Technische Universität Ilmenau
Fakultät für Elektrotechnik und Informationstechnik
Institut für Informationstechnik
Fachgebiet Kommunikationsnetze

Anbindung mobiler Endgeräte über den Terminal Service

Studienarbeit
von
Martin Heise

Verantwortlicher Professor: Prof. Dr. Jochen Seitz
Hochschulbetreuer: Dipl.-Ing. Maik Debes

Ilmenau, im Juli 2005 (v0.6)

Zusammenfassung

Diese Arbeit befasst sich mit den Microsoft Terminal Services, die es erlauben, auch auf Client-Geräten mit relativ geringen Ressourcen die gewohnten Desktop-Applikationen zu nutzen. Dabei liegt die Aufmerksamkeit primär auf der aktuellen Version des Dienstes, die mit dem Microsoft Windows Server 2003 ausgeliefert wird. Nach den Ausführungen zu Grundlagen und der Installation liegt der Schwerpunkt auf der Nutzung des Remote Desktops sowie dem Praxistest der Usability („Benutzerfreundlichkeit“). Es wird auch untersucht, welche Auswirkungen die beim Einsatz mobiler Endgeräte auftretenden Einschränkungen der Nutzerschnittstelle und der zur Verfügung stehenden Bandbreite haben. Betrachtungen weiterer wichtiger Aspekte wie Sicherheit und die Einbindung in ein Active Directory sowie Vergleiche mit ähnlichen Technologien bilden das Rahmenwerk.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Sowohl drahtlose als auch mobile Kommunikation hält immer weiteren Einzug in unser tägliches Leben. Neben der bereits lange Zeit auch schon im Privatbereich üblichen unidirektionalen Kommunikation - Broadcastmedien wie Radio und TV - hat sich im letzten Jahrzehnt auch ein breiter Markt für die bidirektionale, interaktive Kommunikation herausgebildet. Außer der Weiterentwicklung der mobilen Sprachkommunikation (z.B. von Global System for Mobile communication (GSM) zu Universal Mobile Telecommunications System (UMTS)) ist der aktuelle Trend die mobile Datenkommunikation. Dazu zählen neben einfachem Datenaustausch zwischen örtlich benachbarten Geräten (z.B. via BlueTooth) auch die Nutzung des Mobiltelefons als Modem oder eine teilweise schon flächendeckend vorhandene Versorgung mit Wireless LAN (Wireless Local Area Network (WLAN)).
Die Nutzung eines drahtlosen Internetzugangs für elektronische Austauschmedien wie eMail, News oder Surfen im Internet ist vielerorts bereits zum Alltag geworden. Auch immer mehr Intranets werden durch Wireless LANs ergänzt, so dass z.B. auf dem gesamten Firmengelände oder auf dem Campus einer Universität (wie z.B. der TU Ilmenau) eine drahtlose Nutzung der Netzinfrastruktur möglich ist.
Dabei hat sich in weiten Teilen bereits die Nutzung von Web-basierten Anwendungen etabliert. Die Benutzung eines Webbrowser beschränkt sich schon lange nicht mehr auf das reine Betrachten von Websites. Für viele Nutzer gehört es bereits zum Alltag, via Weboberfläche z.B. ihre eMail-Korrespondenz zu erledigen oder Bestellungen auszulösen.
Neben diesen weitverbreiteten Szenarien eröffnet eine lokale breitbandige Anbindung an ein Intranet weitere Anwendungsgebiete. So ist man damit in der Lage, auch komplexere Übertragungen - wie z.B. einen Multimedia-Stream oder den entfernten Zugriff auf den Desktop einer Workstation - zu realisieren. Dadurch werden nicht nur die Endgeräte leistungsmässig entlastet und der Einsatz von sog. „Thin Clients“ überhaupt erst möglich, sondern es vereinfacht sich in den meisten Fällen auch die Administration, z.B. in Bezug auf Konfiguration und Lizensierung der eingesetzten Software. Nach den bekannten Verfahren wie z.B. dem X11-forwarding aus der Unix-Welt bietet auch die Firma Microsoft für ihre Produktreihe seit ein paar Jahren die Möglichkeit der Nutzung eines betriebssystemintegrierten Remote Desktops an. Umgesetzt wird dies durch die sogenannten „Terminal Services“, die Gegenstand dieser Arbeit sein sollen.

1.1 Zielsetzung

Es wird davon ausgegangen, dass bereits eine funktionsfähige LAN-Infrastruktur sowohl in Hardware (Kabel, Switches, AccessPoints, ...) als auch in Software (Router, DNS-Server, 802.1x, ...) existiert. Der Fokus soll stattdessen primär auf der Anwendbarkeit liegen, wobei sich die Terminal Services nicht nur für den Endnutzer eignen, sondern auch dem Administrator die Gelegenheit geben, fast alle Aspekte der Software-Wartung auch remote durchzuführen.
Primär soll dabei die Basisversion des Terminalservices betrachtet werden, wie sie in Verbindung mit dem aktuellen Produkt aus der Microsoft-Server-Reihe - dem Windows Server

2003 - zur Verfügung steht; auf Erweiterungen (wie z.B. die von der Firma Citrix angebotene Software) oder vergleichbare Technologien soll dabei nur am Rande eingegangen werden.
Dabei soll eine nachvollziehbare Dokumentation über die Installation entstehen, anschließend liegt der Schwerpunkt auf der Nutzung des Remote Desktops sowie dem Praxistest der Usability („Benutzerfreundlichkeit“). Es soll auch untersucht werden, welche Auswirkungen die beim Einsatz mobiler Endgeräte auftretenden Einschränkungen der Nutzerschnittstelle und der zur Verfügung stehenden Bandbreite haben. Dazu kommen unterschiedliche Endgeräte sowie verschiedene Anbindungen dieser an den Terminal Services Server zum Einsatz.

1.2 Gliederung

Nach einer kurzen Einführung in Kapitel 1 und 2 wendet sich Kapitel 3 mit dem ersten Hauptschwerpunkt - der Installation des Dienstes und der damit verbundenen notwendigen Komponenten - an die Gruppe der Administratoren. Dabei werden zuerst die Betrachtungen zu den notwendigen Schritten angestellt und diese anschließend nach Server und Client getrennt beschrieben.
Kapitel 4 beschäftigt sich mit der Anwendung des Dienstes und seinen Möglichkeiten und eröffnet damit den Nutzern den Zugang zu den Terminal Services.
Eine Untersuchung des Systemverhaltens, was es bei der Nutzung zu beachten gibt und welche Probleme auftreten können sind genau so Bestandteil von Kapitel 5 wie auch die Untersuchung der Einschränkungen, die durch Thin Clients, deren beschränkte Ressourcen oder geringe Bandbreite auftreten können.
Weiterführende Aspekte, wie z.B. das Thema Sicherheit oder die Vergleiche mit ähnlichen Technologien werden in Kapitel 6 dargestellt.
Zusammenfassung und Ausblick in Kapitel 7 schließen die Arbeit ab.

Hinweise:

- Tritt die Bezeichnung „Windows“ auf, so ist - wenn nicht anders angegeben - die zugehörige Produktreihe der Firma Microsoft [Microsoft] gemeint; die Warenzeichen sind i.A. eingetragen und geschützt (©, ®, ^{TM}usw.). In der Arbeit wird auf eine durchgehende entsprechende Kennzeichnung verzichtet.

- Die Lizenzen für die hier eingesetzte Microsoft-Software (exklusive Office) werden bereitgestellt im Rahmen der Microsoft Developer Network Academic Alliance (MSDNAA) [MSDNAA]; im Speziellen durch das Projekt Munich Administration aNd Internet Access Control for MSDN Academic Alliance (MANIAC) [MANIAC] an der Technischen Universität Ilmenau, mit freundlicher Unterstützung des dortigen Microsoft Student Consultant - Daniel Kirstenpfad <danielk@studentconsultant.org>. Für den Produktionsbetrieb kommen die Volumenlizenzen der TU Ilmenau zum Einsatz.

2 Hintergrund

2.1 Geschichte

Mit den Terminal Services greift Microsoft eine Technologie wieder auf, die früher - aus primär technischen Erwägungen, da die Clients noch nicht die Leistungsfähigkeit heutiger PCs und mobiler Geräte hatten - sehr verbreitet war (Stichworte: MainFrame, 3270, 5250 oder UNISYS).

> Dieser Bedarf an „server-based computing“ wurde im Umfeld von PC- und Windows-Anwendungen zuerst von der Firma Citrix erkannt und in funktionsfähige Produkte umgesetzt: Mit Hilfe einer Quellcodelizenz konnte durch Änderungen am Systemkern eine mehrbenutzerfähig gewordene Version des Betriebssystems Windows NT 3.51 unter dem Namen WinFrame auf den Markt gebracht werden.
> Als auch Microsoft diesen Trend erkannte, erwarb man kurzerhand die zugrunde liegende Citrix-Technologie MultiWin, die unter der Bezeichnung Windows NT 4.0 Terminal Server Edition in das eigene Betriebssystem Windows NT 4.0 integriert wurde. Später floss diese unter der Bezeichnung Terminal Services als integraler Bestandteil in das Betriebssystem Windows 2000 ein. [Dreyer2002]

Die eigene Integration sieht so aus, dass die Terminal Services unter NT noch ein eingenständiges Produkt sind, im 2000 Server integraler Bestandteil und beim 2003er Server zu einem reinen Dienst („Serverrolle“) wurden.
Die Firma Citrix entwickelte derweil ihr eigenes Produkt WinFrame weiter, konzentrierte sich dann aber auf MetaFrame, ein reines Add-On für den Redmonder Terminalserver. Die hier angestellten Betrachtungen beziehen sich nun hauptsächlich auf die aktuelle Version aus Microsofts Server-Produktfamilie, den Microsoft Windows Server 2003.

2.2 Technik & Technologie

Bei den Terminal Services handelt es sich also primär um eine Client-Server-Technologie. Verwendet wird das Remote Desktop Protocol (RDP). In der vorliegenden Version 5.2 bietet es eine maximale Farbtiefe von 24 Bit; die mögliche Auflösung ist nur noch von den Fähigkeiten des Clients abhängig. Das Protokoll erlaubt auch die Weiterleitung einiger lokaler Ressourcen wie z.B. Laufwerke oder Schnittstellen an den Server.

> Bei der Zuweisung von lokalen Ressourcen handelt es sich um das Durchreichen von verschiedenen Anschlüssen und Geräten des Clients in die Terminalsitzung. Das können lokale Laufwerke wie Disketten, Festplatte oder CD-ROMs sowie COM-Ports (z.B. für Smart Card Reader), Druckerwarteschlangen und Soundkarten sein. Die Unterstützung von USB ist nicht implementiert. Lokal eingerichtete USB-Laufwerke und Drucker werden aber erkannt und über RDP zur Verfügung gestellt. [iX 02/2004, Seite 78ff.]

Standardmäßig wird der Terminal Service an Port 3389 TCP gebunden. In beiden Richtungen wird ausserdem noch eine UDP-Verbindung über unpriviligierte Ports etabliert, welche z.B. zur Übertragung von Audiodaten genutzt wird.

Das RDP selber ist eine Erweiterung des ITU-T T.128 (aka T.SHARE) „application sharing protocol“. Dazu findet man auf der Website des RDesktop-Projekts [rdesktop.org] folgende ITU-T drafts:

- T.128 Draft: Application Sharing Protocol
  `http://www.rdesktop.org/docs/t128.zip`
- T.125 Draft: Multipoint Communication Service
  `http://www.rdesktop.org/docs/t125.zip`

Es lassen sich dazu auch entsprechende Request for comments (RFC) finden; es sei jedoch darauf hingewiesen, dass dies nur der Dokumentation der Ansätze des RDP dient.

- RFC 905: ISO Transport Protocol Specification - ISO DP 8073
  `http://www.ietf.org/rfc/rfc905.txt`
- RFC 2126: ISO Transport Service on top of TCP (ITOT)
  `http://www.ietf.org/rfc/rfc2126.txt`

3 Installation

3.1 Voraussetzungen

Bei den Terminal Services handelt es sich primär um eine Client-Server-Technologie. Benötigt werden demzufolge ein oder mehrere via LoadBalancing zusammengeschaltete Server und die gewünschte Anzahl (mobiler) Clients, jeweils Hard- und Software. Außerdem noch ein Lizenzserver (welcher auf dem Terminal Server mit installiert werden kann) nebst notwendigen Lizenzen. Die mögliche Anzahl der Clients ist nur durch die Anzahl der Lizenzen und die Ressourcen des Servers beschränkt.
Darüber hinaus lassen sich auch Windows XP (home & professional) sowie die vorliegende Client Preview von Windows Longhorn mittels Terminal Services remote bedienen - jedoch kann gleichzeitig nur ein einziger Nutzer den Remote Desktop nutzen.

3.1.1 Server

Zum Server gehören auch hier eine Hardware- und eine Softwarekomponente. Die Auswahl der Hardware richtet sich beim Server primär nach der Anzahl der zu bedienenden Clients. Zu beachten gilt hierbei, daß nicht nur aktive Verbindungen auf dem Server Ressourcen verbrauchen (vgl. auch Abschnitt 4.3 „Beenden der Nutzung“ auf Seite 37).

> Wie unter Windows 2000 gibt es in der 2003er-Version verschiedene Serverversionen, wobei im Terminalserverumfeld nur der Standard beziehungsweise Enterprise Server interessant sind. Der Webserver enthält keine Terminaldienste und der Datacenter Server hat bezüglich dieser Dienste keine zusätzlichen Funktionen. [iX 02/2004]

Auf dem Server werden installiert:

1. das Serverbetriebssystem (hier: Windows Server 2003; alternativ: Windows Server 2000 oder Windows NT 4.0 Server mit Citrix-Aufsatz; Windows NT 3.51 Server oder andere ältere Windows-Varianten können nicht genutzt werden)
2. der Terminal Services Server (bei Windows Server 2003: „Serverrolle“)
3. der zusätzlich notwendige Terminal License Server
   - kann auch auf einem separaten Server installiert werden
   - zu Testzwecken auch ohne möglich; siehe weiter unten (TO-DO: Referenz auf Abschnitt)
4. sowie alle gewünschten Anwendungen (Web/eMail/News, Office, Multimedia, scientific, ...)

3.1.2 Client

Beim Client sind von der Hardware her die geringen Mindestanforderungen einzuhalten, damit die Clientsoftware (der Terminal Services Client) überhaupt ausführbar ist; ansonsten richtet sich die Hardware und Ausstattung des Clients nach dem gewünschten Anwendungsprofil (z.B. Soundwiedergabe/Aufnahme benötigt usw. - siehe Abschnitt 3.2 „Kriterien für die Anschaffung von Client-Geräten“ auf Seite 6).
Die Installation von Komponenten für die gewünschten Nutzer-Applikationen auf dem Client ist nicht notwendig.

