezi procesy (*preemptivní multitasking*) a vnitřní chování procesů (*multithreading*) i ve vztahu k víceprocesorovému systému (*multiprocessing*). Dále popíši paměťový model tj. správu paměti, zacházení s virtuálním adresovým prostorem a využitím odkládacího souboru (*pagefile*).

Ve třetí části přistoupím k hodnocení možnosti implementace. Jelikož Windows 2000 jsou rozsáhlý produkt, zaměřím se zde na využití terminálových služeb (*terminal services*). Zde ozřejmím základní informace potřebné pro další kapitoly práce. Jedná se především o vysvětlení principu tenkého klienta, o popis a architekturu terminálových služeb. Následovat bude popis potřebného hardwarového vybavení jak na straně serverů, tak na straně klientů. Samozřejmě nebude chybět ani popis softwarového vybavení a detailní popis použitých protokolů RDP a ICA a jejich vzájemné srovnání. Poté bude následovat blok, který bude věnován praktickému nasazení v praxi. Jedná se o využití terminálových služeb jak PC klienty na platformě x86, tak přenosnými zařízeními s Windows CE. Podrobněji se zaměřím na popis přípravy serveru pro kvalitní fungování terminálových služeb, zaměřím se na přípravu licenční politiky a instalaci potřebných aplikací, a to i na straně klientských zařízení. Pak již popíši vlastní fungování a praktické použití na příkladech počítačové učebny, souborového serveru a vzdálené správy serveru z pohledu obou platforem (PC x86 a HPC). A protože terminálové služby zahrnuté do Windows 2000 nejsou jediným nástrojem pro vytvoření aplikačního serveru a umožnění vzdálené správy, pokusím se o srovnání s konkurenčními produkty Citrix MetaFrame a SCO Tarantella Express II.

Čtvrtá část bude okénkem do budoucnosti, kdy se pokusím nahlédnout pod pokličku vývojářům firmy Microsoft a pokusím se přiblížit budoucnost platformy Microsoft Windows. Nejprve se podívám do blízké budoucnosti v podání Windows XP, následovat bude trochu vzdálenější horizont strategie Microsoft.NET a vzdálené budoucnost projektu Blackcomb, nástroje plného využití strategie Microsoft.NET.

Závěrem nesmí chybět použitá literatura a nezbytný slovníček v podobě vysvětlivek. To, co by se rozsahem nehodilo do diplomové práce, je uvedeno na konci do přílohy.

4. KONCEPCE SYSTÉMU WINDOWS 2000

Microsoft Windows 2000 jsou zcela přepracovanou verzí předchozího operačního systému Microsoft Windows NT 4.0. Oproti předchozí verzi přinášejí velké množství vylepšení a novinek. V první části je popis verzí Microsoft Windows 2000, v té další uvádím výčet novinek a vylepšení a jejich velmi stručný popis, které obsahují Microsoft Windows 2000 oproti starší verzi. Nejsou zde uvedeny ty prvky, které byly součástí Windows NT 4.0. Další informace je možno nalézt na [3].

4.1 VERZE MICROSOFT WINDOWS 2000 A JEJICH ROZDÍLY

Následující tabulka ukazuje jednotlivé verze Microsoft Windows 2000: [18]

Spolehlivý operační systém pro stolní i přenosné počítače používané při obchodování. Systém **Windows 2000 Professional**, který byl navržen s ohledem na potřeby mobilních uživatelů a možnosti využití sítě Internet, pomáhá uživatelům z obchodní oblasti držet krok a neustále pokračovat v činnosti.

Pro pracovní skupiny a malé firmy je nejvhodnější multifunkční síťový operační systém **Windows 2000 Server**, který firmám umožňuje bezpečně a levně obchodovat v síti Internet.

Systém **Windows 2000 Advanced Server** je zvláštní verzí vytvořenou pro elektronické obchodování a obchodní aplikace. Kromě všech funkcí systému Windows 2000 Server zahrnuje navíc funkce týkající se dostupnosti a škálovatelnosti podporující vyšší počet uživatelů a složitější aplikace.

Čtvrtou verzí je systém **Windows Datacenter Server**, který byl do prodeje uveden po vydání platformy Windows 2000. Tento systém zahrnuje veškeré funkce systému Advanced Server a navíc má větší možnosti zpracování a využití paměti, které odpovídají potřebám intenzivního zpracovávání transakcí online a rozsáhlých databází i nárokům velkých poskytovatelů služeb sítě Internet a aplikačních služeb.

Tab. 1, Přehled jednotlivých verzí Windows 2000 a jejich základní charakteristika [3]

Informace o hardwarových požadavcích a možnostech složení do klastru uvádí následující tabulka:

Windows 2000	Windows 2000 Professional	Windows 2000 Server	Windows 2000 Advanced Server	Windows 2000 Datacenter Server
Cílové využití	Pracovní stanice a přenosné počítače určené pro obchod	Soubory, tisk, síť intranet, práce v síti	Obchodní aplikace, elektronický obchod	Rozsáhlé důležité aplikace: zpracování transakcí online, databáze, poskytovatelé aplikačních služeb a služeb sítě Internet
Procesory podporované jedním systémem	2	4	8	32
Podporovaná paměť	4GB	4GB	8GB	64GB
Clustery	Žádné	Žádné	Překlopení mezi dvěma uzly, vyvážení zátěže sítě s 32 uzly	Kaskádové překlopení mezi čtyřmi uzly, vyvážení zátěže sítě s 32 uzly
Minimální požadavky na systém	Procesor kompatibilní s procesorem Pentium o rychlosti 133 MHz, 64 MB paměti RAM, 1 GB místa na disku	Procesor kompatibilní s procesorem Pentium o rychlosti 133 MHz, 128 MB paměti RAM, 1 GB místa na disku	Procesor kompatibilní s procesorem Pentium o rychlosti 133 MHz, 256 MB paměti RAM, 1 GB místa na disku	Procesor kompatibilní s procesorem Pentium o rychlosti 233 MHz, 256 MB paměti RAM, 1 GB místa na disku

Tab. 2, Hardwarové možnosti a nároky jednotlivých verzí Windows 2000 [18]

Tolik tedy obecně o verzích Windows 2000, nyní následuje přehled základních vlastností a novinek, které přišli s Windows 2000 Server [3].

4.2 PODPORA AKTIVIT SPOLEČNOSTÍ V SÍTI INTERNET

Windows 2000 přicházejí s masovou podporou sítě Internet nejen jako součást architektury systému, ale přinášejí velké množství nástrojů pro jejich široké uplatnění v prostředí Internetu:

- **Služba Internet Information Services 5.0 (IIS)**
  Integrované služby pro síť WWW umožňují uživatelům snadno poskytovat hostitelské služby a spravovat servery WWW sloužící ke sdílení informací, vytváření obchodních aplikací založených na síti WWW a rozšíření souborových a tiskových služeb a služeb pro média a komunikaci do sítě WWW.
- **Programovací prostředí Active Server Pages (ASP)**
  Prostředí Active Server Pages je všeobecně hodnoceno jako nejsnáze použitelné a nejvýkonnější dostupné prostředí pro psaní skriptů pro servery WWW.
- **Analyzátor jazyka XML**
  Je možné vytvořit aplikace umožňující serveru WWW výměnu dat ve formátu XML s aplikací Microsoft Internet Explorer i libovolným serverem podporujícím analýzu jazyka XML.
- **Architektura Windows DNA 2000**
  Pomocí architektury *Windows Distributed interNet Applications* (*Windows DNA 2000*), což je model vývoje aplikací pro platformu Windows. Pomocí něj je možné

vytvořit zabezpečená, spolehlivá a škálovatelná řešení usnadňující integraci heterogenních systémů a aplikací.

- **Model COM+ (Component Object Model +)**
  Model COM+ staví na integrovaných službách a funkcích modelu COM a zjednodušuje vytváření a použití softwarových součástí v libovolném jazyce a pomocí libovolného nástroje. Model COM+ zahrnuje služby *Transaction Services* a *Message Queuing* pro spolehlivé distribuované aplikace.
- **Platforma pro multimedia**
  Pomocí integrované služby Windows Media™ Services je možné konfigurovat a spravovat vysoce kvalitní digitální mediální obsah v síti Internet a sítích intranet. Obsah lze živě a na požádání doručit maximálnímu počtu uživatelů.
- **Aplikace podporující službu Active Directory**
  Vývojáři mohou pomocí celé řady standardních rozhraní vytvářet aplikace využívající informace o uživatelích, ostatních aplikacích a zařízeních uložených v adresáři služby Active Directory™. Tím je umožněn vznik jednodušeji vyvinutelných, snadněji spravovatelných, všestranných a dynamických aplikací. Všechny funkce služby Active Directory jsou dostupné prostřednictvím protokolu LDAP a rozhraní ADSI a MAPI a umožňují rozšíření a integraci s jinými aplikacemi, adresáři a zařízeními.
- **Složky sítě WWW**
  Složky sítě WWW přinášejí nové funkce systému Windows pro síť WWW. Pomocí protokolu WebDAV (*Web Distributed Authoring and Versioning*) umožňují publikování v síti WWW jednoduchým přetažením.
- **Tisk v síti Internet**
  Tiskové úlohy lze prostřednictvím sítě Internet odeslat na libovolnou URL adresu.

4.3 VÝKON A ŠKÁLOVATELNOST PODPORUJÍCÍ SÍŤ INTERNET

Windows 2000 přicházejí s velkou podporou víceprocesorových systémů, systémů s velkým množstvím paměti a podporou snížení nákladů na vlastnictví při zvýšení celkového výkonu serveru:

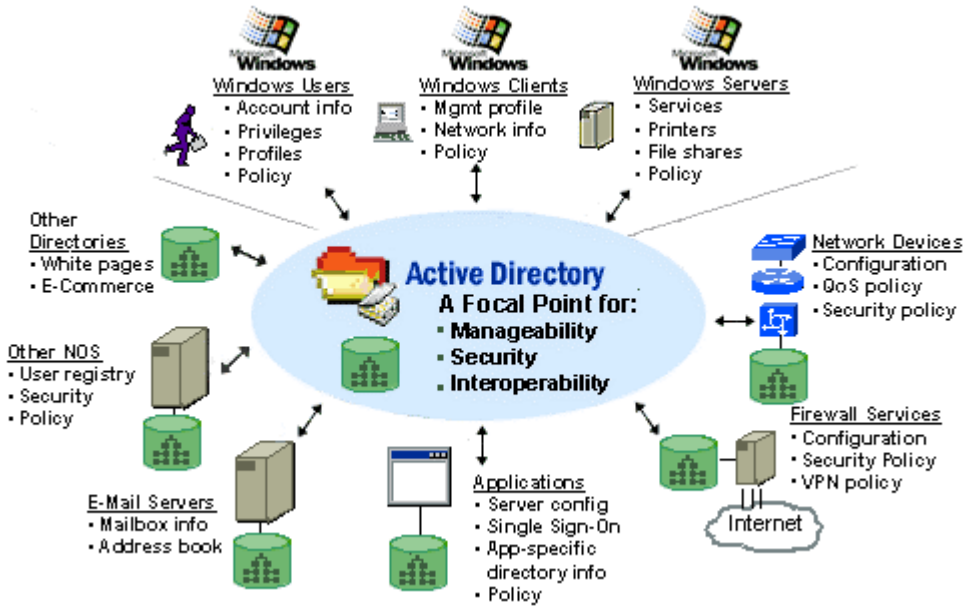
- **Podpora osmi symetrických procesorů**
  Většího výkonu se může dosáhnout škálováním využívajícím nejnovější osmicestné servery podporující symetrické víceprocesorové zpracování. Systém Windows 2000 Server podporuje čtyřcestné servery se symetrickým víceprocesorovým zpracováním.
- **Podpora 8 GB paměti**
  Pomocí větší paměti se může zlepšit výkon a provozovat nejnáročnější aplikace. Podporováno je až 8 gigabajtů (GB) paměti RAM s rozšířením PAE (Physical Address Extension) společnosti Intel. Systém Windows 2000 Server podporuje až 4 GB paměti RAM.
- **Vyrovnávání zatížení sítě**
  Distribucí příchozích přenosů IP mezi několik serverů pro vyrovnávání zatížení sítě je možné rychlé a snadné rozškálování. Přidáváním dalších serverů, na kterých je nainstalována funkce vyrovnávání zatížení sítě, můžete postupně rozšiřovat kapacitu.

- **Služba Terminal Services**
  Software pro emulaci terminálů umožňuje spuštění aplikací pro systém Windows na serveru a přístup ze vzdáleného počítače, terminálu se systémem Windows nebo zařízení nepoužívajícího systém Windows prostřednictvím místních sítí, rozlehlých sítí a připojení s nízkou šířkou pásma. Služba Terminal Services je v systému Windows 2000 až o dvacet procent škálovatelnější a je výrazně zlepšen její výkon u připojení s vysokou i nízkou šířkou pásma.
- **Vyšší výkon prostředí ASP**
  Díky škálovatelnějšímu zpracování stránek ASP (*Active Server Pages*), zlepšenému řízení toku stránek ASP a funkci ASP *Fast Path* pro soubory ASP neobsahující skripty je umožněno rychlejší zpracování stránek WWW.
- **Poskytování hostitelských služeb více virtuálních serverů**
  Služba *Internet Information Services* (IIS) 5.0 umožňuje při zachování vysokého výkonu poskytovat na jednom serveru hostitelské služby více virtuálních serverů WWW.
- **Omezení doby využití procesoru pomocí služby IIS**
  Můžete omezit dobu, po kterou určitá aplikace nebo server WWW využívají procesor, a tím zajistit čas procesoru a lepší výkon i pro ostatní servery WWW a aplikace nepracující v síti WWW.
- **Vysoká propustnost a využití šířky pásma**
  Díky podpoře sítí o rychlosti až 1 Gb poskytuje systém Windows 2000 Server v rychlých sítích výkonné zpracování. Vyšší propustnost umožňuje lepší výkon i bez zvětšení šířky pásma.

4.4 ZABEZPEČENÉ ROZŠÍŘENÍ K ZAMĚSTNANCŮM, PARTNERŮM A ZÁKAZNÍKŮM

Aby mohl operační systém obstát v nebezpečném anonymním prostředí, jakým Internet bezesporu je, přináší systém Windows 2000 širokou podporu nejnovějších způsobů zabezpečení systému, a to nejenom pro síťové prostředí:

- **Podpora nejnovějších standardů zabezpečení**
  Na serverech sítí intranet, extranet a Internet je možné použít nejnovější standardy včetně následujících: 56bitový a 128bitový protokol SSL nebo TLS, protokol IPSec, šifrování SGC (*Server Gated Cryptography*), ověření algoritmem Digest, ověření pomocí protokolu Kerberos v5 a šifrování Fortezza.
- **Integrace služby Active Directory**
  Integrace služby Active Directory a její základní infrastruktury zabezpečení poskytuje centrální umístění pro správu zabezpečení uživatelů, počítačů a zařízení a usnadňuje tak správu systému Windows 2000.



Obr. 1, Využití adresářové služby Active Directory [3]

- **Ověření pomocí protokolu Kerberos**
  Plná podpora protokolu Kerberos verze 5 umožňuje rychlé jednokrokové přihlášení k prostředkům systému Windows i jiných prostředí, která tento protokol podporují.
- **Infrastruktura veřejných klíčů (PKI)**
  Důležitou součástí infrastruktury veřejných klíčů je služba *Certificate Services*, která zákazníkům umožňuje vydávat uživatelům vlastní certifikáty X.509 sloužící pro různé funkce infrastruktury veřejných klíčů, například ověření pomocí certifikátů, protokol IPSec nebo zabezpečenou elektronickou poštu. Díky integraci se službou Active Directory je zjednodušen zápis uživatelů.
- **Podpora karet Smart Card**
  Díky podpoře přihlášení pomocí karet Smart Card je umožněno silné ověřování u citlivých prostředků.
- **Šifrovací systém souborů EFS**
  Zabezpečení dat na pevném disku je možno zvýšit jejich zašifrováním. Data zůstávají zašifrovaná i po zálohování nebo archivaci.
- **Zabezpečená komunikace v sítích**
  Veškerá komunikace v síti společnosti může být zašifrována pomocí protokolu IPSec. Tento protokol je ideální pro ochranu citlivé interní komunikace před úmyslným i náhodným zobrazením neoprávněnými uživateli. Zabezpečení je možné zavést pomocí služby Active Directory, která také poskytuje centrální řízení zásad použití.
- **Služba Routing and Remote Access Service**
  Umožňuje připojení vzdálených uživatelů, uživatelů pracujících doma a poboček k síti společnosti pomocí telefonického připojení, pronajatých linek a sítě Internet.
- **Virtuální privátní sítě (VPN)**
  Sítě VPN jsou plně funkční brány sloužící k šifrování komunikace a zabezpečenému připojení vzdálených uživatelů a poboček prostřednictvím sítě Internet. Tyto sítě nyní podporují aktualizovaný protokol PPTP a rozšířené zabezpečení dosahované šifrováním protokolu Layer 2 Tunneling Protocol protokolem IPSec.

4.5 VYSOKÁ DOBA PROVOZU SYSTÉMU

Pro bezporuchový běh a dlouhou dobu provozu je potřeba i interní bezpečnost systému, kterou Windows 2000 podporují následujícími funkcemi:

- **Ochrana před zápisem v režimu jádra**
  Pomáhá předejít interakci chybného kódu s operacemi systému.
- **Ochrana souborů systému Windows**
  Zabraňuje tomu, aby nově instalovaný software nahradil důležité systémové soubory.
- **Certifikace ovladačů**
  Označuje ovladače zařízení, které byly testovány v laboratořích Windows Hardware Quality Labs, a zobrazí upozornění, pokud chce uživatel nainstalovat necertifikovaný ovladač.
- **Ochrana před aplikacemi pomocí služby IIS**
  Funkce ochrany před aplikacemi spouští aplikace pro síť WWW odděleně od samotného serveru WWW a zabraňuje tím možnosti, že by aplikace způsobily selhání serveru.

4.6 ZVÝŠENÁ DOSTUPNOST SERVERŮ A SÍTÍ

Pokud bude Windows 2000 Server jen tak stát a nebude dostupný okruhu oprávněných uživatelů, nebude k ničemu. Proto přichází s několika službami, které zajistí co nejlepší dostupnost systému:

- **Služba Cluster Service**
  Služba *Cluster Service* se dvěma uzly podporuje překlopení (způsobené selháním hardwaru nebo softwaru) důležitých aplikací včetně databází, aplikací pro správu znalostí, systémů plánování prostředků v rozlehlé síti (ERP) a souborových a tiskových služeb.
- **Vyrovnávání zatížení sítě**
  Ve skupině serverů WWW nebo serverů služby Terminal Services je možné v případě selhání hardwaru nebo softwaru určitého serveru změnit za méně než deset sekund distribuci pracovní zátěže tak, aby funkce převzaly zbývající servery.
- **Rozhraní Job Object API**
  Rozhraní Job Object API a jeho možnosti nastavit spřažení procesorů a časové limity, řídit priority procesů a omezit využití paměti skupinou souvisejících procesů umožňují, aby určitá aplikace spravovala a řídila závislé systémové prostředky. Tato dodatečná úroveň řízení znamená, že rozhraní Job Object API může aplikacím zabránit v negativním ovlivnění celkové škálovatelnosti systému.
- **Certifikace aplikací a ochrana knihoven DLL**
  Aplikace certifikované pro systém Windows 2000 Server prošly testy společnosti Microsoft, které zajišťují jejich vysokou kvalitu a spolehlivost. Knihovny DLL instalované aplikacemi jsou chráněny před konflikty, které by mohly způsobit selhání aplikací.
- **Replikace s více hlavními servery**
  Služba Active Directory pomocí replikace s více hlavními servery zajišťuje vysokou škálovatelnost a dostupnost v konfiguracích distribuovaných sítí. Označení „s více hlavními servery“ znamená, že každá replika adresáře v síti je partnerem všech ostatních replik. Změny mohou být provedeny v kterékoli replice a projeví se i ve všech ostatních.

- **Distribuovaný systém souborů (DFS)**
  Je možno vytvořit jediné hierarchické zobrazení více souborových serverů a jejich sdílených položek v síti. Systém souborů DFS usnadňuje uživatelům vyhledání souborů a zvyšuje dostupnost tím, že uchovává více kopií souborů na distribuovaných serverech.
- **Diskové kvóty**
  U jednotlivých uživatelů a jednotek je možné nastavit kvóty využití místa na disku a dosáhnout tak větší dostupnosti místa na disku a zjednodušit plánování kapacity.
- **Hierarchická správa úložišť**
  Data, která nebyla v poslední době používána, je možné automaticky přenést na levnější paměťová média a maximalizovat tím místo na disku pro nejčastěji používaná data

4.7 DYNAMICKÁ KONFIGURACE SYSTÉMU

U systému s Windows 2000 se předpokládá nepřerušený běh. Nicméně úpravy a nastavení je třeba přeci jen někdy provést a proto jsou zde nástroje a možnosti jejich využití pro dynamické nastavení z správu systému:

- **Podpora inovací se zajištěním provozu**
  Nečinnosti způsobené plánovanou údržbou nebo inovacemi je možno předejít tak, že se využije inovace se zachováním provozu. Tyto inovace používají službu Cluster Service a funkci vyrovnávání zatížení sítě. Převedou se aplikace nebo pracovní zatížení na jeden uzel, inovuje se druhý uzel a potom se převedou aplikace a zatížení zpět. Inovace se zajištěním provozu a bez nutnosti převést aplikace do režimu offline je možné provést u hardwaru, softwaru, a dokonce i operačních systémů. Obě uvedené technologie klastrů systému Windows jsou zpětně kompatibilní se svými předchůdci v systému Windows NT Server 4.0.
- **Dynamická správa jednotek**
  I v době, kdy je server v režimu online, a bez vlivu na koncové uživatele, je možné přidat nové jednotky, rozšířit existující jednotky, přidat zrcadlený svazek, ukončit zrcadlení nebo opravit pole RAID-5.
- **Defragmentace disku**
  Fragmentace může po určité době velmi nepříznivě ovlivnit výkon vytíženého serveru WWW. Nástroje pro defragmentaci disků zvyšují dostupnost a výkon disků.
- **Spuštění v nouzovém režimu**
  Spuštění v nouzovém režimu umožňuje uživatelům během spuštění systému odstranit problémy tím, že změní výchozí nastavení nebo odeberou nově nainstalovaný ovladač, který problém způsobuje.
- **Zálohování a zotavení**
  Funkce zálohování a zotavení usnadňují zálohování a obnovení dat v případě selhání pevného disku. Systém Windows 2000 umožňuje provést zálohování do jednoho souboru na pevném disku nebo páskovém médiu.
- **Automatické restartování**
  Všechny služby operačního systému včetně služby IIS lze nastavit tak, aby byly v případě selhání automaticky znovu spuštěny.
- **Ukončení stromu procesů**
  Bez nutnosti restartovat systém je možné ukončit všechny procesy související s procesem nebo aplikací, u nichž došlo k chybě.

4.8 SNADNÉ ZAVEDENÍ, KONFIGURACE A POUŽITÍ

Instalace operačního systému a nastavení jednotlivých komponent není nikterak zábavná činnost, navíc je časově náročná a pokud se jedná o stanice, tak i donekonečna se opakující. Proto Windows nabízejí několik technologií a nástrojů, jak tyto činnosti provést:

- **Nastavení služby Cluster Service**
  Cluster lze rychle nakonfigurovat pomocí vylepšeného a zjednodušeného průvodce instalací služby Cluster Service. Díky tomu, že službu Cluster Service podporuje program SysPrep, je možné provést vzdálenou instalaci.
- **Integrovaná konfigurace funkce vyrovnávání zatížení sítě**
  Funkce vyrovnávání zatížení sítě je nyní integrovanou součástí síťových funkcí systému Windows 2000 Advanced Server. Umožňuje rychlou konfiguraci bez nutnosti samostatné instalace či restartování systému.
- **Průvodce konfigurací**
  Pomocí průvodce Konfigurace serveru je možno nainstalovat a nastavit souborové, tiskové, síťové a komunikační služby, služby pro síť WWW a služby Active Directory a DNS.
- **Nástroj pro přípravu systému (SysPrep)**
  Při zavádění je možné ušetřit čas tím, že pomocí programu SysPrep se vytvoří bitová kopie pevného disku určitého počítače (včetně operačního systému a aplikací) a tu je potom možno duplikovat do dalších počítačů.
- **Služba Windows Installer**
  Služba Windows Installer sleduje instalace aplikací a bezchybně provádí odinstalování či odebrání.
- **Technologie Plug and Play**
  Tato technologie automaticky rozpozná nově nainstalované součásti a zjednodušuje tak konfiguraci síťového systému a snižuje dobu nečinnosti.
- **Integrace aktualizací Service Pack do operačního systému**
  Aktualizace operačního systému je možné zjednodušit tím, že v síti je uložena jedna hlavní bitová kopie operačního systému.
- **Standard Dynamic DNS**
  Služba DNS (*Domain Name System*) integrovaná se službou Active Directory a založená na standardech sítě Internet zjednodušuje pojmenování a vyhledání objektů pomocí protokolů sítě Internet a zvyšuje škálovatelnost, výkon a možnosti spolupráce. Systémy, které získají adresu ze serveru DHCP (*Dynamic Host Configuration Protocol*), jsou automaticky registrovány službou DNS. Možnosti replikace se staršími systémy DNS a prostřednictvím služby Active Directory mohou zjednodušit a posílit infrastrukturu replikace názvů.
- **Sada Microsoft Connection Manager Administration Kit a služba Connection Point Services**
  Tyto nástroje a jejich průvodci umožňují správcům centrálně konfigurovat a zavádět upravená vytáčení vzdáleného přístupu, která mohou integrovat automaticky aktualizované telefonní seznamy, vlastní akce připojení (například ověření pomocí serveru firewall a antivirovou kontrolu), aktualizace ovladačů a další možnosti.
- **Sdílení připojení k Internetu**
  Umožňuje více uživatelům v malé firmě nebo pracovní skupině sdílet jediné externí připojení k Internetu, čímž zároveň připojení k Internetu usnadňuje.

- **Vyhledání tiskáren a připojení k nim z plochy**
  Publikováním tiskáren v adresáři služby Active Directory je umožněno uživatelům vyhledat tiskárny a připojit se k nim a použít přitom taková kritéria, jako jsou například umístění, možnost barevného tisku nebo rychlost.

4.9 CENTRALIZOVANÁ SPRÁVA SNIŽUJÍCÍ CELKOVÉ NÁKLADY NA VLASTNICTVÍ

Pokud má administrátor na starosti několik málo serverů, je jejich správa při dobré konfiguraci celkem nenáročnou prací. Pokud je ovšem serverů velké množství, navíc fyzicky vzdálených, nabízejících různé služby, bez pomocných nástrojů implementovaných přímo do Windows 2000 se neobejde:

- **Cluster Administrator (Správce klastru)**
  Spuštěním aplikace *Cluster Administrator* z libovolného systému Windows NT nebo Windows 2000 je možné vzdáleně řídit více klastrů z jednoho umístění.
- **Integrované adresářové služby**
  Systém Windows 2000 zahrnuje službu Active Directory, což je škálovatelná, standardům vyhovující adresářová služba, která usnadňuje správu systému Windows 2000, zvyšuje jeho zabezpečení a rozšiřuje možnosti spolupráce s existujícími prostředími. Služba Active Directory prostřednictvím jediného konzistentního rozhraní pro správu centrálně spravuje klienty a servery používající systém Windows a snižuje tím počet redundantních akcí a náklady na údržbu.
- **Služba WMI (Windows Management Instrumentation)**
  Služba WMI poskytuje konzistentní model, jehož pomocí mohou být standardním způsobem spravována data z libovolného zdroje. Samotná služba WMI poskytuje tuto možnost pro software, například aplikace, zatímco její rozšíření pro model WDM (*Windows Driver Model*) poskytují tyto funkce pro hardware a ovladače hardwarových zařízení. Služba WMI v systému Windows 2000 poskytuje vyšší počet funkcí pro správu.
- **Delegovaná správa**
  Služba Active Directory umožňuje správcům delegovat sadu vybraných oprávnění ke správě důvěryhodným jednotlivcům v rámci organizace a distribuovat tak správu i zvýšit její přesnost. Delegování rovněž pomáhá snížit počet domén nutných k podpoře velkých organizací s více pobočkami v různých místech.
- **Konzole MMC (Microsoft Management Console)**
  Tato centrální, upravitelná konzola umožňuje řídit, sledovat a spravovat síťové prostředky a sjednocuje a zjednodušuje tak úlohy v rámci správy systémů. Prostřednictvím konzoly MMC jsou v systému Windows 2000 k dispozici všechny funkce pro správu.
- **Vzdálená správa pomocí služby Terminal Services**
  Službu Terminal Services lze bezpečně použít ke vzdálené správě. Jsou podporovány až dvě současné relace, aniž by jimi byl ovlivněn výkon nebo kompatibilita aplikací.
- **Modul Windows Script Host (WSH)**
  Umožňuje spravovat server a automatizovat úlohy prostřednictvím příkazového řádku a skriptů (namísto nástrojů grafického uživatelského rozhraní).

- **Zásady skupiny**
  Zásady skupiny umožňují centrální správu skupin uživatelů, aplikací a zdrojových prostředků (namísto samostatné správy jednotlivých entit). Integrace se službou Active Directory umožňuje podrobnější a pružnější řízení.
- **Centralizovaná správa počítačů**
  Počítače uživatelů lze spravovat použitím zásad založených na pracovních potřebách a pozici uživatele. Technologie správy IntelliMirror™ pomáhá instalovat a spravovat software, použít správné nastavení počítače a uživatelské nastavení a zajistit, aby byla vždy k dispozici uživatelská data.
- **Sada nástrojů pro konfiguraci zabezpečení**
  Snižuje náklady spojené s konfigurací a analýzou zabezpečení v sítích založených na systému Windows. Pomocí zásad skupiny lze v systému Windows 2000 nastavit a pravidelně aktualizovat konfiguraci zabezpečení počítačů.
- **Správa zásad skupiny infrastruktury veřejných klíčů**
  Je možné centrálně spravovat zásady infrastruktury veřejných klíčů platné pro celou doménu. Je možné zadat, které certifikační úřady bude klient považovat za důvěryhodné, distribuovat nové kořenové certifikáty, upravit zásady protokolu IPSec nebo určit, zda bude při přihlášení uživatele k určitému systému vyžadováno použití karty Smart Card.
- **Nástroje pro přenesení domén systému Windows NT 4.0**
  Zjednodušují proces inovace na domény systému Windows 2000
- **Možnost spolupráce adresářů**
  Technologie metaadresářů umožňují společnostem pomocí služby Active Directory spravovat identifikační informace uložené v heterogenních adresářových službách.
- **Nástroje pro synchronizaci adresářů**
  Umožňují spravovat a synchronizovat data mezi adresáři služby Active Directory, serveru Microsoft Exchange a služby Novell NDS.

4.10 PLNÉ VYUŽITÍ EXISTUJÍCÍCH INVESTIC DO TECHNOLOGIÍ IT

Je nutné předpokládat, že Windows 2000 přijdou do podniku s již existující a fungující IT infrastrukturou a stávajícím HW. Windows 2000 přinášejí nástroje a vlastnosti pro začlenění a plné využití tohoto potenciálu:

- **Velké možnosti spolupráce s klientskými počítači**
  Podporuje operační systémy Windows NT Workstation, Windows 9x, Windows 3.x, Macintosh a Unix. Podpora klientů AppleShare prostřednictvím protokolu TCP/IP vylepšuje sdílení prostředků s operačními systémy Macintosh.
- **Spolupráce aplikací a adresářů**
  Do operačního systému Windows 2000 Server lze nainstalovat nebo inovovat aplikace kompatibilní s tímto systémem. Služba Active Directory může spolupracovat nebo synchronizovat data s ostatními adresářovými službami pomocí protokolu LDAP (*Lightweight Directory Access Protocol*), technologií metaadresářů, nástrojů pro synchronizaci adresářových služeb společnosti Microsoft nebo připojovací aplikace služby Active Directory k serveru Exchange. Je možná integrace s existujícími aplikacemi pro správu a poskytnutí jednotného prostředí prostřednictvím služeb správy systému Windows.

- **Spolupráce serverů a sálových počítačů**
  Služba Message Queuing umožňuje výměnu informací mezi aplikacemi spouštěnými v sálových počítačích. Podpora ověřovacího protokolu Kerberos umožňuje spolupráci s dalšími systémy používajícími tento standardní ověřovací protokol. Doplňkové služby pro systém NetWare zvyšují možnosti spolupráce mezi servery a klienty NetWare a servery a klienty Windows. Doplňkové služby pro systém Unix usnadňují integraci systémů Windows NT 4.0 a Windows 2000 s prostředím UNIX.
- **Nejnovější serverový hardware**
  Podporuje nejmodernější osmicestné servery se symetrickým víceprocesorovým zpracováním používající sadu čipů a architekturu Profusion společnosti Intel a až 8 GB paměti s rozšířením PAE (*Physical Address Extension*) společnosti Intel.
- **Sítě**
  Systém Windows 2000 Server pracuje se síťovými zařízeními podporujícími nejnovější síťové technologie, včetně technologie Plug and Play, linek DSL, sítí VPN, směrování, překladu síťových adres, protokolu DHCP, technologie Quality of Services, přepínačů a směrovačů, síťových zařízení podporujících službu Active Directory, protokolu IPSec, protokolu SSL a asynchronního režimu přenosu.
- **Periferní zařízení**
  Systém Windows 2000 Server pracuje s nejnovějšími periferními zařízeními, například s hardwarem pro správu úložišť, tiskárnami USB, síťovými adaptéry, klávesnicemi a myšmi. Poskytuje rozšířenou podporu ovladačů tiskáren i podporu zařízení 1394, PCMCIA, zařízení pro infračervený přenos a digitálních zařízení.

5. ARCHITEKTURA OPERAČNÍHO SYSTÉMU

Windows 2000 je vícevláknový (*multithreading*) a víceúlohový (*multitasking*) operační systém schopný práce na systémech s více procesory (*multiprocessing*). Navíc se jedná o víceuživatelský operační systém (*multiuser*).

Windows 2000 je objektový operační systém založený na technologii COM respektive DCOM objektů. Nejedná se však o čistě objektový systém ve smyslu „živého" systému (jako např. Smalltalk), ale o objekty zkompilované do podoby binárního kódu. Objektový v tom smyslu, že je jako celek složen z nezávislých částí, které mají vlastní strukturu (atributy) a pro komunikaci používají zasílání zpráv.