Auf den Clients werden installiert:

1. ein die Client-Hardware unterstützendes Betriebssystem
2. der Terminal Services Client („Remote Desktop Connection“)
3. oder alternativ zum Terminal Services Client ein Internet Explorer mit aktiviertem ActiveX

Entsprechende Client-Software ist zur Zeit für folgende Betriebssysteme verfügbar:

- alle Windows-Versionen ab v3.x für die x86-Plattform
- Windows CE
- die drei BSD-Varianten
- Linux
- Apple's MacOS ab Version 8
- die aktuelle Variante des AmigaOS

Für die 64 Bit-Architektur von Intel und AMD sind Clients bereits in der 64 Bit-Version von Windows XP enthalten; bei dem noch nicht als endgülige Version vorliegenden XP-Nachfolger Longhorn ist davon auszugehen, dass sie dort ebenfalls vorzufinden sein werden. Praxistests mit den 64 Bit-Architekturen konnten dabei mangels entsprechender Hardware nicht durchgeführt werden. Gleiches gilt für die von Microsoft mittlerweile nicht mehr gepflegten Windows-Versionen für andere Plattformen wie z.B. MIPS oder die Alpha. Auf Betrachtungen von MacOS vor Version 8 sowie älteren AmigaOS habe ich auf Grund der geringen Relevanz verzichtet.

3.2 Kriterien für die Anschaffung von Client-Geräten

Aus den Anforderungen an die Nutzung der Clients lassen sich (teilweise recht offensichtliche) Kriterien für die Anschaffung von Geräten ableiten, deren folgende Zusammenstellung als Entscheidungshilfe dienen kann.

- Akkulaufzeit, Typ des/der Akkus (z.B. geräteherstellerspezifisch oder handeslübliche Akkus)
- Größe und Gewicht des Gerätes (inkl. Akkus)

- Größe, Auflösung, Helligkeit, Kontrast des Displays
- ggf. mindestens stereophone Klangwiedergabe (oder besser)
- Mikrophon
- Anschlussmöglichkeit für Freisprechanlagen/Headsets (auch z.B. über die passenden BlueTooth-Profile)
- geringe Geräuschbelastung (keine Lüfter, interne Festplatte)
- Möglichkeit, das Display bereits vom Gerät aus vom Seitenverhältnis her umzukehren bzw. um 90° zu drehen
- Bei Geräten, die mit einer Eingabehilfe (z.B. einem Stift) ausgestattet sind, sollte man darauf achten, dass möglichst zum Lieferumfang noch ein Ersatzstift gehört, da dieser als loser Bestandteil des Gerätes leicht verloren gehen kann. Dem beugt eine fixierende, im Gerät integrierte Halterung zumindestens teilweise vor.
- bestimmte Funktionen/Tasten extra vorhanden: Enter, ESC, Cursor, on-screen-keyboard ein/ausblenden, rechte Maustaste (!), ...
- eingebaute Lesegeräte für SmartCard oder Memory-Devices
- Schnittstellen: USB, IrDA, PCMCIA, BlueTooth, FireWire (IEEE 1394), WLAN (IEEE 802-Serie), ...

3.3 Lizensierung

Der Einsatz von Microsoft's Terminal Services erfordert eine mehrstufige Lizensierung. Für mindestens die folgende Software und Komponenten ist eine entsprechende Lizenznahme notwendig:

- Das Basis-Betriebssystem (gilt für alle Windows-Varianten)
- Der Terminal Services Server
- Pro Client, der den Terminal Service nutzen soll, eine Client Access License (Client Access License (CAL)) - unabhängig vom auf dem Client eingesetzten Betriebssystem. Die CALs können sich dabei auf Geräte (Device CALs) oder auf Anwender (User CALs) beziehen. Jeder Lizenzserver verwaltet beide Arten.
  Hinweis: Die via MSDNAA verfügbaren Versionen (inkl. Standard und Enterprise) sind laut Aussage unseres Microsoft Student Consultants jeweils auf zwei CALs beschränkt und nicht upgradebar!
- Die gewünschte Anwendungssoftware. Bei dieser ist insbesondere auf die Art der Lizensierung zu achten: ist sie z.B. pro CPU, pro Server, pro angelegtem Benutzer oder pro gleichzeitig arbeitendem Benutzer - um nur einige mögliche Lizenzierungsmodelle zu nennen. Es ist somit durchaus möglich, dass bestimmte Software einen Lizenzvertrag hat, der eine gleichzeitige Nutzung von mehreren Endgeräten aus via Remote Desktop nicht zulässt, obwohl damit die Software rein technisch trotzdem nur auf einem Rechner (nämlich dem Server) ausgeführt wird.

- und natürlich für das Betriebssystem des Clients; unabhängig davon, ob man dort Produkte unter einer freien Lizenz wie der GPL oder andere einsetzt. Wer die Kosten für eine Lizenz von Produkten wie Windows XP scheut und über keinen Volumenlizenzvertrag verfügt, kann hier z.B. auch vielleicht noch vorhandene Lizenzen wie Windows 98 einsetzen.

Zur Vervolländigung des Lizensierungsvorganges gehört sowohl beim Windows Server 2003 als auch beim Terminal Server die bereits von Windows XP her bekannte Produktaktivierung, die nur bei den Volumenlizenzen entfällt. Die an der TU Ilmenau via MANIAC verfügbare Software unterliegt den Microsoft Developer Network (MSDN)-Lizenzverträgen und daher ebenfalls der Aktivierungspflicht.
Bei unzureichender Lizensierung präsentiert das System ggf. dem Nutzer entsprechende Hinweise, wie sie in Abschnitt 5.5.2 „Lizenzprobleme“ auf Seite 50 zu finden sind. Meine Praxistests haben gezeigt, dass die Client-Lizenzen zumindestens teilweise auf dem Client selber verwaltet werden; so wird z.B. durch Neuinstallation eines Clients eine neue temporäre Lizenz vom Server für diesen Client angefordert, und mit der Linux-Software ist eine Nutzung der Terminal Services nach deren Aktivierung auch ohne Installation von CALs zeitlich unbeschränkt möglich.
Weitere Informationen zum Lizenzmodell gibt es bei Microsoft selber unter der Adresse `http://www.microsoft.com/germany/serverlizenzierung`.
Die Installation des Terminal License Servers wird in Abschnitt 3.6 „Installation des Terminal License Servers (TLS)“ auf Seite 21 beschrieben.

3.4 Installation des Servers

Die Betrachtungen zur Installation des Servers habe ich hierbei auf die aktuelle Version aus Microsoft's Windows Server-Reihe beschränkt, da bei einer Neuinstallation vom Einsatz alter und nicht mehr vollständig von Microsoft unterstützter Software abzuraten ist.
Auch auf PCs, die mit Windows XP laufen, lässt sich remote auf den Desktop zugreifen. Da dies jedoch auf einen gleichzeitig angemeldeten Benutzer beschränkt ist, führe ich das hier nur kurz aus.

3.4.1 Microsoft Windows XP

Für die Nutzung des Remote Desktops unter Windows XP ist bei einer Standardinstallation nur die Freischaltung der gewünschten Benutzerkonten notwendig (TO-DO: screenshot), und dies auch nur, wenn diese Konten nicht zur Gruppe der Administratoren gehören. Ansonsten ist darauf zu achten, dass der entsprechende Dienst („...“ TO-DO: Name einsetzen) auch läuft.
Abschnitt 3 „Installation der Terminal Services“ auf Seite 16
(TO-DO: das noch mal genauer beschreiben, wie man das bei XP aktiviert, Rechte, Unterschiede zu Win2003 Server usw. - WICHTIG!)

3.4.2 Microsoft Windows Server 2003

Der Windows Server 2003 steht seit dem 24. April 2003 zum Verkauf bereit und ist in vier verschiedenen „Editionen“ verfügbar, welche alle nur auf einer x86-Plattform (32 oder 64 Bit, also i386 bzw. IA64) lauffähig sind:

- Web Edition
- Standard Edition
- Enterprise Edition
- Datacenter Edition

Im Gegensatz zu früheren Versionen von Windows NT existiert kein Support mehr für MIPS, die Alpha oder andere Plattformen. Dabei ist dies nicht das einzigste Kriterium, in welchem sich die Versionen unterscheiden. Je nach notwendiger Konfiguration und möglicherweise später in Betracht kommenden Erweiterungen sollte man genau überlegen, welche Version man einsetzen will. Eine kurze Auswahl bietet Tabelle 3.1, genauere Details zu den Unterschieden zwischen den einzelnen Versionen gibt es bei Microsoft [Win2003-Editionen]. Diese technisch schon jeweils unterschiedlichen Versionen gibt es dann auch noch in unterschiedlichen Sprachen. Da es durchaus zu erwarten ist, dass die Terminal Services von unterschiedlichen Leuten genutzt werden, empfehle ich den Einsatz des sogenannten Multilanguage User Interface (MUI) (TO-DO: link), welches es ermöglicht, jedem Benutzer eine individuelle Sprache für seine Oberfläche einzustellen. Das MUI gibt es jedoch nur für die englischsprachige Version als Add-On, dafür dann jedoch in zahlreichen Sprachen (TO-DO: welche genau).
Weitere Unterschiede in der damit dreidimensional werdenden Produktmatrix gibt es schließlich in den verschiedenen Lizensierungsmodellen (siehe dazu Kapitel Abschnitt 3.3 „Lizensierung“ auf Seite 7).

Merkmal	**Web Edition**	**Standard Edition**	**Enterprise Edition**	**Datacenter Edition**
Prozessor-support	x86 32 Bit	x86 32 Bit	x86 32 und 64 Bit	x86 32 und 64 Bit
max. Anzahl Prozessoren	2	4	8	64
max. Arbeits-speicher	2 GB	4 GB (32 Bit) 32 GB (64 Bit)	32 GB (32 Bit) 1 TB (64 Bit)	64 GB (32 Bit) 1 TB (64 Bit)
Ressource Manager	N/A	N/A	verfügbar	verfügbar
Administrativer RemoteDesktop	verfügbar	verfügbar	verfügbar	verfügbar
Terminal Server	N/A	verfügbar	verfügbar	verfügbar
Clustering & SessionDirectory	N/A	N/A	verfügbar	verfügbar

Tabelle 3.1: Unterschiede zwischen den Versionen von Windows Server 2003

getestete Version:

Die hier in der Arbeit vorgestellten Betrachtungen wurden nun an Hand der folgenden Version durchgeführt:

Microsoft Windows Server 2003, Enterprise Edition, build 3790

Dabei wurden sowohl die englische als auch die deutsche Version, die Erweiterung MUI und die Unterschiede durch das mittlerweile erschienene ServicePack (SP)1 (build 1433) auf einer 32 Bit-Plattform untersucht. Zum Test der IA64-Version steht mir zurzeit leider keine Hardware zur Verfügung.

Installation:

Die Grundinstallation unterscheidet sich nur unwesentlich von der eines bisherigen New/Next Technologie (NT)-Servers und ist von halbwegs versierten Admins problemlos meisterbar. Einige Besonderheiten, die ich festgestellt habe und hier erwähnen möchte, befinden sich in Anhang D.

Was mir negativ auffiel:

Zu den Problemen und Wünschen meinerseits an die Microsoft-Produktfamilie führe ich auf meiner Internetseite eine unabhänging von dieser Arbeit existierende „Microsoft Windows - bugreport & wishlist/feature-request-Liste“ [Windows-wishlist], aus der ich einige für die Terminal Services relevanten Punkte hier aufgreifen möchte.

Probleme:

- **Explorer (lokal):** Sobald Windows von sich aus ein Explorer-Fenster updated, verschwindet ein eventuell vom Benutzer bereits aufgerufenes Kontextmenü. Konsequenz: wenn der Aufbau eines Fensterinhaltes länger dauert (z.B. via Netzwerk oder weil es große Dateien sind, aus denen Windows die Medieninformationen extrahiert), muss der Nutzer warten, bis der Prozess abgeschlossen ist, bevor er eine Datei anklicken und deren Kontextmenü aufrufen kann. Dies behindert ein zügiges Arbeiten insbesondere bei den mobilen Endgeräten mit ohnehin schon eingeschränkten Eingabemöglichkeiten (z.B. PDAs mit Stift als Eingabehilfe).
- **Netzwerkumgebung:** Die Angabe des Kommentars zu den Geräten wird doppelt angezeigt, dafür fehlt die Spalte mit den Namen der Geräte (erst seit Windows XP; bei Windows 2000 funktionierte das noch) - die Kommandozeilenversion „net view“ weist diesen Fehler nicht auf. Laut Aussage unseres Microsoft Student Consultant handelt es sich dabei aber nicht um einen Bug, sondern um eine Designänderung. Deren Sinn erschließt sich mir leider nicht, da die Wahrnehmung der Informationen (schnelle Übersicht und gezielte Auffindung bei den Rechnernamen) damit deutlich erschwert wird.
- Bei einem Teil der Netzwerkoperationen (z.B. WinS/NETBIOS-Namensauflösung) „steht“ der Rest des Rechners nahezu. Ein Grund dafür konnte bisher noch nicht ausfindig gemacht werden.

- **Regionaleinstellungen:** Unabhängig von der eingestellten Sprache eines Nutzers werden die Namen der Wochentage aus seinen Regionaleinstellungen abgeleitet. Benutze ich also in Deutschland ein Windows, Sprachversion „englisch“, so heissen die Wochentage dennoch „Montag, Dienstag, ...“.
- **Kopieren/Verschieben:** Die Restzeit wird oft falsch geschätzt, bei sehr langen Zeiten (z.B. ISO-Images) tritt sogar ein direkter Rechenfehler auf (Restzeit wird in mehreren Monaten ausgegeben). Da man die Zeit im Voraus seltenst genau angeben kann, würde ich hier prinzipiell vorschlagen, das Wort „Restzeit“ durch eine Schätzung zu ersetzen und diese Dialogfenster ähnlich denen zu gestalten, die der Internet Explorer beim HTTP-download anzeigt. In Verbindung mit der Nutzung des Remote Desktops kann es durch die falsche Anzeige der Restzeit beim Benutzer zu Verunsicherungen kommen, ob und wie lange er eine Terminalsitzung noch aufrecht erhalten muss oder ob ggf. beim Abbruch der Verbindung mit Datenverlust zu rechnen ist.

Auf meiner Internetseite sind noch weitere Probleme geschildert, die u.a. die Installation des Servers betreffen. Diesbezüglich sei auch wiederum auf Anhang D verwiesen.

Wünsche:

- **generell:** Ist abzusehen, dass irgend ein Vorgang mehrere Sekunden oder länger dauert (als Referenz sollte hierbei ein mindestens ein Jahr altes System dienen), sollte ein entsprechender Hinweis angezeigt werden; wenn möglich mit Fortschrittsanzeige. Dies sollte insbesondere beim Start von Programmen erfolgen, da nicht jedes Programm sofort eine Ausgabe liefert, was bei vielen Nutzern zum erneuten Ausführen der Aktion (z.B. des Programmstarts) und damit meistens zu Fehlern führt.
- **Fenster:** Seit langem wird von vielen Benutzern dringlichst und sehnlichst gewünscht, dass das im Augenblick aktive Fenster auch im Hintergrund sein kann; dass man wie z.B. bei der Amiga-Workbench die Fenster frei staffeln kann und neue Fenster sich nicht zwingend in den Vordergrund drängeln müssen. Insbesondere bei kleinen Auflösungen und dem entsprechend geringeren Platzangebot auf dem Bildschirm, wie es bei mobilen Endgeräten vorkommt, kann dies sehr bei der Arbeit behindern. Beim Benutzen der Tastatur kann ein automatischer Fokuswechsel bei den Fenstern sogar zu Fehleingaben und Datenverlusten führen.
- **Regionaleinstellungen:** Im Hinblick auf die Tatsache, dass an einem universitären Server durchaus auch Benutzer mit unterschiedlicher Nationalität arbeiten, wäre es wünschenswert, wenn man (pro Benutzer) festlegen könnte, mit welchem Tag die Woche beginnt.
- **Einstellungen allgemein:** Bei jeder Einstellung sollte klar ersichtlich sein, ob diese sich nur auf das eigene Profil oder global auswirkt (besonders für Administratoren wichtig).