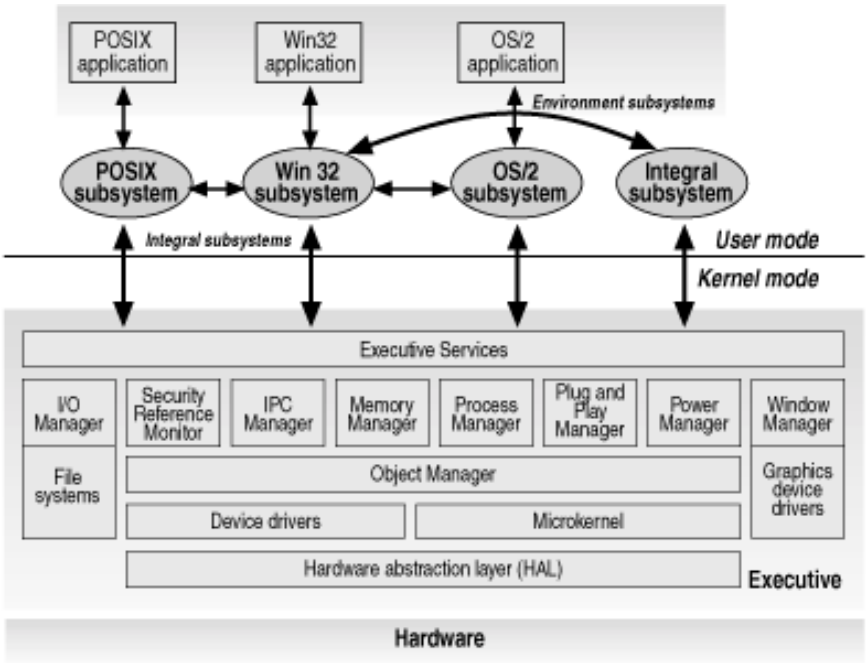
Aplikace používají části OS ve formě sdílených dynamických knihoven DLL, dále ve formě ActiveX komponent a již zmíněných COM / DCOM komponent. Objektem je tedy ve Windows 2000 vše, počínaje částmi ovladači zařízení a konče tlačítkem na okně.

A nyní bude následovat pohled na architekturu Windows 2000 podrobněji. Nejprve rozdělením architektury na vrstvy a jejich podrobným popisem. Další informace lze nalézt na [4].

5.1 ZÁKLADY ARCHITEKTURY WINDOWS 2000

Architekturu Windows 2000 lze uvést citátem: „*Operační systém, to je něco jako socialistická ekonomika: samé plánování a samá fronta*" [Roderik Plevka]. Architektura Windows 2000 je založena na dvou typech technologií - na technologii vzájemně komunikujících vrstvách a na technologii klient-server.

Operační systém Windows 2000, tak jako Windows NT, je složen z jednotlivých vrstev, které mezi s sebou vzájemně komunikují. Každá vrstva má na starosti určitou část operačního systému, která se skládá z jednotlivých subsystémů, které spolu komunikují na bázi technologie klient-server.



Obr. 2, Schéma architektury Windows 2000 [4]

Výše uvedený obrázek 2 zobrazuje architekturu Windows 2000. Základ je tvořen dvěmi hlavními vrstvami – *User mode* a *Kernel mode*. Dále se budu zabývat popisem vyšší vrstvy - *User Mode* .

5.1.1 VRSTVA USER MODE

Windows 2000 mají ve vrstvě *User mode* dva typy komponent: *environment subsystems* a *integral subsystems*.

5.1.1.1 ENVIRONMENT SUBSYSTEMS

Jednou z vlastností Windows 2000 je schopnost spouštět aplikace napsané pro jiný operační systém. Této schopnosti Windows 2000 docílí za pomoci *Environment subsystems* (subsystémy prostředí). *Environment subsystems* emulují odlišný operační systém pomocí prezentace aplikačního programovacího rozhraní (API – *Application Programming Interface*), které daná aplikace požaduje pro svoji činnost. *Environment subsystems* akceptují volání API vytvořené danou aplikací, překládají je do formátu API, kterému rozumí Windows 2000, a posílá přeložené API volání do *Executive services* ke zpracování.

Následující tabulka obsahuje seznam jednotlivých aplikačních subsystémů:

Environment subsytem	**Funkce**
Windows 2000 32-bit Windows - based subsytem (Win32)	Odpovědný za chod Win32 aplikací, dále poskytuje prostředí pro chod Win16 a DOS aplikací
	Řídí všechny zobrazovací vstupy a výstupy mezi jednotlivými subsystémy. Zajišťuje konzistenci uživatelského rozhraní.
OS/2 subsystem	Poskytuje API rozhraní pro 16 bitové znakově orientované aplikace
POSIX subsystem	Poskytuje API rozhraní pro aplikace POSIX

Tab. 3, Seznam jednotlivých aplikačních subsystémů [4]

Výše uvedené subsystémy a aplikace, které v nich běží, mají určité restrikce a limity pro svůj běh:

- nemají přímý přístup k hardware
- nemají přímý přístup k hardwarovým ovladačům
- mají omezenou možnost adresování paměti
- jsou přinuceny odložit obsah paměti RAM na disk, jestliže systém potřebuje paměť
- běží na nižší prioritě než procesy v *Kernel mode*, což zapřičiňuje to, že mají procesy v subsystémech menší frekvenci přístupu k procesoru (CPU), než procesy v *Kernel mode*.

5.1.1.2 INTEGRAL SUBSYSTEMS

Většina odlišných integrálních subsystémů provádí základní funkce operačního systému. Na výše uvedeném obrázku 2 se jedná o systém, který je zcela vpravo s názvem *Integral subsystems*. *Integral subsystems* představují mnoho různých subsystémů, kde některé z nich obsahuje následující tabulka:

Integral subsystem	Funkce
Security subsystem	Sleduje práva a povolení přiřazené uživatelským účtům
	Sleduje, které systémové zdroje jsou auditovány
	Přijímá požadavek uživatele na přihlášení do systému
	Zahajuje prokázání identity přihlášení
Workstation service	Síťový integrální subsystém, který poskytuje API pro přístup na síťový redirektor. Umožňuje uživateli Windows 2000 přistupovat k síťovým službám
Server service	Síťový integrální subsystém, který poskytuje API pro přístup na síťový server. Umožňuje počítači s Windows 2000 poskytovat síťové služby.

Tab. 4, Seznam jednotlivých integrálních subsystémů [4]

5.1.2 VRSTVA KERNEL MODE

Kernel mode má přístup k systémovým datům a k hardware a poskytuje přímý přístup do paměti a běh procesů v izolovaných paměťových oblastech. *Kernel mode* se skládá ze čtyř základních částí.

Windows 2000 Executive

Tato komponenta provádí většinu vstupů a výstupů (I/O) a správu objektů včetně bezpečnosti. Neprovádí I/O operace pro obrazovku a klávesnici, tyto funkce provádí *Microsoft Win32 subsystem*. *Windows 2000 Executive* obsahuje komponenty, které poskytují následující odlišné služby a postupy:

- **system services** – tyto služby jsou dostupné jak uživatelskému módu, tak ostatním komponentám *Windows 2000 Executive*
- **internal routines** – tyto služby jsou dostupné pouze komponentám *Windows 2000 Executive*

Komponenty *Windows 2000 Executive* jsou uvedeny v následující tabulce:

Komponenta	Funkce
I/O Manager	Řídí vstup a poskytuje výstup pro různá zařízení. I/O manager se skládá z následujících komponent:
	File systems: přijímá I/O požadavky a tyto požadavky překládá na specifická volání zařízení
	Device drivers: ovladače na nejnižší vrstvě, které přímo manipulují s hardware za účelem přijmutí vstupu a zápisu výstupu
	Cache manager: zvyšuje rychlost I/O diskových operací tím, že si čtení z disku ukládá do paměti. Dále zvyšuje rychlost zápisu tím, že si ukládá požadavky na zápis do paměti a vlastní zápis pak provádí na pozadí
Security reference monitor	Prosazuje bezpečnostní politiku na lokálním počítači
Interprocess Communication clients and (IPC) Manager	Řídí komunikaci mezi servery, např. mezi *environment subsystem* (jako klient, který požaduje informace) a *executive services* (jako server, který poskytuje informace). IPC manager se skládá z následujících dvou komponent:
	Local Procedure Call (LPC): řídí komunikaci mezi klientem a serverem, pokud oba dva existují na jednom počítači
	Remote Procedure Call (RPC): řídí komunikaci mezi klientem

	a serverem, pokud oba dva existují na různém počítači
Virtual Memory Manager	Realizuje a řídí virtuální paměť, správu paměťového systému, který poskytuje privátní adresní prostor pro každý proces a chrání adresový prostor před všemi procesy. VMM dále řídí stránkování na žádost. Stránkování na žádost umožňuje využít diskový prostor pro odložení procesů a dat z fyzické paměti RAM na disk a zpět
Process Manager	Vytváří a ukončuje procesy a vlákna (*proces* je program nebo část programu, *vlákno* je specifická skupina příkazů uvnitř programu). Dále umožňuje pozastavení a znovuspuštění vláken a ukládání a získávání informací o procesech a vláknech
Plug and Play Manager	Udržuje centrální řízení Plug and Play procesů, komunikuje s ovladači zařízení, přímo řídí ovladače za účelem jejich přidání a spuštění
Power Manager	Řídí power management API, koordinuje události týkající se napájení a generuje žádosti týkající se napájení
Window Manager and Graphical Device Interface (GDI)	Tyto dvě komponenty, implementovány jako jeden ovladač zařízení (Win32k.sys), řídí systém zobrazení. Poskytují následující funkce:
	Window Manager: spravuje zobrazení oken a řídí výstup na obrazovku. Tato komponenta je také zodpovědná za příjem vstupu z klávesnice a myši a za poslání těchto vstupů aplikaci, která je přijme
	GDI: obsahuje funkce, které jsou zodpovědné za kreslení a za manipulaci s grafikou
Object Manager	Vytváří, řídí a maže objekty, které představují zdroje operačního systému jako jsou procesy, vlákna a datové struktury

Tab. 5, Komponenty vrstvy Windows 2000 executive [4]

Device Drivers

Překládá volání ovladače zařízení na obsluhu hardware zařízení.

Microkernel

Tato komponenta řídí pouze mikroprocesor. *Kernel* koordinuje všechny I/O funkce a synchronizuje aktivity *Executive Services*.

Hardware Abstraction Layer

Tato komponenta virtualizuje, resp. schovává detaily o hardware zařízeních, vytváří tak Windows 2000 přenositelné mezi více druhy hardwarových architektur. Vrstva *Hardware Abstraction Layer* (HAL) obsahuje kód pro specifický druh hardware, který řídí I/O operace, přerušení zařízení a komunikaci mezi více procesory. Tato vrstva tak umožňuje běh Windows 2000 jak na platformě Intel, tak na platformě Alpha, pouze výměnou vrstvy HAL bez potřeby měnit celou vrstvu *Windows 2000 Executive*.

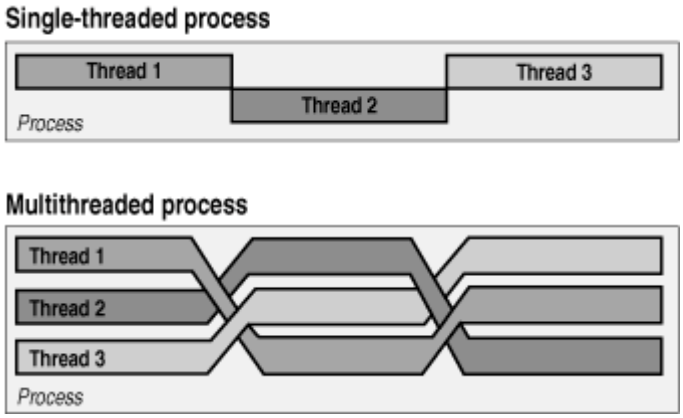
Tím jsme se seznámili se základním schématem architektury Windows 2000 a nyní bude následovat kapitola o tom, jak systém vytváří a spravuje procesy a vlákna.

5.2 WINDOWS 2000 PROCESSING

Windows 2000 je vicevláknový a víceúlohový operační systém, který je schopen pracovat i na systémech s více procesory. V dalším textu budu používat raději anglické názvy tj. *multithreading* a *multitasking*, které jsou odborné veřejnosti více známé a běžně používané.

5.2.1 MULTITHREADING

Jestliže jeden proces dokáže provozovat více než jedno vlákno, nazýváme tuto vlastnost *multithreading*. Jako příklad je možné uvést práci aplikace Word, kdy jedno vlákno provádí vstup z klávesnice, druhé kontrolu pravopisu a třetí zarovnání textu. V případě jednovláknového procesu (*singlethreading*) se tyto vlákna provedou postupně za sebou, ve vícevláknovém procesu probíhají paralelně vedle sebe. Situaci popisuje následující obrázek 3.



Obr. 3, Rozdíl mezi jednovláknovým a vícevláknovým procesem [4]

Proces obsahuje spustitelný program, který provádí sekvenci jednotlivých spojitých kroků. *Program* obsahuje následující části:

- počáteční kód a data
- privátní adresový prostor
- systémové zdroje jako jsou soubory, komunikační porty a zdroje Windows
- jedno nebo více vláken

Vlákno je aktuální komponenta procesu, která je prováděna v daný čas. Proces musí obsahovat minimálně jedno vlákno ještě před tím, než začne cokoliv provádět. Všechna vlákna běží ve stejném adresovém prostoru alokovaném pro daný proces a mohou používat všechny systémové zdroje přiřazené tomuto procesu. Vlákno obsahuje následující části:

- jedinečný identifikátor přiřazený systémem, který se nazývá *client ID*
- obsah registrů, které reprezentují stav mikroprocesoru
- jeden zásobník (*stack*) pro běh v *User mode* a jeden zásobník pro běh v *Kernel mode* (*stack* je část rezervované paměti, kde si program ukládá stavová data)
- odkládací prostor pro subsystémy, dynamické knihovny (DLL) a run-time knihovny

5.2.2 MULTITASKING

Programátoři mohou psát aplikace, které obsahují více než jedno vlákno výkonného programu. Pokud proces obsahuje více jak jedno vlákno, může proces vykonat více úloh (*task*) najednou. Jedná se o proces, který se nazývá víceúlohový (*multitasked*).

Jestliže mikroprocesor může vykonávat najednou pouze jednu úlohu, víceúlohový operační systém může spouštět více úloh najednou. Aby Windows 2000 tuto vlastnost zabezpečily tak, aby byla pro uživatele zcela transparentní, používají *context switching*, které pracuje následujícím způsobem:

1. vlákno pracuje tak dlouho, dokud není přerušeno operačním systémem nebo pokud musí čekat na zdroj
2. systém uloží kontext vlákna
3. systém nahraje kontext jiného vlákna a spustí jej

Tento proces se opakuje tak dlouho, dokud existují vlákna čekající na provedení.

5.2.3 PREEMPTIVNÍ MULTITASKING[1]

V preemptivním multitaskingu kontroluje operační systém přístup k mikroprocesoru. Operační systém přeruší běh vlákna jedním z následujících dvou důvodů:

- vlákno běží již po dobu (*quantum*), která mu byla přidělena a na konci tohoto přiděleného času operační systém přeruší práci vlákna a umožní dalšímu vláknu využívat mikroprocesor
- jestliže existuje jiné vlákno s vyšší prioritou připravené ke spuštění, operační systém přeruší běh právě běžícího vlákna a umožní běh vlákna s vyšší prioritou

Řízení spouštění a běhu vláken řídí *kernel* Windows 2000.

5.2.4 PRIORITY PROCESŮ A VLÁKEN

Kernel Windows 2000 řídí přístup na mikroprocesor pomocí použití tzv. *priority levels*. Existuje 32 úrovní (*levels*) číslovaných od 0 do 31, které jsou rozděleny do následujících skupin:

- úroveň 0-15 je pro komponenty pracující v *User mode*
- úroveň 16-32 je pro komponenty pracující v *Kernel mode*

Kernel Windows 2000 přiřazuje automaticky každému procesu úroveň označovanou jako *base priority level*. Tuto prioritu přiřazuje i vláknům uvnitř procesu. Základní prioritou (*base level*) pro procesy je tzv. *single level*, např. 4. Základní prioritou pro vlákna je hodnota +/- 2 od *single level*, v našem případě tak mohou mít vlákna prioritu od 2 do 6.

Vlákna mají ještě další prioritu, která se jmenuje *dynamic priority level*. Na začátku má hodnotu rovnou hodnotě *base level* a na základě aktivity vlákna ji může OS dynamicky měnit směrem nahoru. Tato dynamika přiřazování je vysoce efektivním nástrojem k využití mikroprocesoru. Jako příklad lze uvést přepočítání tabulky v programu Microsoft Excel, kdy je priorita zvýšena pro zrychlení této operace a poté je opět snížena na *base level*.

[1] Kromě preemptivního multitaskingu existuje také kooperativní multitasking, který se používal ve Windows 3.x. Jeho princip spočíval v tom, že přístup k mikroprocesoru neřídil operační systém, ale každá aplikace musela uvolňovat čas pro ostatní aplikace. Pokud došlo k zacyklení běhu aplikace, neuvolnila procesor pro ostatní a došlo tak ke zhroucení operačního systému.

5.2.5 MULTIPROCESSING

Multiprocessing znamená, že operační systém dokáže využít výkon dvou a více mikroprocesorů. Existují dva typy multiprocesorových systémů: asymetrický a symetrický.

Asymetrický multiprocessing – operační systém přiřazuje procesy ke konkrétnímu mikroprocesoru. Proces po spuštění běží na přiděleném mikroprocesoru bez ohledu na aktivity ostatních mikroprocesorů. Asymetrický *multiprocessing* je značně neefektivní, protože při nevytíženosti ostatních mikroprocesorů nelze práci na ně rozdělit a pomoci tak v dokončení procesu.

Symetrický multiprocessing – Windows 2000 podporují tento typ multiprocesingu. operační systém provozuje jak systémové procesy, tak aplikační procesy na všech mikroprocesorech. Windows 2000 navíc kombinují SMP s multitaskingem. *Kernel* Windows 2000 tak dokáže rozdělit čekající vlákna všech procesů mezi všechny mikroprocesory a zrychlit tak jejich provádění.

Další kapitola je věnována tomu, jak Windows 2000 spravují a zajišťují práci s pamětí.

5.3 WINDOWS 2000 MEMORY MODEL

Paměťový model Windows 2000 je založen na plochém lineárním 32 bitovém adresovém prostoru (*32 bit flat linear memory model*). Pro správu paměti Windows 2000 používají *virtual memory management* (VMM). Tento systém poskytuje několik výhod:

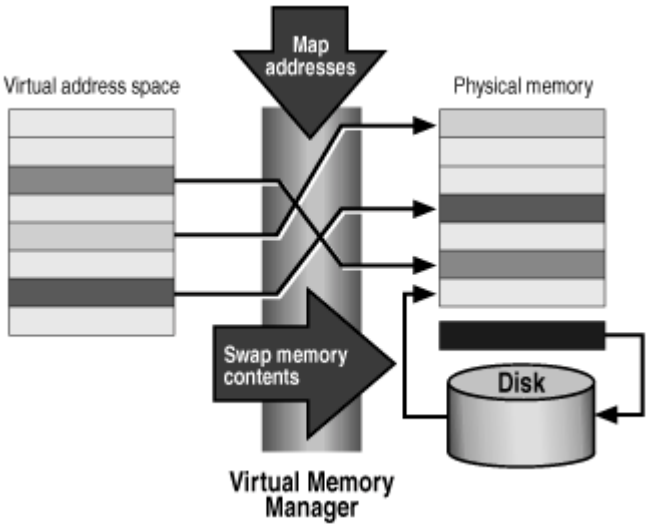
- spustit mnohem více aplikací současně, než kolik umožňuje fyzická paměť počítače
- ochranu paměťových zdrojů. VMM zabrání procesům vzájemně si zasahovat do cizího adresového prostoru

Fyzická paměť odkazuje na fyzickou RAM umístěnou v počítači. *Virtuální paměť* je cesta, kterou operační systém připravuje fyzickou paměť dostupnou pro aplikace.

Windows 2000 reprezentují každý bajt paměti jak fyzické tak virtuální s unikátní adresou. Množství fyzické paměti limituje počet fyzických adres, které jsou k dispozici. Počet virtuálních adres je limitován pouze velikostí virtuálního adresového prostoru. Windows 2000 obsahují 32 bitové adresové schéma, mají tak k dispozici 4 GB virtuálního adresového prostoru.

Virtual Memory Manager spravuje paměť a má dvě specifické role:

- udržuje tabulku *memory-mapping*. Tato tabulka udržuje seznam virtuálních adres, které náleží každému procesu a kde data odkazovaná těmito adresami leží (viz obr. 4). Jakmile vlákno požaduje přístup do paměti, požaduje přístup na virtuální adresu. VMM převede požadavek virtuální adresy na fyzickou adresu a poskytne data na této adrese vláknu
- přesouvá obsah paměti na disk a zpět, když jsou data požadována. Tomuto procesu se říká *paging*

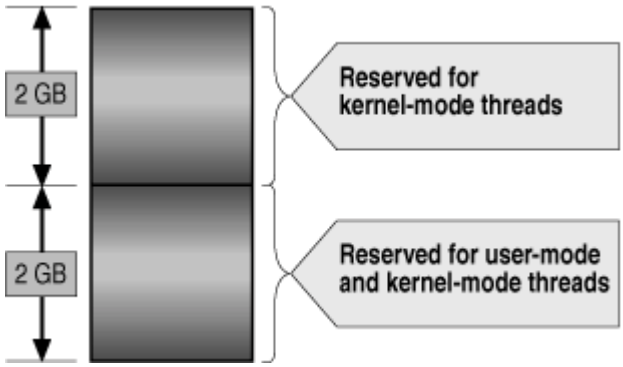


Obr. 4, Virtuální paměť a její vztah k fyzické paměti [4]

5.3.1 VIRTUÁLNÍ ADRESOVÝ PROSTOR

Virtuální adresa je adresa, kterou používá aplikace jako odkaz na paměť. Spuštěný proces dostane od Windows 2000 4 GB virtuálního adresového prostoru. Tento prostor je rozdělen na dvě části, jak ukazuje obr. 5:

- horní 2 GB jsou rezervovány pro vlákna *Kernel mode*. Spodní část je přímo mapována hardwarem, přístup do této části je extrémně rychlý
- spodní 2 GB jsou dostupné vláknům jak *Kernel mode* tak *User mode*. VMM je může kdykoliv odložit na disk, je-li to potřeba. Windows 2000 rozdělují horní část na *paged* a *non-paged* blok. Adresy v *paged* bloku mohou být odloženy na disk, v *non-paged* bloku musí zůstat ve fyzické paměti. Velikost každé stránky je 4 KB.

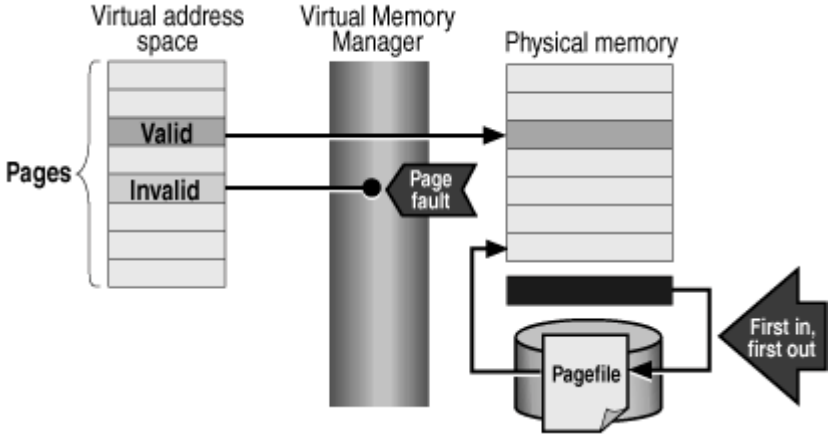


Obr. 5, Rozdělení virtuálního adresového prostoru [4]

5.3.2 PAGING

Přesouvání dat z a do fyzické paměti se nazývá *paging*. Jestliže se začíná fyzická paměť zaplňovat a vlákno potřebuje přístup ke kódu a k datům, která nejsou ve fyzické paměti, VMM přesune některé stránky z fyzické paměti do odkládacího souboru na

disk, který se jmenuje *pagefile*. (viz obr. 6). VMM nahraje kód a data požadovaná vláknem do paměti, kterou VMM předtím uvolnil.



Obr. 6, Řešení odkládacího prostoru při nedostatku fyzické paměti [4]

Virtuální adresní prostor přidělený procesu je rozdělen buď na *valid pages* nebo na *invalid pages*. *Valid pages* jsou stránky, které jsou umístěny do fyzické paměti a jsou přístupné procesu. *Invalid pages* jsou stránky, které nejsou ve fyzické paměti. Nejsou dostupné procesu a jsou odloženy na disk. Jakmile proces vyžaduje přístup na *invalid page*, mikroprocesor vygeneruje signál *page fault*. VMM provede přerušení, nalezne příslušnou stránku na disku a nahraje ji do paměti. Pro uvolnění paměti pak VMM vezme obsah určitých stránek a odloží je na disk. VMM vykonává tři úlohy jako část *paging* procesu:

- určuje, které stránky odstraní z fyzické paměti, když je paměť plná. VMM udržuje seznam stránek, které jsou v paměti pro každý proces. Skupina těchto stránek je uvedena jako *process working set*. VMM používá metodu FIFO jako politiku určování, které stránky odloží na disk. Data, která byla v paměti dlouhou dobu, odloží jako první. Když vlákno způsobí *page fault*, VMM prozkoumá *working set* procesu vlákna a přesune na disk stránky, které byly v paměti příliš dlouho.
- nahrává stránky z disku zpět do paměti, tomuto procesu se říká *fetching*. VMM používá metodu nazvanou *demand paging with clustering*. Znamená to, že když je spuštěn *page fault*, VMM nahraje požadovanou stránku do paměti plus další stránky, které s ní sousedí. Pomáhá tak redukovat počet vygenerovaných *page faults*.
- určuje, kam umístit stránky nahrané z disku. Jestliže fyzická paměť není plná, VMM nahraje data do první volné stránky. Jestliže je fyzická paměť plná, VMM vyhledá stránky, které je možno odložit na disk, aby tak uvolnily místo pro stránky, nahrávané z disku.

5.4 WINDOWS 2000 FILE SYSTEM

Souborový systém Windows 2000 NTFS (*New Technology File System*) byl původně navržen pro Windows NT. Windows 2000 také podporují HPFS (navržený pro OS/2) a FAT (navržený pro DOS), ale tyto souborové systémy mají omezené možnosti a nesplňují podmínky kladené dnešními potřebami. Těmito nedostatky jsou zejména

omezená velikost disku a bezpečnost. Rovněž FAT32 podporovaný Windows 2000 tyto požadavky nesplňuje.

Vývojáři FAT a HPFS nevěnovali pozornost bezpečnosti, ale NTFS je postavena na bezpečnosti a Windows 2000 používají stejný bezpečnostní model jako NT. Seznamy řízení libovolného přístupu (***D**iscretionary **A**ccess **C**ontrol **L**ists* – DACL) a seznamy řízení systémového přístupu (***S**ystem **A**ccess **C**ontrol **L**ists* – SACL) řídí, kdo vykoná akci se souborem a zajistí její zaznamenání.

FAT nemá žádné opatření proti chybám na disku. Při pádu systému se systémové struktury mohou stát nekonzistentní, což může způsobit ztrátu dat. NTFS má zabudováno transakční zaznamenávání akcí, proto se může po pádu systému pokusit obnovit data při jejich minimální ztrátě. K uživatelským datům jsou přidružena tzv. metadata, ve kterých jsou informace o organizaci dat na disku. Na disku NTFS existuje 11 souborů s metadaty:

MFT jméno	Záznam	Popis
$MFT	0	Master File Table — hlavní část NTFS
$MFTMIRR	1	Kopie prvních 16-ti záznamů MFT
$LOGFILE	2	Transakční logovací soubor
$VOLUME	3	Obsahuje sériové číslo svazku, čas vytvoření
$ATTRDEF	4	Definice atributů
.	5	Kořenový adresář disku
$BITMAP	6	Obsahuje mapu použití clusterů (použité vs. volné)
$BOOT	7	Boot record jednotky
$BADCLUS	8	Seznam špatných clusterů na disku
$QUOTA	9	Obsahuje informace o uživatelských kvótách
$UPCASE	10	Přidělení velkých znaků k malým

Tab. 6, Soubory s metadaty v NTFS

Aby se zabránilo ztrátě dat, NTFS chrání své datové struktury na disku podpisem. Když nastane chyba při čtení dat, NTFS označí clustery jako špatné, přemapuje umístnění dat jinam a aktualizuje $BADCLUS, aby příště nebyly chybné clustery použity znovu. Jestliže je v systému chybám odolný diskový driver, tak vrací do NTFS informaci, že použil svou schopnost na ochranu dat.

Master File Table

Podobně jako v souborovém systému FAT je hlavní částí *file allocation table*, tak v NTFS je hlavní částí MFT, protože udržuje informace o rozložení všech souborů, adresářů i metadat na disku. MFT je rozdělena na jednotky, které se nazývají záznamy. V jednom nebo více MFT záznamech NTFS ukládá metadata, která popisují vlastnosti souboru nebo adresáře (bezpečnostní nastavení, atributy) a jeho umístění na disku. Protože MFT je také soubor, je i on zaznamenán v MFT. Uložení informací v těchto záznamech umožňuje, aby MFT mohla růst nebo zmenšovat se. NTFS vnitřně určuje soubory a adresáře podle pozice jejich záznamů v MFT, které označují začátek jejich metadat. Soubory metadat v Tab. 6 mají určené první záznamy v MFT. Velikost záznamu je obvykle 1kB, ale může být i větší.

Záznamy v MFT

Záznam obsahuje malou hlavičku, ve které jsou základní údaje o tomto záznamu. Za hlavičkou následuje jeden nebo více atributů, které popisují data nebo typ souboru či adresáře odpovídajícího záznamu. Hlavička obsahuje čísla, která NTFS používá pro ověření integrity, ukazatel na první atribut v záznamu, ukazatel na první volný bajt v záznamu a číslo prvního (hlavního) záznamu v MFT, jestliže záznam není první.

Logování NTFS

Každá změna v souboru, adresáři nebo v metadatech je zapsána do souboru, ve kterém jsou zaznamenávány všechny změny na disku. Program CHKDSK používá tento soubor na minimalizaci ztrát dat na disku při pádu systému a k jeho udržení konzistence. V tomto souboru jsou dva druhy záznamů *redo* a *undo*. V *redo* záznamech jsou uloženy informace o změnách, které musí být znovu udělány, jestliže systém selže a změněná data nejsou na disku. Například *redo* operací se signalizuje, že smazání souboru musí být dokončeno, jestliže nastane selhání, ale pouze některé datové struktury byly aktualizované. NTFS používá *undo* operace k vrácení změn, které nebyly dokončeny kvůli pádu systému. Jestliže NTFS připojí data k souboru a systém selže, mezi tím kdy NTFS zvětší velikost souboru a tím kdy zapíše nová data, *undo* záznam určí, o kolik se má zkrátit délka souboru do původní velikosti.

Velikost logovacího souboru (obvykle 2 až 4 MB) je závislá na velikosti disku. Logovací soubor není naplněn, dokud NTFS nezajistí, že *redo* a *undo* záznamy, které se ukládají do logovacího souboru, nejsou požadovány pro obnovu. NTFS obnovuje logovací soubor periodicky každých 5 sekund.

NTFS ve Windows 2000

NTFS má v této verzi Windows další zlepšení. Jedním z nových rysů je vestavěná podpora pro šifrování, která zabráňuje programům jako NTFSDOS obcházet bezpečnostní nastavení a zobrazit data. NTFS nešifruje přímo, ale je v něm přidán driver, který to zajišťuje. Tato část komunikuje se systémem zabezpečení NT, aby bylo zajištěno, že se k zašifrovaným datům dostane pouze oprávněný uživatel.

Přestože metadatový soubor $QUOTA existoval již ve verzi NT 3.5, kvóty byly implementovány až ve verzi NT 5.0. NTFS přiděluje kvóty na uživatelském základě a soubor $QUOTA v dalších metadatech ($Extend) ukládá specifikace kvót pro jednotlivé svazky. Kvóta určuje limit množství dat uživatele na svazku.

Podrobnější informace o souborovém systému Windows NT / 2000 je možno najít na [17].

To je vše, co tvoří základ architektury Windows 2000. V další části mé práce se věnuji praktickému nasazení Windows 2000 za použití terminálových služeb.

6. HODNOCENÍ MOŽNOSTI IMPLEMENTACE

Platforma Microsoft Windows 2000 obsahuje velké množství komponent, které dohromady tvoří komplex poskytující veškeré služby potřebné pro vytvoření podnikového síťového prostředí.

Vzhledem k tomu, že diplomová práce je omezena rozsahem stránek, není možno zhodnotit veškeré komponenty Microsoft Windows 2000. Proto jsem se v další části práce zaměřil na jednu komponentu a to na terminálové služby (*Terminal Services*). V dalším textu budu pro terminálové služby, pokud to bude vhodné, používat zkratku TS.

Zaměřil jsem se jak na dvě odlišné HW i SW platformy na straně klientské (jak x86 s MS Windows tak HPC s Windows CE), tak na dva různé způsoby využití terminálových služeb. Jak už vyplývá z jejich možností, je vhodné použít je jak pro vzdálenou správu systému, tak pro provozování v aplikačním režimu. Zkombinoval jsem tedy tyto platformy a způsoby do celkových čtyř modelových příkladů použití.

Nejprve se zaměřím na obecné pojmy, vysvětlím použité operační systémy a aplikace pro přístup na terminálové služby. Následuje popis protokolů pro přístup k TS a vlastní popis praktického využití.

6.1 ZÁKLADNÍ POJMY

Než se dostanu k popisu terminálových služeb, je zapotřebí ozřejmit, co je to tenký klient. Terminálové služby jsou totiž službou, která je určena právě pro podporu a rozvoj technologie tenkého klienta.

6.1.1 CO JE TENKÝ KLIENT ?

Bližší popis a další informace o technologii tenkého klienta (*thin client*) lze nalézt na [2]. Dále uvádím jen stručný souhrn základních faktů.

6.1.1.1 POPIS

Dnes organizace rostou velkou rychlostí a mnoha různými směry. Zaměstnanci jsou rozmístěni v pobočkách po celém světě nebo pracují doma, v hotelech, u zákazníků a na mnoho dalších místech.

Tento fakt vytváří řadu úkolů pro oddělení informačních technologií těchto organizací. Jak snížit celkové náklady na vlastnictví, při zachování přístupu k firemním aplikacím roztroušeným uživatelům bez ohledu na jejich připojení, umístění nebo klientská zařízení. Jak zajistit odpovídající výkon aplikací, jednoduchou a cenově efektivní správu a podporu uživatelů a dostatečnou bezpečnost těchto systémů.

Technologie tenkého klienta přináší oproti dosavadním řešení výhody především z těchto čtyřech hledisek:

a) Správa

Tradiční správa aplikací je velmi časově náročná, drahá a obtížná na údržbu. Administrátoři musí nejenom fyzicky instalovat aplikace každému uživateli, ale musí také provádět podporu uživatelů, udržovat vícenásobné kopie systémů a provádět replikaci dat. Při stovkách uživatelů rostou náklady na správu takového systému velmi rychle a nekontrolovaně.

b) Přístup

Dnešní výpočetní systémy organizací jsou tvořeny směsicí různých typů desktopových zařízení, síťového propojení a operačních systémů. Přístup k životně důležitým Windows aplikacím je obtížný nebo v případě intranet/Internet síťovému systému nemožný a často vyžaduje nákladné upgrady, problematický emulační software a kompletní přepis aplikací.

c) Výkon

Většina firemních aplikací dnes vyžaduje rychlé síťové propojení a výkonné desktopové počítače. Tyto typy aplikací kladou velké nároky na zahlcené firemní sítě a poskytují slabý výkon přes pomalejší spoje, vzdálená připojení. Následkem toho se mnoho uživatelů jednoduše vyhýbá používání těchto životně důležitých aplikací a dat k plnění svých pracovních úkolů. Potom jsou často výsledkem zbytečné pracovní činnosti a podstatné snížení výkonnosti.

d) Bezpečnost

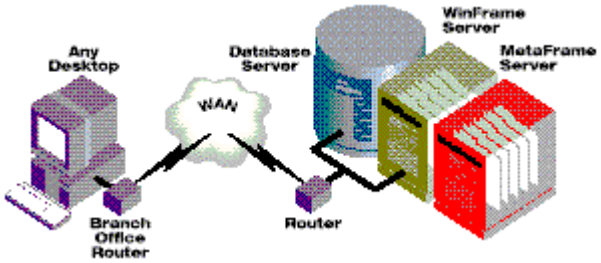
Bezpečnost je další problém, neboť v tradiční klient/server architektuře jsou kritické aplikace a data jak na serveru tak na klientech roztroušeny po světě. Toto nejen zvyšuje riziko neautorizovaného přístupu, ale také ztráty nebo krádeže citlivých informací.

6.1.1.2 TECHNOLOGIE

Jinými slovy, *server-based computing* je technologie, kdy všechny aplikace jsou zpřístupňovány, spravovány a provozovány centrálně na serveru. Tato technologie poskytuje výhody lepší správy, přístupu, výkonu a bezpečnosti, které pomáhají snižovat náklady na celkové vlastnictví. Klientská zařízení, "tlustá" či "tenká", mají okamžitý přístup k firemním aplikacím přes server, bez nutnosti přepisu těchto aplikací nebo jejich nahrávání (*downloading*). A protože technologie tenkého klienta pracuje se stávající výpočetní infrastrukturou a na stávajících standardech, velmi rychle se stává nejjistější a nejbezpečnější cestou ke snížení komplexnosti a celkových nákladů na informační systémy organizací.

Následující příklady demonstrují, jak technologie tenkého klienta umožňuje organizacím elegantně a levněji řešit jejich potřeby:

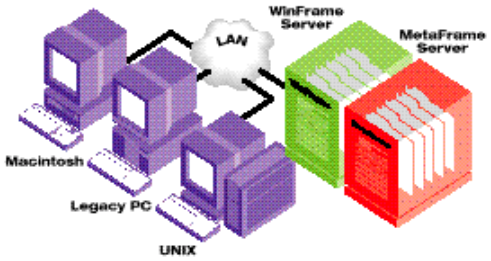
Firma s pobočkami (*Branch Computing*)



Obr. 7, Tenký klient v prostředí vzdálených poboček [2]

Použití technologie tenkého klienta minimalizuje síťový provoz i při používání Windows aplikací. Díky tomu, že jsou nainstalovány a běží na serveru, jejich zpřístupnění, podpora a správa je možná z jednoho místa. Není potřeba mít v každé pobočce administrátora.

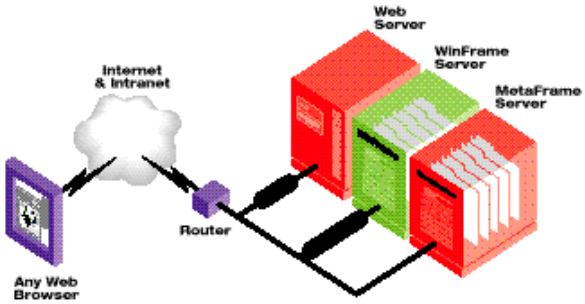
Heterogenní prostředí (*Cross-platform Computing*)



Obr. 8, Tenký klient zapojený do heterogenního prostředí [2]

Technologie tenkého klienta umožňuje virtuálně z libovolného typu zařízení přistupovat k Windows aplikacím bez použití speciálního emulačního software, beze změn konfigurace systému nebo přepisu aplikací. Organizace mohou maximálně využít jejich stávajících technologií a umožnit uživatelům pracovat na jejich oblíbených platformách.

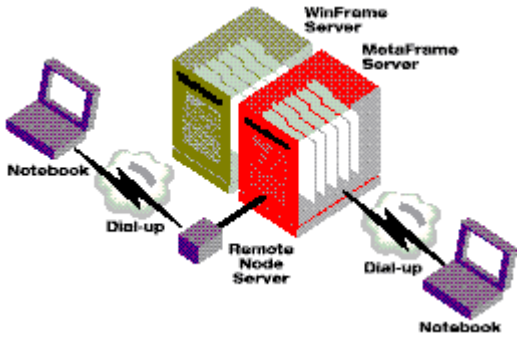
Web Computing



Obr. 9, Tenký klient přistupující z webového prostředí [2]

Citrix WinFrame/MetaFrame, jakožto základní stavební kámen technologie tenkého klienta, umožňuje vkládat aplikace do HTML stránek a odtud je spouštět pomocí internetového prohlížeče, přičemž není potřeba přepisovat jediný řádek zdrojového kódu aplikací. Odpadá tedy nutnost spravovat dva rozdílné programové kódy a přitom umožnit přístup velkému množství uživatelů Internetu při zajištění maximální bezpečnosti kritických dat.

Vzdálený přístup (*Remote Computing*)



Obr. 10, Tenký klient přistupující na server přes dial-up připojení [2]

Technologie tenkého klienta je optimální řešení pro vzdálené uživatele, neboť všechny aplikace běží na serveru, což velmi snižuje provoz na lince. RDP protokol na terminálových službách, nebo ICA protokol ve WinFrame/MetaFrame, je optimalizován pro nízkorychlostní připojení, takže uživatelé mohou pracovat s vysokou výkonností i při spojení přes analogové nebo ISDN modemy, WAN spoj, bezdrátovou LAN a Internet. Eliminuje se též potřeba podpory uživatelů v místě, neboť administrátoři mohou zpřístupňovat aplikace a poskytovat podporu všem vzdáleným uživatelům z jednoho místa.

6.2 TERMINAL SERVICES

Windows 2000 přinášejí jednu z největších novinek, vedle adresářových služeb Active Directory, to jsou právě terminálové služby. Byly zde již dříve ve formě jak pro Windows NT 3.51 jako produkt MultiWin do firmy Citrix, tak Windows NT 4.0 Terminal Server, který vznikl ve spolupráci firem Citrix a Microsoft. Jednalo se o samostatný produkt, který byl takovým pokusem firmy Microsoft prosadit se na trhu v této oblasti. Pro jeho řádné využití bylo vhodné dokoupit MetaFrame od firmy Citrix s podporou protokolu ICA. Ve Windows 2000 Server jsou terminálové služby integrální součástí operačního systému, obsahují vylepšený protokol RDP verze 5 (Windows NT 4.0 Terminal Server obsahovaly verzi 4)

Co přináší použití terminálových služeb a jaké jsou jejich výhody a nevýhody ? Jaké jsou praktické možnosti a zkušenosti s jejich nasazením ? Na tyto otázky odpovím v následujících kapitolách

6.2.1 STRUČNÝ POPIS SLUŽBY TERMINAL SERVICES

Terminálové služby jsou silnou zbraní Windows 2000. Jejich uplatnění vidím ve čtyřech základních rovinách – nasazení na pracovištích, která obsahují velké množství starších počítačů, na které není možno nainstalovat Windows 2000 Professional a provozovat na nich nové a náročné aplikace. Za druhé pro vybudování nových sítích založených na terminálových službách – jedná se především o počítačové učebny, kde je potřebná rychlá a kvalitní obnova po proběhlé výuce, samozřejmě lze takto vybudovat i klasické kancelářské pracoviště či celé firmy. Dojde tak k úspoře nákladů na HW vybavení, správu apod. je zřejmé. (více informací dále). Třetí rovina využití je pro připojení vzdálených pracovišť k firemní síti, podpora mobilních uživatelů apod. Poslední rovinou použití je správa serveru z kteréhokoliv počítače, který má nainstalován klienta terminálových služeb. Administrátor tak nemusí být přítomen kvůli maličkosti fyzicky u serveru a může provádět správu např. po Internetu.

Velkou výhodou terminálových služeb je jejich jednoduchost jak instalace, tak nastavení a vlastní správa. Je to dáno právě integrací přímo do Windows 2000.

O tom, jak terminálové služby fungují, píši dále v kapitole 5.2.2. Důležité pro začátek je vědět, že TS lze zprovoznit ve dvou módech – jako *aplikační server* a *vzdálená správa*. V aplikačním módu je základem to, že aplikace fyzicky běží sdíleně na serveru(ů) a na klientské stanice se přenáší pouze obrazovky resp. jejich změny, na server se přenášejí stisky kláves a pohyb myši. Více o funkci je popsáno v odstavci věnovanému RDP protokolu.

To, že aplikace běží sdíleně na serveru, přináší velké množství výhod. Pro správce je to především úspora času, neboť se aplikace instaluje jen jednou na server a používat jej mohou stovky uživatelů. Většina aplikací má chyby a proto se často

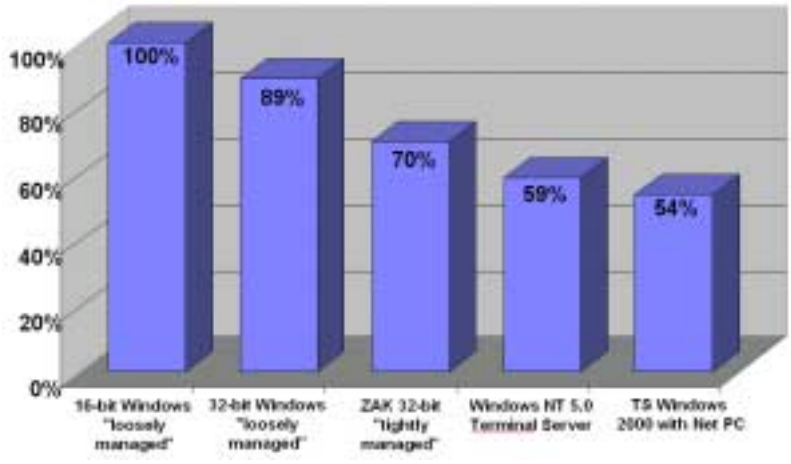
vydávají opravné balíčky (service pack). Tyto opravné balíčky je pak třeba aplikovat na všechny stanice, což je v případě terminálových služeb zbytečné, neboť se oprava nainstaluje pouze jednou na server.

Co je především důležité je to, že je možno uživatelům poskytnout např. Windows 2000 a Office 2000, ačkoliv jejich HW vybavení by neumožnilo instalaci, natož běh tohoto SW. Jedná se o počítače např. 386 se 4MB paměti a 200 MB diskem s nainstalovanými Windows 3.11. Navíc je tak možno dosáhnout kompatibility aplikací – staré aplikace by již pod Windows 2000 neběžely a tak uživatel si může jednoduše přepínat mezi původním operačním systémem a Windows 2000.

Uživatelé při práci se často setkají s problémem, který nevědí jak vyřešit. Proto se obrací na administrátora nebo někoho z technické podpory, aby jim pomohl problém odstranit. Administrátor musí dojít k uživateli a poradit či vyřešit jeho problém. Při použití terminálových služeb toto odpadá. Administrátor se může interaktivně připojit na uživatelovo sezení (*session*) a převzít ovládání počítače pomocí svého terminálu.

Tím, že je vše na serveru, má administrátor zjednodušenou práci hned několikanásobně. Může jednoduše provádět zálohování jak jednotlivých instalovaných aplikací, tak především dat a osobních nastavení všech uživatelů. Navíc není možné, aby si uživatel úmyslně či neúmyslně smazal systémové soubory Windows a docílil toho, že nebude moci pracovat a administrátor bude muset provést opravu nebo reinstalaci systému a aplikací. Jak jsem už uvedl výše, administrace takové sítě, včetně převzetí kontroly nad stanicí, lze provádět odkudkoliv, třeba i po Internetu. Více o vzdálené správě je v odstavci věnovaném praktickému nasazení terminálových služeb.

Windows 2000 přišli s možností hibernace. Jedná se o uložení obsahu paměti na disk a po opětovném spuštění počítače k rychlému obnovení stavu, tak jak jsme Windows zanechali, tedy včetně otevřených aplikací a dokumentů. Ani terminálové služby toto neopomíjejí a tak připojený uživatel se může pouze odhlásit, jeho nastavení se uloží na disk a při dalším přihlášení se dostane do takového stavu, v jakém svoje připojení zanechal.



Obr. 11, Snížení celkových nákladů na vlastnictví (TCO) při použití různých metod, jak tohoto snížení dosáhnout (Zdroj: Microsoft)

Mimo výše uvedené výhody patří snížení celkových nákladů na vlastnictví (TCO – *Total Cost of Ownership*). Jedná se především o snížení jak nákladů na pořízení hardware pro stanice, tak na pořízení licencí či upgradů operačních systémů na stanice a na nainstalovaný software. Pokud se jedná o nové počítače, úspora za licence na OS není aktuální. Dále je možno ušetřit na administrátorech, kterých nebude tolik potřeba a ve velké společnosti jich bude moci být méně resp. se budou moci věnovat rozvoji infrastruktury a ne neustálým „obíháním“ uživatelů. Naopak je potřeba počítat s nákupem licencí terminálových služeb, aplikace umožňující běh na TS vyžadují další licence. Jak ukazuje obrázek 11, lze dosáhnout snížení TCO až o 46 procent při použití terminálových služeb Windows 2000 ve spojení s tenkými klienty Net PC.

A když už hovořím o licencování, terminálové služby je možno nainstalovat a bez licencí používat po dobu 90 dní od instalace. Tato lhůta slouží k celkovému nastavení a konfiguraci terminálových služeb. Registrace licencí pak probíhá po Internetu na serveru firmy Microsoft. Server obdrží jedinečné číslo, které se ovšem nezachová při reinstalaci serveru. Proto ta 90 denní lhůta na konfiguraci. Bližší informace i této lhůtě jsou uvedeny v kapitole věnované licencování (5.5.1.1).

Terminálové služby mají také své zápory. Hlavní nevýhodou (ale pochopitelnou) je velká hardwarová náročnost kladená na servery. Je to pochopitelné, vždyť na serveru běží všechny aplikace všech uživatelů. Tam, kde výkonnostně končí špičkové pracovní stanice, tam teprve začínají servery pro terminálové služby. A náklady na pořízení těchto serverů jsou vysoké. Blíže o praktických doporučeních na konfiguraci serveru hovořím v části věnované praktickému nasazení terminálových služeb (5.3.1).

Terminálovým službám je také vytýkána absence některých funkcí a služeb. Chybí podpora ne - Windows klientů, protokol RDP podporuje jen přenosový protokol TCP/IP. Velkou nevýhodou je absence tzv. *server farming*. Uživatel si tak musí pamatovat, na kterém terminál serveru je nainstalována určitá aplikace a podle toho se k němu připojit. Tuto záležitost má Citrix MetaFrame vyřešenu mnohem lépe. Uživatel se připojuje k nejbližšímu serveru a ten pošle klientské stanici *link* na požadovanou aplikaci. S tím souvisí i vyrovnávání zátěže mezi více serverů (*load balancing*), které je dostupné až ve verzi Windows 2000 Datacenter. Terminálové služby zatím umí lokálně přesměrovat pouze COM a LPT porty (jedná se o použití tiskáren, skenerů apod. lokálně připojených na stanici, ale obsluhované z aplikace spuštěné v terminálové relaci).

Tolik tedy k celkovému popisu terminálových služeb, teď se hlouběji podíváme na to, jak terminálové služby fungují uvnitř.

6.2.2 ARCHITEKTURA SLUŽBY TERMINAL SERVICES

Terminálové služby běžící na Windows 2000 Serveru poskytují všem klientům možnost spouštění aplikací, zpracování a ukládání dat na serveru. Poskytují vzdálený přístup na serverový desktop přes terminálovou emulaci. Software terminálové emulace může běžet na různých typech HW - na PC, na Windows CE Handheld zařízeních, nebo na terminálech (zařízení *NetPC*) nebo WBT (*Windows Based Terminal*). Jedná se o zařízení zvaná tenký klient (*thin client*), která mají možnost připojit se jako terminál na víceuživatelský operační systém. Terminálové služby provádí veškeré datové manipulace lokálně a výsledky posílají na klienta.

Dále umožňují vzdálené ovládání serveru a centrální správu aplikací, minimalizují celkové zatížení sítě mezi serverem a klienty. Připojení probíhá na základě TCP/IP ve spojení s *Remote Access*. Spojení lze realizovat po Internetu, bezdrátově, po

sítích WAN (*Wide Area Network*), LAN (*Local Area Network*), VPN (*Virtual Private Network*). TS poskytují vzdálenou administraci síťových zdrojů.

Výhody terminálových služeb:

- umožňují provozovat 32bitové aplikace na zařízeních, která nejsou založena na 32bit Windows, jako například:
  - Windows for Workgroups 3.11
  - Windows CE zařízení
  - MS-DOS
  - UNIX terminál
  - Macintosh
- klienti, kteří nejsou postaveny na platformě Windows, musí použít add-on třetích firem (Citrix MetaFrame)
- minimalizace potřeby diskového prostoru, paměti a potřeby konfigurace klienta
- zjednodušená správa klientských stanic z důvodu vzdálené správy
- centralizované zabezpečení a správa

Terminálové služby lze zprovoznit ve dvou základních módech:

1. Vzdálená správa (*Remote Administration*)

Vzdálená správa poskytuje systémovému administrátorovi silnou podporu pro vzdálenou správu všech Windows 2000 Serverů přes jakékoliv TCP/IP připojení. Lze administrovat sdílení souborů a tiskáren, editovat databázi registry z jakéhokoliv počítače na síti, nebo provádět jakýkoliv požadovaný úkol.

Tento mód instaluje pouze komponenty TS Remote Access. Neinstaluje sdílení aplikací. TS podporují maximálně dvě konkurenční administrátorská připojení současně. Nejsou potřeba dodatečné licence ani není třeba mít na síti licenční server.

2. Aplikační server (*Application Server*)

V tomto módu lze provozovat a spravovat aplikace z centrálního místa, ušetřit tak čas pro instalaci, správu a upgrade aplikací na klientech. Po zprovoznění TS se mohou uživatelé připojit různým způsobem z různých zařízení a používat aplikace, které by na jejich zařízeních nefungovaly resp. jejich HW by nestačil výkonově na jejich správnou a efektivní činnost.

Instalovat aplikace lze přímo nebo je možno použít vzdálenou instalaci (je možné pomocí *Group Policy* a *Active Directory* vytvořit instalační balíček na TS a aplikace bude na klienta nainstalována pouze v případě, jestli to umožní *Group Policy*).

Rozšíření od třetích stran

Citrix MetaFrame používá Citrix Independent Computing Architecture (ICA) protokol, který poskytuje následující rozšíření:

- další zařízení
- další síťová připojení
- lokální systémové zdroje

Dále poskytuje řadu administračních nástrojů, podrobnější informace jsou napsány v odstavci věnovaném protokolu ICA (5.4.3.2).

Bližší informace o architektuře lze najít v [6], [7], [11] a [23].

6.3 TERMINAL SERVICES – HARDWARE

V této části mé práce jsem se zaměřil na to, jaký hardware je potřeba pro vybudování terminálových služeb. Rozdělil jsem je na požadavky na server a požadavky na klienta. Klientský hardware ovlivníme jen v tom případě, pokud budujeme síť novou. Pokud podnik vlastní klientské stanice, je třeba definovat a znát stávající strukturu HW. Minimální požadavky na použití TS z klientů jsou uvedeny v následující kapitole 5.3.2.

Na straně serveru je situace jednoznačná. Ve většině případů je potřeba zakoupit nové servery případně rozšířit stávající resp. doplnit stávající serverovou infrastrukturu o další stroje. Při nákupu nových strojů je potřeba dobře zvážit rozšiřitelnost serverů a jejich dostatečný počet s odpovídajícím výkonem. Jaké jsou požadavky je uvedeno hned v následující kapitole 5.3.1.

6.3.1 POŽADAVKY NA SERVER

Při budovaní terminálových služeb je nejdůležitější serverová část. Server pro TS by měl být samostatný, tj. neměl by sloužit k jiným účelům a neměl by provozovat např. SQL server, poštovní server nebo být souborovým serverem. Microsoft poskytuje i testovací utility pro výpočet kapacity serverů pro dané možnosti využití a počty plánovaných klientů. Základní požadavky uvádí následující tabulka:

User type / Server config.	Structured Task Worker	Knowledge Worker	Data Entry Worker	Data Entry Worker Dedicated
8 x Pentium III 500 MHz 2 MB L2 Cache 4096 MB RAM	105 Users	160 Users	Not Tested	Not Tested
4 x Pentium III 500 MHz 2 MB L2 Cache 4096 MB RAM	90 Users	135 Users	Not Tested	Not Tested
2 x Pentium III 450 MHz 0.5 MB L2 Cache 1024 MB RAM	40 Users	70 Users	320 Users	350 Users
1 x Pentium III 450 MHz 0.5 MB L2 Cache 1024 MB RAM	25 Users	35 Users	280 Users	280 Users
4 x Pentium Pro 200 MHz 0.5 MB L2 Cache 1024 MB RAM	30 Users	50 Users	Not Tested	Not Tested

Tab. 7, Hardwarové vybavení serveru pro různé typy uživatelů a jejich počty [5]

Důležité je, aby server byl vybaven možností přidání dalších procesorů. Za rozumný základ považuji dvouprocesorový server, který umožňuje doplnění o další dva procesory. Množství a výkon procesorů záleží na typu provozovaných aplikacích.

Co se týče otázky paměti RAM, 128 MB paměti je základ pro samostatný operační systém. Pro každou *session* je potřeba 16-20 MB paměti, dalších cca 13 MB je potřeba pro každého uživatele pro běh aplikací. Je potřeba si uvědomit, že 16ti bitové aplikace potřebují o 25 procent více paměti než aplikace 32 bitové. Pokud uživatelé využívají aplikace, které potřebují hodně paměti (typicky aplikace CAD, grafické programy, databázové aplikace, modelovací a matematické aplikace), je potřeba počítat

s větším množstvím RAM. Pokud uživatelé používají stejné aplikace, které nejsou náročné na výkon počítače (typicky aplikace MS Office), dochází ke sdílení binárního kódu a není potřeba tolik fyzické RAM. Optimální řešení je do dvouprocesorového serveru dát 1GB RAM.

Základní vzorec pro výpočet množství paměti ukazuje následující tabulka:

User type / Memory	Structured Task Workers	Knowledge Workers	Data Entry Workers	Data Entry Workers Dedicated
Memory per user (MB)	9.3	8.5	3.5	3.3
System Memory (MB)	128			
Total Memory	System + (# of Users x Memory per User)			

Tab. 8, Vzorec pro výpočet množství paměti serveru v závislosti na typu uživatelů a jejich počtu [5]

Prostor na disku pro odkládací soubor musí být minimálně ve jeden až jeden a půl násobek velikosti fyzické RAM. Nejlepší řešení je umístit TS na jeden fyzický disk a odkládací soubor na druhý (ne na jiný logický oddíl, skutečně jiný fyzický disk). Pokud má server hodně fyzické paměti, je potřeba, aby na disku bylo dostatek místa pro *dump files* (soubory, do kterých se provede výpis obsahu paměti při havárii systému). Velikost místa na disku pak samozřejmě záleží na instalovaných aplikacích a na poskytnutí místa pro uživatelské soubory. Registrační databáze má dynamickou velikost danou instalacemi aplikací a založenou na velikosti odkládacího souboru. Kvóta pro její velikost je také dána velikostí fyzické paměti.

Konkrétně by server měl být vybaven procesory Intel XEON řádově na taktu 1GHz. Pro vyšší výkon doporučuji procesory AMD Athlon resp. Thunderbird, bohužel zatím nepodporují práci ve víceprocesorovém systému. Jak jsem napsal výše, paměť minimálně 512 MB, ale čím větší, tím lépe. Disky samozřejmě na rozhraní SCSI, nejlépe RAID pole typu 4 nebo 5, velikost dle počtu klientů a typu používaných aplikací. Vybaven samozřejmě musí být síťovými kartami - záměrně hovořím v množném čísle - druhá karta je vhodná pro propojení mezi servery. Asi je zbytečné zdůrazňovat, že komponenty musí být kvalitní, nejlépe certifikované firmou Microsoft nebo zakoupit značkový server s certifikátem Microsoftu (HP, Compaq, Dell, IBM).

Pokud bude na servery nainstalována podora ICA protokolu za použití Citrix MetaFrame (resp. WinFrame), je servery možno spojovat do farem a rozložit tak nejen síťovou zatěž mezi několik serverů, ale umožnit tak připojení klientů k těm serverům, které jsou nejblíže jeho lokaci. Pak je třeba servery vhodně rozmístit podle toho, které aplikace na nich budou nainstalovány s ohledem na blízkost pro připojení klientů, které je budou používat. Tato vlastnost není ve TS podporována, ačkoliv Windows 2000 Server (verze Advanced a Datacenter) podporuje spojování serveru do klastrů (*Cluster Service*). Bližší informace viz část 5.5.1.1, věnovaná přípravě sítě na terminálové služby.

6.3.2 POŽADAVKY NA KLIENTA

X86 klient

Pokud budeme stavět terminálovou síť s využitím protokolu RDP, tak hardwarové zařízení počítačů platformy X86 je takové, aby bylo schopno provozovat

alespoň operační systém Windows for Workgroups 3.11. Minimálně se jedná o počítač s procesorem 386, 33 MHZ, 16 bit VGA grafická karta a MS TCP/IP, 500 KB místa na disku, 4MB RAM. Pokud je zapnuté *bitmap caching*, je potřeba dalších 10 MB na disku. Pro optimální běh je minimum 8MB paměti pod WfW 3.11 nebo Win95, 24 MB paměti pro Win98 a 32 MB pro Windows 2000.

Vzhledem k tomu, že v současné době se tyto počítače vyskytují velmi zřídka, neměl by být problém s nasazením RDP na stávající HW v podniku. Pokud se rozhodneme pro nasazení ICA protokolu, můžeme nároky na HW snížit až na úroveň počítačů s procesorem 286 a operačním systémem DOS. Samozřejmě je potřeba, aby byl klient vybaven síťovou kartou buď na ISA nebo na PCI sběrnici s výstupem BNC na koaxiální kabel nebo s RJ45 na kroucenou dvoulinku (záleží na struktuře sítě podniku). Při použití ICA protokolu si můžeme vystačit i s připojením přes sériový kabel (jen ICA) nebo přes modem (i RDP).

HPC klient

Tento klient má zvláštní určení. Je samozřejmě možno jej využít i v aplikačním módu, jeho hlavní využití bude ale v módu administrátorském. Vzhledem k tomu, že přenosná zařízení jsou vesměs zařízení nová, prakticky neexistují HW omezení.

Podporovány jsou různé typy procesorů - SH3, SH4, MIPS, ARM, PowerPC a StrongARM na frekvencích řádově od 80 do 200 MHz. Rychlý procesor urychlí překreslování obrazu. Důležité je, aby displej zařízení podporoval minimálně 16 odstínů šedi, resp. aby byl barevný. Také musí obsahovat síťovou kartu, která je většinou ve formátu PC Card (dříve označované jako PCMCIA). Ne každé přenosné zařízení je ovšem vybaveno slotem na tyto karty. Je možno ovšem sehnat karty i ve formátu Compact Flash. Nevýhodou je, že síťové karty mají velký odběr energie a tak většinou nepřichází v úvahu připojení na TS bez připojení zařízení k síťovému adaptéru. Výstup z těchto karet je většinou kombinovaný, tj BNC i RJ45. Existují i karty kombinované s modemem (včetně GSM), některé přenosné zařízení mají zabudovaný modem a a lze se tak připojit pomocí telefonní linky. Použít lze i připojení pomocí sériového kabelu resp. pomocí infraportu (pouze ICA protokol).

6.4 TERMINAL SERVICES – SOFTWARE

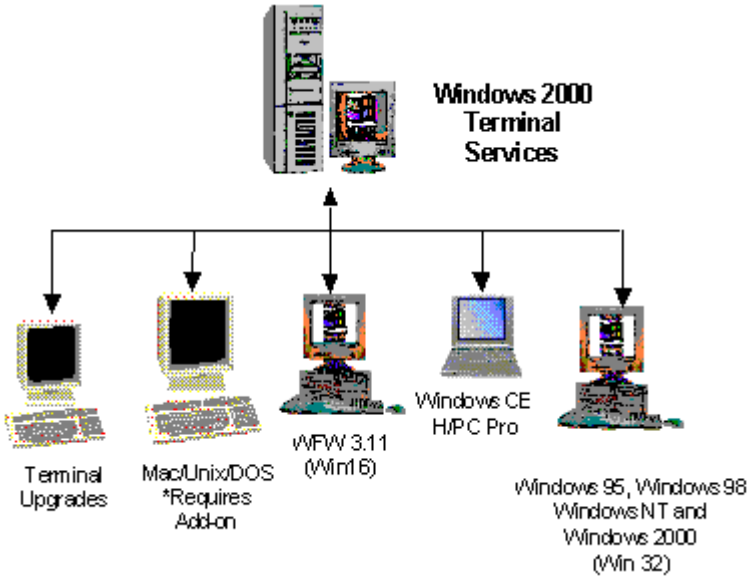
Základem veškeré práce s terminálovými službami je software. V tomto případě se jedná o dvě základní kategorie a to o operační systémy jak na straně serveru, tak na straně klienta, a dále o klientské aplikace na straně klienta.

6.4.1 OPERAČNÍ SYSTÉMY

Pokud se jedná o operační systém na straně serveru, zde je volba jasná již z hlediska této práce – je potřeba Windows 2000 Server, Advanced Server nebo Datacenter Server. Všechny verze plně podporují terminálové služby [11].

Na straně klientské volba není tak jednoznačná. Microsoft samozřejmě podporuje své operační systémy, ale ne všechny. Na instalačním CD Windows 2000 Server jsou klienti pro 16-bitové Windows for Workgroups 3.11, tak pro 32-bitové Windows 9.x a NT 4.0 / 2000. Podporovány jsou Windows CE 2.11 (operační systém přenosných zařízení Handheld PC). Na instalačním CD jsou však i klienti, kteří podporují Citrix ICA protokol a to jak pro Windows 3.1 (RDP klient chybí) a 3.11, tak pro Windows 9.x a NT 4.0 / 2000 a pro Windows CE 2.1 (RDP klient chybí). Pro jejich

použití je potřeba na Windows 2000 Server doinstalovat Citrix WinFrame nebo Citrix MetaFrame, který přidá do terminálových služeb podporu pro protokol Citrix ICA.



Obr. 12, Typy připojitelných klientů k Windows 2000 Terminal Services [23]

Není zde ovšem klient pro DOS a pro Windows 3.1, chybí podpora startu přímo pomocí BootPROM ze síťové karty. Je zvláštní, že je dodáván klient RDP podporující Windows CE 2.11 a klient ICA, podporující Windows CE 2.1. Obzvláště pak proto, že Windows CE 2.1 jsou mnohem rozšířenější. Dále chybí podpora pro NonPC klienty (Apple, Network terminal apod.) – tato nepodpora je dána architekturou protokolu RDP, která je založena na využívaní Windows API, které není přenositelné na jiné platformy. (více je uvedeno v kapitole věnované popisu protokolu RDP). Jak je ovšem popsáno v dalším odstavci věnovaném klientský aplikacím, lze pomocí softwarové emulace provozovat RDP klienta i na jiných platformách.

6.4.2 KLIENTSKÉ APLIKACE

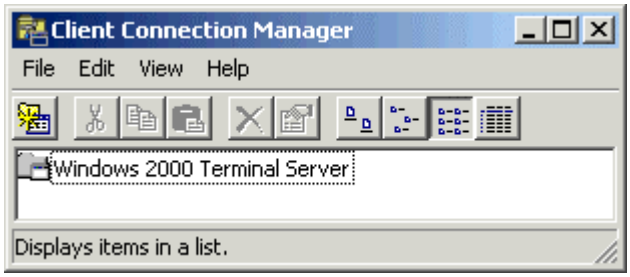
Klientské aplikace slouží k připojení klientských zařízení k terminálovým službám. Klientská část je malá aplikace instalovaná na disku nebo ve firmware. Jak jsem uvedl v předchozím odstavci, podporovány jsou jen některé OS a HW platformy. V dalším odstavci se budu věnovat popisu vlastností jednotlivých typů klientů a jejich možnosti použití a využití. Ani jeden z těchto klientů není možno použít pro přímé připojení na TS bez existence operačního systému na stanici. Každý klient potřebuje OS jako základ své práce. Pro přímé připojení bez existence OS na stanici je třeba použít protokol Citrix ICA a produkt Citrix MetaFrame / WinFrame.

6.4.2.1 KLIENT FIRMY MICROSOFT

Microsoft dodává v zásadě tři typy klientských aplikací, všechny pracují s protokolem RDP verze 5: [11]

1. Windows 16 bit klient resp. Windows 32 bit klient

Jedná se o klasickou Windows aplikaci, která umožňuje vytvoření několika připojení buď na různé TS servery nebo na stejný TS server, ale s jinými parametry. Touto aplikací je *Client Connection Manager*.