Was mir positiv auffiel:

- siehe dazu auch Abschnitt 3.4.4 „Windows Server 2003 security“ auf Seite 14
- **default-Einstellungen:** das Administrator-Konto sowie die Anmeldung verzichten auf einen Teil der bunten Gimmicks, die bei XP das System für den Endanwender schmackhafter machen sollen (das bei XP eingeführte „Luna“-Thema kann jedoch trotzdem bei Bedarf aktiviert werden)

- **default-Einstellungen:** beim Beenden des Servers (Neustart, Herunterfahren) wird die Angabe eines Grundes verlangt:

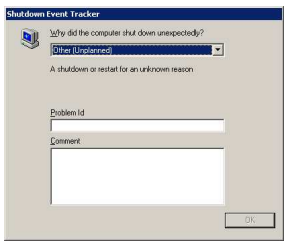

Abbildung 3.1: Shutdown Event Tracker

Dieses „*Shutdown Event Tracker*“ genannte Feature kann man mit Hilfe des in Abschnitt 3.4.3 „Active Directory“ auf Seite 12 noch näher beschrieben „*Group Policy Editor*“ auch wieder abschalten. Die notwendige Einstellung findet man dort unter „*Local Computer Policy - Computer Configuration - Administrative Templates - System*“ im Punkt „*Display Shutdown Event Tracker*“.

3.4.3 Active Directory

Soll der Terminal Server in ein Active Directory (AD) eingebunden werden oder gar selber als AD-Server fungieren, so sind einige Besonderheiten zu beachten. Ich führe hier nur die grundlegendsten Eigenschaften auf, die beim Einsatz von Terminal Services zu beachten sind; für weiterführende Betrachtungen zum Thema Active Directory sei auf weitere Literatur (z.B. [Spealman2003]) verwiesen.

Wird der Terminal Server selber zusätzlich noch als Domain Controller betrieben, so gibt Microsoft selber an, dass folgende Windows-Versionen sich nicht an der Domain anmelden und auch keine Ressourcen der Domain nutzen können (vgl. Abb. 3.2):

- Windows 95
- Windows NT 4.0 SP3 oder älter

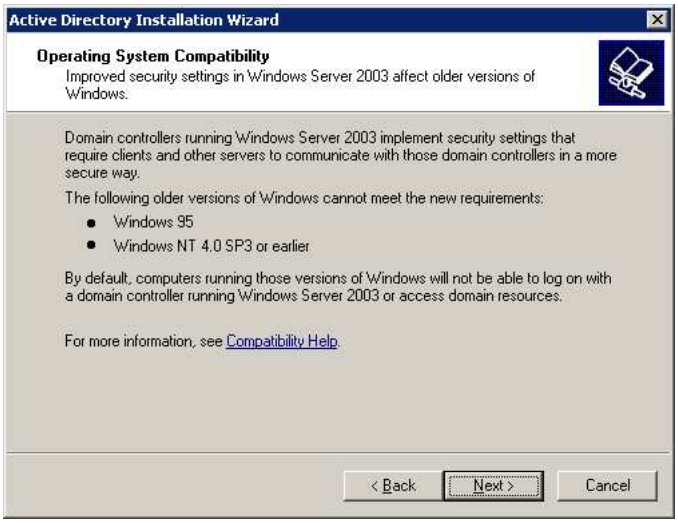

Abbildung 3.2: Hinweis zur Betriebssystemkompatibilität bei Aufstufung zum Domain Controller

Hierbei sei ausdrücklich darauf hingewiesen, dass sich das auf die Anmeldung des Clients selber an der Domainan bezieht - eine Windows 95-Workstation kann deswegen trotzdem als Terminal Services (TS)-Client genutzt werden, da die Anmeldung innerhalb einer Terminal-Session ja nicht nur an, sondern auch auf dem Server selber erfolgt.
Neben der Betriebssystemkompatibilität sind jedoch auch die (verschärften) Sicherheitseinstellungen beim Windows Server 2003 zu beachten. So wird bei der Aufstufung zum Domain Controller automatisch das Anmelden via Terminal Services auf die Gruppe der Administratoren beschränkt:

Abbildung 3.3: Hinweis zur Änderung der Sicherheitsrichtlinien bei Aufstufung zum Domain Controller

Diese Einschränkung kann mit Hilfe des „*Group Policy Object Editor*“ wieder reduziert werden. Dieser Editor ist entweder als Snap-In für die Microsoft Management Console (MMC) oder über direktes Ausführen von „`gpedit.msc`“ zu erreichen.
Dort ist dann unter „*Local Computer Policy - Computer Configuration - Windows Settings - Security Settings - Local Policies - User Rights Assignment*“ die Richtlinie „*Allow log on through Terminal Services*“ zu bearbeiten und um die gewünschten zugelassenen Benutzer zu ergänzen, wie ich es in Abb. 3.4 am Beispiel des Benutzers „Joe“ dargestellt habe.

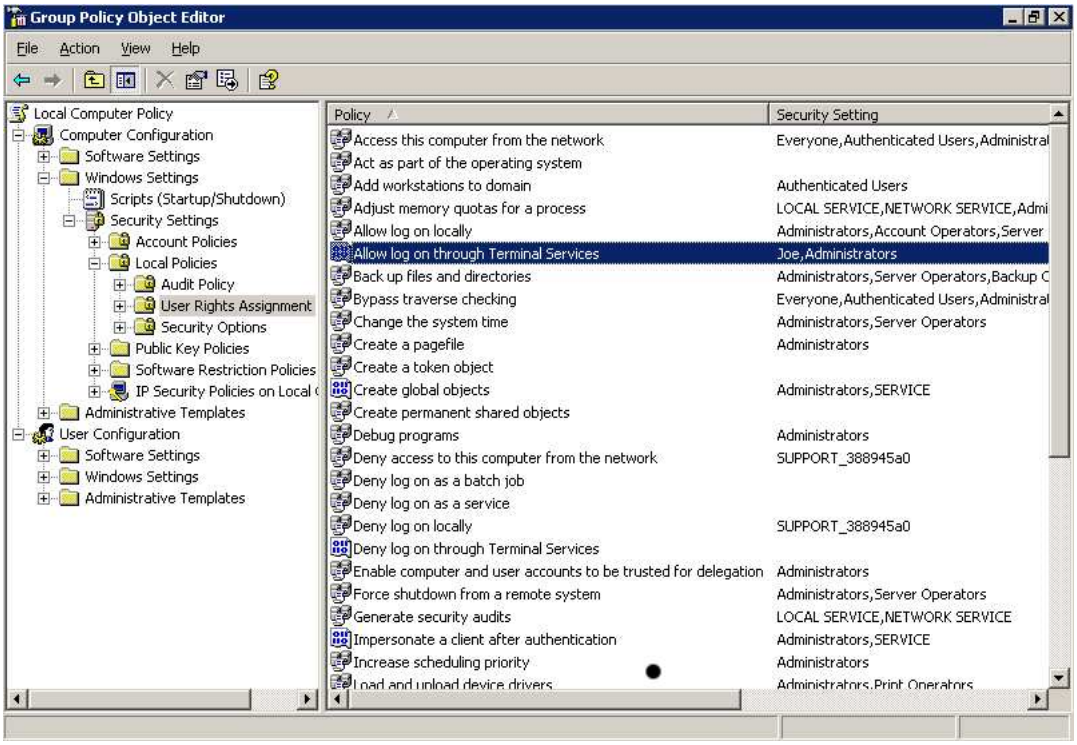

Abbildung 3.4: Richtlinie zum Festlegen der erlaubten Terminal Services-Logins bei einem Domaincontroller

Zur einfachereren Verwaltung der Gruppenrichtlinien gibt es seit 2003 von Microsoft die „*Group Policy Management Console*“; weitere Informationen dazu finden sich bei Microsoft unter `http://www.microsoft.com/windowsserver2003/technologies/management/grouppolicy` und `http://www.microsoft.com/windowsserver2003/gpmc` und auch in Sekundärliteratur wie z.B. [LANline spezial III/2005, Seite 22].

3.4.4 Windows Server 2003 security

Bezüglich der Sicherheitsaspekte hat sich bei Windows Server 2003 gegenüber den Vorgängerversionen erfreulicherweise einiges getan. So wurden einige Default-Einstellungen restriktiver gefasst, bestimmte Komponenten (wie z.B. der Internet Informations Server IIS) werden standardmäßig nicht mehr mit installiert und auch einige nicht zwingend benötigte Dienste sind deaktiviert.
Sicherheit scheint seit Windows Server 2003 bzw. Windows XP SP2 bei Microsoft erstmals wichtiger zu sein als Funktionalität, so wurden laut [tec 04/2004] die Entwickler zu einer Reihe von Schulungen über die Erstellung von sicherem Code geschickt.
Die Sicherheitsimplikationen durch Integration des Servers in ein Active Directory habe ich bereits in Abschnitt 3.4.3 „Active Directory“ auf Seite 12 angesprochen; hier nun noch einige weitere Aspekte:

- default-Einstellungen: der Bildschirmschoner ist per default auf „password protect“ gestellt
- Microsoft Internet Information Server (IIS) stark überarbeitet, nach der Standardinstallation ist er nur noch bei der WebEdition sofort aktiv

- da ein Server eigentlich keine Workstation sein sollte (dedizierter Server), sind im Microsoft Internet Explorer (IE) verstärkte Sicherheitseinstellungen vorgenommen worden (TO-DO: screenshots - WICHTIG!)
- (TO-DO: ActiveX+JavaScript: per default enabled oder disabled? - WICHTIG!)
- Verbesserungen beim automatischen Software-update über die Microsoft-Dienste System Update Service (SUS) und Windows Update Service (WUS)
- Gruppe „Everyone“ stark eingeschränkt gegenüber früher
- Anonyme Nutzer sind nicht länger Mitglied der Gruppe „Everyone“
- Dienste laufen nicht mehr immer unter dem lokalen System-Account
- Login via Netzwerk ist mit nicht gesetztem (leeren) Passwort nicht mehr möglich
- „Windows Server 2003 Security Guide“ und „Threats and Countermeasures Guide“ (siehe Linksammlung)
- Security Templates: MMC - Security Templates & Security Templates Analysis Tool (TO-DO - ggf. verschieben in Sicherheits-Abschnitt)
- allein bei den Gruppenrichtlinien 150 neue Parameter im Vergleich zu Windows 2000 (na gut, ob das jetzt gut ist ... - KISS ...)
- drei Sicherheitsstufen, vier DomainController-Richtlinien (TO-DO ...)
- (TO-DO: IPsec)

Weitere grundlegende Hinweise zum Verbessern der Systemsicherheit gibt es auf meiner Homepage im Bereich IT-Security unter „Härten/hardening“ [hardening].

3.5 Installation der Terminal Services

Für die Installation der Terminal Services sind mehrere Schritte notwendig, die im Nachfolgenden am Beispiel des Windows Server 2003 beschrieben werden sollen. Dabei beschränke ich mich in den Ausführungen auf die Installation eines einzelnen Servers ohne den Citrix-Aufsatz. Für die Einrichtung einer Terminalserverfarm sei auf externe Literatur - wie z.B. [LANline spezial III/2005, Seite 18] - verwiesen.
(TO-DO: Was davon ist fuer den Browser-basierten Zugang notwendig?)

1. *Hardware*
   Ein geeigneter PC (siehe Abschnitt 3.1.1 „Server“ auf Seite 5) mit Netzwerkanschluss je nach gewünschtem Typ. Es wird aus Sicherheitsgründen empfohlen, den Anschluss an das Netzwerk erst herzustellen, wenn das Einspielen der Patches und updates sowie die Konfiguration abgeschlossen sind.
2. *Betriebssystem: Windows Server 2003*
   Ausführliche Informationen zum Windows Server 2003 finden sich in Abschnitt 3.4 „Installation des Servers“ auf Seite 8.

3. *Rolle hinzufügen: Terminal Services*
   ACHTUNG: Hierbei wird der Server unter Umständen ohne Rückfrage neu gestartet!
   Ist der Server bereits Teil einer Windows-Domain, kann diese Administration u.U. nicht lokal vorgenommen werden.
   (TO-DO: Bildsche)
   Der Server muss anschließend noch für remote-logins freigeschaltet werden. Dies geschieht in der Systemsteuerung unter „System“. Dort den Reiter „Remote“ auswählen und „Allow users to connect remotely to your computer“ aktivieren.

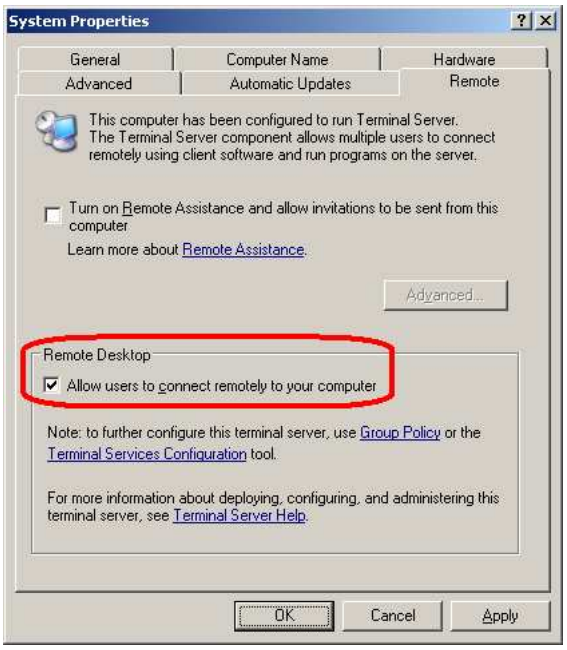

Abbildung 3.5: Freischalten des Remote-Logins

4. *Anlegen der Benutzer und Hinzufügen der Benutzer zur Gruppe „Remote Desktop Users“*
   Mitglieder der Gruppe “Administratoren“ können jetzt den Remote Desktop nutzen. Alle anderen Benutzer müssen erst explizit mit entsprechenden Rechten ausgestattet werden. Dies erfolgt im Großen und Ganzen wie bisher gewohnt unter Windows NT. Wie die Einrichtung erfolgt, welche Gruppen gebildet werden usw. sollte der vorher festgelegten Policy entsprechen (siehe Abschnitt 6.1 „Sicherheit“ auf Seite 52). Hier die wichtigsten Schritte am Beispiel meines Testservers:

   a) Im Computer Management unter System Tools - Local Users and Groups - Users findet man die aktuelle Nutzerliste. Dort kann man neue Nutzer anlegen, wie dies bereits von Windows NT her bekannt ist durch Rechtsklick mit der Maus oder Aktivierung des Menüs „Action“ und Anwählen des Menüpunktes „New User...“.