Obr. 13, Client Connection Manager pro Windows na platformě x86

Pro každé připojení je možné nastavit rozlišení terminálové relace (menší nebo shodné s rozlišením hostitelského OS), vlastnosti komprese (data a *bitmap caching*), zobrazení do okna nebo na celou obrazovku, automatické přihlášení a automatické spuštění aplikace po přihlášení. Podmínkou provozu je správná instalace a funkčnost protokolu TCP/IP. Klient je pro Windows 2000, 98, 98, Me, Windows for Workgroups 3.11, Windows NT 3.51.

2. Windows CE klient

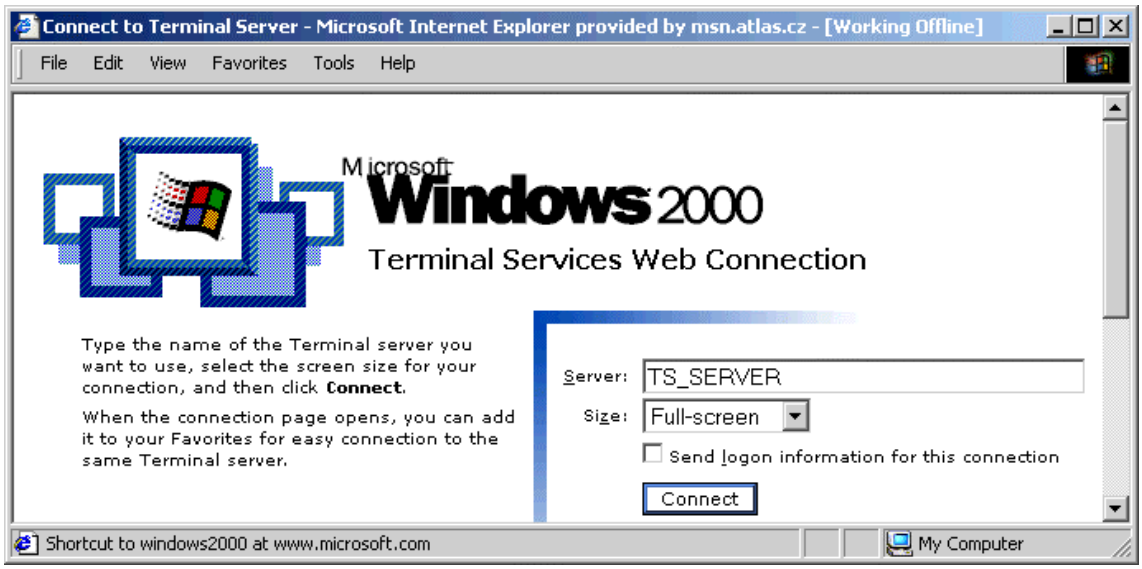
Tento klient je vzhledově velmi podobný předchozímu klientu. Zdrojový kód pro jeho napsání je shodný s předchozím, jen byl zkompilován pro Windows CE 2.11. Instalace je použitelná jen pro verzi 2.11, na verzi 2.1 nefunguje. Windows CE klient je typicky nakonfigurován lokálně a konfigurace představuje:

- použití DHCP (jedná se o mobilní uživatele a tak není reálné používat pevnou IP adresu)
- připojení k síti LAN, nastavení protokolu PPP, IP adresa, subnet mask a gateway
- zapojení DNS pro komunikaci s TS pro zjištění jeho jména

Existuje mnoho zařízení, některá ale nepodporují šifrování při procesu logon a je potřeba je nastavit tak, aby hesla posílala jako obyčejný text. Tato zařízení mohou obsahovat různé druhy terminálových emulací a mohou je používat současně na více serverech.

3. Terminal Services Advanced Client

Terminal Services Advanced Client (TSAC) je klient, který je ve formě ActiveX komponenty. Výhodou použití ActiveX komponenty je především to, že TSAC klient je přístupný jako součást HTML stránky přes Internet odkudkoliv pomocí Internet Exploreru nebo jiné aplikace, která umí používat ActiveX komponenty, napsané ve Visual Basicu nebo Visual C++. Výhodou tohoto řešení je částečná přenositelnost na jiné platformy (Apple), dále pak možnost využití tohoto klienta pro Windows CE 2.1, pro které neexistuje klasický RDP klient. Další informace a aktuálního klienta lze najít na [25].



Obr. 14, Připojení na terminálové služby pomocí ActiveX komponenty z webového prohlížeče

6.4.2.2 KLIENT FIRMY HOB ELECTRONIC

Klient HOBLink JWT je zatím jediný klient, který podporuje RDP protokol a není od firmy Microsoft. Je kompletně napsán v jazyce Java a existuje pro velké množství operačních systému a platforem.

Instalace tohoto produktu umožňuje dvě varianty – buď se klient nainstaluje jako samostatná aplikace na klientskou stanici, nebo je možno provést serverovou instalaci. Jako serverová aplikace pak může být integrována na www stránky a tak přístupna přes síť Internet. Protože se jedná o *Java applet*, je tak její platformová nezávislost dost vysoká, neboť pro většinu operačních systémů existují prohlížeče, kteří podporují *Java applets*.

Instalace existuje pro Windows, Unix, Apple Macintosh, OS/2, NCs, a Handheld PC, tak i pro platformy, které nemají GUI (např. AS/400 nebo OS/390). Jako síťový protokol používá TCP/IP. Poskytuje zobrazení jak do okna libovolného rozměru, tak na plnou obrazovku, i do okna internetového prohlížeče. Podporuje šifrování terminálových služeb a šifrování na bázi 128 bitového SSL protokolu. Klient využívá i *load balancing* (vyrovnávání zátěže mezi více serverů). Podporuje různé rozložení klávesnic, čeština mezi nimi bohužel chybí. Pro připojení je možno nechat vyhledat jednotlivé TS servery a nastavit port pro připojení. Nechybí možnost automatického přihlášení zadáním jména, hesla a domény a možnost automatického spuštění aplikace po přihlášení na TS.

Aktuální instalaci klienta a další informace lze najít na [20].

6.4.2.3 KLIENT FIRMY CITRIX

Klient firmy Citrix jsou založen na protokolu ICA. Tento protokol je platformově nezávislý. Kromě komunikace přes síťový protokol TCP/IP umožňuje připojení pomocí NetBIOS, IPX, SPX a pomocí modemu a sériového portu. ICA klient existuje pro další platformy a jeho podpora je hodně obsáhlá, více informací je v odstavci věnovanému protokolu ICA. Pro funkci ICA protokolu v rámci TS je potřeba

nainstalovat na Windows 2000 Server Citrix MetaFrame for Windows 2000 nebo Citrix WinFrame server. Ani jednoho z níže uvedených klientů jsem neměl možnost v praxi vyzkoušet.

Citrix dodává spolu s CD Windows 2000 Serveru klienty pro tyto platformy:

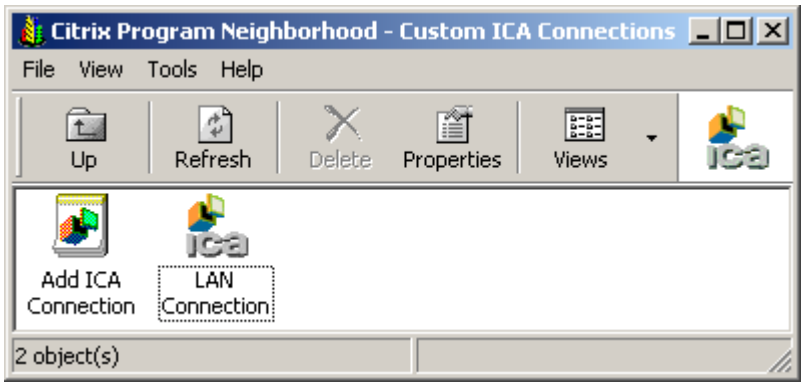
1. Windows 3.1 a Windows for Workgroups 3.11

Tato verze je určena pro Windows 3.1 běžící v *enhanced mode* a pro Windows for Workgroups 3.11. Instalace zabere kolem 3.5 MB prostoru na disku, pro svůj běh potřebuje 8 MB paměti a více, VGA/SVGA kartu a barevný monitor.

2. Windows 95/98 a Windows NT/2000

Tato verze je určena pro Windows 95, Windows 98, Windows NT 3.51, Windows NT 4.0 a Windows 2000. Instalace zabere kolem 4 MB místa na disku, pro svůj běh potřebuje 8 MB (Windows 9.x) resp. 16 MB (Windows NT/2000) paměti.

Pro správu jednotlivých připojení slouží klasická Windows aplikace, která se jmenuje *Citrix Program Neighborhood*. Průvodce pro vytvoření připojení nabízí spojení přes lokální síť, Internet, dial up (PPP/SLIP) a Citrix DialIn. Na výběr je jeden z těchto síťových protokolů: TCP/IP, NetBIOS, IPX, SPX. Nechybí ani možnost předdefinovat si jméno, heslo a doménu pro automatické připojení. Rozlišení může být libovolné, i větší než je nastavené aktuální na hostitelském OS. Možno je nastavit barevnou hloubku buď na 256 nebo 16 barev (vhodné pro spojení přes modem).

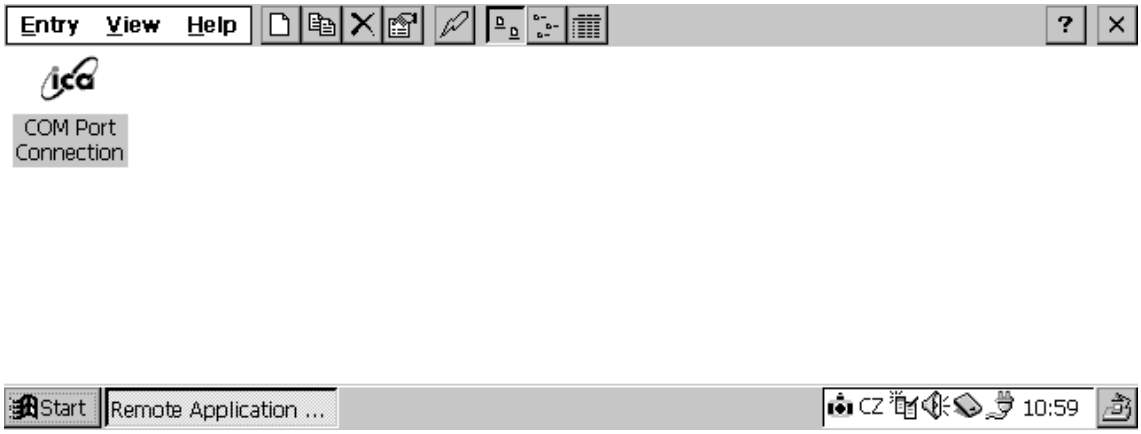


Obr. 15, Citrix Program Neighborhood pro Windows na platformě x86

Pro všechna připojení je možno definovat velikost bitmapové cache paměti, klávesové zkratky pro obsluhu aplikací uvnitř klienta a logování událostí. Dodávaný klient umožňuje pouze základní zabezpečení přenosu dat (více v odstavci věnovanému ICA protokolu v kapitole 5.4.3.2). Postup nastavení klienta je v obrazové příloze B.4.

3. Windows CE klient

Pro provoz této verze je potřeba mít zařízení Handheld PC s Microsoft Windows CE 2.0 nebo 2.11. Musí obsahovat síťovou nebo modemovou kartu (nejčastěji ve formátu PC Card případně Compact Flash). Tento klient funguje na zařízeních, které používají procesory SH3, SH4, MIPS, PowerPC, nebo ARM. Display musí podporovat minimálně 16 odstínů šedi nebo barev.



Obr. 16, Remote Application Manager pro Windows CE (ICA protokol)

Všechna nastavení jsou shodná jako pro verze v předchozím odstavci. Jen rozlišení je dáno fyzickým rozlišením zařízení (typicky 640x240 bodů). Aktuální instalaci klienta a další informace lze najít na [26]. Postup nastavení klienta je v obrazové příloze B.5.

6.4.3 PROTOKOLY

Pro komunikaci mezi klientem a serverem je potřeba definovat protokol, který umožní přenos dat v obou směrech. Existují dva nejpoužívanější protokoly pro tento typ přenosu dat – Remote Desktop Protocol (RDP) od firmy Microsoft a Independent Client Architecture (ICA) od firmy Citrix. V následujícím textu se budu zabývat oběma protokoly a na závěr kapitoly provedu jejich vzájemné srovnání.

6.4.3.1 POPIS PROTOKOLU MICROSOFT RDP5

Nejprve začnu protokolem RDP, který je implementován v terminálových službách Windows 2000. Bližší informace lze nalézt na [10].

Co je protokol RDP

Protokol RDP slouží pro zobrazování vzdáleného displeje a pro vzdálené ovládání klientských počítačů po síti. Protokol je určen pouze pro aplikace na bázi Microsoft Windows, není tedy multiplatformní jako ICA (viz. dále). Protokol je založen na bázi rodiny protokolů ITU T.120 (*International Telecommunications Unions*), mezinárodní, standardní vícekanálový konferenční protokol. Tak jako ICA protokol, dokáže i RDP spolehlivě a efektivně pracovat i na sítích s nízkou propustností. RDP obsahuje šifrování a kompresi dat.

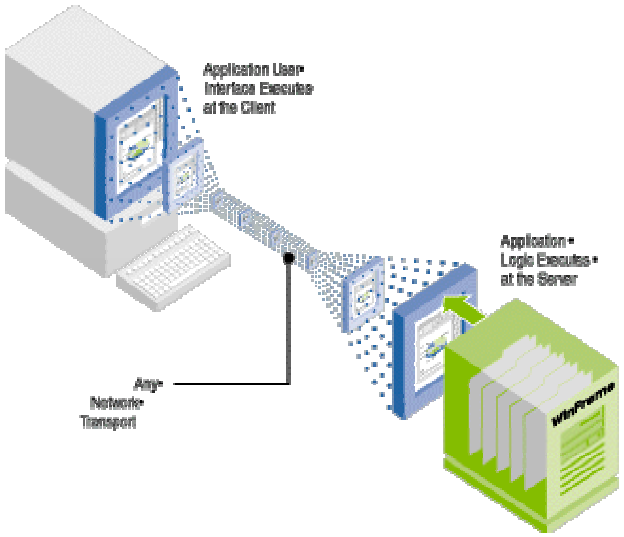
Windows 2000 obsahuje protokol RDP ve verzi 5, předchozí verze Windows, Windows NT 4.0 Terminal Server, obsahuje verzi 4. Verze 5 je lépe optimalizována a je bezpečnější. Tento protokol je mimo jiné v současné době používaný i v aplikaci Microsoft NetMeeting (konferenční software).

Ve spojení s protokolem RDP se používá pojem *Super-Thin Client* - klientský software, který reprezentuje nebo zobrazuje rozhraní, které je shodné s 32 bitovým rozhraním Windows a fungujícím na širokém množství stolního HW - PC s Windows 9x, Windows NT Workstation 4.0, Windows 3.11, Windows CE atd.

Popis protokolu RDP

RDP je založen na rozhraní standardu rodiny protokolů ITU T.120. Jedná se o vícekanálový protokol, který dovoluje po více virtuálních kanálech šifrovaný přenos obrazu, kliknutí myši a úhozy do klávesnice. Podporuje až 64 000 oddělených kanálů pro přenos dat, např. přesměrování tiskáren, sdílení schránky a další. Dále je schopen podporovat více protokolů, zatím jen TCP/IP, po síti WAN používá PPP (*Point to Point Protocol*) k „tunelování“ (*tunnelling*) IP. Na požadavek zákazníků v budoucích verzích mohou být přidány další protokoly.

RDP obsahuje vlastní ovladač obrazovky, který na straně serveru poskytuje data pro přenos obrazu (pomocí RDPDD - *Microsoft Win32R application programing interface display driver*, který provádí snímání obrazovky – *capture* - a překládá ho do formy čitelné RDP protokolu převedením pomocí RDPWD), které balí do síťových paketů a posílá je klientovi. Klient data přijímá a převádí je na odpovídající informace pro Win32 GDI API (proto je tento protokol použitelný pouze pro platformu Windows).



Obr. 17, Schéma posílání obrazovek ze serveru na klienta [10]

Pro vstup dat jsou data z myši a z klávesnice posílána z klienta na server. Na serveru RDP se používá pro příjem dat od klienta vlastní virtuální ovladač klávesnice a myši.

Základní vlastnosti protokolu RDP v5

1. Šifrování dat

Bez šifrování dat z obrazovky, myši a klávesnice je velice jednoduché zachytit uživatelovo jméno a heslo. Obzvláště je to pak nebezpečné pro administrátora, který se přihlašuje na server po Internetu bez použití zabezpečeného přihlášení.

Protokol používá pro ochranu dat tzv. *scrambling*, který je nejvhodnější pro data obsahující obyčejný text. Všechny verze RDP používají šifru RC4 (více informací o šifře na *www.rsasecurity.com/rsalabs/faq/3-6-3.html*). Jedná se o proudovou šifru, která byla navržena pro efektivní šifrování malého množství dat variabilní délky. RC4 je vhodná pro zabezpečení komunikace po síti, používá se např. v protokolu SSL, kde zabezpečuje bezpečnou komunikaci mezi klientem a WEB serverem.

Ve Windows 2000 může administrátor zvolit, jestli data budou šifrována pomocí 56 nebo 128 bitovým klíčem. Šifrování je obousměrné, kromě nastavení bezpečnosti na "low", kdy jsou data šifrována pouze ve směru od klienta na server (chrání se tak citlivá data jako jsou hesla). Implicitní nastavení šifrování je "medium", kdy se používá 56 bitový klíč pro obousměrné šifrování dat. 128 bitový klíč může být nastaven a používán až po doinstalování *Windows 2000 High Encryption Pack*.

2. Redukce objemu dat

Protokol RDP podporuje několik mechanismů, jak redukovat množství dat přenášených po síti. V první řadě je to komprese dat (ta je doporučená jako implicitní volba pro všechny připojení přes terminálové služby), dále pak *bitmap caching*, *piktogram and fragments caching* v paměti RAM[2]. RDP5 přidává podporu perzistentního *bitmap chaching*, která vyžaduje tak cca 10 MB diskového prostoru na stanici. Tato data pak mohou být dostupná pro následující připojení.

3. Sdílené odpojení

Uživatel se může od běžící terminálové relace kdykoliv odpojit, aniž by se odhlašoval, případně pokud dojde k poruše na klientském počítači a jeho havárii, nepřijde o rozdělanou práci. Jakmile se uživatel přihlásí znovu ze stejného či jiného počítače, je automaticky připojen k minulé relaci a může pokračovat v rozdělané práci. Jestliže se uživatel znovu připojí pod jiným rozlišením obrazovky, RDP automaticky změní i rozlišení terminálové relace.

4. Mapování schránky

Uživatelé mohou vyjmout, kopírovat a vkládat text a grafiku mezi aplikacemi na lokálním počítači a aplikacemi, které běží na terminálových službách a mezi jednotlivými relacemi terminálových služeb.

5. Přesměrování tisku

Aplikace běžící na relaci terminálových služeb mohou automaticky tisknout na tiskárnu připojenou na lokální počítač.

6. Vzdálené ovládání

Obsluha tzv. helpdesku může prohlížet a ovládat jinou relaci terminálových služeb. Klávesové vstupy, pohyby myši a obrazovka jsou sdíleny mezi dvěmi TS relacemi a poskytují tak podporu uživateli, kterému pomohou diagnostikovat a vyřešit konfigurační problémy nebo poslouží k zacvičení uživatele na dálku. Tato volba je vhodná pro velké firmy nebo toho lze využít pro týmovou práci na společném úkolu.

Pro převzetí ovládání jiné TS relace lze na klientovi nastavit volbu povolení převzetí a sledování jeho relace. Jak bylo výše uvedeno, převzít TS relaci lze jen z jiné TS relace, nelze tak učinit z libovolného PC nebo z Windows 2000 Serveru (na rozdíl např. od aplikací jako je pcAnywhre, VNC apod.).

[2] Spíše než používání převodu fontů používá RDP piktogramy a fragmenty. *Piktogram* je bitmapa, která představuje jedno písmeno a informace o fontu. Např. písmeno „A“ v Times New Roman je reprezentováno jiným piktogramem než písmeno „A“ v Arialu. Použitím piktogramů je možno přesněji a kvalitněji zobrazovat text bez ohledu na fonty instalované na klientovi. Řetězec piktogramů se nazývá *fragment*. Piktogramy a fragmenty jsou uloženy lokálně na klientech, nedochází tak k zahlcování sítě daty, které se opakují.

7. Rozložení síťové zátěže

Protokol RDP přináší výhody funkce NLB (*Netwotk Load Balancing*), která je dostupná ve verzích Windows 2000 Advanced Server a Datacenter Server. NLB nabízí klientům terminálových služeb připojit se na skupinu serverů používajících terminálové služby. Je tak možno eliminovat možnost výpadku terminálových služeb a je možno rozložit zátěž na více serverů podle množství právě připojených uživatelů.

Rozdíl mezi *Netwotk Load Balancing* a *Cluster Service* je uveden v kapitole věnované instalaci serveru a jeho komponent (5.5.1.1).

6.4.3.2 POPIS PROTOKOLU CITRIX ICA

Druhým v pořadí je protokol ICA od firmy Citrix. Aktuální informace jsou na adrese [26].

Co je protokol ICA

Citrix Independent Protocol je prezentační protokol primárně určen pro Microsoft Windows. Koncepčně vychází z podobného protokolu použitého v systémech UNIX jako *X-Window* protokol. ICA dovoluje aplikacím běžet na aplikačním serveru, od klienta se přenášejí znaky z klávesnice a pohyby myší, na klienta pak změny obrazu. Důsledkem je pak malé zatížení klienta. ICA je postaven tak, aby dokázal fungovat na všech standardních síťových protokolech, jako je TCP/IP, NetBEUI, IPX/SPX, a PPP a na dalších síťových standardech nebo síťových architekturách jako je ISDN, Frame Relay a ATM.

ICA protokol je postaven na bázi *thin-client / server* architektuře, která umožňuje vysoký výkon aplikací i na velmi pomalých linkách o nízké propustnosti. Umožňuje používání jak 16-bitových tak 32-bitových aplikací jak na klasických PC, tak i na speciálních odlehčených zařízeních (NetPC, HandheldPC, Pocket PC apod.). Standardně ICA neobsahuje šifrování, je nutné protokol doplnit o šifrovací vrstvu resp. Citrix nabízí vlastní řešení pod názvem SecureICA. Toto řešení je založeno na bázi šifry 128bit Diffie-Hellman poskytující bezpečné posílání soukromých klíčů, během autentizace se používá 128bit šifrování. Data jsou pak šifrována náhodně generovanými 40, 56, 128 bit klíči šifry RC5.

Vlastnosti ICA protokolu

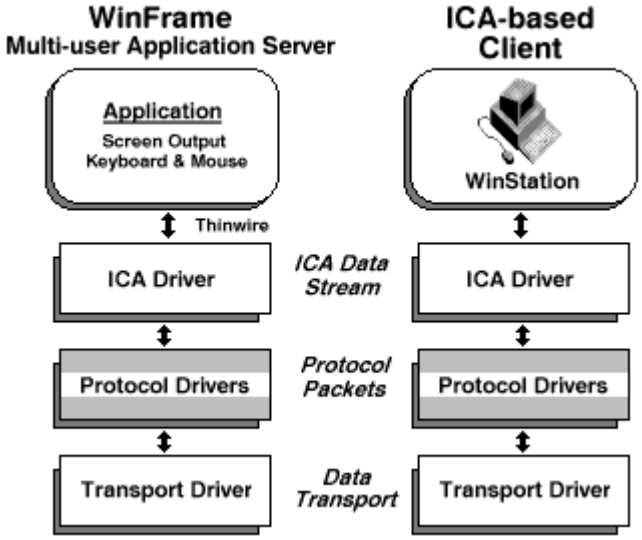
ICA je robustní rozšiřitelný protokol, který obsahuje následující vlastnosti:

- plnoobrazovkový textový režim
- zobrazování Windows GUI
- vstup klávesnice a myši
- kontrola relace (*session*)
- asynchronní a rámcové připojení
- detekce chyb a zotavení
- šifrování dat
- komprese dat
- přesměrování systému souborů
- přesměrování tiskáren
- vícenásobné virtuální kanály
- *cut* a *paste* mezi několika servery
- přesměrování COM portů

Jak ICA pracuje

ICA pracuje na fyzické úrovni při komunikaci mezi klientským PC (nebo jiným zařízením, které umí používat ICA protokol) a aplikačním serverem Citrix MetaFrame\WinFrame. *Thinwire* je název datového protokolu, který exportuje obrazovky aplikací. *Thinwire* je logický datový tok, který je přenášen zabalený do ICA paketů. *Thinwire* není fyzický protokol, neběží na fyzické vrstvě. Fyzický protokol ICA musí zabezpečit doručení datového proudu *Thinwire* bez chyb a bez ztráty či porušení dat.

Z pohledu aplikačního serveru WinFrame, hlavní devizou protokolu *Thinwire* je jeho začlenění do GDI a video driveru. Komponenta *Thinwire* je jako součást WinFrame začleněna do Win32 subsystému a dokáže tak optimalizovaně vykreslovat obrazové primitivy.



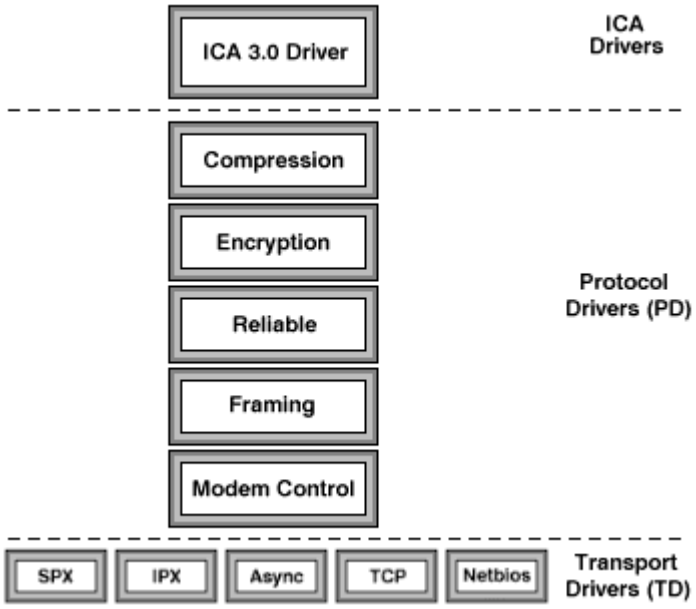
Obr. 18, Architektura Citrix WinFrame a ICA protokolu

Výstupem ovladače *Thinwire* je datový proud, který je posílán zpět po virtuálním API kanálu, který převezme datový proud a zabalí ho do ICA paketů. Jakmile je ICA paket zformován, je volitelně dále zpracován např. šifrováním, kompresí nebo rámcováním. Paket je předán transportní vrstvě a poslán klientovi. Jakmile dorazí ke klientovi, je proveden opačný postup a data jsou zobrazena na klientovi.

ICA protokol a transportní vrstvy

Pod datové pakety ICA je možno vložit mnoho volitelných ovladačů protokolových vrstev. ICA není závislá na těchto vrstvách. Ačkoliv tyto vrstvy leží pod ICA, mohou být vynechány nebo nahrazeny. Mohou být také dodány další ovladače pro jiné protokoly. Velké množství podporovaných protokolů předurčuje využití ICA protokolu pro práci s běžnými transportními technologiemi, jako TCP/IP, NetBIOS, IPX/SPX a PPP/SLIP, podporující skutečnou ICA nezávislost.

Zásobník ICA protokolu je dynamicky konfigurovatelný tak, aby vyhovoval všem typům protokolů. Např. IPX není spolehlivý, ale spolehlivý ovladač protokolu může být přidán nad transportní vrstvu IPX.



Obr. 19, Vrstvy ICA protokolu

Popis k obrázku:

- **Compression** - kompresní protokol může zabalit šifrované ICA pakety. Je systémově nahraditelný a není striktně definovaný v definici ICA protokolu
- **Encryption** - šifrovací protokol může zabalit šifrované ICA pakety a je také nahraditelný
- **Reliable** - je přenosový paketový protokol používaný k detekci chyb a k požadavkům ke znovuposlání dat. Tento protokol je používán ve spojení s ostatními transportními mechanismy, které neposkytují záruku doručení dat na místo určení
- **Framing** - je transportní paketový protokol používaný pro správu proudově orientované komunikace jako je TCP. Je používán ve spojení s ovladačem *Reliable* aby poskytoval bezchybný přenos dat.
- **Modem control** - je protokol, který dovoluje detekci a inicializaci modemu před jeho použitím

Rozšiřitelnost ICA protokolu

ICA je rozšiřitelný a flexibilní protokol. Za prvé, protokol podporuje různé schopnosti různých klientů. Dokáže spolupracovat jak s monochromatickými terminály tak s high-end pracovními stanicemi.

Z důvodu architektury virtuálních kanálů, ICA protokol může být rozšířen o nové datové typy jako je zvuk a video. Virtuální kanály dále podporují pomocná klientská zařízení například čtečky čárových kódů nebo skenery.

A konečně ICA protokol je možno rozšířit v jednotlivých vrstvách o podporu dalších protokolů. Např. šifrovací vrstva může být rozšířena o RSA nebo DES, dále konverze z ICA na X.11 nebo může být přidána podpora ATM.

6.4.3.3 SROVNÁNÍ PROTOKOLU MICROSOFT RDP5 S CITRIX ICA PROTOKOLEM

Není snadné provést srovnání těchto dvou protokolů. Oba mají společnou to, že jsou určeny ke stejnému účelu. Hlavní rozdíl pak je v tom, kde který protokol je vhodné použít. Základní srovnání parametrů těchto protokolů ukazuje tabulka v příloze A.1. Jsou zde srovnány vlastnosti Windows 2000 Terminal Services (používají RDP protokol) a Citrix MetaFrame (používající ICA protokol). Již první část tabulky ukazuje základní rozdíl – ICA protokol podporuje mnohem větší množství operačních systémů. To je oproti RDP velká výhoda a z toho plyne určení protokolu ICA – použít ho tam, kde máme síť založenou na různých operačních systémech od Microsoft Windows přes Apple až po různé klony systému UNIX. To samé pak platí pro HW platformy, kdy RDP prakticky podporuje jen zařízení PC a Handheld PC (včetně Pocket PC). ICA je opět vhodný do heterogenního prostředí, vynikající pak pro budování sítě založené na terminálech. ICA klient je možno zabudovat do internetového prohlížeče (pro RDP je tato možnost až na klientu od firmy HOB Electronic). Omezenost RDP protokolu na Windows API se tak projevuje v neschopnosti pokrýt nároky celé struktury sítě.

V další části tabulky jsou sice jasně zdůrazněné výhody ICA protokolu vůči RDP, ale nejsou již tak jednoznačné. ICA protokol podporuje přenos datově náročných multimediálních aplikací. Jedná se především o přenos stereo zvuku a videa. Opět zde platí pravidlo, pokud toto nepotřebujeme, tak není použití protokolu ICA podmínkou.

Podpora více transportních protokolů je vlastní ICA protokolu, nicméně moderní sítě jsou již stavěné převážně na TCP/IP a tak se opět hodí tam, kde je velká variabilita sítě, případně na staré sítě založené na protokolu IPX/SPX firmy Novell.

ICA protokol lze použít i pro připojení přes sériový kabel, což může být vhodné pro připojení notebooku k serveru bez instalace síťové karty na přenosný počítač (typicky staré počítače, které nemají slot pro PC Card). Je tak možné provozovat nové a náročné aplikace na počítači, který by výkonově na provoz nestačil.

Z dalších vlastností zbývá jen větší podpora spolupráce mezi servery v případě nasazení MetaFrame\WinFrame, především o kvalitní způsob vyrovnávání zátěže, sdílení aplikací mezi servery, automatická aktualizace klientů a další.

ICA protokol je mnohem otevřenějším. Je možno do něj doplňovat vrstvy, rozšiřovat zabezpečení a celkově ho přizpůsobit konkrétním podmínkám. RDP protokol je ale mnohem rychlejší právě proto, že je podporován přímo jádrem operačního systému. Navíc je zadarmo, neboť je součástí operačního systému. Pokud chcete provozovat ICA protokol, je potřeba zakoupit WinFrame nebo MetaFrame Server pro Windows 2000 Server. Náklady na pořízení serveru jsou řádově ve statisících + náklady na licence pro jednotlivé klienty.

Jaký z toho plyne závěr? RDP protokol použít všude tam, kde máme stanice založené na operačních systémech Microsoft Windows a přenosovém protokolu TCP/IP, kdy se jedná o počítače, které nejsou na HW výkonnosti potřebné pro provoz nových a moderních aplikací. Je tak možno provozovat jednotné prostředí pro všechny uživatele sítě, jednoduchou správu aplikací a dostatečný výkon. (za podmínky dostatečné výkonnosti serverů). ICA protokol je ideální pro nasazení v hetergonním protředí jak HW platforem, tak operačních systémů a přenosových protokolů. Vhodný pro přenos velkého objemu dat i na pomalých modemových spojích, kvůli své dobré škálovatelnosti vhodný do různých prostředí s možností přizpůsobení na míru. Pokud nevíme, jaké klienty v budoucnosti budeme používat, nebo chceme budovat terminálovou síť, není vhodnější volby než ICA protokol. Navíc klient nepotřebuje

hostitelský operační systém a je tak možno jej použít na bezdiskových stanicích (narozdíl od RDP).

6.4.3.4 DALŠÍ PROTOKOLY PRO VZDÁLENOU PRÁCI SE SYSTÉMY

Nakonec uvádím další protokoly, které se používají na jiných operačních systémech a platformách. [19]

X PROTOCOL

Tento protokol je založen na protokolu IP, obsahuje 2 vrstvy - první adaptační vrstva je závislá na zařízení, druhá je nezávislá reprezentační vrstva. Neobsahuje žádné optimalizační rutiny ani sofistikovanou kompresi dat, je tedy nevhodný pro použití přes modemové připojení. Používá se ve spojení X Server na UNIXU pro terminálové relace (X.11). Jako šifrování se používá např. DES nebo Kerberos 5.

XDM Comunication Protocol (XDMCP)

Tento protokol se používá při logování uživatelů na X-Server v UNIXu

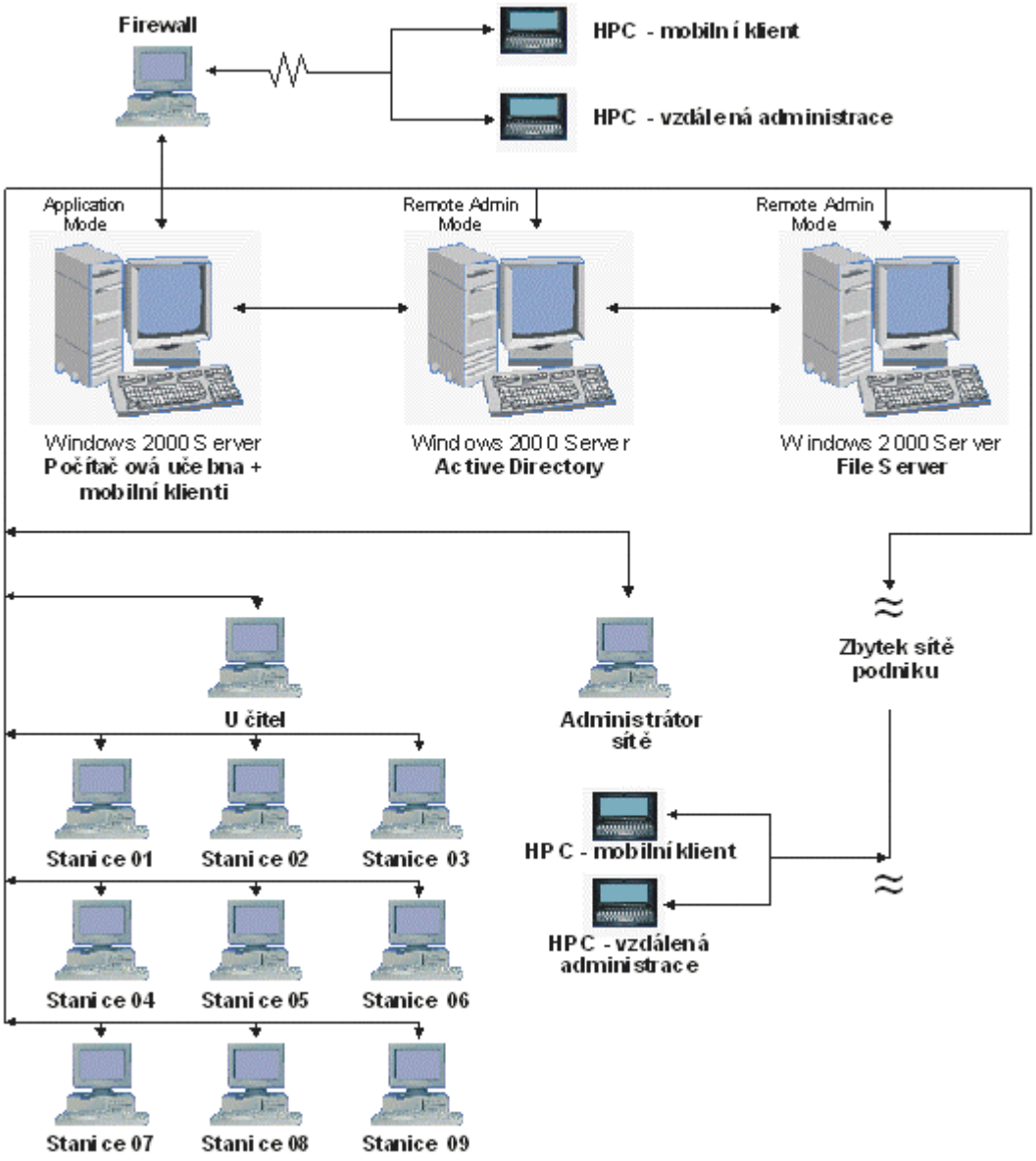
Remote FrameBuffer Protocol (RFB)

Je to jednoduchý protokol pro vzdálené grafické uživatelské rozhraní, který je nezávislý na platformě a pracuje na úrovni framebufferu. Server a viewer jsou dostupné pro většinu běžných operačních systémů. Konceptuálně se jedná o bezstavový protokol tj. klient se může kdykoliv odhlásit a znovu přihlásit a najde desktop takový, jaký ho zanechal.

RFB běží nad TCP/IP, ale je možno použít i jiný protokol. Dále nabízí několik možností, jak přenést obsah framebufferu ze serveru na klienta - na začátku spojení se použije jednoduchý přenos bez kódování a komprimace obsahu čtverců, dále lze použít různé druhy komprese a různé druhy optimalizačních technologií. Update framebufferu probíhá na základě požadavku klienta a ne jako proud dat. Šifrování probíhá pouze při autentizaci na základě DES, data lze posílat šifrovaně za použití SSL.

6.5 PRAKTICKÉ NASAZENÍ TERMINÁLOVÝCH SLUŽEB V PRAXI

Jak bylo uvedeno již v úvodu věnovaném popisu TS, TS umožňují běh ve dvou základních módech. Proto jsem se v praktické části zaměřil na použití obou těchto módů. Pro všechny uvedené příklady jsem použil podporu protokolu RDP, protokol ICA jsem vzhledem k nedostupnosti Citrix MetaFrame netestoval.



Obr. 20, Schéma praktického nasazení terminálových služeb v praxi

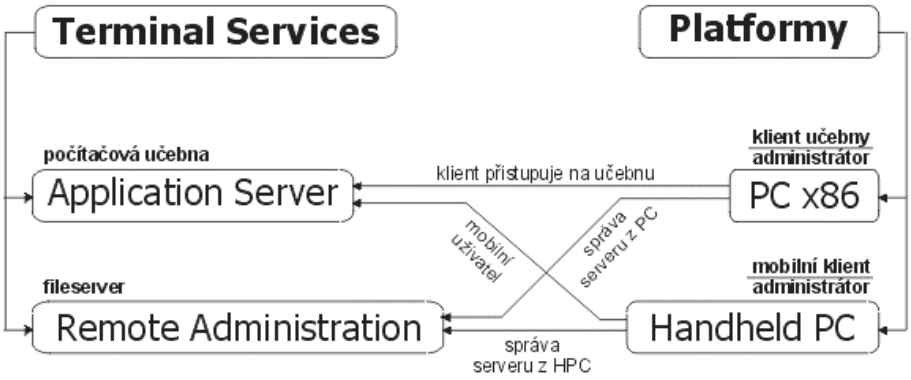
První část je použití aplikačního módu (*Application Server*). Jedná se o vytvoření počítačové učebny s devíti stanicemi plus jeden školitelský počítač ve školícím středisku firmy. V této učebně probíhá výuka použití software firmy a školení produktu Microsoft Offfice 2000 (viz obr. 19).

Stanice jsou připojeny na vyhrazený server. Ten dále slouží k připojení mobilních pracovníků pomocí přenosných zařízení s WCE přes lokální síť a síť Internet a umožňuje využít tak nejen aplikace, které nejsou na WCE (Microsoft Office 2000), ale i prohlédnout si poštu a zpracovat aktuální dokumentaci a pracovat na svém prostředí, i když jsou daleko od svého pevného pracoviště.

Výhody řešení učebny tímto způsobem jsou následující:

- nová verze školeného produktu nemusí být aktualizována na všech stanicích
- je možno jednoduše nainstalovat další aplikace potřebné pro školení uživatelů
- pokud by byly školené aplikace instalovány na každou stanici, musela by být učebna po každém školení přeinstalována, aby další školení probíhalo za stejných podmínek
- školitel může převzít ovládání stanice ze svého školitelského počítače a pomoci uživateli, aniž by musel být fyzicky přítomen u uživatele. Může tak promítat na projektor nejenom svůj výklad, ale i ukázat ostatním způsob řešení problémů
- snadná nastavitelnost a udržovatelnost jednotného prostředí všech stanic, ochrana před smazáním důležitých souborů
- jelikož klient TS běží na hostitelském OS, je proveden image disku, který je uložen na serveru a v případě nefunkčnosti hostitelského systému je z tohoto image pomocí bootovací diskety během několika minut stav stanice obnoven do původního stavu.

Druhá část se zabývá administračním módem (*Remote Administration)*. Jedná se o běžný fileserver, který bude spravován administrátorem z jeho stanice resp. bude spravován z mobilního zařízení během jeho nepřítomnosti buď na pracovišti přes Internet nebo z kteréhokoliv místnosti na pracovišti pouhým připojením mobilního zařízení do počítačové sítě (viz obr. 19).



Obr. 21, Schéma využití aplikačního a administrátorského módu

Pro obě modelové situace jsem použil server s následující konfigurací: Procesor AMD Thunderbird 1.2 GHz, deska Abit KT7A, paměť 1GB SDRAM 133 MHz, Ultra SCSI disk Seagate ST336704FC Cheetah 36LP 36.7GB, SCSI řadič Adaptec ASC-39160, 2x síťová karta pro slot PCI 3COM 3C980C. Windows 2000 Server, pro použití bylo zakoupeno 14 licencí na TS (10 pro počítačovou učebnu plus čtyři pro připojení WCE klientů).

Klientské stanice pro počítačovou učebnu jsou v následující konfiguraci: procesor AMD K6-2 300 MHz, deska FIC VA503+, 64MB SDRAM 100 MHz, IDE disk Western Digital 4 GB, síťová karta Realtek RTL 8029(AS). Nainstalován je operační systém Windows 98 v české verzi.

Mobilní zařízení jsou v následující konfiguraci: Casio Cassiopeia A20, procesor SH3 80 MHz, 8MB RAM, síťová karta EP-4000A Ethernet PCMCIA PC Card. Operační systém je Windows CE 2.0

Administrátorská stanice je v následující konfiguraci: procesor AMD Duron 850 MHz, deska Microstar MSI MK7A, paměť 128 MB SDRAM 133 MHz, IDE disk IBM 20 GB, síťová karta Realtek RTL 8029(AS). Instalován je operační systém Windows 2000 Professional v anglické verzi.

6.5.1 PŘÍPRAVA SERVERU

Před vlastním použitím TS je potřeba provést důkladnou analýzu problému, který chceme řešit. Je potřeba vědět, kolik bude maximálně současně připojených klientů, v jakém módu bude server běžet, jaké aplikace se budou používat. Detailní postupy pro přípravu a realizaci lze nalézt na [11].

V mém případě je výsledkem analýzy výše uvedená konfigurace serveru, která by měla stačit pro provoz učebny i mobilních klientů. Používané aplikace jsou uvedeny v části věnované přípravě a instalaci klientských stanic.

Prvním krokem k instalaci terminálových služeb je instalace *License Serveru* na *Domain Controler*. Server pro sledování licencí musí být nainstalován na Windows 2000 Server a to i v případě, že ve skupině serverů je počítač s Windows NT 4.0. Windows 2000 Server musí být nastaven jako *Domain Controler*.

Pokud se pro přístup do interní sítě používá zabezpečení přes *firewall* nebo přes *router*, které filtrují příchozí pakety do sítě, je třeba nastavit tyto zařízení tak, aby nebránila TS komunikovat s klienty. Jedná se především o blokování TCP/IP portu *3389*, který používá protokol RDP. Při použití přístupu na TS přes Internet je třeba si ověřit, zda použitý *firewall* pracuje na *paketové* nebo na *aplikační* úrovni. Pokud pracuje na *paketové* úrovni, je jednoduché ho nakonfigurovat pro používání nového protokolu, v tomto případě RDP. Pokud pracuje na *aplikační* úrovni, je potřeba u výrobce zajistit filter pro protokol RDP.

Klienti se připojují pomocí TCP/IP. Připojení může probíhat jak po dial-up lince, tak po LAN, WAN, nebo VPN síti. Je třeba si dobře naplánovat, kolik klientů se bude připojovat po jakém připojení. Pokud se jeden uživatel bude připojovat po lince 28,8 kb, tak připojení bude plynulé. Pokud ovšem bude linka sdílena mezi 100 uživatelů, její kapacita nebude stačit.

Před přípravou musíme sepsat HW klientských stanic, které se budou připojovat na TS (CPU, OS, prostor na HDD, RAM a video). Z tohoto seznamu je třeba vyloučit stanice, které nevyhovují minimálním požadavkům na realizaci TS klienta.

Je třeba sestavit soupis aplikací, které budou provozovány na TS. Některé aplikace nejsou přizpůsobeny pro běh na TS a je třeba je ze seznamu vyřadit nebo nahradit jejich novějšími verzemi. Pokud je nutné používat tyto aplikace, je vhodné informovat jejich uživatele o tom, že je musí provozovat lokálně. Jedná se především o aplikace, které pracují se skenery nebo čtečkami čárových kódů. Tato zařízení nejsou RDP klientem rozpoznány a pod TS klientem nepracují správně. Následně je třeba vyloučit aplikace, které jsou multimediální resp. mají náročný grafický výstup, který se často mění - typicky se jedná o přehrávání videa nebo počítačové hry. Potom je vhodné prověřit aplikace, které vyžadují speciální instalaci nebo spouštěcí skripty. Příkladem může být např. MS Windows Installer Technology, která nemůže být na TS použita, pokud uživatel není zároveň administrátorem systému.

6.5.1.1 INSTALACE SERVERU A JEHO KOMPONENT

Po provedení identifikace potřeb se provede inventarizace vhodného HW pro běh TS klientů a sestaví se seznam aplikací, které se budou používat na TS a přejde se k vlastní realizaci. Obrazová dokumentace postupu instalace je v příloze B.1 a na CD příloze. Pro další informace doporučuji podrobný scénář na [9] a [21].

A. Instalace a nastavení License Serveru (LS)

LS je nutný pro provozování TS v aplikačním módu. Jedná se o službu, která shromažďuje zakoupené klientské licence a kontroluje jejich správné použití. LS musí být aktivován přes službu *Microsoft Clearinghouse*. LS je spouštěn pouze při dotazu z TS na obdržení nové licence a je potřeba jej administrovat pouze pro obdržení nových licencí z *Microsoft Clearinghouse*.

Je doporučováno nainstalovat LS na jiný počítač, než na který je nainstalován TS. Existují dva typy LS - *domain* a *enterprise*. Před instalací LS je třeba se rozhodnout, který typ se bude používat:

- **domain license server** je vhodný tam, kde je třeba použít jeden LS na doménu, především ve spojení se sítí, která obsahuje Windows NT 4.0 Server. Tento model lze nainstalovat při instalaci Windows 2000 Server
- **enterprise license server** poskytuje svoje služby kterékoliv doméně v hnízdě (*site*), domény ale musí být spravovány Windows 2000 Serverem. Vhodný je tam, kde je více domén. Tento model není možno nainstalovat při instalaci Windows 2000 Server, ale později přes volbu *Add/Remove programs*.

Vřele je doporučováno instalovat LS na počítač, který má přístup na Internet, neboť licence je získána z *Microsoft Clearinghouse* právě touto cestou a je uložena právě na LS. Při reinstalaci LS je třeba opětovného připojení k *Microsoft Clearinghouse*[3].

1. Aktivace LS

Aby mohl LS poskytovat licence pro klienty na TS, je třeba provést aktivaci LS pomocí *Licensing wizard*. Existují 4 metody aktivace – přes Internet, WEB aplikace, FAX či telefonicky. Přes Internet se jedná o nejrychlejší a nejlehčí metodu. Po aktivaci licence server obdrží digitální certifikát o vlastnictví licencí. LS použije tuto licenci pro získání požadovaného počtu licencí na TS.

2. Instalace licencí

Závisí na způsobu získání licencí Windows 2000:

- **Licence pořízené přes Microsoft Select** - budete dotázání na *Enrolment Agreement Number*
- **Microsoft Open License** - budete dotázáni na *Open License and Authorization Number*
- **Microsoft License Pack** - 25 písmenný *License Code*

[3] Pozn: License Server musí být zprovozněn do 90-ti dnů od zprovoznění Windows 2000 Terminal Services. Pokud do této doby nebude zprovozněn LS, přestane TS fungovat (resp. při každém připojení klienta bude hlásit, že licence již vypršela). Toto opatření je provedeno proto, aby administrátor měl čas na konfiguraci, nastavení a odzkoušení TS. Poté, co má systém odladěn, zaplatí licence na provoz.

Po instalaci licencí bude 90-ti denní licence nahrazena *Terminal Services Client Access Licence* při prvním přihlášení klienta na TS. Při překročení klientů připojených na TS, dojde k uložení upozornění do *Event Viewer* (system log) s požadavkem na dokoupení dalších licencí.

3. Zálohování LS

Je důležité po instalaci a zprovoznění LS provést jeho zálohu a to jak systému samotného, tak především adresáře *Lserver*, který se nachází v adresáři *%windir%/system32/Lserver*. Pro opětovné obnovení ze zálohy je třeba, aby byl LS spuštěn. Pokud by záloha byla obnovena na jiný LS, tak budou obnoveny pouze historické a nikoliv aktivní licence.

B. Příprava sítě na terminálové služby

Při vytváření síťové infrastruktury je třeba přihlédnout k některým zvláštnostem, které jsou vyžadovány TS. TS nemohou posílat aplikacím informaci o IP klientského zařízení. Víceuživatelské aplikace, které vyžadují znalost jedineční IP adresy klienta, nebudou na TS pracovat, protože každý klient bude posílat informaci o IP adrese, kterou má TS. Příkladem jsou například firewally, které používají IP adresu k identifikaci polohy klienta a jeho zabezpečení.

1. Vyrovnávání síťové zátěže a TS

Network Load Balancing (NLB) se používá pro rozdělení práce na dva a více serverů. NLB představuje skupinu serverů s jednou virtuální IP adresou, která poskytuje mechanismus dynamického rozdělování zátěže. Tato metoda je vhodná tam, kde se připojuje velké množství uživatelů a/nebo kde je kladen důraz na 100 procentní dostupnost dat.

Protože TS se nedají používat ve spojení do klastru je NLB jedinou možností, jak poskytovat kvalitně služby pro velké množství uživatelů. V této souvislosti je vhodné uvést rozdíl mezi *Netwotk Load Balancing* a *Cluster Service*.

- *Netwotk Load Balancing* je rozložení síťové zátěže a z hlediska TS klienta to znamená, že se uživatel připojí na nejbližší server. Pokud dojde k výpadku serveru, je automaticky přepojen na jiný nejbližší. Vždy se tedy jedná o připojení na nejbližší server. Je nutné, aby všechny servery měli stejné aplikace a definovány stejné uživatele.
- *Cluster Service* představuje několik serverů spojených dohromady, které vystupují pod jednou IP adresou a jedním DNS jménem. Při práci s aplikacemi dochází k rozložení zátěže na procesory, paměť a disky mezi jednotlivé servery. Terminálové služby Windows 2000 *Cluster Service* nepodporují, protože TS neposílají IP adresu jednotlivých klientských počítačů aplikacím, což služba *Cluster Service* vyžaduje. Toto je velká nevýhoda oproti konkurenčnímu řešení firmy Citrix, neboť nelze servery spojovat do farem pod jedno DNS jméno.

2. Naplánování a vytvoření doménové struktury

TS je třeba vhodně zakomponovat do doménové struktury sítě. Existují tři způsoby, jak to provést:

- **Struktura sítě bez domén** - uživatelé potřebují zvlášť účty na každý Windows 2000 Server s *Terminal Services*. Je tím omezeno rozšiřování a špatně se tento způsob administruje

- **Implemetace TS do existující Windows NT 4.0 doménové struktury** - tato volba umožňuje plné využití služeb TS, ale je potřeba stávající databázi *Security Account Manager* (SAM) doplnit o dodatečné informace potřebné pro TS (podrobnosti o nastavení je možno najít ve Windows 2000 Server Resource Kit [22])
- **Zapojení do struktury *Active Directory*** (AD) – Windows 2000 Server obsahují plnou podporu TS v AD - podpora tisíců uživatelů v databázi, podpora skupinové politiky (*Group Policy)*. V AD je doporučeno vložit TS do samostatné organizační jednotky (OU – *Organisation Unit*) odděleně od ostatních počítačů a uživatelů. Tato OU by měla obsahovat pouze počítače určené pro provoz TS.

3. Použití Windows 2000 *User Profiles* nebo *Roaming User Profiles*

Profil představuje konfiguraci Windows 2000 pro jednotlivého uživatele, obsahující nastavení prostředí a nastavení systému - instalované aplikace, barvy, ikony, desktop, start menu. Pro TS je možno definovat vlastní profil uživatele jako *Terminal Services Profile*. Samozřejmě je možno použít stávající uživatelův profil, nicméně se může hodit pro TS některá nastavení změnit. Při připojení klienta probíhá načtení profilů v tomto pořadí:

- uživatelův Terminal Services Profile
- uživatelův Windows 2000 Roaming Profile
- uživatelův Windows 2000 Profile

Roaming profiles umožňují uživatelům přecházet z jednoho počítače na druhý a mít přístup ke svým nastavením a ke svému prostředí.

4. Skupinová politika (*Group Policy*)

Je efektivní mechanismus jak spravovat a nastavovat chování TS na síťovém prostředí. Pomocí skupinové politiky lze nastavit hodnoty registrační databáze a přístupová práva k souborům, která jsou společně definována v AD, doméně nebo v organizační jednotce[4]. Skupinová politika je založena na základní funkcionalitě registry tj. obsahuje bezpečnostní nastavení, instalaci software, logon / logoff a startup / shutdown skripty, zabezpečení souborů a přesměrování speciálních adresářů (desktop, start menu apod.).

Skupinová politika je velmi obsáhlé téma, odkazuji proto na dostupnou literaturu [12] a [13].

5. Přístup k aplikacím

Administrátor může řídit přístup k aplikacím na TS dvojím způsobem:

- **Mandatory Profiles** – je profil specifikující, které aplikace jsou viditelné pro uživatele
- **System Policies** - politika zabraňující uživateli spustit aplikaci přes Windows Explorer nebo přes příkaz Run. Politika je založena na doménách tj. při přihlášení se spojí politika na doméně s lokální politikou.

[4] Skupinovou politiku lze používat pouze tehdy, pokud je na síti instalován server s Active Directory. Způsob používaný na Windows NT 4.0 pomocí souboru config.pol vytvořeného nástrojem Police Editor nebude na Windows 2000 Serveru fungovat.

6. Domácí adresáře uživatelů

Je vhodné pro každého TS uživatele vytvořit domácí adresář, neboť některé aplikace si musí ukládat specifické informace pro daného uživatele. Můžeme vytvořit například adresář *Homedirs* a nastavit mu přístupová práva *Everyone*. Pak jako domácí adresář nastavit např. *p:/homedirs/%username%*. TS automaticky vytvoří adresář se jménem uživatele a nastaví přístupová práva pro uživatele. Tj. uživatel má plný přístup, administrátor může data do adresáře kopírovat, nesmí je však mazat a číst. Doporučuji uživateli na tento domovský adresář přiřadit písmeno, protože instalační skripty vyžadují znát, kam se program instaluje.

7. Plánování zabezpečení

Naplánovat zabezpečení je nedílnou součástí plánu na zavedení TS. Pro používání TS je více než nutné použít NTFS než FAT a to na všech oddílech disku. FAT nenabízí žádné zabezpečení souborů a není možno nastavit diskové kvóty pro uživatele. Částečný popis NTFS jsem uvedl v kapitole 4.4, podrobný je v [17].

TS jsou dodávány s přednastavenými uživatelskými právy, které je možno upravit či přidělit další práva. Aby se uživatel mohl na TS přihlásit, musí mít právo lokálního přihlášení na server. Je proto vhodné dát uživatele do *Users Local Group*, která je založena TS.

Členové administrátorské skupiny na TS mají kontrolu nad přístupem uživatelů, nad jejich právy a nad aplikacemi, které mohou spouštět. Mají tedy stejná práva, jako lokální správce Windows 2000 Serveru a další rozšířená práva:

- **Server Management** - pomocí *Terminal Services Configuration Tool* mohou nastavit uživatelská omezení, odpojit uživatele atd.
- **User Control** - nastavení uživatelských práv na TS, nastavení profilu
- **Session Control** - monitoring aktivních uživatelů, relací a procesů, připojení k aktivní relace a násilné ukončení relace
- **Application install** - pouze administrátor může instalovat aplikace

8. Automatické přihlášení (*Auto-logon procedure)*

Pokud uživatel TS pracuje např. jen s jednou aplikací (např. databáze), je možné specifikovat pomocí *Client Connection Manager* aplikaci, která se automaticky spustí po přihlášení uživatele na TS.

Dále je vhodné nastavit připojení klienta tak, že nemusí zadávat svoje jméno a heslo. Tuto vlastnost je rozumné používat s velkou obezřetností a používat ji tam, kde je to nutné např. pokud aplikace vyžaduje specifické heslo zadané při přihlášení. Je třeba myslet na to, že Windows 2000 nabízejí tzv. *secondary logon*, který umožňuje uživateli spustit aplikaci pod jiným uživatelským kontextem (provádí se pomocí funkce *runas*).

9. Editace specifických nastavení uživatele

Když se uživatel přihlásí do systému, je proveden přihlašovací skript *UsrLogon.cmd* v adresáři *System32*, který nastaví uživatelské prostředí.

10. Změna přihlašovacího procesu

V přihlašovacím skriptu jsou obsaženy dvě proměnné typické pro TS - *%CLIENTNAME%* a *%SESSIONNAME%* Tyto proměnné jsou nutné, aby v přihlašovacím skriptu byly pro spuštění a správnou funkci např. antivirového programu.

C. Zabezpečení přenosu dat šifrováním

Přenos dat mezi klientem a TS může být šifrován jedním ze tří způsobů:

1. Low encryption - pro přenos dat z klienta se používá algoritmus RC4 s 56ti bitovým klíčem. Data ze serveru pro klienta nejsou šifrována. Tato ochrana slouží především pro bezpečný přenos citlivých dat jako je heslo a aplikační data.

2. Medium encryption – přenos je oboustranně šifrován pomocí algoritmu RC4 s 56ti bitovým klíčem.

3. High encryption - přenos je oboustranně šifrován pomocí algoritmu RC4 se 128mi bitovým klíčem.

6.5.1.2 NASTAVENÍ SERVERU, LICENCOVÁNÍ

Nyní se budu věnovat popisu nastavení serveru a dalším otázkám přípravy TS, především způsobu licencování klientů.

1. Nastavení serveru

Rád bych zdůraznil, že pro nejlepší provozování a nastavení klientů je třeba, aby na síti existovala **Active Directory**, která podporuje **Group Policy**. Group Policy se nastavuje tak, že se nainstaluje do MMC snap-in - nastaví se desktop konfigurace pro skupinu uživatelů nebo pro uživatele. Nastavení Group Policy je obsaženo v Group Policy Object (GPO) a je ve spojení s objektem v AD (site, domain, OU). Ve Windows NT 4.0 se používal *System Police Editor*, který sloužil k úpravě informací uložených v registry. Můžeme ho používat, ale jen pro zpětnou kompatibilitu s Windows NT. Na Windows 2000 nemají nastavení vliv. Nastavení je zvlášť pro uživatele (vše je vázáno na uživatele - tedy chování operačního systému, aplikací, desktopu, logon a logoff skriptů, přesměrování adresářů - vše se nastaví při přihlášení uživatele na počítači) a zvlášť pro počítače (chování operačního systému, chování desktopu, nastavení aplikací, bezpečnostního nastavení, spouštěcích a ukončovacích skriptů - vše se nastaví při inicializaci operačního systému).

Nejprve se vytvoří jednotliví uživatelé v AD, každý uživatel má práva lokálního přihlášení pro přístup na TS. Jak bylo uvedeno v předchozí kapitole, je potřeba vytvořit domácí adresáře uživatelů a adresáře pro jejich profily. Pak je vhodné se připojit na své lokální stanici jako zvláštní uživatel a začít vytvářet jednotlivé nastavení start menu a pracovní plochy tak, že příslušné adresáře *Start menu* a *Desktop* uživatele nakopírujeme do adresáře profilů jednotlivých uživatelů.

Pak již můžeme přistoupit ke konfiguraci TS, obrazová dokumentace postupu je zobrazena v příloze B.2 a na CD příloze.

TS se dodávají jako *Windows 2000 MultiLanguage Version*, tj. podporují instalaci a konfiguraci **vícejazyčného** uživatelského prostředí. Nastavení jazykového prostředí se provádí pomocí *Group Policy*. Uživatel si pak vybere nastavení jazyka v *Regional Options* v *Control Panel*. Informace je uložena v *Roaming Profile*.

Pro **nastavení tiskáren** máme několik možností: tiskárny mohou být připojeny *lokálně* na server přes paralelní port nebo *síťově*. Automaticky jsou dostupné všem TS klientům. Tiskárny ovšem mohou být připojeny *lokálně* na klientské stanice, TS provede automatické přesměrování tisku na lokální port.

Přesměrování tisku může být dvojího druhu - *automatické* a *manuální*. Automatické přesměrování je podporováno všemi Win32 klient platformami (Win9.x, NT). Když se klient přihlásí do TS, lokální tiskárny připojené na LPT, COM a USB

jsou automaticky detekovány a jsou vytvořeny patřičné tiskové fronty. Když se uživatel odhlásí, tisková fronta je smazána a všechny probíhající i připravené tisky jsou zrušeny.

Manuální přesměrování je nutné u klientů WfW 3.11 a WBT klientů. V tomto případě je tiskárna manuálně přidána pomocí *Add Printers wizard* v *Control Panel*. Jméno klientského počítače je použito pro výběr portu. Přesměrování tisku je pak provedeno buď pomocí *Terminal Services Connection Configuration* (pro připojení per-connection), nebo pomocí AD *Users and Computers* nebo *Local Users and Computers* (pro připojení per-user).

Sdílené síťové tiskárny, tak jako lokální disky sdílené pomocí *net share*, umožňují uživatelům přístup na tiskárny vzdáleně ze serveru. Pokud je tiskárna lokální a má nainstalovanou síťovou kartu, není tato tiskárna následně dostupná lokálně. Lokální tiskárny sdílené na TS klientech nejsou dostupné všem klientům, ale jen lokálně. Tiskárny jsou definovány jako per-user a protože jsou definovány pro určitého uživatele, jsou dostupné pouze pro něj v průběhu jeho session. Tato metoda je vhodná pouze pro WfW. Uživatelé WBT nemohou používat lokální tiskárny sdílné touto metodou.

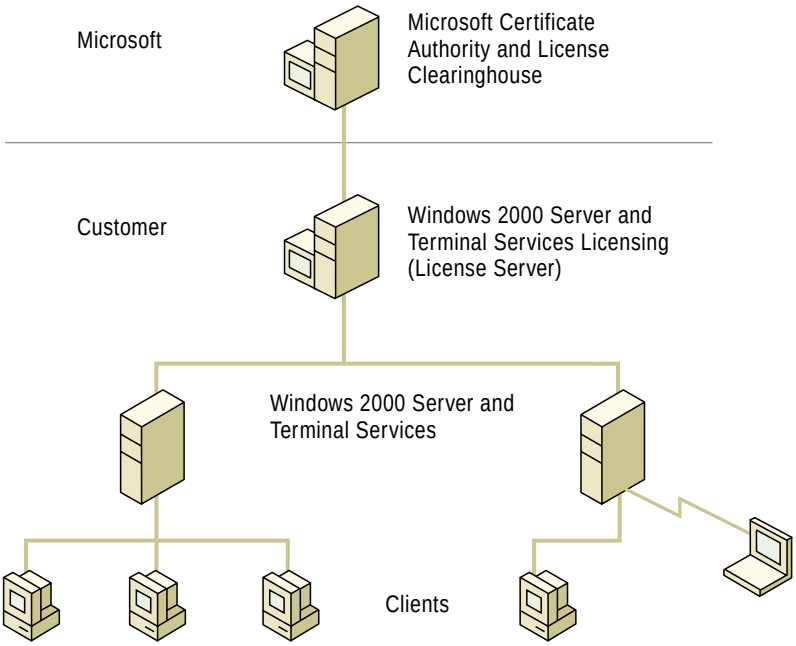
Pro tisk přes WAN a Dial-up připojení si musíme uvědomit, jaká je propustnost přenosových cest, neboť tisková fronta může být rozsáhlá a pokud jich bude hodně, může dojít k zahlcení linky. Je třeba minimalizovat velikost grafiky, barevný tisk apod.

2. Licencování

Pro provozování aplikačního módu je třeba licenčního serveru. Každá klientská stanice musí mít vlastní *Terminal Services Client Access Licence*. TS má vlastní metodu pro licencování klientů, která je odlišná od licencování Windows 2000 Server klientů. Jsou to tyto metody:

- **Microsoft Clearinghouse**
  Jedná se o databázi Microsoftu, která obsahuje všechny aktivované licence serverů a klientů. Lze se na ní připojit pomocí Licensing Wizardu.
- **Licence server**
  Ukládá všechny TS klientské licence. které byly nainstalovány na TS. TS se musí nejdříve připojit k Licence serveru, než se připojí klienti. Jeden LS obslouží více TS.
- **Terminal Server**
  Poskytuje přístup pro klienty na bázi Windows. Při připojení klienta si ověří klientskou licenci. Pokud klient licenci nemá, TS si vyžádá licenci na Licence serveru.
- **Klientská licence**
  Každý klient, který chce používat TS, musí mít vlastní licenci. Je uchovávaná lokálně a posílaná na TS vždy při připojení. Server si ověří licenci a umožní přístup.

Následující obrázek ukazuje využití výše uvedených licencí:



Obr. 22, Schéma fungování licenční politiky terminálových služeb

Existují další dodatečné licence:

- **Windows 2000 Terminal Services Internet Connector Licence**
  Umožňuje maximálně 200 konkurenčních uživatelů, kteří se mohou anonymně připojit po Internetu na TS. Toto je vhodné pro organizace, které chtějí demonstrovat Windows aplikace pro uživatele WEBu a nechtějí aplikace přepisovat na WEB aplikace.
- **Work at Home Windows 2000 Terminal Services Client Access Licence**
  Určena pro organizace, jejíž zaměstnanci pracují doma a chtějí jim zpřístupnit firemní aplikace.

Podrobnější informace o licenční politice aplikované na terminálové služby je možno nalézt v [9] a v [21].

6.5.1.3 INSTALACE APLIKACÍ

Instalace aplikací na terminálové služby probíhá trochu odlišným způsobem než tradiční instalace. Samozřejmě jen v tom případě, že TS server běží v aplikačním módu. Při pokusu o spuštění instalace pomocí např. *setup.exe* nebo *install.exe*, nedojde ke spuštění, ale k zastavení tohoto procesu s výzvou a popisem, jak aplikaci nainstalovat. Většina kvalitních aplikací má na instalačním CD skript pro instalaci na terminálové služby. Před koupí SW je potřeba se u výrobce přesvědčit o tom, že daná aplikace spolehlivě funguje pod TS. Bližší informace o instalaci a provozu aplikací na TS lze najít v [8], [14] a [22].