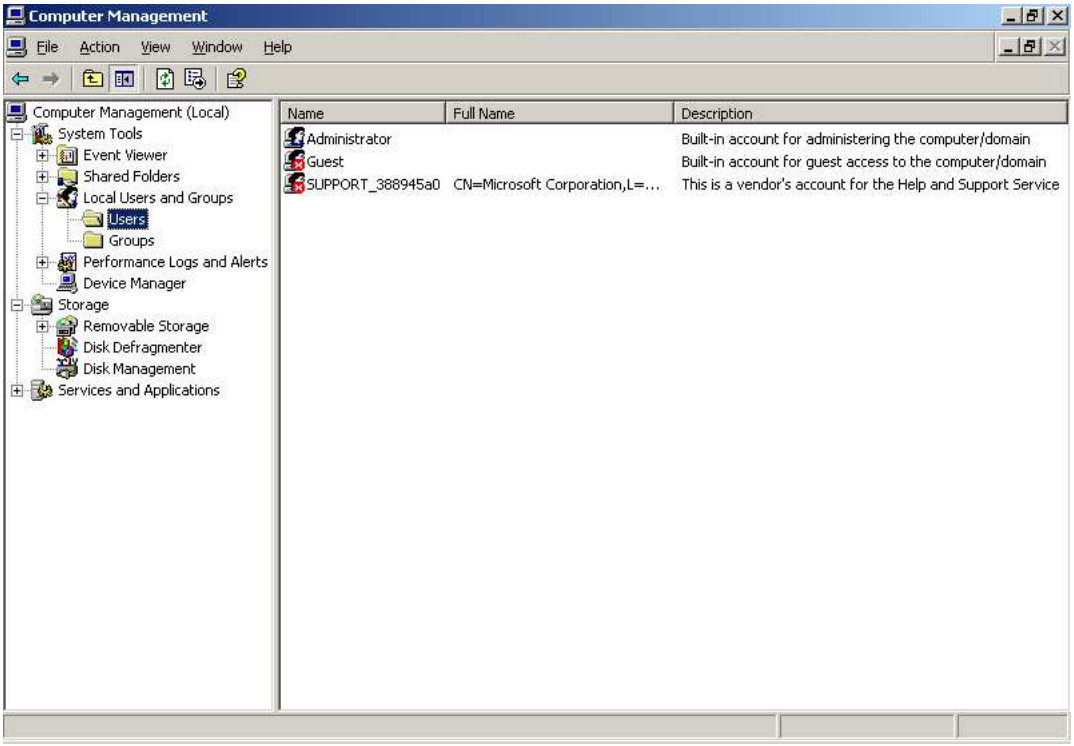

Abbildung 3.6: Lokale Benutzer

b) Der daraufhin erscheinende Dialog zum Erstellen eines neuen Nutzers entspricht den bisheriger NT-Versionen und weist keine Remote Desktop (RD)-Spezifika auf.

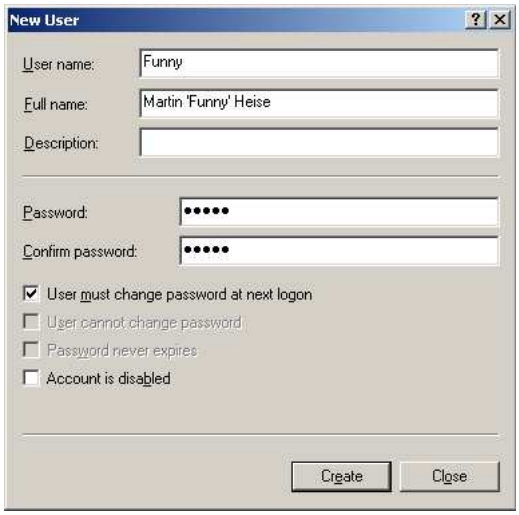

Abbildung 3.7: Dialog zum Erstellen eines neuen Nutzers

c) Anschließend öffnet man die Eigenschaften des Benutzers. Unter dem Reiter „Member of“ gilt es nun, die benötigten Gruppenmitgliedschaften festzulegen. Weiter geht es dann mit der Schaltfläche „Add“ ...

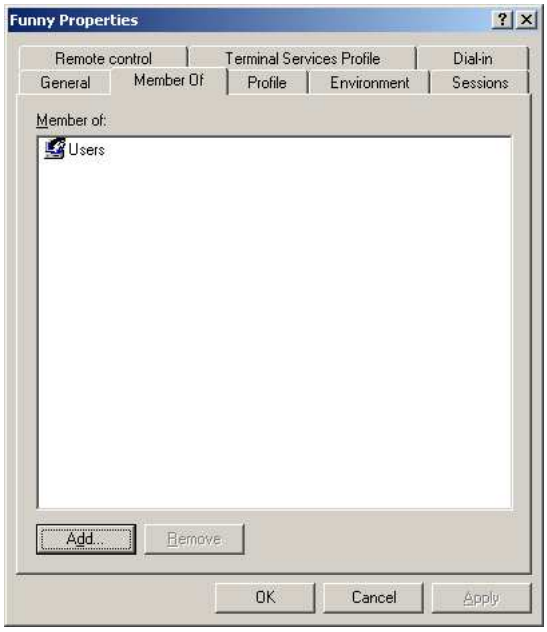

Abbildung 3.8: Gruppenmitgliedschaften eines Nutzers

d) Im nun folgenden Dialog wird man aufgefordert, die gewünschten Gruppen auszuwählen. Da das Beispiel rein lokal arbeitet, kann direkt mit der Schaltfläche „Advanced“ zur Gruppenauswahlliste weitergeschaltet werden. Bei nicht-lokaler Definition von Nutzern und/oder Gruppen wäre vorher noch die Auswahl des Servers/DomainControllers mit Hilfe der Schaltfläche „Locations“ notwendig; oder man spezifiziert die Domain direkt durch Voranstellen des Domainnamens und eines „\“ vor dem Nutzernamen, wie es auch an anderen Stellen bei Windows üblich ist.

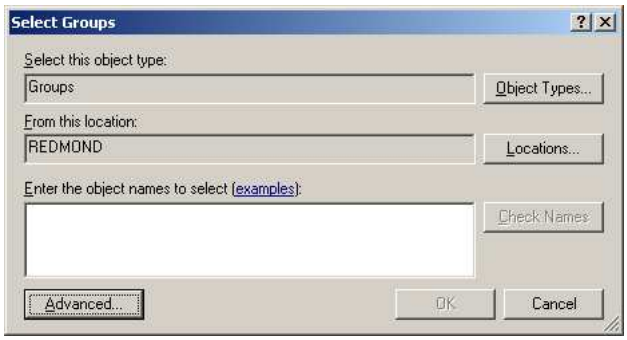

Abbildung 3.9: Gruppenauswahl

e) Durch Betätigen der Schaltfläche „Find Now“ wird die darunter befindliche Liste mit den gewünschten Suchobjekten - in diesem Fall also den Nutzergruppen - gefüllt. Primär wichtig ist hierbei die Auswahl der Gruppe „Remote Desktop Users“. Weiterhin je nach der security policy z.B. die Gruppen „Users“ und „Power Users“. Ist die Auswahl komplett, kann sie mit „OK“ bestätigt werden. Der Dialog wird damit wieder verlassen.

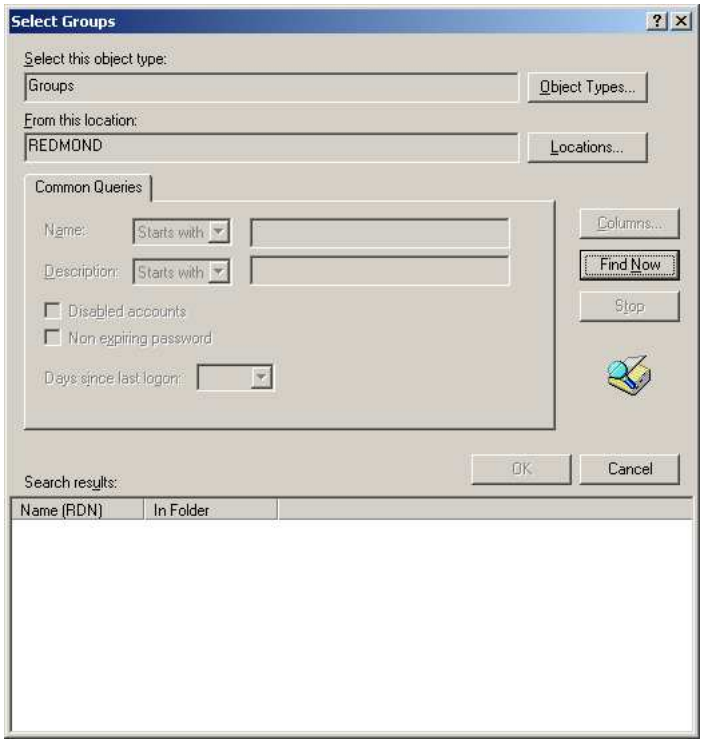

Abbildung 3.10: erweiterte Gruppenauswahl

f) Nun werden einem noch einmal die ausgewählten Objekte (in unserem Fall: Gruppen) zusammengefasst präsentiert. Es ist auch möglich, dieses Textfeld direkt zu editieren und mit Hilfe der Schaltfläche „Check Names“ deren Schreibweise und ggf. Namen und Prefix zu überprüfen. Mit „OK“ wird auch hier wieder die Auswahl bestätigt und der Dialog geschlossen. Damit ist die Gruppenauswahl abgeschlossen und der Nutzer kann sich von nun an via RDP anmelden.

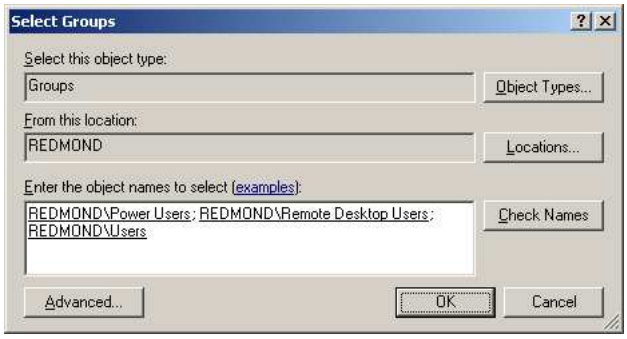

Abbildung 3.11: getätigte Gruppenauswahl

3.5.1 Remote Desktop Web Connection

(TO-DO: Quelle fuer den Download)
Getestet wurde hierbei die serverseitig installierte Version „Remote Desktop Web Connection 5.2.3790“.
Mit Hilfe der Remote Desktop Web Connection ist es möglich, auch von Arbeitsstationen aus auf den Server zuzugreifen, auf denen kein Terminal Services Client installiert ist.

Stattdessen muss auf dem Client der Internet Explorer mit aktiviertem ActiveX auf dem Client installiert sein. Dieses Zusammenspiel funktionierte im Praxistest aber nur auf der Windows-Plattform und nicht auf Apple's MacOS. Von einem generellen Browser-basierten Zugang, wie ihn z.B. Citrix Metaframe bietet, kann hier also nicht gesprochen werden.
Auf dem Server ist dafür neben der Installation des IIS zusätzlich noch die Installation der „*Remote Desktop Web Connection*" notwendig, bei der es sich im Wesentlichen um ein ActiveX-Control handelt. Ausserdem wird eine Standard-Website unter der URL `http://servername/TSWeb` installiert. Mit folgendem Code-Ausschnitt lässt sich das ActiveX-Control auch auf eigenen Websites einbinden („xxxx" ist dabei durch die build-Nummer des ActiveX-Controls zu ersetzen):

```
<OBJECT language="vbscript" ID="MsRdpClient">

  CLASSID="CLSID:9059f30f-4eb1-4bd2-9fdc-36f43a218f4a"

  CODEBASE="msrdp.cab\#version=5,2,xxxx,0"

  WIDTH=<%
    resWidth = Request.QueryString("rW")
    if resWidth < 200 or resWidth VIEWASTEXT > 1600 then
      resWidth = 800
    end if
    Response.Write resWidth
  %>

  HEIGHT=<%
    resHeight = Request.QueryString("rH")
    if resHeight < 200 or resHeight > 1200 then
      resHeight = 600
    end if
    Response.Write resHeight
  %>

</OBJECT>
```

Das ActiveX-Control selber heist dabei `msrdp.ocx` und befindet sich in der Cabinet-Datei `msrdp.cab`, welche sich wiederum nach der Installation der Remote Desktop Web Connection in deren Installationsverzeichnis (Standard: `C:\InetPub\wwwroot\TSWeb`) befindet.
Die Bedeutung der Parameter des ActiveX-Controls lassen sich mit Hilfe von Tools wie `oleview.exe` oder dem „*Visual Basic Object Browser*" anzeigen.

3.5.2 Weitere Konfigurationsoptionen

Neben der grundlegenden Einrichtung der Terminal Services gibt es noch weitere Konfigurationsmöglichkeiten, von denen ich einige hier vorstellen möchte.
(TO-DO) - Anzahl Logins pro User auf 1 beschraenken = sinnvoll
- Admin besser nicht oder auf 2 Logins beschraenken; sonst Gefahr des Aussperrens

3.6 Installation des Terminal License Servers (TLS)

Der Terminal Service kann ohne Installation des Terminal License Server (TLS) nur für 120 Tage genutzt werden. (90 Tage bei Windows 2000 Server), danach läuft er im sogenannten „administrative mode“ (max. 2 Verbindungen gleichzeitig). In der Praxis ließ der 2003er Server jedoch nur noch Consolen-Verbindungen zu; ansonsten war auch keine Verbindung als Administrator mehr möglich, ebensowenig das lokale Übernehmen von Sitzungen. Erst nach der Produktaktivierung konnten Sitzungen wieder aufgenommen werden.

Laut [iX 02/2004, Seite 78] ist bei Windows 2000 nur ein Lizenzserver innerhalb einer Domain im Active Directory erlaubt; ohne ServicePack kann es u.U. dazu kommen, dass Clients keine echte Lizenz erwerben können und daher nur die temporäre 90-Tage-Lizenz erhalten.

> Unter Windows 2003 sieht das anders aus. Der Lizenzserver funktioniert nun ohne Reboot, er muss nicht mehr auf einem Domain Controller installiert sein und es dürfen mehrere Lizenzierungsserver in einer Domain aktiv sein. Diese teilen sich zwar nicht die Lizenzen, aber bei Ausfall des Hauptlizenzservers gibt es wenigstens noch jemanden, der temporäre Lizenzen ausstellen kann, die neuerdings sogar 120 Tage gültig sind. Von welchem Lizenzserver sich ein Terminalserver bedient, kann der Administrator über die Registry steuern, womit er zum Beispiel Lizenzen einzelner Abteilungen dediziert verwalten kann. [iX 02/2004, Seite 78f.]

Weitere Informationen zu den benötigten Lizenzen bietet Abschnitt 3.3 „Lizensierung“ auf Seite 7. Im Einzelnen sind nun folgende Schritte notwendig:

1. *Installation des TLS*
   Der TLS ist beim Windows Server 2003 als Windows-Komponente über die Systemsteuerung auszuwählen:

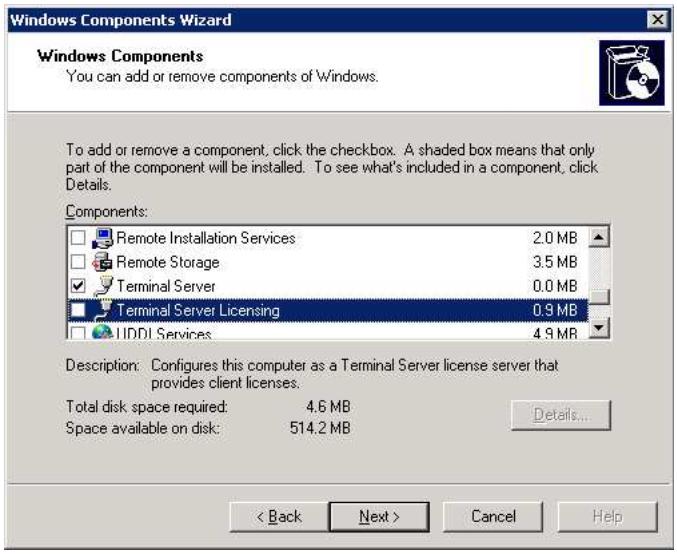

Abbildung 3.12: Windows-Komponente hinzufügen: Terminal License Server

Als einzigste Option bei der Installation ist der Gültigkeitsbereich des TLS sowie der Speicherpunkt der Lizenzdatenbank anzugeben:

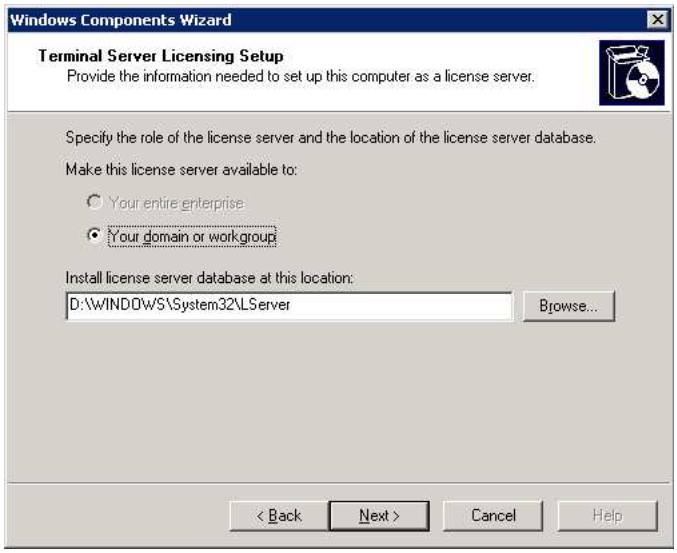

Abbildung 3.13: Optionen bei der Installation des Terminal License Server

2. *Aktivierung des TLS*
   Der grundlegende Sachverhalt ist wie beim Server selber oder wie schon von XP bekannt. Zum Aktivieren wird in der Gruppe „Administrative Tools“ im Startmenü oder der Systemsteuerung der Punkt „Terminal Server Licensing“ aufgerufen.

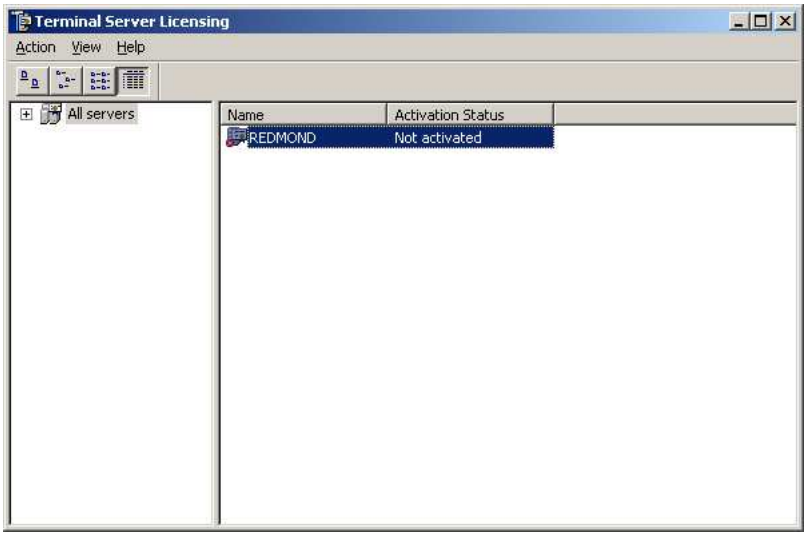

Abbildung 3.14: Terminalserverlizenzierung

Im Kontextmenü des gewünschten Servers startet man über „Aktivate Server“ den „Terminal Server License Server Activation Wizard“:

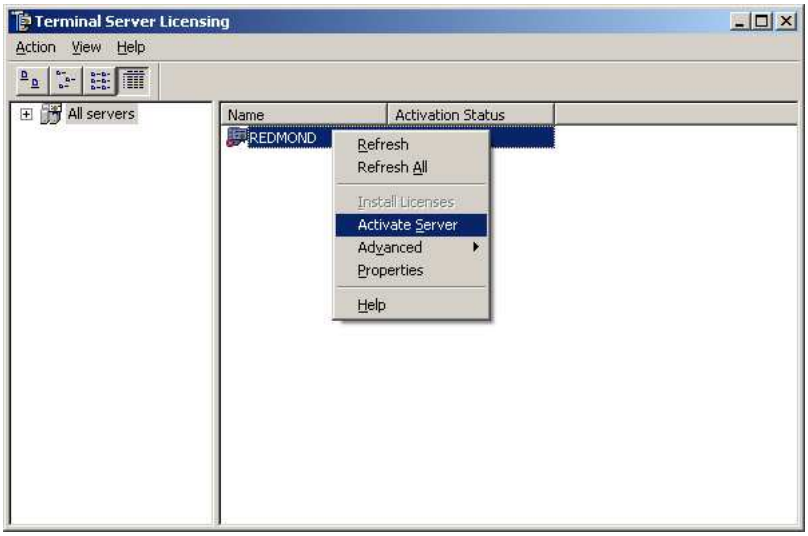

Abbildung 3.15: Aktivierung des Terminal License Servers

Abbildung 3.16: Terminal Server License Server Activation Wizard

Die Aktivierung erfordert zwingend die Angabe persönlicher Daten wie Firma, Ansprechpartner und Telefonnummer:

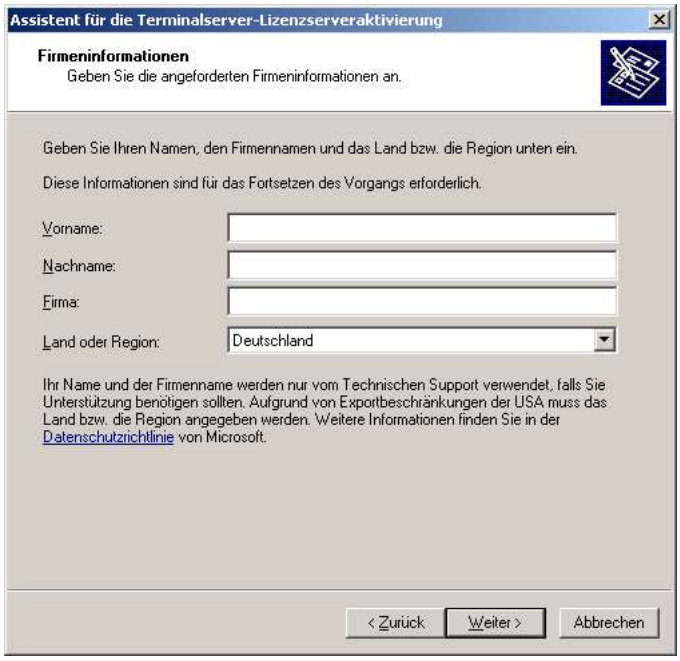

Abbildung 3.17: TLS-Aktivierung: notwendige persönliche Daten

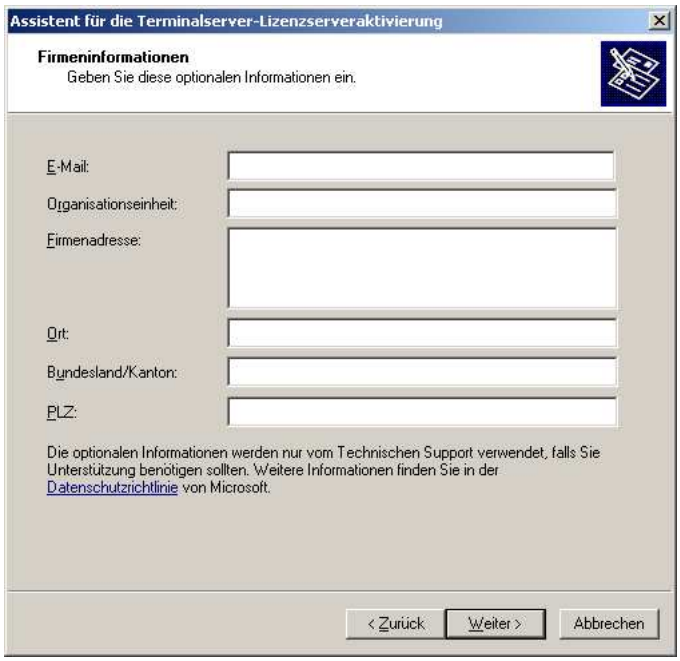

Abbildung 3.18: TLS-Aktivierung: optionale persönliche Daten

Der Assistent fragt im Folgenden nun nach der gewünschten Aktivierungsmethode. Die Aktivierung kann auch via Telephon (0800-freecall) erfolgen. Jedoch ist hier zum Zeitpunkt dieser Arbeit kein automatisiertes Verfahren vorgesehen, sondern man wird mit einem Mitarbeiter verbunden.

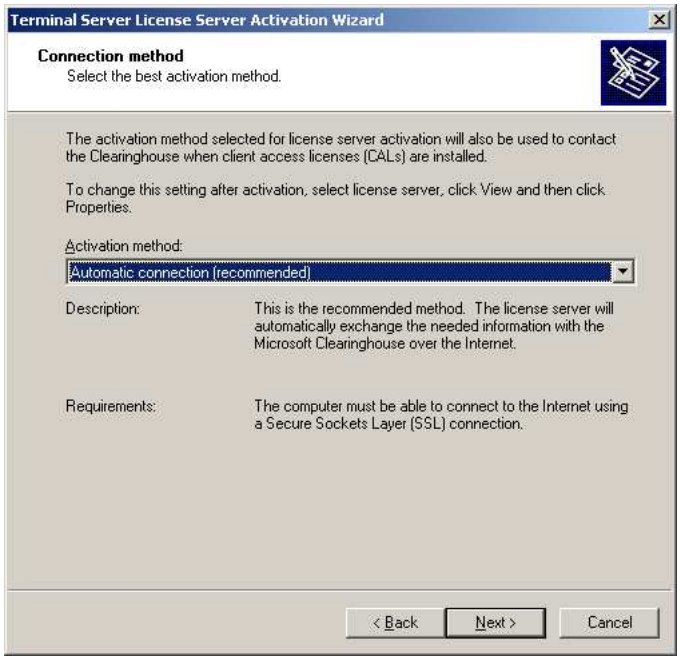

Abbildung 3.19: Auswahl der Aktivierungsmethode des Terminal License Servers

Die nun folgende Auswahl des eigenen Landes dient hauptsächlich zum Ermitteln der naheliegendsten Microsoft-Abteilung, über die die Aktivierung vorgenommen werden kann.

Abbildung 3.20: Regionsauswahl für die Aktivierung des Terminal License Servers

Daraufhin wird im nächsten Fenster die Rufnummer angegeben, unter der man Microsoft zum Zwecke dieser Aktivierung erreichen kann. Außerdem findet man hier die „Product ID“, die man dem telefonischen Support mitteilen muss. Dieser erteilt

einem daraufhin eine „License Server ID“, die man zum Abschluss der Aktivierung in diesem Dialog eingeben muss.

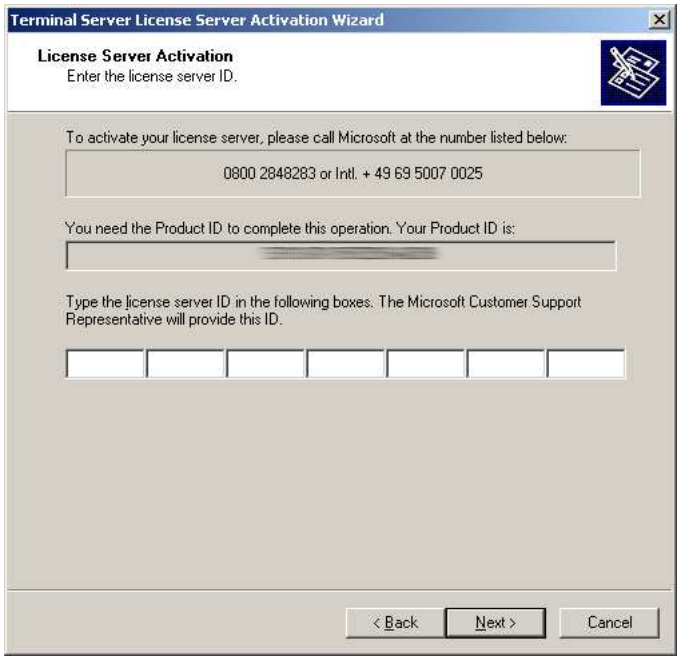

Abbildung 3.21: Letzer Schritt bei der Aktivierung des Terminal License Servers

Damit ist die Aktivierung des Terminal License Servers abgeschlossen und der Assistent startet automatisch den Assistenten zur Installation der Client Access Licenses (CALs).

3. *Erwerb und Installation der Client Access Licences (CALs)*
   Der Assistent zur Installation von CALs kann auch nachträglich gestartet werden. Dazu ist wieder das Programm „Terminal Server Licensing“ zu starten und diesmal im Kontextmenü des betreffenden Servers der Punkt „Install Licenses“ auszuwählen.

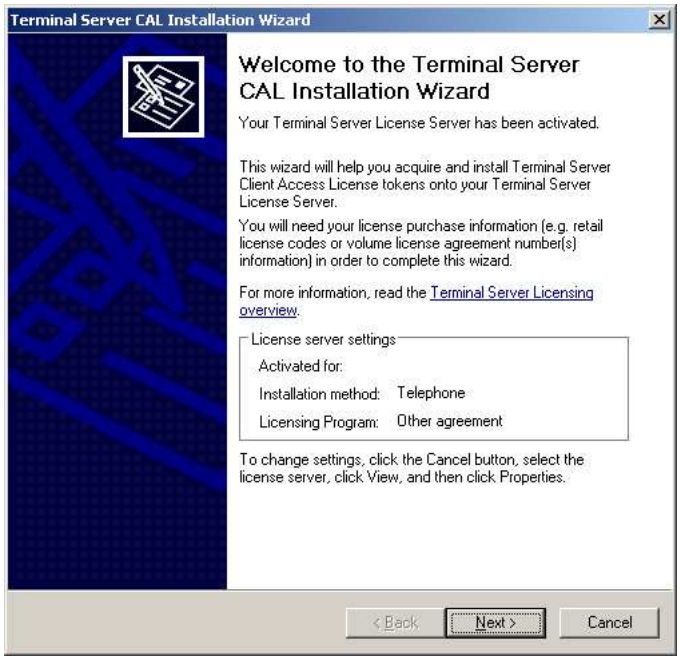

Abbildung 3.22: Terminal Server CAL Installation Wizard

Dies konnte ich jedoch an meinem Testserver nicht durchführen, da ich über keine CALs verfüge und mir die Universität diese aus rechtlichen Gründen auch nicht zur Verfügung stellen kann.