Způsoby, jak aplikaci na TS nainstalovat, jsou v zásadě dva, i když princip je stejný, způsob realizace je odlišný. První způsob je ruční, druhý automatický. V zásadě se jedná o to, že musíme TS přepnout do instalačního režimu, provést instalaci a po instalaci přepnout TS zpět do aplikačního režimu.

Při ručním způsobu provedeme přepnutí do instalačního režimu z příkazové řádky (příkaz *change user /install*). Poté můžeme spustit instalaci a nainstalovat potřebné aplikace. Pomocí příkazu *change user /execute* provedeme přepnutí TS zpět do aplikačního režimu. Výhodu tohoto způsobu je možnost nainstalování většího množství aplikací najednou tedy při počáteční konfiguraci a instalaci TS.

Druhý způsob je automatický, tj. TS si sami provedou přepnutí z aplikačního na instalační režim a zpět. Tato instalace se provede přes *Add/Remove programs* z *Control Panel*, kde je možnost instalace aplikace. Při vstupu do této fáze TS se přepne na instalační režim, po dokončení instalace správce potvrdí dokončenou instalaci a TS se přepne zpět do aplikačního režimu.

Bohužel ne každá aplikace může být nainstalována a provozována na TS. Instalace se povede většinou vždy, pokud si instalační program neohlídá instalaci na TS. Provozování této aplikace ovšem může způsobit problémy. Jedná se především o aplikace, které se instalují jako služby (především antivirové aplikace, diskové defragmentační utility) a pak aplikace, které používají *multithreading* (tj. více vláken v jedné aplikaci). Pokud aplikace používá vlákna, musí jejich používání a správa být v souladu s TS, tj. nemůže používat standardní funkce Windows, ale funkce používané TS.

Některé aplikace se navíc instalují ještě mnohem komplikovanějším způsobem. Typickým příkladem je balík kancelářských aplikací Microsoft Office 2000. Pro jeho instalaci se používá speciální odpovědní soubor *TermSrvr.mst*, který se pomocí utility *Office Custom Installation Wizard* upraví dle konkrétní jazykové verze Microsoft Office 2000. Tento soubor obsahuje předdefinovaný postup instalace, včetně komponent, které se nainstalují, registračního čísla apod. Soubor i aplikace jsou na *Microsoft Office 2000 Resource Kit*, jsou ale i volně ke stažení na stránkách firmy Microsoft (*www.microsoft.com/office/ork/2000/two/30t3.htm*). Instalace se provede spuštěním instalačního programu Microsoft Office 2000 s tímto souborem zcela automaticky.

Je důležité si uvědomit jednu zásadní věc a to ještě před koupí produktu. Na každý produkt se vztahuje licence na používání a při koupi krabicové verze je vztažena na jednoho uživatele. Proto je třeba zakoupit i patřičný počet licencí pro provoz na TS a pokud neexistují, tak pro provoz na síti. Co se týče konkrétně Microsoft Office 2000, existují speciální licence na TS.

Po úspěšné instalaci všech aplikací se provedou individuální nastavení pro jednotlivé uživatele TS. Všechny aplikace, které jsme nainstalovali, jsou dostupné všem uživatelům terminálových služeb, což jistě není stav, který potřebujeme. Již při instalaci serveru a vytvoření uživatelských účtů TS lze specifikovat profil každého uživatele včetně adresářů. Jedná se o domácí adresáře uživatele, o systémové adresáře, které obsahují nastavení prostředí klienta (tedy obsah pracovní plochy, struktura start menu), nastavení registry atd. Jelikož tyto struktury (desktop, start menu) jsou běžné adresáře, není problém je vytvořit individuálně pro každého uživatele specifickou strukturu nakopírování zástupců příslušných aplikací. Každý uživatel tak dostane v nabídce jen takové aplikace, které má právo používat.

Pak už je jen na správci serveru, aby pomocí *System Police Editor* a *Group Policy* provedl omezení přístupu k nastavení TS relace přes Control Panel, omezil spuštění jiných aplikací přes volbu *Run* a pod.

6.5.2 PŘÍPRAVA KLIENTŮ

Klientské stanice není třeba zvláště připravovat na provoz terminálových služeb. Důležité je, aby stanice měli správně nakonfigurovány TCP/IP a byly schopny se připojit na Windows 2000 Server, který provozuje TS. Je lhostejné, zda stanice mají pevnou IP adresu, nebo ji získávají pomocí DHCP serveru.

6.5.2.1 INSTALACE A NASTAVENÍ X86 KLIENTA S MICROSOFT WINDOWS

Jako klientskou aplikaci TS pro Windows 98 jsem zvolil aplikaci přímo dodávanou firmou Microsoft na instalačním CD Windows 2000 Server. Jedná se jak o instalaci TS klienta na počítačovou učebnu, tak o instalaci administrátorské konzole na počítač administrátora. Všeobecně platí následující zásady, které je vhodné dodržet pro každého TS klienta:

- minimalizovat grafiku jako animované kurzory, šetřiče obrazovky, animované ikony, *Office Assistant* apod.
- vypnout *Active Desktop*
- vypnout *smooth scroling* (plynulý pohyb obsahu okna při rolování jeho obsahem)
- minimalizovat velikost všech menu, včetně obsáhlé nabídky Start menu - je lepší ho nahradit plochým stylem umístěním ikon na plochu
- vyvarovat se umístění bitmap na plochu a nastavit jako podklad jednolitou barvu, ne vzor.
- zakázat provoz aplikací MS DOS nebo 16 bitových aplikací, pokud je to ovšem možné
- nastavit TS server tak, aby vracel uživatelovo přihlašovací jméno místo jména počítače (pro potřeby aplikací) ve spojení s funkcí NetBIOS
- naučit uživatele používat klávesové zkratky. Zkratky používané ve Windows 2000 jsou odlišné od zkratek používaných v TS

Počítačová učebna

Každý počítač má výše uvedenou konfiguraci s nainstalovanými Windows 98. Každá stanice dostává IP adresu od DHCP serveru na síti. Stanice se při spuštění hlásí na Windows 2000 Server s TS. Na serveru mají vytvořeny své účty a profil adresáře, které obsahují start menu a desktop. Omezení jsou provedeny pomocí *System Police Editor* a uloženy na server do souboru *config.pol* do adresáře *Netlogon*.

Následuje instalace a nastavení klienta TS. Toho je možno nainstalovat ze sdíleného adresáře na serveru (*%systemroot%\system32\clients\tsclient*) nebo z instalačního CD Windows 2000 Server (*%cdroot%\valueadd\3rdparty\mgmt\Citrix\eng* resp. *%cdroot%\valueadd\msft\mgmt\mstsc_hpc)*. Existují dva způsoby instalace - nasdílet adresář na serveru oprávněným uživatelům nebo z aplikace *Terminal Services Client Creation* z menu *Administrative Tools* vytvořit instalační *image*, který se použije pro instalaci klientů z diskety.

Po instalaci je potřeba vytvořit připojení na TS. Obrazová dokumentace je uvedena v příloze B.3.

Stanice se automaticky připojí na server, dojde k automatickému spuštění TS klienta a přihlášení na server. Klient TS je otevřen na fullscreen. Uživatel během startu nemůže nic provádět a je rovnou uveden do prostředí TS. Omezení uživatelů jsou

taková, že prakticky mohou počítač pouze vypnout, na lokální stanici nemůže nic spouštět, kromě klienta TS.

Po instalaci klienta je provedena záloha (*image* disku) na server. Existuje bootovací disketa, která slouží k obnovení havarované stanice. Jednou za čas je třeba i lokální systém přeinstalovat, což časově náročné. Pomocí této diskety lze provést obnovení stanice během několika málo minut z *image* disku uloženého na serveru.

Učitelský počítač je nakonfigurován stejně jako ostatní stanice s tím rozdílem, že tato stanice má na serveru administrátorská práva nastavená tak, aby mohl převzít session kterékoliv stanice.

Počítač administrátora

Počítač administrátora má nainstalován operační systém Windows 2000 Professional. Konfigurace je uvedena v kapitole věnované HW (kapitola 5.5). Administrátor používá Windows 2000 především z důvodu stability a integrace administrátorských nástrojů vhodných jak pro správu Windows 2000 Server, tak i ostatních operačních systémů.

Na tento počítač je nainstalován běžný TS klient, který má na serveru nastavena administrátorská práva. Ve svém domovském adresáři má administrátor připraveny důležité nástroje pro správu, včetně potřebných aplikací jako Microsoft Office. Veškerá další nastavení a popis funkce klienta je uveden v kapitole 5.5.3.1.

6.5.2.2 INSTALACE A NASTAVENÍ HPC KLIENTA S WINDOWS CE

Jako klientskou aplikaci pro Windows CE 2.0 jsem zvolil aplikaci od firmy HOB Electronic, která jako jediná umožňuje použití RDP protokolu na Windows CE 2.0. Dále jsem testoval klienta od firmy Microsoft ve formě ActiveX prvku. Obě tyto klientské aplikace jsou dostupné volně ke stažení na Internetu [25] a [20]. Oba klienti se dají použít jak pro aplikační mód tak pro administrátorský mód.

6.5.2.3 JAK FUNGUJE PŘIPOJENÍ KLIENTA POMOCÍ RDP PROTOKOLU NA TS

Připojení klienta

Klient zahajuje připojení na server pomocí TCP portu. Terminal server poslouchá daný port a na žádost o připojení vytvoří *RDP stack instance* a nadále poslouchá port. Následně se pro danou relaci nastaví úroveň šifrování.

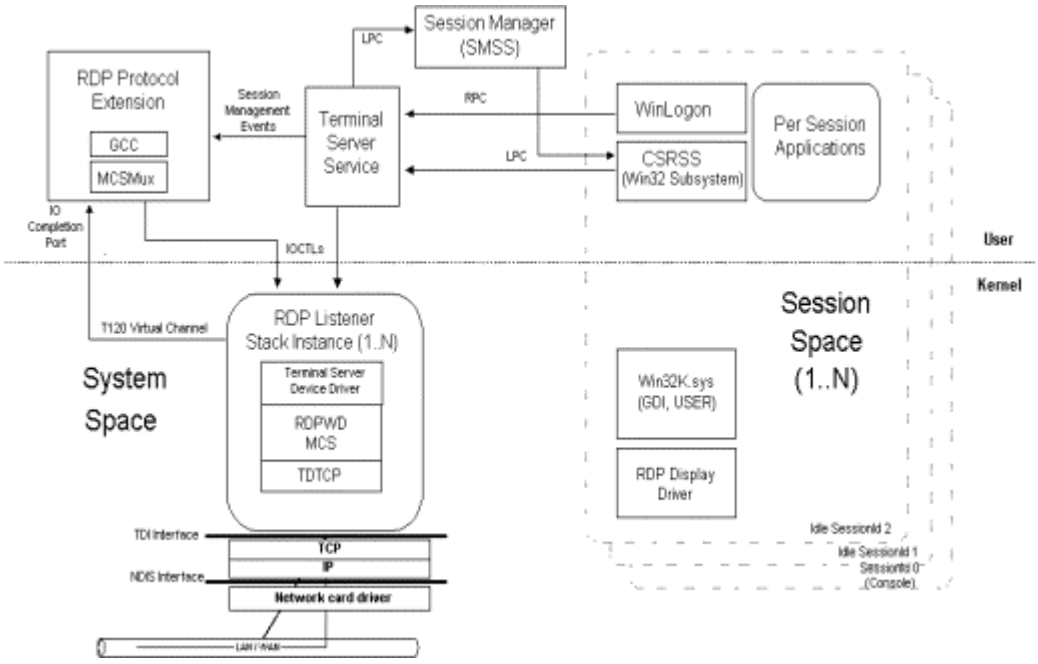
Každý klient si standardně rezervuje 1.5 MB RAM paměti pro *bitmap cache*, která se používá pro ikony, toolbary, kurzory, ale ne pro *unicode* texty. Cache je přepisována za použití algoritmu LRU (*Least Recently Used*). Terminal server také obsahuje cache pro kontrolu a posílání obrazovek na klienty místo konstantního datového proudu.

Jestliže uživatel silně zatěžuje systém (píše na klávesnici a pohybuje myší), buffer je posílán (*flushed*) cca 20x za vteřinu, při malé zátěži pak 10x za vteřinu. Když je intenzivně používána grafika, nepoužívá se timer pro ukládání dat, ale data jsou posílána tak rychle, jak se plní buffer na serveru.

Jakmile je sestaveno spojení, uživatel je vyzván k zadání jména a hesla - pokud je nakonfigurován pro automatický logon, je jméno a heslo v zašifrované podobě posláno na server. Jestliže není volná Win32k relace, zavolá se *Terminal Services Session Manager* a vytvoří novou relaci, která sdílí kód s ostatními relacemi. Ke každému připojenému klientovi přiřadí *SessionID*, který jednoznačně identifikuje

klienta (jaké paměťové bloky používá, při odhlášení a znovupřihlášení obnovení jeho nastavení a nahrání odložených dat do paměti apod.)

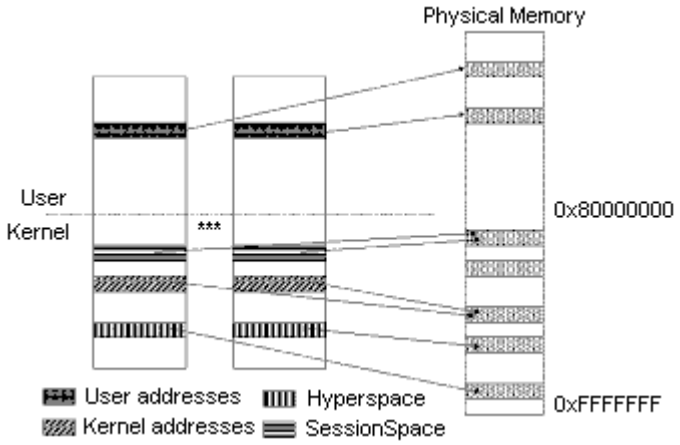
Jakmile uživatel napíše jméno a heslo, pakety jsou zašifrovány a poslány na server. Winlogon process provede autentizaci, jestli má uživatel právo se přihlásit do domény.



Obr. 23, Schéma funkce připojení klienta pomocí RDP protokolu [27]

Spouštění aplikací

Po přihlášení uživatele se zobrazí desktop. Jestliže uživatel myší vybere aplikaci ke spuštění, příkaz je poslán na server a ten spustí vybranou aplikaci v novém virtuálním paměťovém prostoru



Obr. 24, Umístění aplikací v paměti serveru [27]

Všechny procesy na TS sdílejí kód v *kernelu*, pro dosažení sdílení kódu mezi procesy používají *Windows NT Virtual Memory manager copy-on-write page protection*. Když více procesů potřebuje číst a zapisovat stejný paměťový obsah, *Virtual Memory Manager* (VMM) přiřadí *copy-on-write page protection* na paměťový region. Všechny procesy používají stejný obsah paměti dokud operace zápisu není dokončena. V této době VMM zkopíruje fyzický *page frame* na jiné místo, zaktualizuje virtualní adresu procesu tak, aby ukazoval na nové místo a označí místo jako *read/write*. *Copy-on-write* je extrémně použitelný a efektivní pro aplikace běžící na TS.

Jakmile je Win32 aplikace, například Microsoft Word, nahrána do fyzické paměti jako jeden proces (relace), je označena jako *copy-on-write* a je mu přiřazen *SessionID* klienta. Jestliže další proces (nová relace) spustí Word, a protože je aplikace již nahrána do paměti, *image loader* ukáže novému procesu, kde běží existující kopie aplikace a přiřadí mu další *SessionID* dalšího klienta. Když je požadována práce s vlastními daty (např. uložení souboru), potřebné stránky paměti jsou zkopírovány na nové fyzické místo v paměti a označeny jako *read/write* pro ten daný proces (relaci). VMM zabezpečí tuto část paměti před nedovoleným přístupem před ostatními procesy.

Některé aplikace ovšem neumí sdílet kód a nevědí, kolikrát byly spuštěny. Proto je důležité na TS provozovat 32 bitové aplikace, které podporují TS. 32 bitové aplikace podporují sdílení kódu a dokáží fungovat pod víceuživatelským rozhraním.

Je možno provozovat 16 bitové aplikace pod Win32app rozhraním vytvořením virtuálního DOS stroje (VDM – *Virtual DOS Machine*). Všechny 16 bitové volání jsou převáděny na 32 bitové. Protože aplikace Win16 jsou spouštěny ve vlastním VDM, kód nemůže být sdílen mezi relacemi. Překlad z 16 bit na 32 bit také spotřebovává výkon procesoru (o cca 40 procent než srovnatelná 32 bit aplikace).

Odpojení relace

Jestliže se uživatel rozhodne odpojit se od TS, procesy a obsah virtuální paměti jsou uloženy na disk (pokud je paměť potřeba pro další relace a procesy). Protože si TS udržuje mapu *domain / user name* a *SessionID*, jakmile se stejný uživatel znovu přihlásí, existující relace je nahrána zpět do paměti. Schopností RDP je změnit rozlišení obrazovky v závislosti na tom, co uživatel potřebuje od nové relace. Například uživatel pracoval v rozlišení 800x600 a pak se přesunul na počítač, který umí jen 640x480. TS změní rozlišení existující relace na rozlišení požadované novým připojením.

User Logoff

Jakmile uživatel ukončí práci s TS, všechny procesy přiřazené k *SessionID* jsou ukončeny a paměť je uvolněna pro další relace a procesy. Např. pokud uživatel spustil Word, tak ten je z paměti odstraněn až když se odpojí poslední uživatel, který ho používá.

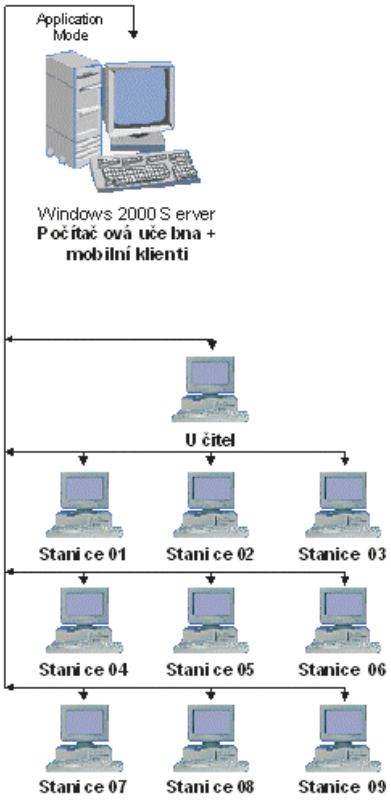
Další informace o funkci protokolu RDP lze nalézt v [10], [27].

6.5.3 PROVOZOVÁNÍ POČÍTAČOVÉ UČEBNY A MOBILNÍCH KLIENTŮ

Nyní se budu věnovat popisu fungování počítačové učebny a práci mobilních klientů. Jedná se vlastně o první možnost využití TS jako aplikačního serveru.

6.5.3.1 KLIENT X86

Počítače po zapnutí automaticky spustí Windows 98, přihlásí se pod defaultním jménem *TSClient1 - TSClient9* a stejným heslem. Pomocí *System Police Editor* je jim na serveru nastaveno značné omezení, ale především je nastaveno automatické spuštění TS klienta. Volba spuštění klienta pomocí skupinové politiky místo umístění do *StartUp* adresáře je z bezpečnostních důvodů odstraněna - uživatele by lákalo smazat tuto položku. Toto lze samozřejmě zabezpečit, nicméně řešení přes skupinovou politiku je bezpečnější.



TS klient je automaticky spuštěn a dojde k přihlášení na TS pod stejným jménem a heslem. Pro každého klienta se nastaví desktop a Start menu s připravenými aplikacemi na určitý druh školení. Tato nastavení jsou uložena na serveru, který spravuje databázi AD a se kterou server TS komunikuje. Učitelský počítač je trochu odlišný od ostatních počítačů. Především má v AD nastavena práva pro převzetí ovládání klienta.

Následuje školení, používaní aplikací, práce s daty atd. Data se ukládají na sdílený disk na serveru, který je při ukončení session vymazán, nedochází tak k uložení nastavení desktopu a prostředí, aby stav pro další školení byl totožný.

Pokud je potřeba uvést učebnu do původního stavu, stačí použít bootovací disketu, která obsahuje skript pro kompletní obnovení stanice. Po startu DOSu z diskety dojde ke spuštění skriptu, který provede připojení na server, naformátuje lokální disk a ze zálohy na serveru provede zkopírování instalace Windows 98 včetně klienta TS a veškerých nastavení. Obnova jedné stanice trvá něco okolo 10-15 minut.

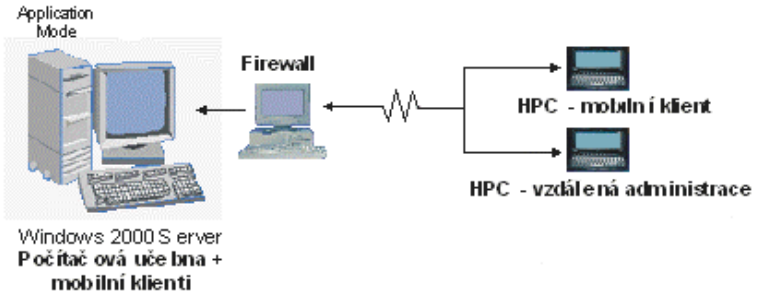
Obr. 25, Schéma počítačové učebny

6.5.3.2 KLIENT HPC

Provozování klienta s Windows CE je mnohem zajímavější a užitečnější, než na první pohled vypadá. Vezměme si následující situaci jako příklad.

Obchodník má na svém stole pracovní PC. Na serveru je vytvořen *roaming profile*, který obsahuje jak nastavení desktop a start menu, tak jeho Word dokumenty, Excel tabulky, prezentace v PowerPoint, poštu Outlook a další. Při jeho přihlášení z PC má vše k dispozici. Obchodník ovšem často jezdí mimo firmu a potřebuje mít své dokumenty a poštu stále při sobě. Přistupovat k poště není problém s notebookem a modemem. Mít s sebou dokumenty je možné i pomocí HPC, ale je třeba je nejprve zkopírovat na HPC včetně převodu do jiného formátu. Tento převod přináší velké problémy právě ve spojení s poštou, kdy není možné zpracovat přílohu Word dokumentu. (poznámka - mobilní klient může samozřejmě být i notebook, práce je pak

stejná, jako u klientů počítačové učebny – práce je mnohem příjemnější, protože se pracuje ve stejném prostředí, jako na stolním PC).



Obr. 26, Připojení mobilních klientů pomocí HPC na terminálové služby jak na aplikační server, tak za účelem vzdálené administrace serveru

Proto je *roaming profile* nastaven i pro klienta TS. Obchodník se pomocí síťové karty nebo modemu připojí na Internet a pomocí TS klienta se připojí na svůj účet. Zadá své přihlašovací jméno a heslo. Po chvilce se zobrazí jeho prostředí tak, jak ho zná ze svého stolního PC. Nevýhodou je bohužel malý rozměr displeje HPC (většinou 640x240 bodů). Nicméně uživatel má k dispozici to, co by měl na svém PC. Může pracovat na rozpracovaných dokumentech, která může ze svého HPC přes infračervený port vytisknout na lokální tiskárně ve stejné kvalitě, jako na PC. Může využít všech možností Excelu, neboť verze Pocket Excel neobsahuje tolik možností, jako jeho PC verze. Lze pracovat s dokumenty typu PDF, na které pro HPC neexistuje prohlížeč, pracovat s databází Access, Oracle či SQL Server, na které se pro HPC těžko najde klient.

Práce s poštovním klientem je ovšem také mnohem praktičtější. Přílohy lze jak přijímat, tak odesílat ve formátu stolního Office, je možno využít korektur atd. Hlavně není zatěžována přenosová kapacita připojení klienta na server, neboť soubor či soubory nejsou na HPC, ale na serveru, odkud se i posílají či kam se přijímají. Lze tak posílat či přijímat poštu i s obsáhlými přílohami.

Využíti HPC jako TS klienta je celá řada a záleží jen na potřebách uživatele, jaké aplikace využije na cestách. Samozřejmě není nutné, aby *roaming profile* byl stejný jako na lokální PC - je možné pro mobilní uživatele vytvořit zcela jiné, šité na míru mobilnímu cestování.

6.5.4 VZDÁLENÁ ADMINISTRACE

Vzdálená administrace je druhá možnost využití TS. Administrátor tak má možnost starat se o servery s Windows 2000 centrálně z jednoho místa, a to i mimo pracoviště.

6.5.4.1 KLIENT X86

První způsob je administrace přímo na pracovišti ze svého PC. Jak bylo uvedeno v kapitole věnované TS, je potřeba, aby administrátor měl Windows 2000 Professional. Hlavním důvodem je jednodušší integrace administrátorských nástrojů do systému.

Vzdálenou administraci lze provádět trojím způsobem. Za prvé je to využití stávajících nástrojů, které jsou obsaženy ve verzi Professional. Nástroje typu *Regedit* (editor registrační databáze Windows), konzole nástrojů MMC (*Microsoft Management Console)* a další umožňují ve své nabídce vzdálené připojení na jiný systém. Například editor registru umožní editaci registru na serveru či na jiné stanici, defragmentaci disku lze také provést vzdáleně atd. (nástroje administrace viz. obrazová příloha B.6).

Za druhé je možné doinstalovat administrátorské nástroje pro služby, které běží na serveru. Instalace se nachází buď na CD serveru (*%cdroot%\i386\adminpak.msi)* nebo je na serveru (*%systemroot%\system32\adminpak.msi)*. Je tak možno vzdáleně provádět správu Active Directory, DNS, DHCP Serveru, Licence Serveru a dalších služeb, které jsou na serveru. Tyto úkony lze provádět i bez instalace terminálových služeb na server. Lze samozřejmě nainstalovat i nástroje pro správu TS.

Za třetí je možné využít TS klienta. Tak jako v případě mobilního uživatele či klienta počítačové učebny, administrátor si vytvoří svůj roaming profile. V *Terminal Services Client Manager* si připraví připojení na všechny Windows 2000 servery. Při spuštění svého počítače si může nastavit automatické otevření připojení na všechny servery a při práci mezi nimi jednoduše přepínat. Jelikož má nastavena administrátorská práva, může si nastavit profil tak, aby prostředí bylo stejné jako na serveru. Může tak využívat nástroje pro správu, aniž by si je musel instalovat na lokální počítač. V tomto případě nejsou potřebné předchozí dva způsoby, stačí jen tento klient.

Microsoft doporučuje na každém Windows 2000 serveru zprovoznit TS v administračním módu. Pro administrátora to je významná pomoc hlavně při správě velkého počtu serverů.

6.5.4.2 KLIENT HPC

Druhý způsob je administrace pomocí HPC. Tato možnost je velice výhodná hlavně v případě, kdy administrátor není na svém pracovišti.

Na rozdíl od administrace pomocí lokálního PC zde odpadají první dvě možnosti tj. využití stávajících nástrojů a doinstalace administračních nástrojů. Windows CE jsou jinou platformou a neumožňují připojit se na nástroje serveru nebo je doinstalovat. Jedinou možností je tak instalace TS klienta a správa s jeho pomocí.

Jeho použití je stejné jako v předchozím příkladě. Opět je možné mít nadefinována odlišná připojení na různé servery. Vzhledem k tomu, že HPC se vlastně nerestartují, je tak možné mít více připojení otevřeno ihned, jakmile je to třeba. Administrátor může přes Internet nebo ze vzdálené kanceláře (jak od svého pracoviště, tak od serveru) provádět činnosti, které jsou zapotřebí. Může operativně přidat nového uživatele, či jej odstranit, změnit přístupová práva jak uživatelům, tak skupinám, nastavit práva na adresáře apod. Lze takto spouštět či pozastavovat systémové služby, zálohovat server, měnit nastavení DNS a DHCP, spravovat AD, Exchange a SQL server a mnoho dalších činností.

Tak jako u vzdáleného klienta, nevýhodou je malá plocha displeje HPC, která neumožňuje rychlou a pohodlnou práci jako na stolním PC. Nicméně je to způsob, jak urychlit a zkvalitnit práci administrátora.

6.6 POROVNÁNÍ S KONKURENČNÍMI PRODUKTY

Aby se uživatel mohl rozhodnout, zda využije možnosti terminálových služeb obsažených ve Windows 2000, je nutné znát také konkurenční produkty. Tyto produkty nabízejí i jiné vlastnosti a je jen na uživateli, zda je potřebuje. Je potřeba zvážit především to, že terminálové služby jsou v ceně operačního systému a platí se jen za licence. V případě produktů třetích stran je třeba za nemalý obnos pořídit jak software, tak licence.

6.6.1 CITRIX METAFRAME FOR WINDOWS 2000 SERVERS

MetaFrame - produkt firmy Citrix hodně rozšiřuje schopnosti terminálových služeb Microsoft Windows 2000 – rozšiřuje možnosti *load balancing*, podporu heterogenních klientů, další síťové protokoly, podporu lokálních zařízení atd. **WinFrame** je samostatný produkt, obsahující OS, založený na Windows NT 3.51. Produkt firmy Citrix, MetaFrame for Windows 2000 Servers vychází z předchozí verze, která byla dodávána pro Windows NT 4.0 Terminal Server. Vylepšuje služby, které poskytuje Microsoft Windows 2000 Terminal Services a přidávají podporu dalších služeb a možností připojení[5].

Mezi základní rozdíly oproti Microsoft Windows 2000 Terminal Services patří zejména [1]:

a) Architektura MetaFrame serveru

Citrix MetaFrame pro Windows 2000 Server používá nejpokrokovější architekturu *server-based computingu*:

- rozšiřuje produkt MS Windows 2000 Server, Advanced Server a Datacenter Server
- seskupuje více serverů do logicky distribuovaných serverových farem
- obsahuje Citrix ICA (*Independent Computing Architecture*) protokol
- umožňuje spouštět 16 a 32-bit Windows aplikace

b) Pokročilý management a ovládání

Systémů - robustní nástroje pro management systémů zajišťují špičkovou rozšiřovatelnost, dostupnost a bezpečnost.

- Citrix Load Balancing Services
- administrace z konzole nebo pomocí LAN a dial-up připojení
- ICA Browse Management
- šifrování dat
- seznam přístupných aplikací
- Citrix SecureICA Services
- omezení přístupu k diskům serveru, omezení podle disku, adresáře, souboru, uživatele
- integrace s NetWare NDS, Bindery a Windows 2000 doménami a AD
- podpora autentifikace a šifrování od třetích stran

[5] Je otázkou, proč Microsoft Windows 2000 TS obsahují jen podporu RDP a ne ICA protokolu, a tak málo služeb a klientů. Zřejmě se jedná o dohodu mezi společností Microsoft a Citrix, že nebude Microsoft implementovat pokročilé služby TS po nějakou dobu, aby tak negativně neovlivnila svého partnera, který se podílel na Windows NT 4.0 Terminal Serveru.

Aplikací - rychlá implementace a správa aplikací z jednoho místa pro optimální výkon a běh serveru

- Citrix Installation Management Services
- spouštění a vkládání aplikací (ALE =Application Launching and Embeding)
- ALE Wizard
- publikování aplikací
- Citrix Resource Management Services
- EMS
- automatický update ICA klientů

Uživatelů – je možné provádět kontrolu nad uživatelskými desktopy. Uživatelé dostávají přístup pro připojení a k aplikacím.

- Program Neighborhood
- podpora anonymních uživatelů
- sdílení sezení (*Session Shadowing*)
- sdílení a obnova licencí v rámci serverové farmy (*License Pool Recovery*)
- licencování na klientské zařízení - pro více serverových sezení postačí jedna licence (*Client Device Licensing*)
- vylepšený ICA klient
- mapování lokálních disků umožňuje jejich použití i v serverových aplikacích
- kopírování a vkládání (*cut and paste*) mezi lokálními a vzdálenými aplikacemi
- tisk na lokální nebo síťové tiskárny
- automatické mapování tiskáren
- klientský tiskový správce
- jedním kliknutím připojení k serveru
- automatické obnovení sezení (po přerušení spojení, vypnutí terminálu)
- přenos souborů na pozadí
- podpora zvuku
- Citrix VideoFrame

c) Publikování aplikací na Web

Integrace - integruje stávající a nové aplikace do standardního web browseru.

- Citrix aplikační portálová technologie *NFuse*, nabízí možnost integrovat libovolnou aplikaci do standardního web browseru
- pro jednoduchou integraci aplikací lze vytvořit aplikační portál s pomocí *NFuse Web portal wizard* nebo skriptů
- integruje uživatele přes web browser k libovolné aplikaci, z libovolného zařízení, s libovolným operačním systémem

Personalizace - personalizuje aplikace, uživatelské zdroje, browser a seznam aplikací dle uživatele.

- personalizuje uživatelské stránky přidáním libovolného HTML, skriptů, grafiky a dalších objektů do web stránky nebo šablon
- aplikace běží uvnitř HTML stránky nebo v samostatném okně

Ovládání - používá robustní nástroje pro správu aplikací v MetaFrame

- úplná správa v rámci celého podniku
- implementace aplikací z centrálního místa

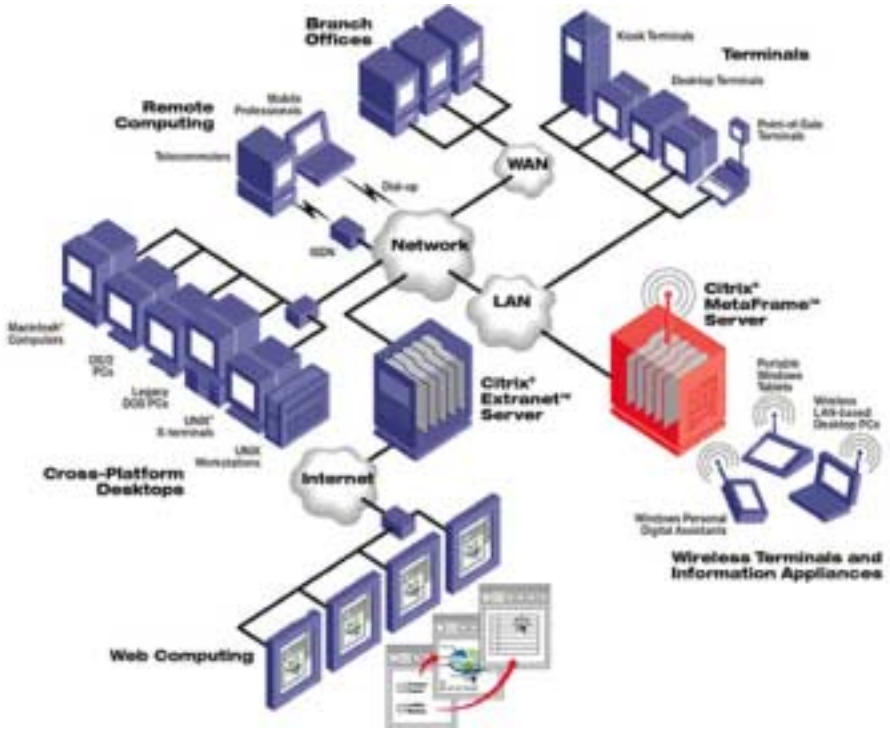
d) Flexibilní přístup k aplikacím na požádání, libovolný uživatel, z libovolného místa

Aplikace - rychlá implementace a správa aplikací z jediného místa pro optimální výkon a běh serveru.