Durch einen Eintrag in der Registry kann der Terminalserver einem bestimmten Lizenzserver zugeordnet werden. Damit ist es dann möglich, dass Lizenzen nur von z.B. einer einzelnen Abteilung genutzt werden können. Der RegKey kann mit folgendem Template per Group Policy Objects (GPO) eingerichtet werden. Beim Windows Server 2003 hat sich dieser Wert gegenüber der Vorversion geändert, dort hieß es noch „`DefaultLicenseServer`“. [iX 03/2004, Seite 10]

```
Class Machine
Category "DATAGROUP"
  KEYNAME "System\CurrentControlSet\Services"
  POLICY "TS License Server"
    PART "Standard Lizenz Server (NetBIOS Name):" EDITTEXT
      KEYNAME "System\CurrentControlSet\Services\TermService\Parameters"
      VALUENAME "LicenseServers"
      MAXLEN 15
      REQUIRED
    END PART
  END POLICY
END Category; DATAGROUP
```

3.7 Installation der Clients

Nachdem nun der Terminal Services Server installiert ist, folgen die Clients. Bei mobilen Endgeräten kommt hier oft Windows CE zum Einsatz.

Da es sich beim Remote Desktop Client um eine Netzwerk-Applikation im User-Space des Betriebssystems handelt, ist nur das Vorhandensein einer funktionierenden TCP/IP-Verbindung notwendig; jedoch keine zusätzlichen Treiber oder Kernel-Module. Je nach Netzwerkverbindung ist noch die Installation weiterer Komponenten - z.B. eines VPN-Clients - notwendig. Der Terminal Services Server sollte sich anschließend anpingen lassen. Die reinen zum Starten einer Remotedesktopverbindung notwendigen Software-Anpassungen sind beim Client im Vergleich zum Server gering und werden im Folgenden beschrieben.

3.7.1 Browser-basierter Zugang

Der Browser-basierte Zugang setzte im Praxistest eine Windows-Plattform und als Browser einen IE mit aktiviertem ActiveX voraus, was diese im ersten Moment plattformunabhängig erscheinende Zugangsart dann doch wieder auf das klassische Szenario reduziert. Da der IE bei Windows immer automatisch mitinstalliert wird, sind für den Browser-basierten Zugang keine weiteren Installationen nötig; es ist nur darauf zu achten, dass in den Sicherheitseinstellungen des IE für die Website des Terminal Servers die Ausführung von ActiveX zugelassen ist.

3.7.2 Apple MacIntosh

Für den Apple ab MacOS Version 8 existiert ein eigener Client, wenngleich der Einsatz unixoider Clients bei MacOS X auf Grund der geänderten Betriebssystembasis ebenso möglich ist.
Der Client wird dabei sowohl auf der Internetseite von Apple als auch der von Microsoft zum freien Download angeboten:

- `http://www.apple.com/downloads/macosx/networking_security/remotedesktopconnectionclie`
  `html`
- `http://www.microsoft.com/mac/otherproducts/otherproducts.aspx?pid=remotedesktopclient`

3.7.3 Unixoide (wie BSD & Linux)

Da die meisten Plattformen jenseits von Microsoft mehr oder weniger kompatibel zu gängigen Unix-Standards sind, habe ich diese Betriebssysteme hier zusammengefasst. Einzelne Spezifika für die verschiedenen BSD-Varianten, Linux-Distributionen oder für Apple sind dem Administrator in der Regel bekannt oder aber im Fall der openSource-Unix-Derivate vollständig dokumentiert.
Unter Unixoiden stehen mehrere Client-Varianten zur Verfügung; z.B.:
(TO-DO: Links)

- grdesktop: GNOME frontend for the rdesktop client
- rdesktop: RDP client for Windows NT/2000 Terminal Server
- tsclient: Windows Terminal Services (RDP) client for GNOME
- krdc: KDE Remote Desktop Client
- grcm: GNOME Remote ... (TO-DO: kann der ueberhaupt WTS?)

Die Installation ist abhängig von der eingesetzten Distribution; z.B. unter Debian GNU/Linux mittels „`apt-get install tsclient`“. (TO-DO: Trennen Front- und Backend, Dependencies)

Bei Verwendung von KDE ab v3.3 muss rdesktop ab v1.3.2 installiert oder die v1.3.1 gepatched werden:

1. Patch für rdesktop v1.3.1 downloaden (`http://webcvs.kde.org/cgi-bin/cvsweb.cgi/~checkout~/kdenetwork/krdc/rdp/rdesktop.patch?rev=1.1;content-type=text\%2Fplain`) und in den Source-Path von rdesktop legen
2. im Source-Path von rdesktop ausführen: `patch -p 0 -i rdesktop.patch`
3. rdesktop neu kompilieren & installieren (z.B. mit „`make && make install`“)

3.7.4 Windows 16 Bit (v3.x)

Auch für die noch vorhandenen 16bit-Versionen von Microsoft Windows gibt es einen Terminal Services Client. Dieser hat jedoch im Gegensatz zum 32bit-Remote-Desktop-Client einen weitaus geringeren Funktionsumfang, und zwar die klassische KVM-Variant (Keyboard, Video, Maus) - auf Zusatzfunktionen wie die Weiterleitung lokaler Laufwerke oder Schnittstellen und auch auf die Audio-Übertragung muss der Anwender hier verzichten. Die Installation enthält keine weiteren Besonderheiten; nach der Installation findet man - wie unter Windows 3.x gewohnt - eine neue Programmgruppe vor. Weitere Details zur 16 Bit-Version des Terminal Services Client befinden sich in Anhang C.
Die 32 Bit-Version des Remote Desktop Clients lässt sich auch nach Installation des Windows-32 Bit-Subsystems für 16 Bit-Windows („Win32s“) nicht installieren.

3.7.5 Windows 32 Bit (Versionen 9x/ME, NT & 2000)

Der Remote Desktop Client lässt sich ohne Probleme auf dem üblichen Weg installieren und steht dann zur Ausführung unter „Start - Programs - Remote Desktop Connection“ bereit.

3.7.6 Windows XP

Der Remote Desktop Client ist sowohl bei „Windows XP home“ als auch bei „professional“ im Lieferumfang enthalten und über die Hierarchieebene „Programs - Accessories - Communications - Remote Desktop Connection“ im Startmenü erreichbar. Die mitgelieferte Version ist jedoch mittlerweile nicht mehr die Aktuellste. Es empfiehlt sich daher, diese Windows-Komponente über die Systemsteuerung zu deinstallieren und die aktuelle Version zu installieren. Dies geschieht analog zur Installation unter den anderen 32 Bit-Versionen von Windows. Danach befindet sich allerdings ggf. der Eintrag im Startmenü direkt unter „Programs“ und nicht mehr in der in der anderen Hierarchieebene.

3.7.7 Windows Code Name Longhorn

Longhorn liegt zum Zeitpunkt dieser Arbeit noch nicht als finale Version vor. Getestet wurde daher die „*Client Preview 2 (build 4074.idx02.040425-1535)*“. Dort ist der Remote Desktop Client wie bei Windows XP mit enthalten und analog über das Startmenü erreichbar.

3.7.8 Windows embedded/mobile (CE, HPC, PPC)

Bei Windows „Consumer Electronics“ oder „Compact Edition“ oder „Compact Embedded“; Compactness, Compatiblity, Companion and Efficiency (CE) muss der Remote Desktop Client bereits bei Erzeugung des Images für das mobile Endgerät dabei sein, eine separate Nachinstallationsroutine gibt es nicht.
Zur Konfiguration von Windows CE kann zusätzlich noch ein PC mit geeigneter Verbindung zum mobilen Gerät notwendig sein. Auf dem Personal Computer (PC) muss „Microsoft Active Sync“ (TO-DO: download-Link - WICHTIG!) installiert werden. Auf dem mobilen Gerät sollte bereits Windows CE oder ein vergleichbares Operating System (OS) (... (HPC), ... (PPC)) installiert sein.

Microsoft Windows CE .NET v4.1

Bei [MANIAC] findet man folgende Beschreibung:

> Windows CE .NET delivers a robust real-time operating system for rapidly building the next generation of smart mobile and small footprint devices. With a complete operating system feature set and end-to-end development environment, Windows CE .NET contains everything you need to create a custom Windows CE based device that requires rich networking, hard real-time, and a small footprint, as well as rich multimedia and Web browsing capabilities.

Der Platform Builder für Windows CE .NET v4.1 umfasst ganze 6 CDs und braucht installiert ca. 8GB Plattenplatz. Auf dem Windows 2003 Server liess er sich nicht installieren - die Software beschwerte sich, man hätte den Installationsvorgang abgebrochen und führte anschließend ein Rollback des Installationsvorgangens durch. Unter Windows XP ließ sich die Software installieren, jedoch nur dann, wenn die 8GB auf einem lokalen Laufwerk zur Verfügung stehen - die Installation auf einem via SMB freigegebenen und mit Laufwerksbuchstaben gemountetem Netzwerklaufwerk brachte folgende Fehlermeldungen: (TO-DO: Bildsche)

Microsoft Active Sync

Microsoft Active Sync ist ein Tool, welches auf dem PC installiert wird und für folgende Aufgaben im Zusammenhang mit mobilen Endgeräten verwendet werden kann:

- zum Installieren & Entfernen von Software auf dem mobilen Gerät
- zum Abgleichen von Daten (z.B. Outlook)
- zum Transferieren von Dateien zwischen Host und mobilem Gerät

Hier exemplarisch die Kurzanleitung für die Einrichtung der notwendigen Netzwerverbindung:

1. Einstellung der korrekten PC-Verbindung (z.B. IrDA)
2. Starten der PC-Direktverbindung
3. auf dem PC: sollte sich „Microsoft Active Sync“ automatisch starten; sonst manuell starten

4. auf dem PC: das Festlegen einer Partnerschaft - eine Art Profil, die eine Vertrauensstellung zwischen dem PC und dem mobilen Endgerät zum Zweck des Datenabgleichs beschreibt ist erstmal nicht nötig
5. auf dem PC: Installation der notwendigen Treiber & Software
6. auf dem PC: in ActiveSync auswählen: „Tools - Add/Remove Programs“
7. auf dem PC: zu installierende Treiber & Software auswählen und mit OK bestätigen
8. jetzt überträgt ActiveSync die Daten zum mobilen CE-Gerät
9. dort sind ggf. noch weitere Einstellungen notwendig - den Anweisungen auf dem Bildschirm folgen
10. nach Installation der Netzwerkkartentreiber sind nun u.a. die korrekten Einstellungen für die Infrastruktur (bei WLAN z.B. noch: SSID, Verschlüsselung) sowie die IP-Einstellungen vorzunehmen (abhängig von der LAN-Struktur ist DHCP evtl. ausreichend)

4 Anwendung

Nach erfolgreicher Installation aller benötigten Komponenten, wie sie in Kapitel 3 beschrieben wurde, kann nun die Nutzung der Terminal Services als Remote Desktop Connection beginnen. Wie der Benutzer Sitzungen startet, diese wieder beendet oder auch Konzepte wie das Parken und Übernehmen von Sitzungen werden in diesem Kapitel beschrieben.

4.1 Starten einer Remote Desktop Connection

Im Großen und Ganzen sind der Start einer Remote Desktop Connection (RDC) und die dabei möglichen Optionen bei den getesteten Clients nahezu identisch. Benötigt wird primär natürlich der Name des Servers, auf dem die Terminal Services laufen und zu dem verbunden werden soll sowie die zugehörigen Login-Daten (meistens Benutzername und Kennwort). Werden diese Kredenzien nicht korrekt und vollständig beim Client-Programm mit angegeben, präsentiert der Server nach Herstellen der RDC den gewohnten Windows-Login-Bildschirm.
Daneben ist es u.a. noch möglich, Auflösung und Farbtiefe sowie lokale Ressourcen, die mit dem Server verbunden werden sollen, zu spezifizieren. Die Ausführung des Clients ist danach als Fenster oder im Vollbildmodus möglich. Änderungen an diesen Einstellungen sind zwar während einer Sitzung möglich, aber nur, indem diese geparkt, die Einstellungen geändert und danach die Sitzung wieder aufgenommen wird. Bei solcherlei Änderungen kann jedoch nicht garantiert werden, dass alle Anwendungen fehlerfrei weiterlaufen - auch nicht dann, wenn diese Anwendung auf einer lokalen Windows-Arbeitsstation keine Probleme beim Ändern der lokalen Auflösung gezeigt hat (Bsp.: ICQ).

4.1.1 Browser-basierter Zugang

Die Standard-Website der Remote Desktop Web Connection befindet sich auf dem Server selber unter dem Verzeichnis „TSWeb“, also am Beispiel meines Testservers „redmond“ vollständig „`http://redmond/TSWeb`“, wie dies in Abb. 4.1 ersichtlich ist. Bei Nutzung eines anderen Browsers als dem IE (getestet wurden Konqueror, Mozilla-Firefox, Opera und Safari) oder selbst beim IE unter Apple's MacOS wird zwar die Website angezeigt, jedoch ist die Schaltfläche „Connect“ inaktiv.

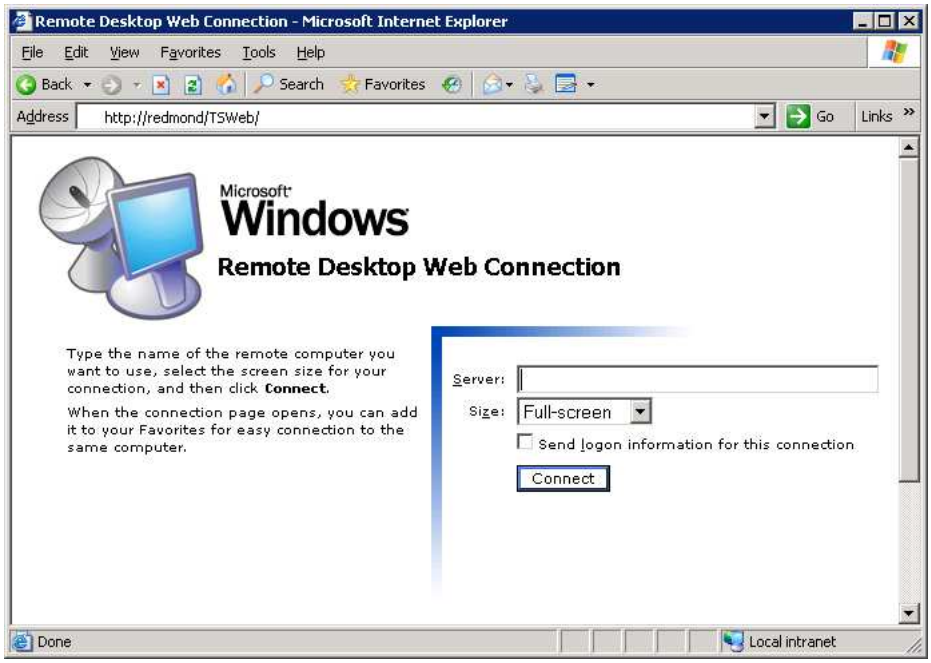

Abbildung 4.1: Remote Desktop Web Connection

Das Web-Formular erwartet als Eingaben den Namen des Servers, zu dem die Verbindung aufgebaut werden soll, sowie die Angabe der gewünschten Desktop-Größe für den Remote Desktop, der anschließend im Browser-Fenster dargestellt wird. Eine Ausnahme bildet die Option „Full-screen“, bei der nach Starten der Verbindung zusätzlich zum Explorer ein neues Fenster geöffnet wird, welches sich anschließend genau so wie beim normalen Microsoft Remote Desktop Client verhält. Durch Auswahl der Option „Send login information for this connection“ ist es möglich, bereits Anmelde-Informationen an den Server mit zu übertragen, wie dies in Abb. 4.2 dargestellt ist. Dies ist jedoch optional, genau wie die Angabe des Servernamens - wird keiner spezifiziert, wird die Verbindung zu dem Server aufgebaut, von dem man die Website bezogen hat.