- spouštění a vkládání aplikací (Application Launching and Embeding - ALE)
- ALE Wizard
- publikování aplikací
- Citrix Resource Management Services
- automatický update ICA klienta

Zařízení - přístup z libovolného klientského zařízení, Windows i non-Windows.

- Windows 3.x, 95, 98, NT, 2000, CE
- MS-DOS, OS/2
- Java
- MS Internet Explorer (ActiveX)
- Netscape Navigator (plug-in)
- síťové počítače (např. IBM Network Station)
- Windows terminály (např. Wyse Winterm)
- Macintosh
- UNIX pracovní stanice
- X-terminály (s podporou třetích stran)



Obr. 27, Podpora klientských zařízení a různých typů síťových připojení pomocí služeb Citrix MetaFrame Server

Připojení - přístup přes libovolné připojení. LAN, WAN, Internet, bezdrátově.

- ICA Network Services
- Windows 2000, NT domény, skupiny, Active Directory a NDS
- Novell NetWare 3.x a 4.x sítě
- IBM LAN Server
- TCP/IP, IPX, SPX a NetBEUI protokoly
- přímé asynchronní spojení (do 230 kb/s)
- vysokorychlostní analogové modemy (více než 400 modelů)
- ISDN, Frame Relay, X.25, T1, T3, E1
- 10/100 ethernet, token ring, ATM, FDDI

6.6.2 SCO TARANTELLA ENTERPRISE II

Tarantella Enterprise II je *web-enabling* řešení určené pro velké organizace. Tarantella produkty obsahují rysy speciálně určené pro oblast *Small to Medium Business* (SMB) a pro oblast *Application Service Provider* (ASP). Tarantella integruje *Microsoft Remote Desktop Protocol* pro přímý přístup k aplikacím Windows 2000 a Windows NT 4.0 Terminal Server Edition (TSE) z Windows a non Windows klientů. Tarantella Enterprise II je v prodejní síti od ledna 2000. Tarantella Enterprise II existuje pro následující platformy [24]:

- UnixWare 7
- HP-UX® 10.01+
- SCO® UnixWare® 2.1.2+
- IBM® AIX® 4.2+
- SPARC™ Solaris® 2.5.1+
- Siemens® Reliant® UNIX® 5.43+

Tarantella užívá RDP pro přímý přístup k Windows NT 2000 a Windows NT 4.0 Terminal Server Edition. Tarantella poskytuje management přístupu k aplikacím Windows NT 2000 a Windows NT TSE stejně tak jako k UNIX a mainframe aplikacím.

Díky produktu Tarantella je možné využívat a ovládat více aplikací z více serverů, pro více uživatelů a rychleji, než kdykoliv předtím. Tarantella poskytuje centralizovaný *deployment* a management aplikací, založených na server-based technologii. Je navržena pro IT profesionály, kteří musejí poskytovat uživatelům okamžitý přístup k aplikacím a službám. Na standardech založená technologie produktu Tarantella poskytuje přístup k aplikacím, které mohou být upraveny zákazníkem pro splnění všech požadavků.

Tarantella je ideální řešení pro organizace, které chtějí integrovat přístup k rozmanitému mixu dat a služeb ve firmě. S produktem Tarantella mohou organizace budovat dostupné, bezpečné a rozšiřitelné informační portály. Dokonce i aplikace napsané ještě v době před technologií WWW, mohou být web-enabled (webově zpřístupněny) bez přepsání jediného řádku kódu. Začleněním produktu Tarantella do organizační struktury, je možné dát uživatelům rychlý a bezpečný přístup ke službám a datům. Tyto zdroje mohou být dostupné z jakéhokoliv klientského zařízení. Každý uživatel má nastavitelný osobní webtop - což je grafické uživatelské rozhraní k aplikacím a obsahu. Uživatelé přijdou do styku pouze s aplikacemi a zdroji, které jim byly přiděleny. Webtop je dostupný odkudkoliv (přes

browser) - z kanceláře nebo z domova. Webtop lze nastavovat tak, aby odrážel vzhled a zvyky celé firmy nebo dokonce i jednotlivých oddělení.

Tarantella pro uživatele představuje snadno dostupné a cenově efektivní aplikace a zdroje. Aplikace pro mainframe, Windows a UNIX nemusí být přepisovány a uživatelé mohou pokračovat v užívání standardních klientských zařízení. Nové a updatované verze aplikací mohou být dostupné uživatelům okamžitě, tudíž nemusejí čekat na někoho, kdo jim manuálně rekonfiguruje jejich klienta.

Tarantella dovoluje ovládat všechny aplikace v organizaci z jediného místa. Jejich nasazování je mnohem rychlejší, neboť není třeba nainstalovat nic jiného než prohlížeč. Mohou být publikovány pro specifické skupiny uživatelů. Nový uživatel může být přidán interaktivně systémovým administrátorem, za použití grafického rozhraní nebo s pomocí *Tarantella Control Center*. Alternativně může být proces přidávání uživatelů vložen jako část dávkové úlohy. Když se nový uživatel přihlásí do Tarantelly, získává okamžitý přístup pro něj odpovídající skupině aplikací.

Moderní návrh Tarantelly zajišťuje vzdáleným uživatelům práci přes jejich dial-up připojení, které je stejně rychlé, jako kdyby byli připojeni přes LAN. Klíčem k tomu je Tarantella *Adaptive Internet Protocol* (AIP), technologický průlom optimalizující výkonnost sítě, kdy nezáleží na tom, jak je uživatel připojen. AIP se neustále přizpůsobuje změnám zátěže sítě. Tarantella nepotřebuje opravy ani rozšiřování existující sítě, v případě zvětšení počtu uživatelů přistupujících k web aplikacím.

Podobné řešení nabízí i firma Citrix jako Citrix NFuse.

7. BUDOUCNOST MICROSOFT WINDOWS

Windows NT je zcela odlišná platforma od Windows 9.x. Je od počátku čistě 32bitová, nemá za základ operační systém MS DOS. Proto firma Microsoft směřuje k postupnému odbourávání platformy Windows 9.x a podporuje plný přechod na tuto platformu. Prvním produktem, který povede k faktickému ukončení podpory Windows 9.x jsou Windows XP – základ .NET platformy.

7.1 MICROSOFT WINDOWS XP

Windows XP jsou následovníkem Windows 2000 a Windows Millennium. Konečně tedy spojují platformu NT a nadstavbu DOSu ve formě Windows 9.x do jediného produktu. Tyto Windows se budou dodávat jak ve známých verzích již od Windows 2000, tak ve verzi *Consumer*, která bude silně zjednodušená a bude určená pro uživatele stávajících verzí Windows 9.x a Millennium. Dojde tak ke sjednocení obou platforem, což zjednoduší správu systémů a sníží náklady na vývoj dalších verzí operačního systému i aplikací jak Microsoftu tak ostatních firem.

Microsoft přechází od číselného a letopočtového označení k písmennému označení, zavedeném již Windows Millennium (zkratka Me). XP znamená eXPerience (zážitek, zkušenost). Nové písmenné značení verze bude dle mého názoru ještě zmatenější než dříve opuštěné číslování verzí. Zatímco logickou úvahou odhadneme, zda je verze 4.0 novější než verze 3.5, běžní uživatelé budou rozlišováním mezi Windows ME a Windows XP zmateni.

Původně Microsoft plánoval dvě verze Windows s kódovým označením *Neptune* a *Odyssey*. První z nich měl být určen pro běžné uživatele („konzumní“) a druhá pro business oblast. Nakonec se Microsoft rozhodl pro spojení do jediného produktu s kódovým označením Whistler (nyní XP). Současně se budou nová Windows prvotním testem .NET platformy a jedná se tudíž o Microsoft.NET 1.0. (blíže o této technologii v další kapitole 6.2).

Velká část vzhledu Windows bude založena na HTML resp. XML. Beta verze je založena na UI Windows 2000. Desktop bude nahrazen HTML "Start page" a nejspíše zmizí Start menu nebo bude hodně předěláno. Vzhled Windows bude "skinovatelný" tj. bude možnost zvolit si vzhled takový, jaký uživateli vyhovuje. Tato možnost je u současných Windows pomocí různých utilit (Window Blinds). Windows XP budou obsahovat tzv. *Agent technology*, což je postavička známá z Microsoft Office, která bude ovladatelná hlasem nebo napsanými příkazy. Jeho úkolem bude hledání informaci na Internetu, hledání souborů na disku a další úkoly.

Aktuální informace o současném stavu vývoje lze nalézt na [28].

7.2 MICROSOFT.NET

Microsoft tvoří moderní novou generaci softwaru, která propojí práci s počítačem a komunikaci zcela novým revolučním způsobem a nabídne všem vývojářům nástroje potřebné k transformaci webu a všech dalších aspektů stávajících zkušeností s počítačem. Tato iniciativu se nazývá Microsoft.NET a historicky poprvé umožní vývojářům, podnikatelům i spotřebitelům využívat technologii podle jejich vlastních požadavků. Microsoft.NET umožní tvorbu distribuovaných webových služeb, které se mohou integrovat a spolupracovat s řadou dalších doplňkových služeb a vytvářet pro zákazníky nabídku, o

které se dnešním internetovým firmám může jen zdát. Microsoft.NET bude zdrojem rozvoje Internetu nové generace. Doopravdy umožní získávání informací kdykoliv, kdekoliv a z jakéhokoliv zařízení.

Základní myšlenkou Microsoft.NET je to, že se přesouvá zaměření z individuálních webových míst nebo přístrojů, připojených k Internetu, k sestavám počítačů, přístrojů a služeb, spolupracujících společně na poskytování rozsáhlejších a bohatších řešení. Lidé budou mít kontrolu nad tím jak, kdy a jaké informace jsou jim poskytovány. Počítače, přístroje a služby budou schopné navzájem spolupracovat na poskytování bohatých služeb, místo aby byly izolovanými ostrůvky, jejichž integraci zajišťuje pouze samotný uživatel. Podniky budou schopné nabízet své produkty a služby způsobem, který uživatelům umožní snadno je zahrnout do své vlastní elektronické struktury. Je to vize, která dále rozšiřuje možnosti jednotlivců získané v roce 1980 vznikem osobního počítače.

Microsoft.NET pomůže s transformací Internetu, který bude kromě prezentací na bázi HTML obsahovat i programovatelné informace na bázi XML. XML je široce podporovaný průmyslový standard, definovaný World Wide Web konsorciem, stejnou institucí, která vytvořila standardy pro webový prohlížeč. Byl vyvinut za rozsáhlé účasti Microsoftu, ale není chráněnou technologií Microsoftu. XML poskytuje prostředky k oddělení vlastních dat od jejich grafické prezentace. Je klíčem k Internetu nové generace, protože nabízí způsob, jak vyjmout informaci tak, aby mohla být organizována, programována a editována, způsob, jak distribuovat data užitečnějším způsobem k množství nejrůznějších digitálních přístrojů. Umožní webovým místům navzájem spolupracovat a tvořit seskupení webových služeb, které budou schopné vzájemných interakcí.

Microsoft.NET zahrnuje následující:

- **Platformu Microsoft.NET** – obsahuje infrastrukturu a nástroje pro tvorbu a provoz nové generace služeb, nové uživatelské možnosti, služby bloků, novou generaci vysoce distribuovaných megaslužeb a software, který umožňuje zrod nových druhů různých internetových přístrojů.
- **Produkty a služby Microsoft.NET** – obsahuje Windows.NET s integrovanou základní sadou služeb stavebních bloků, MSN.NET, služby pro osobní subskripce, Office.NET, Visual Studio.NET a bCentral for .NET.
- **Služby pro .NET od dalších dodavatelů** – široké spektrum partnerů a vývojářů bude mít příležitost tvořit firemní a vertikální služby na bázi platformy .NET.

Microsoft.NET posune práci s počítačem a komunikaci daleko za jednosměrný web k bohatému, spolupracujícímu a interaktivnímu prostředí. Zajištěn novým moderním softwarem bude Microsoft.NET využívat souborů aplikací, služeb a přístrojů k vytvoření individualizované digitální zkušenosti, která se bude průběžně a automaticky adaptovat pro potřeby vašeho domova a podnikání. Znamená to zcela novou generaci softwaru, který bude pracovat jako integrovaná služba, pomáhající zvládat život a práci v éře Internetu.

Pro spotřebitele to znamená jednoduchost integrovaných služeb, sjednocené prohlížení, editování a tvorbu dokumentů, přístup ke všem vlastním souborům, práci a médiím on-line i off-line, dokonalou konzistenci mezi všemi používanými přístroji, ve všech situacích a případech individualizovaný přístup a žádnou práci s údržbou. Znamená to např., že jakákoliv změna ve vašich informacích bude okamžitě a automaticky k dispozici všude, kde může být této informace zapotřebí.

Pro duševní pracovníky a podniky to znamená sjednocené prohlížení, editování a tvoření dokumentů, bohatě koordinovanou komunikaci, bezproblémovou „mobilní“ práci, výkonnou správu informací a nástroje pro elektronický obchod, které se budou transparentně pohybovat mezi interními a internetovými službami a podpoří novou éru dynamických obchodních vztahů.

Pro nezávislé softwarové vývojáře to znamená příležitost k tvorbě nových moderních služeb pro éru Internetu – služeb, které umí automaticky získávat a využívat informace z lokálních i vzdálených zdrojů, pracují s jakýmkoliv přístrojem a programovacím jazykem, aniž by bylo nutné je pro každé prostředí znovu programovat. Vše na Internetu se stane potenciálním stavebním blokem pro tuto novou generaci služeb a každá aplikace může být umístěna na Internet jako služba.

Vize Microsoft.NET znamená větší možnosti pro spotřebitele, podnikatele, softwarové vývojáře a pro celý průmysl. Znamená odkrytí plného potenciálu Internetu. A znamená to pro vás takový web, jaký budete chtít.

Další informace lze nalézt na [16].

7.3 MICROSOFT BLACKCOMB

Jméno Blackcomb je kódové označení Windows, která budou pravděpodobně následovat po Windows XP. Někdy jsou tyto Windows označovány jako *Second release of Windows 2000*, vydány nebudou dříve než na konci roku 2002, respektive v průběhu roku 2003 a měly by být základem .NET 2.0. Zatím jsou ve fázi beta testování a bližší informace nejsou dostupné. Bližší a aktuální informace je možno nalézt na [15].

8. ZÁVĚR

Cílem této práce nebylo popsat veškeré vlastnosti Windows 2000 a to ve všech dostupných verzích. Windows 2000 obsahují ohromné množství vlastností a možností použití, že nebylo možno do tak malého prostoru vyhrazeného pro diplomovou práci vměstnat všechny důležité informace.

Proto jsem se věnoval jen obecným informacím a především jednomu z nejzajímavějších nových prvků Windows 2000, a to terminálovým službám. Snažil jsem se o co nejsrozumitelnější vysvětlení principu práce a architektury terminálových služeb, zaměřil jsem se na požadavky na hardware a software jak pro server, tak pro klienty, včetně popisu práce jednotlivých technologií, hlavně protokolů. Nejlepším způsobem pro nejsrozumitelnější vysvětlení použití terminálových služeb je uvedení na příkladech. Proto jsem se dále věnoval popisu praktického využití terminálových služeb v praxi – jak využití terminálových služeb jako aplikačního serveru, tak pro vzdálenou administraci serverů s Windows 2000, a to ve spojení s dvěma odlišnými architekturami klientských zařízení. Aby bylo možno posoudit kvalitu a výhody terminálových služeb ve Windows 2000, věnoval jsem část práce porovnání s konkurenčními produkty firem Citrix a SCO. Pro posouzení vhodnosti nasazení Windows 2000 je na konci práce přehled budoucnosti vývoje platformy Windows 2000.

A na úplný závěr práce trochu zajímavostí okolo vývoje Windows 2000. Náklady na Windows 2000 činily přes 2 miliardy USD, vývojový tým měl kolem 5 000 lidí a testy zabraly kolem 500 člověkoroků. Přestože jsou Windows 2000 následovníkem Windows NT, nejsou jejich kopií. Bill Gates uvedl, že zatímco Windows 95 bylo nutné restartovat průměrně jednou za 2,1 dne, Windows NT 4.0 Workstation vydržely v průměru mírně přes pracovní týden (5,2 dne), Windows 2000 při testování nebylo nutné restartovat ani jednou za 90 dní, po které test probíhal.

9. SEZNAM LITERATURY

[1] **CALYX – Tenký klient**
http://www.calyx.cz/Citrix_Metaframe.htm

[2] **CALYX – Tenký klient**
http://www.calyx.cz/Tk_technologie.htm

[3] **Microsoft – Popis funkcí systému Windows 2000 Server**
http://www.microsoft.com/cze/windows/windows2000/guide/server/features/default.asp

[4] **Microsoft – Microsoft TechNet Online Support**
http://www.microsoft.com/technet/Examining the Windows 2000 Architecture.htm

[5] **Microsoft – Windows 2000 Terminal Services Capacity and Scaling**
http://www.microsoft.com/windows2000/terminalservices/tsscaling.doc

[6] **Microsoft – Windows 2000 Terminal Services: An Integrated, Server-Based Computing Solution**
http://www.microsoft.com/windows2000/terminalservices/tssol.doc

[7] **Microsoft – Using Terminal Services for Graphical Remote Administration of the Windows 2000 Server Family**
http://www.microsoft.com/windows2000/terminalservices/tsremote.doc

[8] **Microsoft – Optimizing Applications for Windows 2000 Terminal Services and Windows NT Server 4.0, Terminal Server Edition**
http://www.microsoft.com/windows2000/terminalservices/tsappdev.doc

[9] **Microsoft – Microsoft Windows 2000 Terminal Services - Licensing Technology White Paper**
http://www.microsoft.com/windows2000/terminalservices/tslicences.doc

[10] **Microsoft – Remote Desktop Protocol (RDP) Features and Performance**
http://www.microsoft.com/windows2000/terminalservices/rdpfp.doc

[11] **Microsoft Windows 2000 Server Resource Kit – Chapter 16 – Deploying Terminal Services**
http://www.microsoft.com/windows2000/terminalservices/Chapt-16.doc

[12] **Microsoft Windows 2000 Server Resource Kit – Chapter 22 – Group Policy**
http://www.microsoft.com/windows2000/terminalservices/Chapt-22.doc

[13] **Microsoft – Introduction to Windows 2000 Group Policy**
http://www.microsoft.com/windows2000/terminalservices/gpi.doc

[14] **Microsoft – Using Office 2000 with Windows Terminal Server**
http://www.microsoft.com/office/ork/2000/two/30t3_1.asp

[15] **Whistler and Blackcomb - the Windows 2000 .NET future**
http://www.theregister.co.uk/content/1/14662.html

[16] **Microsoft – Microsoft .NET: Realizace internetu nové generace**
Informační materiál (White Paper) společnosti Microsoft

[17] **Živě – Detailní popis NTFS**
http://www.zive.cz/r-art.asp/id=6724

[18] **Microsoft – Platforma Windows 2000**
http://www.microsoft.com/Cze/windows/windows2000/guide/platform/default.asp

[19] **Protocol Analysis**
http://www.w3c.org/dtd.html

[20] **HOB's HOBLink JWT Java-based RDP client**
http://www.hobsoft.com

[21] **Microsoft Windows 2000 Terminal Services Licensing**
http://www.microsoft.com/TechNet/win2000/tslicens.asp

[22] **Microsoft – Optimizing Applications for Windows 2000 Terminal Services and Windows NT Server 4.0, Terminal Server Edition**
http://www.microsoft.com/technet/index/default.asp?url=/technet/win2000/win2kpro

[23] **Microsoft – Windows 2000 Terminal Services Reviewers Guide**
http://www.microsoft.com/technet/index/default.asp?url=/technet/win2000/win2kpro

[24] **CALYX – SCO Tarantella**
http://www.calyx.cz/SCO_Tarantella.htm

[25] **Microsoft – Terminal Services Advanced Client (TSAC) FAQ**
http://www.microsoft.com/windows2000/library/operations/terminal/tsacfaq.asp

[26] **Citrix ICA Technology Brief**
http://www.newtechgrp.com/resources/thinclientsrvr/thin_ica.htm
[27] **Xiaochun Hu - ICS 690 Report - Windows NT Terminal Server Technology**
http://www.ics.org/ 690repor.htm
[28] **Paul Thurrott's SuperSite for Windows**
http://www.winsupersite.com

10. VYSVĚTLIVKY

ActiveDirectory	Adresářová služba Windows 2000, obdoba NDS firmy Novell
ActiveX	DCOM objekty nejčastěji využívané jako součásti web stránek
AIP	Adaptive Internet Protocol - protokol firmy SCO, který se přizpůsobuje zatížení sítě
ALE	Application Launching and Embeding - technologie firmy Citrix pro provoz libovolných aplikací přes webový prohlížeč
API	Application Programming Interface - základní rozhraní pro komunikaci aplikací s operačním systémem
ASP	Active Server Pages - skriptovací jazyk používaný nejčastěji pro zobrazení dat z databáze
Cache	Rychlá mezipaměť pro ukládání nejpoužívanějších dat, může být hardwarová nebo řízená softwarově jako ukládání dat na disk
Cluster	Spojení serverů do skupiny za účelem rozdělení zátěže a zajištění dostupnosti serverů
COM/DCOM	Objektová architektura klient-server, na které jsou postaveny Windows 2000
Compact Flash	Paměťová karta menší než je karta kreditní, používá se do zařízení HPC, digitálních fotoaparátů apod.
CPU	Central Processing Unit - mikroprocesor
DFS	Distributed File System - propojování souborových systémů serverů do kompaktní adresářové struktury
DHCP	Dynamic Host Configuration Protocol - dynamické přiřazování IP adres stanicím
DNA	Distributed interNet Application - tvorba škálovatelných a distribuovatelných aplikací
DNS	Domain Name Service - přiřazení jmen na IP a zpět
Domain	Doména - hierarchické seskupení stanic a serverů
Domain Controller	Server, který má na starosti doménu - udržuje hlavní databázi uživatelských účtů, je základním kamenem domény
Driver	Ovladač hardwarového zařízení
EFS	Encrypted File System - šifrování dat na systému souborů NTFS
Event Viewer	Prohlížeč událostí (LOGů) systému ve Windows NT / 2000
Farma	Spojení serverů za účelem rozložení zátěže a zpřístupnění výkonu připojeným klientům, zabezpečení dostupnosti serverů
Firewall	Počítač či samostatné zařízení, které odděluje privátní síť od sítě veřejné
GDI	Graphic Device Interface - rozhraní pro vykreslování grafických primitiv
Group Policy	Skupinová politika, která slouží k nastavení práv uživatelů v doméně
GSM	Global System for Mobile Communication - celosvětový standard pro mobilní komunikaci
HAL	Hardware Abstraction Layer - vrstva ležící těsně nad hardwarem počítače a zajišťující komunikaci s ním
HPC	Handheld PC - počítače do dlaně s operačním systémem WCE
HTML	HyperText Markup Language - jazyk pro tvorbu www stránek
I/O	Vstup / Výstup - používá se pro označení vstupně - výstupních operací
ICA	Independent Client Architecture - protokol pro komunikaci mezi klientem a serverem v Citrix MetaFrame / WinFrame
IIS	Internet Information Server - WWW server, který je součástí Windows 2000

IntelliMirror	Inteligentní instalace a správa software, i vzdáleně
IPSec	IP Security - rozšíření protokolu IP o bezpečnostní mechanismy
IPX/SPX	Síťové protokoly Novell Netware
Kerberos	Bezpečnostní protokol pro autorizaci v síti Windows 2000
Kernel	Jádro operačního systému
LAN	Local Area Network – lokální počítačová síť, nejčastěji uvnitř podniku
LPC	Local Procedure Call - řídí komunikaci mezi klientem a serverem, pokud oba dva existují na jednom počítači
MFT	Master File Table - tabulka uložení souborů, adresářů a metadat v NTFS
MMC	Microsoft Management Console - aplikace pro správu administrátorských nástrojů
Multiprocessing	Běh vícevláknového procesu na několika procesorech
Multitasking	Běh několika aplikací zdánlivě současně
Multithreading	Rozdělení procesu na více paralelně pracujích částí
NDS	Novell Directory Services - adresářová služba firmy Novell
NLB	Network Load Balancing – vyrovnávání síťové zátěže mezi více serverů
NTFS	New Technology File System – souborový systém Windows NT a Windows 2000
Pagefile	Odkládací soubor Windows
PCMCIA	Nebo také PC Card - zařízení velikosti kreditní karty, především pro notebooky a přenosné počítače HPC a Pocket PC – modemy, síťové karty, rozšiřující paměti
Plug & Play	Schopnost BIOSu, resp. operačního systému detekovat hardware
Pocket PC	Následovník přenosných zařízení HPC, bezklávesnicový
PPTP	Point to Point Tunneling Protocol - protokol pro přenos TCP/IP protokolů přes telefonní linky
RAID	Hardwarové zařízení umožňující propojení disků do diskových polí
RC4	Symetrická šifra používaná pro šifrování dat mezi klientem a serverem terminálových služeb
RDP	Remote Desktop Protocol - protokol pro komunikaci mezi klientem a serverem terminálových služeb Windows 2000
RPC	Remote Procedure Call - řídí komunikaci mezi klientem a serverem, pokud oba dva existují na různém počítači
Service	Služba - část operačního systému, která provádí činnosti na pozadí, většinou bez uživatelského rozhraní
Session	Sezení - připojení klienta na server terminálových služeb
SLIP	Protokol pro přenos IP paketů po seriové lince (modem)
SSL	Secure Socket Layer - vrstva pro šifrování dat pro přenos přes TCP/IP po Internetu
System Police Editor	Nástroj systémové politiky - slouží pro nastavení práv uživatelů v doméně
TCO	Total Cost of Ownership - náklady na vlastnictví - označení pro snížení nákladů na správu a údržbu IT
TCP/IP	Rodina protokolů pro přenos dat po síti typu Ethernet
Thin Client	Tenký klient - technologie snižující TCO
Thinwire	Datový protokol firmy Citrix, který provádí export obrazovek
Transaction	Transakce - úkol není potvrzen, že byl dokončen, pokud tomu tak skutečně není
TS	Terminal Services - terminálové služby Windows 2000
TSAC	Terminal Services Advanced Client - jeden z TS klientů, založen na technologii ActiveX
UI	User Interface – uživatelské rozhraní

VDM	Virtual DOS Machine – virtuální paměťový prostor, ve kterém Windows NT / 2000 provozují 16-ti bitové a DOSové aplikace
VMM	Virtual Memory Manager - správce paměti Windows
VNC	Produkt vyvíjený pod Open Source License, který umožňuje vzdálené ovládání počítače, existuje pro velké množství platforem včetně Windows CE
VPN	Virtual Private Network - virtuální bezpečný kanál v potencionálně nebezpečném prostředí nechráněných sítí
WAN	Wide Area Network – síť spojující jednotlivé LAN
WBT	Windows Based Terminal - speciální zařízení, která jsou vybavena Windows a připojují se na terminálové služby
WCE	Microsoft Windows CE
Whistler	Kódové označení nástupce Windows 2000, dnes označované jako Windows XP
WMI	Windows Management Instrumentation - zlepšená správa hardware pod Windows 2000
WSH	Windows Scripting Host - skriptovací jazyk pod Windows 2000 vycházející z programovacího jazyka Visual Basic
XML	eXtensible Markup Language - rozšíření jazyka HTML pro dynamickou tvorbu web stránek

11. TEXTOVÁ PŘÍLOHA

11.1 POROVNÁNÍ MICROSOFT WINDOWS 2000 TERMINAL SERVICES A CITRIX METAFRAME FOR WINDOWS 2000 SERVERS

Vlastnost	Windows 2000 Server	Windows 2000 Server + MetaFrame 1.8
Podpora klientů		
Windows NT/2000	Ano	Ano
Windows 95/98	Ano	Ano
Windows 3.11 (Workgroups)	Ano	Ano
Windows 3.1	Ne	Ano
Windows CE	Ano	Ano
DOS	Ne	Ano
Macintosh (Motorola, PowerPC)	Ne	Ano
Browser - Internet Explorer	Ne	Ano
Browser - Netscape	Ne	Ano
UNIX - Solaris/SPARC	Ne	Ano
UNIX - Solaris/x86	Ne	Ano
UNIX - SunOS	Ne	Ano
UNIX - DEC	Ne	Ano
UNIX - HP/UX	Ne	Ano
UNIX - IBM	Ne	Ano
UNIX - SGI	Ne	Ano
UNIX - SCO	Ne	Ano
UNIX - Linux (RedHat, Caldera, SuSE, Slackware)	Ne	Ano
Java - JDK 1.1	Ne	Ano
Java - JDK 1.0	Ne	Ano
RISC OS	Ne	Ano
PSOS	Ne	Ano
NCI OS	Ne	Ano
Net OS	Ne	Ano
QNX OS	Ne	Ano
Klientská zařízení		
PC (Windows 3.11 a vyšší)	Ano	Ano
PC (DOS, UNIX, Linux)	Ne	Ano
Macintosh (Motorola, PowerPC)	Ne	Ano
Handheld PC (HP Jornada, Compaq CSerie, atd.)	Ano	Ano

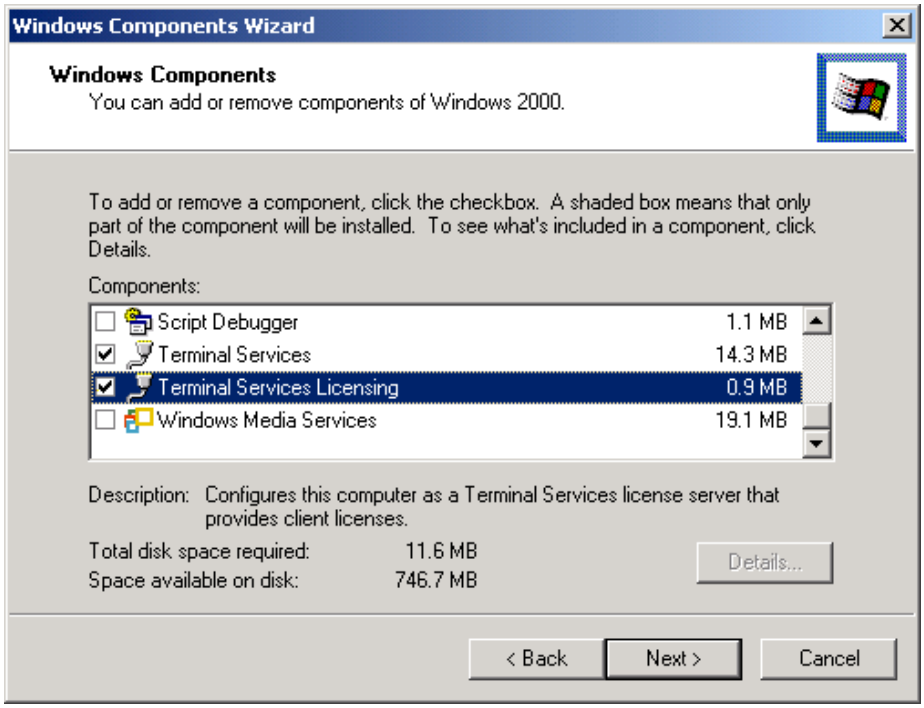
Síťové počítače (IBM Network Station, Sun JavaStation, atd.)	Ne	Ano
Windows terminály (s WinCE)	Ano	Ano
Windows terminály (s DOS, Linux, atd.)	Ne	Ano
Set top zařízení (BocaVision STB121, atd.)	Ne	Ano
Mobilní Handheld zařízení	Ne	Ano
Možnosti klientů		
Manuální mapování disků	Ano*	Ano
Cache bitmap	Ano	Ano
Trvalý cache bitmap	Ano	Ano
Automatické mapování lokálních tiskáren	Ano	Ano
Přesměrování clipboardu	Ano	Ano
Automatické mapování lokálních disků	Ne	Ano
SpeedScreen2	Ne	Ano
Seamless Windows (intergrace terminálových aplikací do desktopu)	Ne	Ano
Business Recovery Client	Ne	Ano
Program Neighborhood	Ne	Ano
* PC klienti s RDP protokolem mohou mapovat lokální disky přes Windows networking (sdílení), to není vlastnost RDP protokolu		
Podpora lokálních zařízení		
Lokální tiskárny	Ano	Ano
Lokální klientská tisková fronta (spooler)	Ano	Ano
Přesměrování COM portů	Ne	Ano
Podpora multimedií na klientovi		
Systémové zvuky (beep)	Ano	Ano
16-bit stereo (WAV, AVI)	Ne	Ano
Podpora videa	Ne	Ano*
Ovládání šířky pásma pro multimedia	Ne	Ano*
* Citrix MetaFrame pro Windows 2000 je připraven na video jak na straně serveru, tak na straně 32-bit klienta. Podpora video streamů je obsažena s produktem Citrix VideoFrame.		
Přenosové protokoly		
TCP/IP	Ano	Ano
IPX	Ne	Ano
SPX	Ne	Ano
NetBEUI	Ne	Ano
Možnosti připojení klientů		
LAN	Ano	Ano
WAN	Ano	Ano
RAS dial-up	Ano	Ano
Přímé asynchronní	Ne	Ano

Přímý dial-up	Ne	Ano
Procházení (browsing) dostupných serverů	Ne	Ano
Serverové vlastnosti		
Jeden na jeden shadowing	Ano	Ano
Jeden na více shadowing	Ne	Ano
Více na jednoho shadowing	Ne	Ano
Shadowing na jiný server	Ne	Ano
Publikování aplikací	Ne	Ano
Program Neighborhood	Ne	Ano
Správa přes více domén	Ne	Ano
Správa přes subnet	Ne	Ano
Automatický update klientů	Ne	Ano
Shadow Task Bar	Ne	Ano
Publikování aplikací na web (ALE)	Ne	Ano
MetaFrame/WinFrame interoperabilita a správa	Ne	Ano
Administrátorský toolbar	Ne	Ano
Správcovské nástroje a služby		
Resource Management Services	Ano	Ano
Kryptování	Ano	Ano
Správa bezpečnosti - Security Management Services (RSA RC5 128-bit)	Ne	Ano
Load Balancing	Ano*	Ano
Pokročílý Load Balancing	Ne	Ano
Installation Management Services	Ne	Ano
* Windows 2000 Terminal Services s NLB (Network Load Balancing) je limitován na 32 serverů a je dostupný pouze u Windows 2000 Advanced Server.		