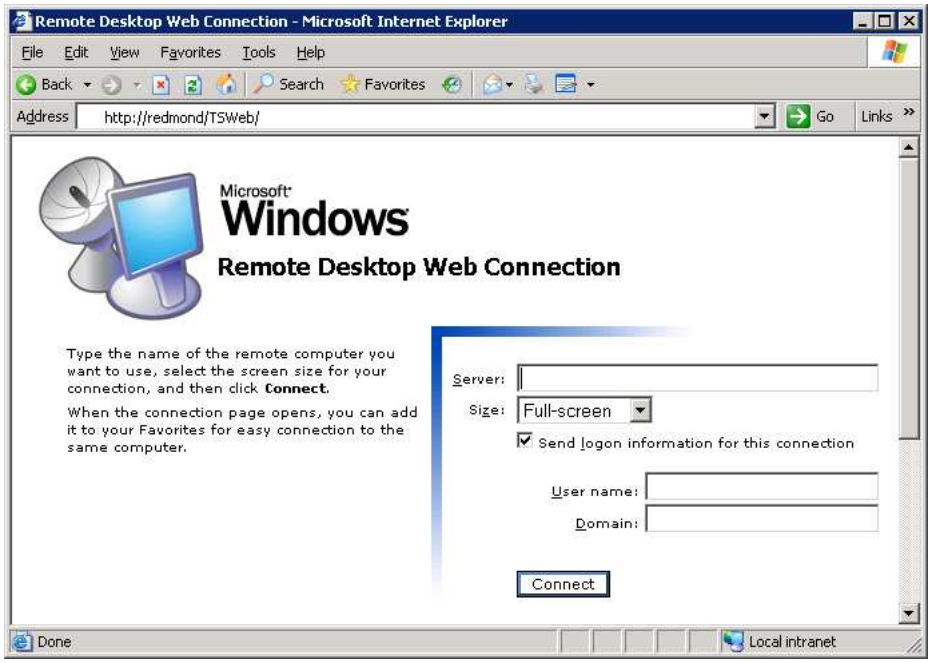

Abbildung 4.2: Remote Desktop Web Connection mit Anmeldeinformationen

Damit erschöpfen sich auch schon die Optionen der Web Connection - gegenüber dem nativen Client fehlen hier die Möglichkeiten zur Anbindung lokaler Geräte und Laufwerke ebenso wie dessen erweiterte Einstellungen.
(TO-DO: wird Audio übertragen?)

4.1.2 Apple MacIntosh

Für den Apple und sein MacOS gibt es einen speziell an das Look&Feel angepassten Client, der sich wie folgt präsentiert:

Abbildung 4.3: Der Remote Desktop Client auf dem Apple MacIntosh unter MacOS X

Die Optionen entsprechen weitestgehend denen des Microsoft-Clients für Windows; daher sei diesbezüglich auf Abschnitt 4.1.5 „Windows 32 Bit (Versionen 9x/ME, NT, 2000, XP, Longhorn)“ auf Seite 36 verwiesen. Im Vollbildmodus ist - anders als beim Windows-Client - Apple-spezifisch das „Dock“ am unteren und die Apple-Menüleiste als Teil des „Finder“ am oberen Rand sichtbar:

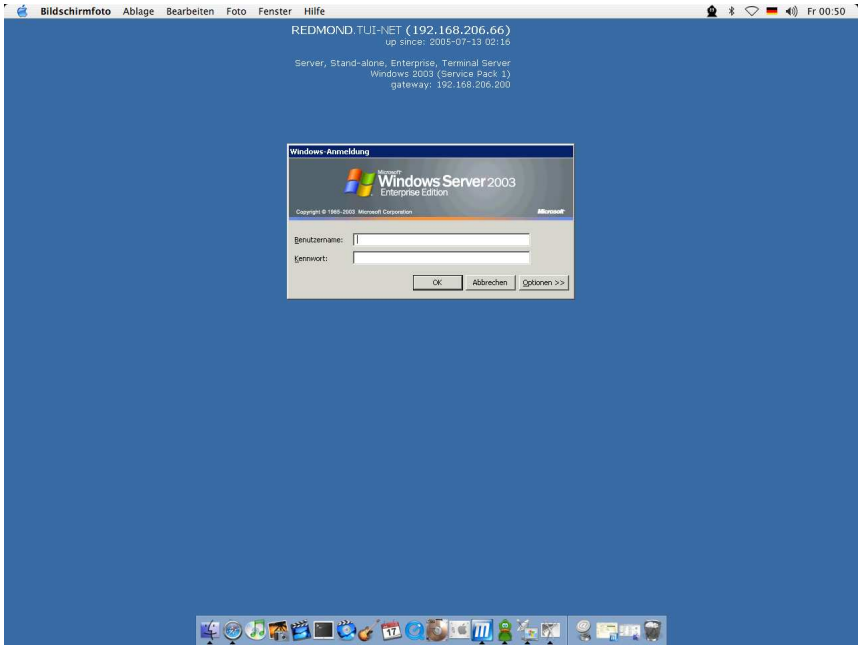

Abbildung 4.4: Apple's Windows Remote Desktop im Vollbildmodus

4.1.3 Unixoide (wie BSD & Linux)

Stellvertretend für die Unixoiden habe ich unter Linux zwei Oberflächen getestet: grdesktop und tsclient.
(TO-DO: grdesktop, rdesktop, tsclient, krdc, grcm?)
(TO-DO: jeweils Startbildschirm, Optionsbildschirme, CLI-Optionen, Config-Files - WICHTIG!)

grdesktop

So präsentiert sich der Startbildschirm von grdesktop:
Das Programm bietet eine Reihe von Optionen:

rdesktop

tsclient

Das Programm tsclient unterstützt neben dem RDP (auch Version 5) auch noch die Protokolle VNC, XDMCP und Citrix'ICA. Der Startbildschirm zeigt gleich die Optionen mit an:
Die weiteren Optionen sind denen von grdesktop ähnlich:

krdc

grcm

4.1.4 Windows 16 Bit (v3.x)

Auf Grund der Analogie der möglichen Konfigurationsoptionen zur aktuellen Version des Remote Desktop Clients sowie der geringen Relevanz der 16-Bit-Version wird nur kurz der Aufbau einer Verbindung in Anhang C dargestellt und ansonsten auf Abschnitt 4.1.5 „Windows 32 Bit (Versionen 9x/ME, NT, 2000, XP, Longhorn)“ auf Seite 36 verwiesen.
Nach der Installation findet man In der Programmgruppe „TSClient“ sowohl den sogenannten „Client Connection Manager“ (CCM), als auch die zugehörigen, benutzerdefinierten Konfigurationsdateien (`*.CNS`).

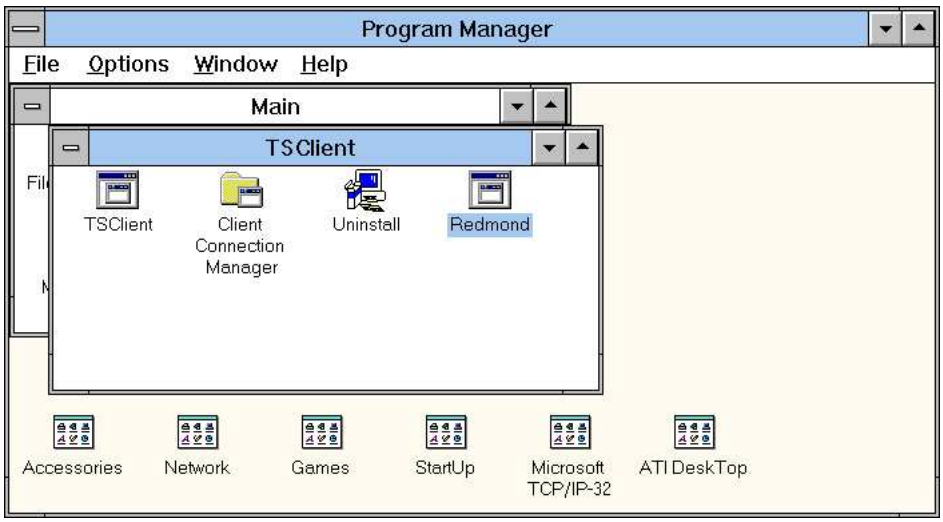

Abbildung 4.5: Programmmanager mit Programmgruppe „TS-Client“

4.1.5 Windows 32 Bit (Versionen 9x/ME, NT, 2000, XP, Longhorn)

Der Client von Microsoft (getestet wurde v5.2) kann sowohl auf dem gewohnten Weg über das Startmenü als auch via Kommandozeile (Command Line Interface (CLI)) gestartet werden. In wie weit sich das Verhalten des Client bei der finalen Version von Longhorn ändert, ist noch nicht abzusehen - in der vorliegenden Client Preview gleicht es jedenfalls demjenigen unter XP.

Im Startmenü findet man den Client standardmäßig unter „Programs - Accessories - Communications - Remote Desktop Connection“ oder direkt unter „Programs - Remote Desktop Connection“, abhängig von der installierten Version. Graphisch präsentiert er sich folgendermaßen:
(TO-DO: Bild einfuegen)

Gegenüber der bei Windows XP mitgelieferten Version 5.1 bietet die aktuelle Version u.a. die Möglichkeit, die lokale Zeitzone des Clients miteinzubeziehen. Die weiteren Optionen sind in den folgenden Bildern dargestellt und weiter unten beschrieben. (TO-DO: Optionen beschreiben)

Die ausführbare Datei (binary) für die Kommandozeile heißt „`mstsc.exe`“ und befindet sich bei der vorinstallierten Version im Verzeichnis „`%SystemRoot%\system32`“ und kann direkt aufgerufen werden, da sich dieses Verzeichnis per default auch im Pfad befindet. Wird der Remote Desktop Client separat installiert bzw. aktualisiert, so befindet er sich anschließend standardmäßig im Verzeichnis „`%Program Files%\Remote Desktop`“.

Für die Nutzung via CLI gilt folgende Syntax:

```
mstsc [<ConnectionFile>] [/v:<server[:port]>] [/console] [/f[ullscreen]]
      [/w:<width> /h:<height>] | /edit"ConnectionFile" | /migrate | /?
```

Dabei haben die Parameter die in Tabelle 4.1 aufgelistete Bedeutung:

Parameter	**Bedeutung**
<ConnectionFile>	Spezifiziert eine „`.RDP`“-Datei mit den gewünschten Einstellungen
/v:<server[:port]>	Spezifiziert den Terminal Server, der genutzt werden soll
/console	Verbindet zur lokalen Console des Servers (ohne Bedeutung bei Verbindung zu einem WinXP-Rechner; TO-DO: wie ist das bei Win2k(hat doch eh kein RDP, oder?) und Win2k Server?)
/f	Startet den RDP-Client im Vollbildmodus
/w:<width>	Spezifiziert die Breite des Remote Desktop-Bildschirms (in Pixeln)
/w:<height>	Spezifiziert die Höhe des Remote Desktop-Bildschirms (in Pixeln)
/edit	Öffnet das mit „ConnectionFile“ spezifizierte Config-File zur Bearbeitung
/migrate	Migriert Konfigurationsdateien des „Client Connection Manager“s in das .RDP-Format
/?	gibt Informationen zu den CLI-Parametern aus

Tabelle 4.1: Parameter von `mstsc.exe`

4.1.6 Windows embedded/mobile (CE, HPC, PPC)

4.2 Handling

Wie man eine Sitzung benutzt und was es zu beachten gibt, damit beschäftigt sich Abschnitt 5.3 „Handling“ auf Seite 47.
(TO-DO: oben die Leiste beim Vollbildmodus - pin/unpin - WICHTIG!)

4.3 Beenden der Nutzung

Neben dem regulären und schon von anderen Systemen her bekannten Beenden einer Sitzung durch Abmeldung des Benutzers gibt es bei den Terminal Sessions noch weitere Varianten:

- Der Benutzer „parkt“ die Sitzung (trennt die Verbindung)
- Der Benutzer meldet sich ab
- Die Sitzung wird administrativ getrennt (dazu zählen auch StandBy oder Hibernation des Servers)
- Die Sitzung wird administrativ beendet (darunter fallen auch Reboot und Shutdown des Servers)
- Die Sitzung wird von einem anderen Nutzer oder anderen Client übernommen
- Die Sitzung wird unerwartet getrennt (z.B. durch Verlust der Netzwerkverbindung oder Absturz des Clients)
- Die Sitzung wird unerwartet beendet (z.B. durch Serverabsturz)

Welche Meldungen bei noch aktiven Sitzungen dazu jeweils der Nutzer angezeigt bekommt, ist in Abschnitt 5.5.3 „Trennung der Sitzung“ auf Seite 50 dokumentiert.

4.4 Wiederaufnahme und Übernehmen einer Sitzung

Voraussetzung für die Wiederaufnahme ist, dass die Sitzung noch auf dem Server läuft; sprich: nur „geparkt“, nicht aber beendet wurde. Ausserdem ist es möglich, laufende Sitzungen direkt zu übernehmen. Auch hier sei wieder auf Abschnitt 5.5.3 „Trennung der Sitzung“ auf Seite 50 bezüglich der vom System an den Nutzer geschickten Meldungen verwiesen.

(TO-DO: Uebernahme remote-remote, local-remote, remote-local, mehrere Sitzungen, noch laufende Sitzungen - WICHTIG!)
(TO-DO: Trennung /console und ohne; Bei mehreren offenen Sitzungen zu meiner Benutzerkennung: wie waehle ich da eine aus? - WICHTIG!)

5 Leistungsanalyse

5.1 Testumgebung

In einer lokalen Installation wurden mehrere Clients mit dem Server verbunden. Die stationären Clients waren dabei direkt über einen 100 Mbit-Switch **FDX!** (FDX) angeschlossen, die mobilen Clients wurden über einen unter Linux 2.6 laufenden Router mit WLAN (802.11b & g) angebunden. Das „Class-C"-Netz `192.168.206.0/24` stellt dabei das kabelgebundene, `192.168.207.0/24` das drahtlose Netz dar.
(TO-DO: Bildchen von der Netzwerkarchitektur zeichnen & einfuegen - WICHTIG!)
Die Auswahl der Hardware richtete sich beim Server hauptsächlich auf die zum Einsatz überhaupt notwendige Hardware, während auf Client-Seite versucht wurde, möglichst mehrere auftretende Anwendungsfälle zu berücksichtigen.