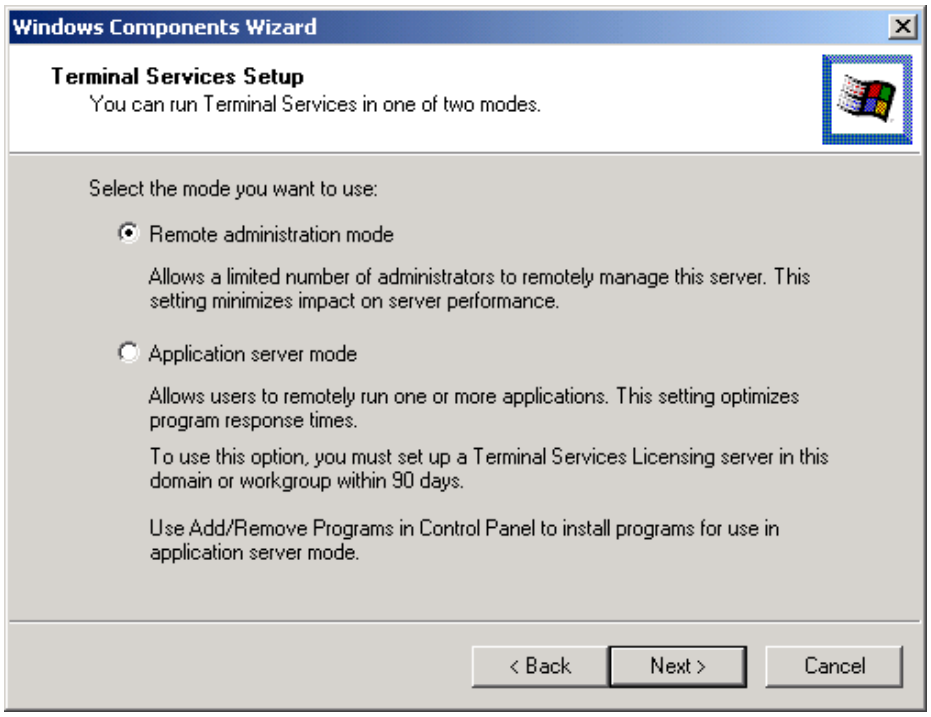
Tab. 9, Porovnání Microsoft Windows 2000 Terminal Services a Citrix MetaFrame for Windows 2000 Servers

12. OBRAZOVÁ PŘÍLOHA

12.1 INSTALACE TERMINÁLOVÝCH SLUŽEB

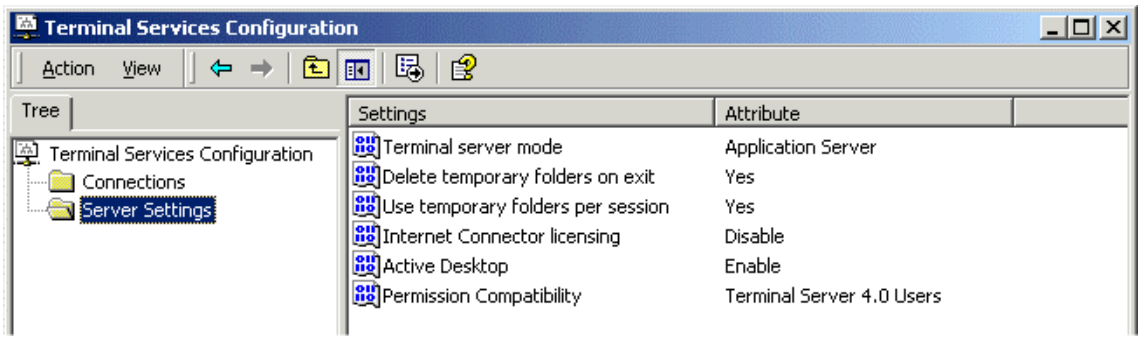


Obr. 28, Instalace terminálových služeb přes Add / Remove programs

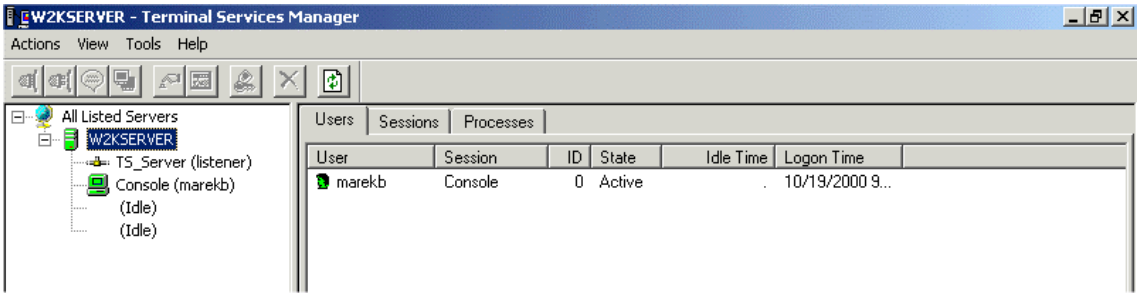


Obr. 29 Nastavení typu módu provozu TS – vzdálená administrace resp. aplikační server

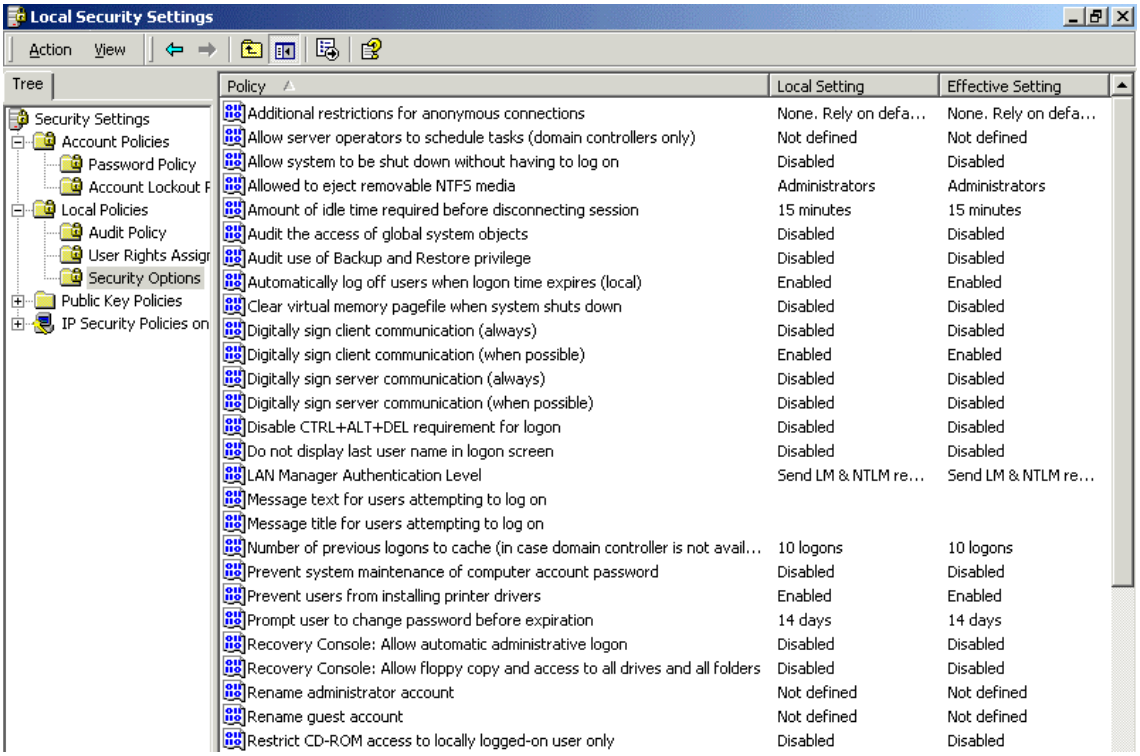
12.2 NASTAVENÍ TERMINÁLOVÝCH SLUŽEB



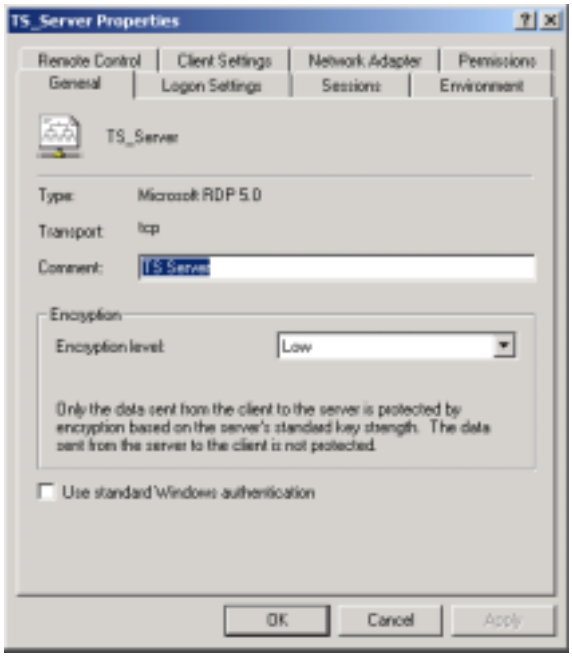
Obr. 30, Nastavení základních parametrů terminálových služeb z konzole MMC



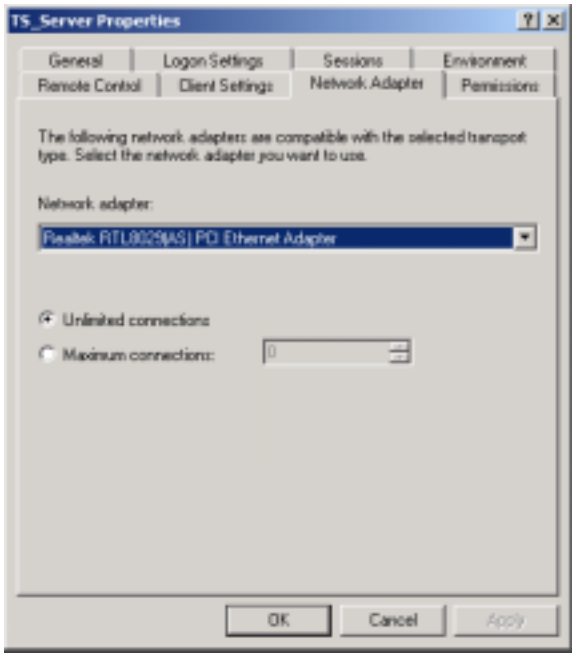
Obr. 31, Správce terminálových služeb – Terminal Services Manager



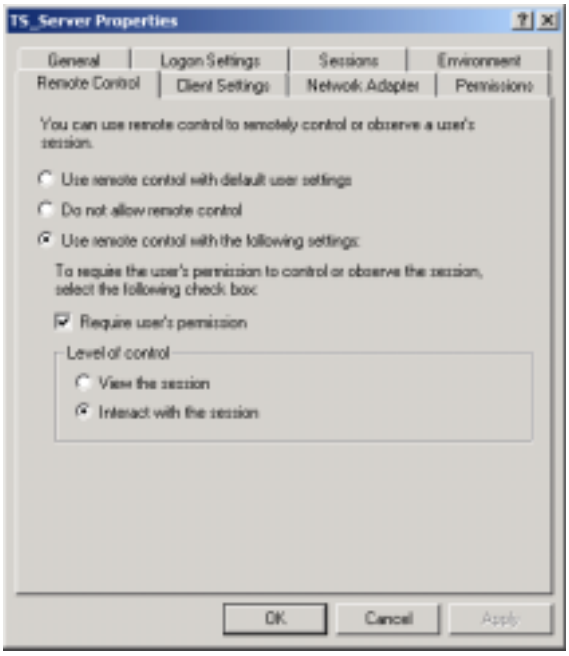
Obr. 32, Nastavení bezpečnostních opatření



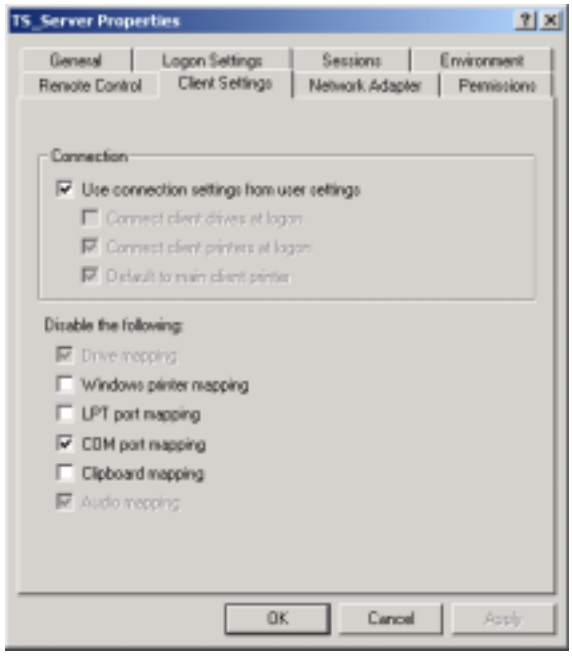
Obr. 33, Nastavení síly šifrování TS



Obr. 34, Nastavení síťové karty, po které bude probíhat komunikace TS

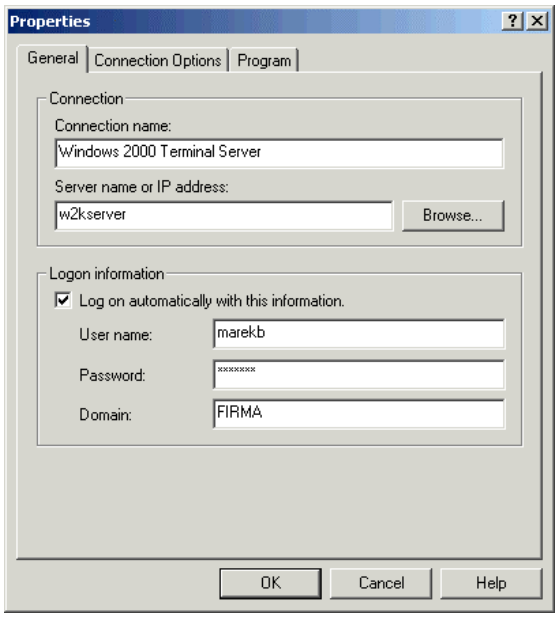


Obr. 35, Nastavení možnosti převzetí session jiného uživatele

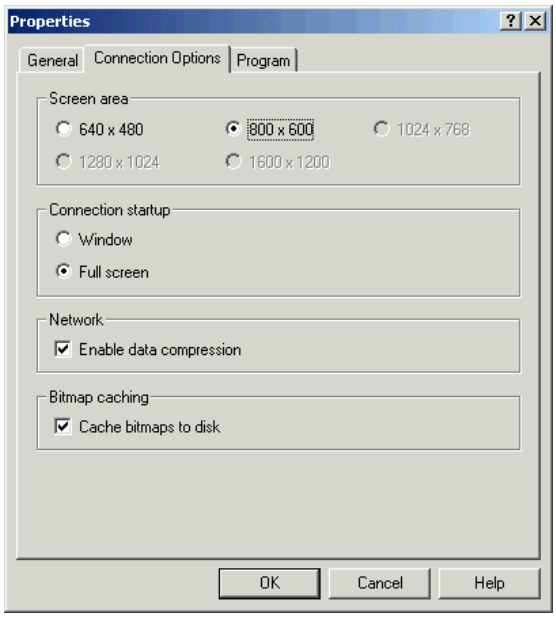


Obr. 36, Nastavení mapování lokálních zařízení z aplikací na TS

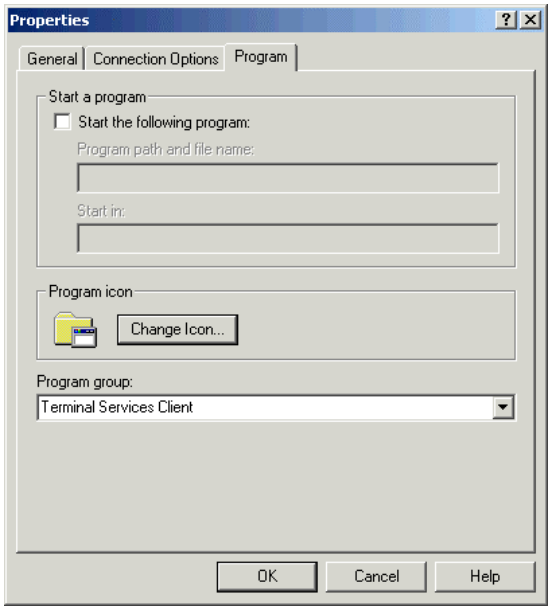
12.3 RDP KLIENT PRO WINDOWS 9.X, NT, 2000



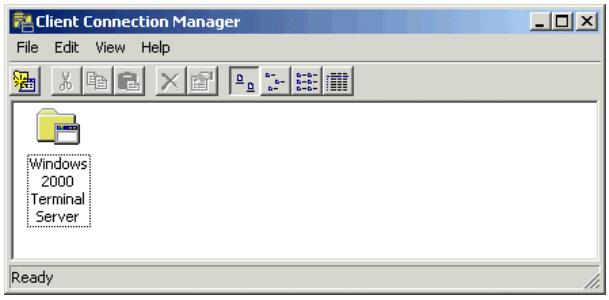
Obr. 37, Pojmenování připojení na TS a nastavení přihlášení uživatele



Obr. 38, Nastavení rozlišení, použití komprese a bitmap cache



Obr. 39, Nastavení automatického spuštění aplikace po přihlášení



Obr. 40, Správce jednotlivých připojení na TS

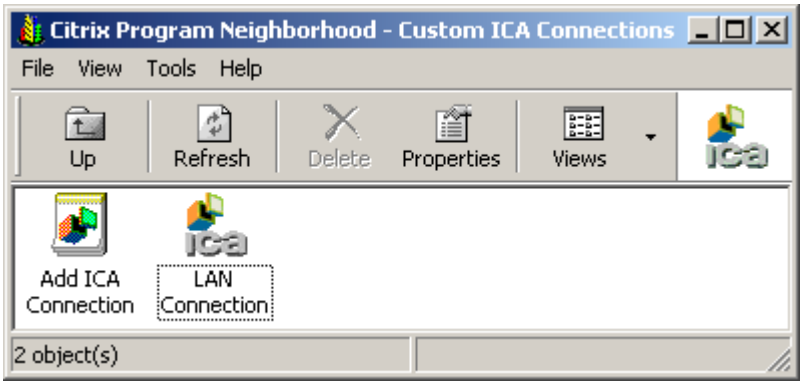
12.4 ICA KLIENT PRO WINDOWS 9.X, NT, 2000

Obr. 41, Nastavení typu síťového připojení

Obr. 42, Nastavení síťového protokolu

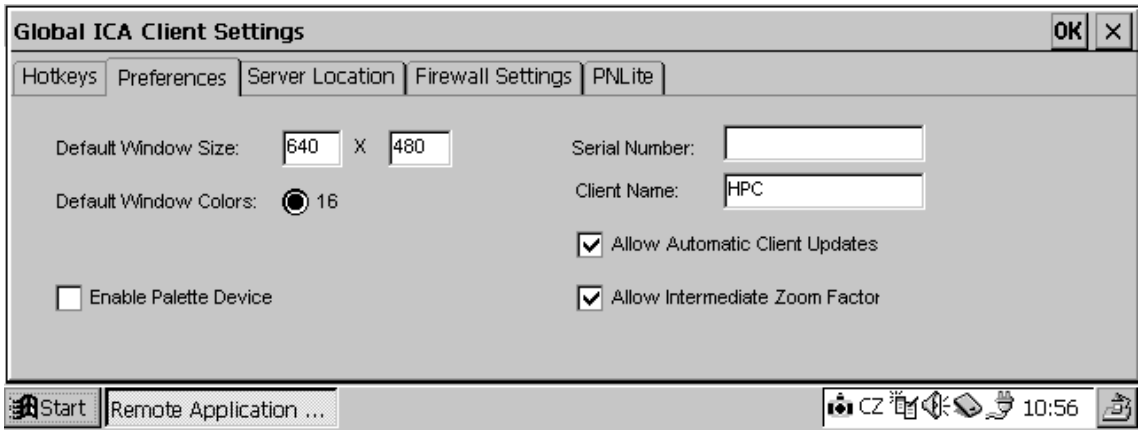
Obr. 43, Nastavení jména, hesla a domény pro přihlášení

Obr. 44, Nastavení počtu barev a rozlišení obrazovky

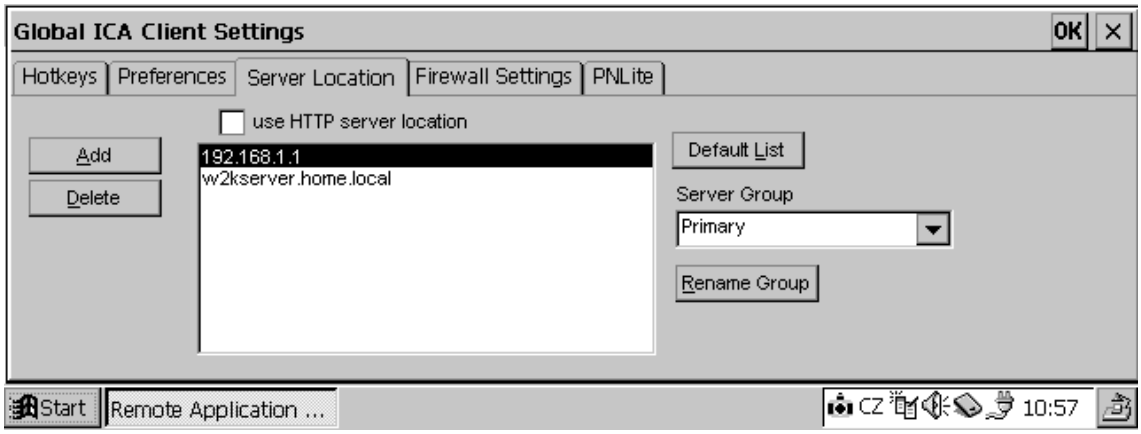


Obr. 45, Správce jednotlivých připojení na TS

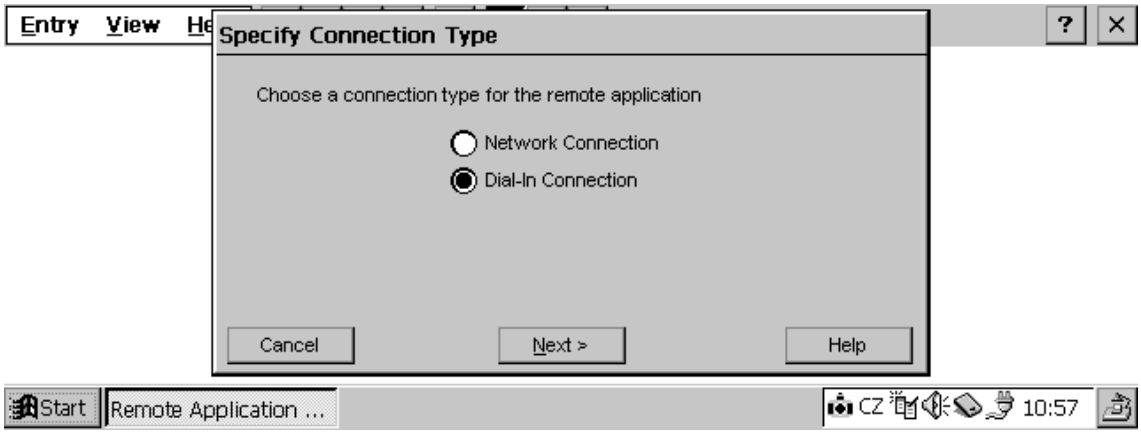
12.5 ICA KLIENT PRO WINDOWS CE



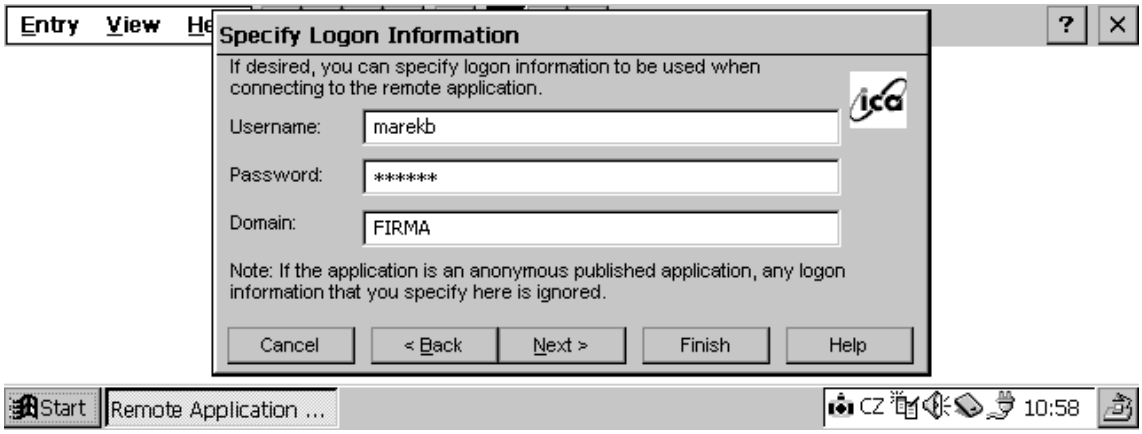
Obr. 46, Nastavení výchozího rozlišení globálně pro všechna připojení



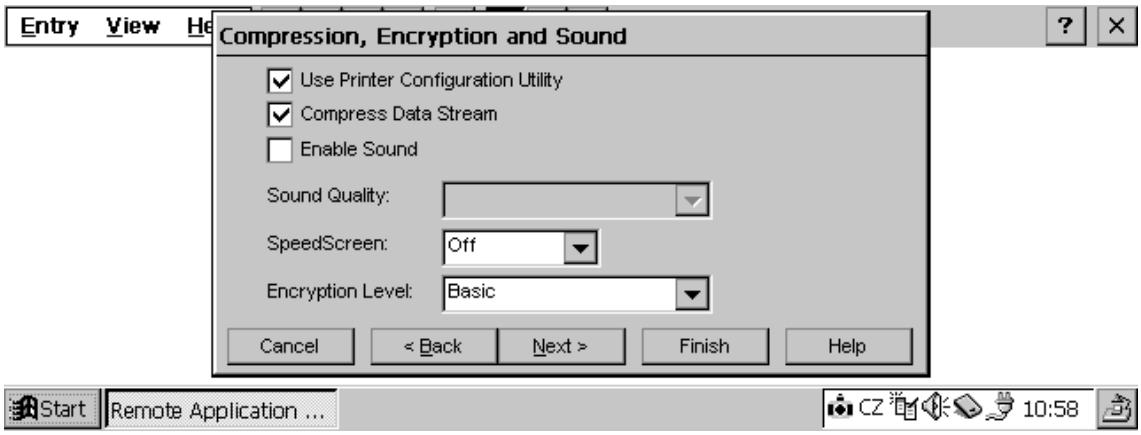
Obr. 47, Nastavení připojení na servery, které poskytují terminálové služby



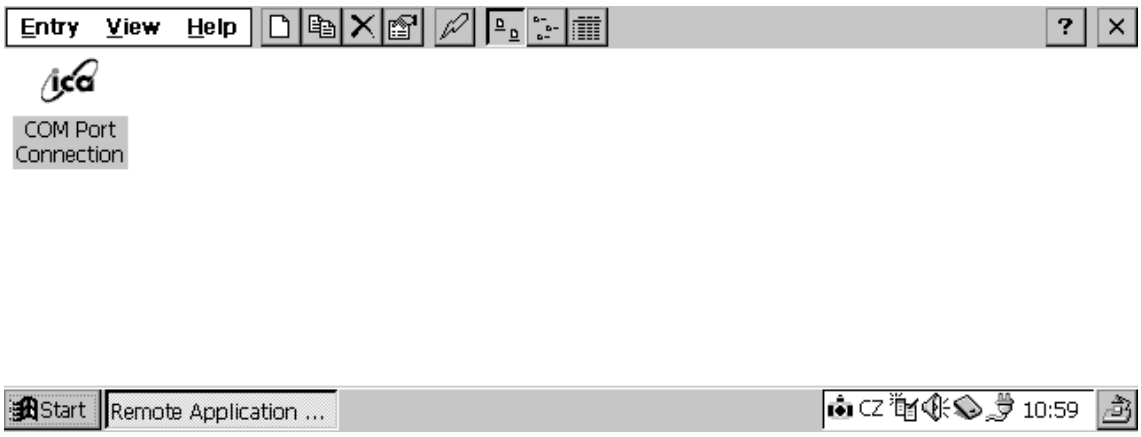
Obr. 48, Výběr typu připojení



Obr. 49, Nastavení jména, hesla a domény pro připojení

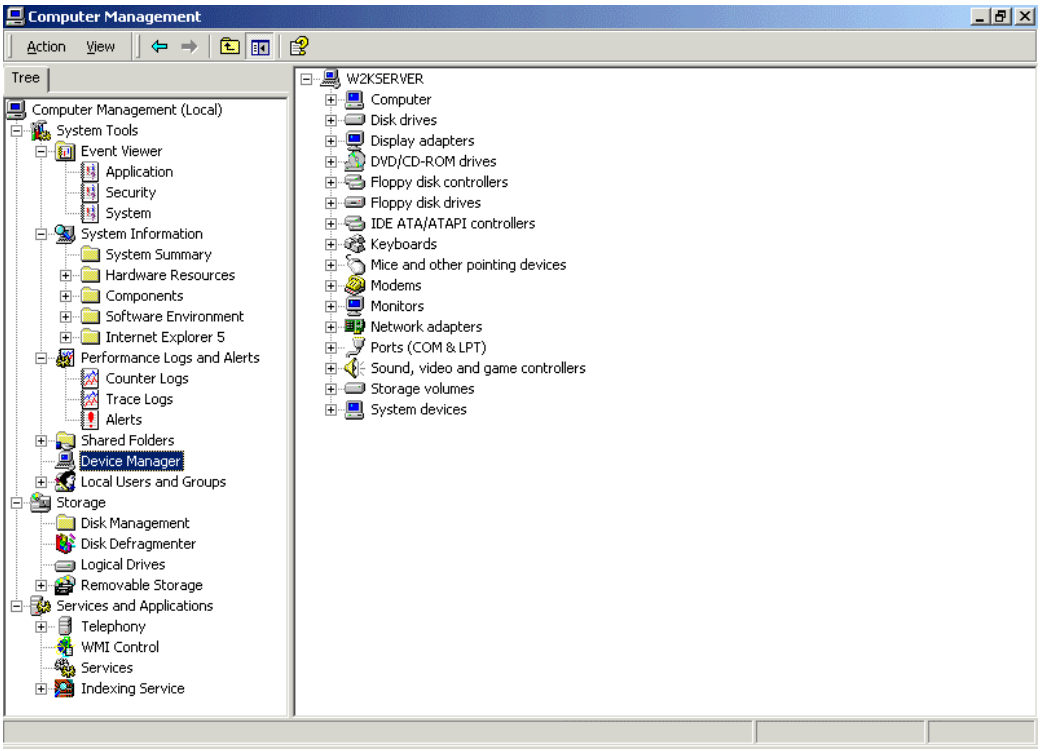


Obr. 50, Nastavení komprese, kvality obrazu a šifrování dat

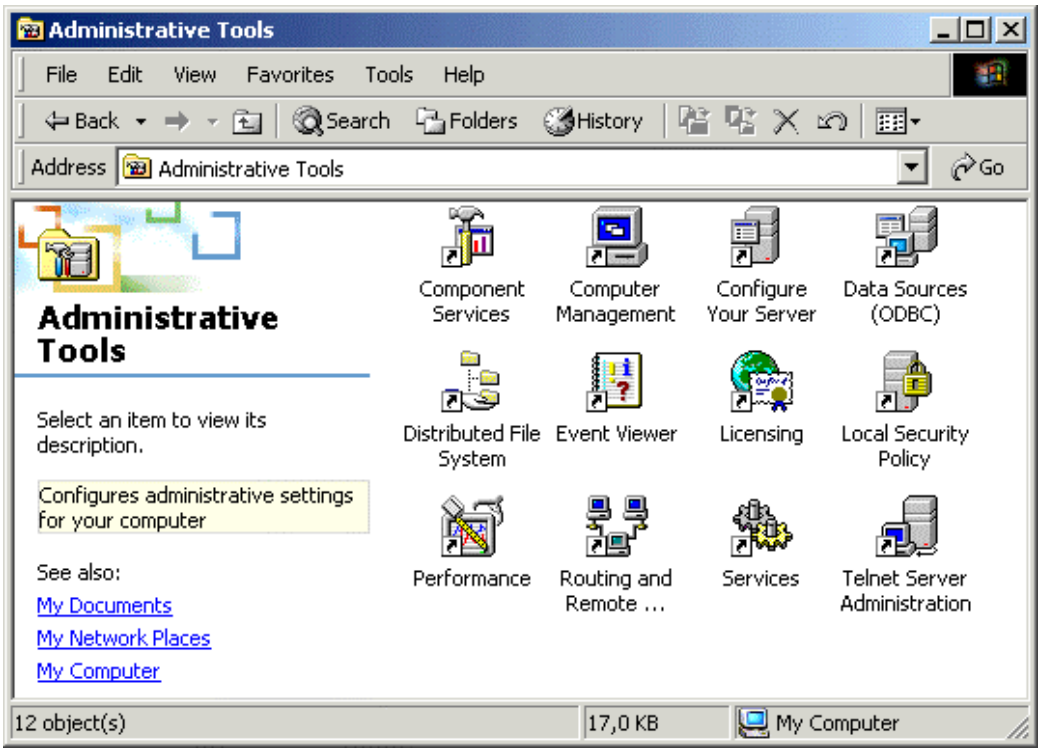


Obr. 51, Správce připojení na jednotlivé TS servery

12.6 SPRÁVA SYSTÉMU



Obr. 52, MMC – Microsoft Management Console – souhrn nástrojů správy systému



Obr. 53, Další nástroje správy systému dostupné přes Control Panel

13. VLASTNÍ INTERNETOVÉ STRÁNKY

Obr. 54, 55, Ukázka vlastních stránek věnovaných problematice Windows 2000