Im Folgenden werde ich nun die einzelnen Server und Client-Systeme vorstellen, die ich zum Testen herangezogen habe. Die Geräte wurden dabei nach dem Aspekt möglichst unterschiedlicher Charakteristika und Bauform, Hardwareausstattung und Betriebssysteme ausgewählt.

5.1.1 Test-Server

Server #1

ID	"Redmond-MANIAC "(192.168.206.67)
Betriebssystem	Microsoft Windows Server 2003, Enterprise Edition
System	PC, iPII-300/100/512, 512MB, IDE 6GB
NICs	ISA & PCI, 3Com 10 & 100Mbit

Tabelle 5.1: Konfiguration Test-Server 1

Server #2

ID	"Redmond "(192.168.206.66)
Betriebssystem	Microsoft Windows Server 2003, Enterprise Edition
System	PC, AMD Athlon 1.8 GHz, 1.5GB, IDE 60GB
NICs	PCI, 3Com 100Mbit

Tabelle 5.2: Konfiguration Test-Server 2

5.1.2 Test-Clients

Client #1

Bei diesem Client handelt es sich um einen normalen, stationären PC. Er wurde hauptsächlich zu Vergleichszwecken mit in den Reigen der Clients aufgenommen.

ID	"blackmore "(192.168.206.23)
Betriebssystem	Microsoft Windows XP Professional
System	PC, iPIII-800/133/512, 512MB, IDE 80GB
NICs	PCI, 3Com 100Mbit

Tabelle 5.3: Konfiguration Test-Client 1

Was mir negativ auffiel:

- nicht mobil
- Heutige PCs sind recht laut auf Grund einiger mechanischer Komponenten wie der Festplatte und der notwendigen Belüftung; die hauptsächlichen Komponenten mit aktiver Kühlung in Form eines mechanisch drehenden Lüfters sind dabei die **CPU!** (CPU) und oft auch Grafikkarte sowie klassischerweise das Netzteil.
- Man muss relativ lange warten (bis zu mehreren Minuten), bis das Gerät einsatzbereit ist (Bootvorgang).

Was mir positiv auffiel:

- Auf Grund der Natur/des Ursprungs der über die Terminal Services angebotenen Dienste („Windows-Applikationen“) ist dieser Client noch am besten zu deren Nutzung geeignet (vgl. dazu auch Abschnitt 5.3 „Handling“ auf Seite 47).

Client #2

Auch bei diesem Client handelt es sich prinzipiell um einen normalen PC aus der i386-Klasse. Jedoch handelt es sich hier um ein tragbares Modell, welches üblicherweise als Laptop oder Notebook bezeichnet wird.

ID	"Armada "(192.168.206.123 & 192.168.207.123)
Betriebssystem	Microsoft Windows XP Professional
System	PC-Laptop, iPII-333/100/512, 128MB, IDE 6GB
NICs	PCMCIA, 3Com 100Mbit Fast Ethernet, Lucent/Orinoco 11Mbit WLAN

Tabelle 5.4: Konfiguration Test-Client 2

Was mir negativ auffiel:

- man muss relativ lange warten, bis das Gerät einsatzbereit ist (Bootvorgang)
- größtes und schwerstes (ca. 3,5 kg) tragbares Gerät im Test

Was mir positiv auffiel:

- mobile Variante eines Desktop-PCs mit nahezu dessem vollem Funktions- und Leistungsumfang

Client #3

ID	"Compaq iPAQ H3600 "(192.168.207.31)
Betriebssystem	Microsoft Windows CE v3.0.9348 (build 9616)
System	StrongARM SA-1110, 32MB
NICs	PCMCIA

Tabelle 5.5: Konfiguration Test-Client 3

Abbildung 5.1: Compaq iPAQ H3600

Was mir negativ auffiel:

- Display zu klein (bauartbedingt)
- Display nicht bei allen verfügbaren Betriebssystemen um 90° drehbar
- Audiowiedergabe nur monophon, wenn keine Kopfhörer eingesetzt werden

Was mir positiv auffiel:

- kleinste Bauform im Test

Client #4

ID	"Siemens SIMpad SL4 "[SIMpad](192.168.207.32)
Betriebssystem	Microsoft Windows for Handheld PC 2000 v3.0
System	StrongARM SA-1110, 206MHz, 64MB
NICs	PCMCIA

Tabelle 5.6: Konfiguration Test-Client 4

Abbildung 5.2: Siemens SIMpad SL4

Was mir negativ auffiel:

- Audiowiedergabe nur monophon (TO-DO: auch beim Einsatz von Kopfhoerern?)
- Stift rastet nicht in Halterung ein - Verlust leicht möglich
- Die Eingabe über den TouchScreen reagiert oft nur träge und ist schnell dekalibriert. Mit abnehmender Akkukapazität verschlimmert sich diese Situation stark, bis hin zur Unbenutzbarkeit des TouchScreens. Selbst die Schaltfläche zum Rekalibrieren ist dann kaum noch erreichbar.
- stark verbesserungswürdige Schrifterkennung (betriebssystembedingt)
- mangelnder Support durch Hersteller (z.B. neue Betriebssystemreleases)

Was mir positiv auffiel:

- gesonderte Tasten (z.B. ESC, Enter)
- rechte Maustaste ebenfalls als gesonderte Taste ausgeführt
- eingebauter SmartCard-Reader (Funktionsumfang bisher ungetestet)

Client #5

ID	"skeye.pad SL "[skeye.pad] (192.168.207.33)
Betriebssystem	Microsoft Windows CE .NET v4.10 (build 908)
System	StrongARM SA-1110, 206MHz, 64MB
NICs	PCMCIA

Tabelle 5.7: Konfiguration Test-Client 5

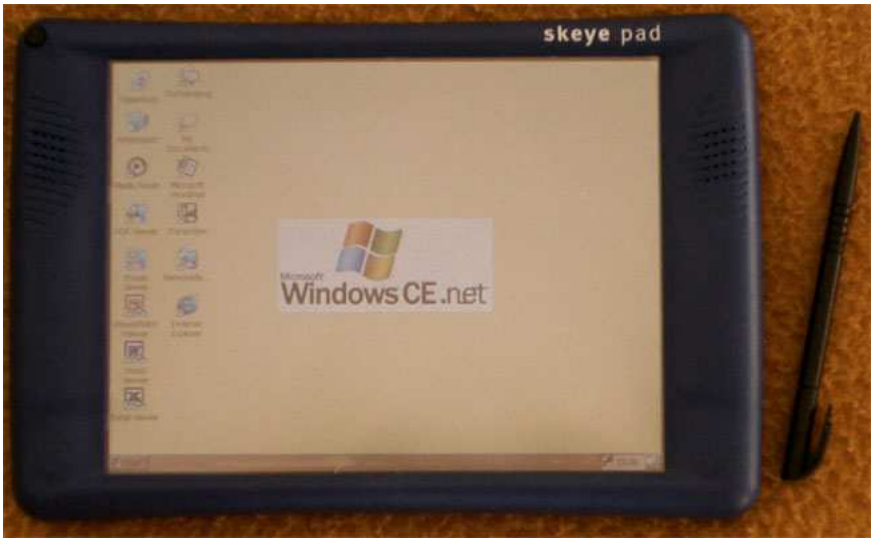

Abbildung 5.3: skeye.pad SL

Was mir negativ auffiel:

- keine separaten Tasten
- Audiowiedergabe trotz zweier Lautsprecher nur mono (TO-DO: wie ist das bei Kopfhoerern?)
- Bei gleichzeitiger lokaler Audio-Wiedergabe und Nutzung von Audio via Terminal Services gab es Probleme, so dass das Gerät resettet werden musste.

Was mir positiv auffiel:

- ...

5.1.3 Bemerkungen zu den Test-Clients

Die Clients haben alle eine unterschiedliche Ausstattung. Bei dem PC und dem Notebook handelt es sich quasi um „vollständige“ Geräte mit Maus, Tastatur und großem Bildschirm. Der PC ist das einzige stationäre Gerät. Von den mobilen Geräten ist das Notebook als einziges mit einer Tastatur ausgestattet; die Maus ist hier aber bereits eingeschränkt, da sie durch ein TouchPad repräsentiert wird (Alternativen bei anderen Notebooks sind hier der 'Stick' wie z.B. bei vielen IBM-Modellen oder der heutzutage weniger verwendete Trackball). Es existiert jedoch die Möglichkeit, das Notebook mit einer externen Maus auszustatten. Daneben weist das Notebook im Gegensatz zu den anderen Mobilen eine geringere Akkulaufzeit aus. Die Betriebsszeit der Mobilen liegt im Schnitt beim zwei- bis fünffachen gegenüber herkömmlicher PC-Technik (Notebooks). Dem entgegen stehen jedoch die Nachteile wie kleineres Display (eine Auflösung von 1024x768 Pixeln kann bei PCs derzeit durchaus als Standard angesehen werden) mit zum Teil anderem Seitenverhältnis (z.B. beim iPAQ), kein Keyboard/Maus, eingeschränkte Peripherieanschlussmöglichkeiten (zumindestens weisen alle Testgeräte eine IrDA- und PCMCIA-Schnittstelle auf; jedoch z.B. kein USB) und fast schon Nebensächlichkeiten wie daß das skeye.pad die einzige Mobile mit stereophoner Audiowiedergabemöglichkeit ist (TO-DO: stimmt das ueberhaupt?). Abhilfen sollen hier ein Stift als Eingabegerät (Mausersatz) sowie ein „on-screen-keyboard“ nebst Schrifterkennung als Tastaturersatz darstellen. Maus und Tastatur sind mit Sicherheit nicht der Eingabegeräte letzter Schluss, jedoch ist heutige PC-Software eben nun mal darauf ausgelegt - und damit muss man wohl auch noch in absehbarer Zeit beim Einsatz mobiler Windows-Terminals leben. Doppel- oder Rechtsklick werden daher zur Qual, verhindern zügige Benutzung und sollten daher beim Design geeigneter User Interface (UI)s für diese Geräte vermieden werden. Je nach Software kann es durchaus sein, dass der Rechtsklick gar nicht emuliert wird - dann ist man auf eine extra Taste am Gerät angewiesen, wie sie z.B. das Siemens SIMpad bietet. Mit der Linux-basierten Oberfläche „OPIE“ für PDAs wird dagegen der Rechtsklick ermöglicht, in dem man mit dem Stift länger an einer Stelle verweilt - es erscheint dann ein Kontextmenü, welches einem u.a. die Möglichkeit bietet, hier jetzt einen Rechtsklick an die Applikation zu senden. Dies ist - insbesodere in mobilen Umgebungen wie beim Autofahren - ähnlich kompliziert wie ein exaktes Doppelklicken auf dem kleinen und oft rutschigen Display bei Handheld-Geräten.
Alle Mobilen haben natürlich aus Gründen wie Gewicht und Größe ein TFT-Display (Stand der Technik), welches gegenüber der herkömmlichen CRT-Technik eine wesentlich geringere Helligkeit (Leuchtkraft) sowie ein geringeres Kontrastverhältnis zu eigen hat. Zwar sind TFTs auch schon dabei, an stationären Bildschirmarbeitsplätzen die CRTs zu verdrängen, jedoch sind gerade Kontrast und Helligkeit zwei Eigenschaften, die in geschlossenen Räumen weniger wichtig sind als bei Mobilen, da diese auch im Freien oder sogar bei direktem Sonnenlicht betrieben werden.
Auch die Leistung der CPU sowie die Größe des integrierten Speichers liegen hinter der eines herkömmlichen Windows-Rechners - zudem existiert kein Massenspeicher (wie z.B. eine Festplatte). Einzig das Notebook weist hier als mobiles Gerät heutzutage ähnliche Parameter auf wie sein stationäres Gegenstück. So kann auf Notebooks auch die vom Desktop-PC her bekannte Betriebssystem-Software eingesetzt werden, wohingegen - im Falle von Windows - für die Mobilen eine gesonderte Version nötig ist (HPC, PPC, CE). Leider sind diese Sonderversionen nicht binärkompatibel zu ihren Desktop-Pendants und da es bei Windows-Software unüblich (bzw. in den meisten Fällen auf Grund des Geschäftsmodelles von Firmen wie Microsoft sogar unmöglich) ist, den Quellcode mitzuliefern, muss man hier auch für die eingesetzte Anwendungssoftware gesonderte Versionen erwerben. Übrigens ein

Grund, der für den Einsatz der Terminal-Services spricht - kann man doch damit (mit den hier zu betrachtenden Einschränkungen) seine gewohnte Software auch auf mehreren Endgeräten nutzen (Lizenzverträge beachten - siehe auch Kapitel Abschnitt 3.3 „Lizensierung“ auf Seite 7).

5.2 Testapplikationen

Um nun zu untersuchen, wie es sich mit verschiedenen Applikationen arbeiten lässt, ist zuerst eine geeignete Auswahl zu treffen. Dabei habe ich verschiedene Klassen gebildet, die die verschiedenen Anwendungsszenarien abdecken sollen.

- **Klasse Standard:** Notepad, Taschenrechner, Solitär, ...
  Dabei handelt es sich um Standard-Applikationen, die teileweise bei Windows mitgeliefert werden und vom ersten Eindruck her keine besonderen Ansprüche an die zur Verfügung stehende Übertragungsbandbreite oder das Nutzerinterface haben.
- **Klasse Web/eMail/News:** NetScape, Mozilla, Opera, Outlook [Express], ICQ
  Die klassischen Kommunikationsprogramme, die auf Grund ihres „online“-Charakters seit einigen Jahren wohl mit zur meistgenutzten Softwaregruppe gehören. Zu Outlook und Outlook Express ist zu sagen, dass ich es zwar mit aufgenommen habe, da es recht weit verbreitet ist; seinen Einsatz kann ich jedoch wegen der Nichteinhaltung verschiedener Standards nicht empfehlen (als Stichworte seien hier nur mal das Problem mit der falschen Abtrennung der Signature, das Kammquoting oder das Datenschutzproblem der erschwert zugänglichen BCC:-Option genannt).
- **Klasse Office:** openOffice, Microsoft Office
  Textverarbeitung, Tabellenkalkulation - klassische Büroprogramme und damit auch klassische PC-Anwendungen.
- **Klasse Skins:** WinAMP, Microsoft Office 2003+, openOffice 2.0+, SwyxIt!
  Bei dieser Klasse liegt der Schwerpunkt auf der Übertragung, da diese Anwendungen zusätzlich zu den Standard-Windows-Fensterelementen diese noch mit sog. „Skins“ überlagern, was einen rein optischen Effekt hat. Diese Skins sind letztenendes Bilder, die extra mit übertragen werden müssen.
- **Klasse audio:** WinAMP, MediaPlayer
  Hierbei geht es um die Übertragung von Audio-Daten.
- **Klasse video:** DirectX, openGL, Videowiedergabe, TV
  Von allen hier gebildeten Klassen stellen bewegte Bilder heutzutage wohl die höchste Anforderung an ein Übertragungsmedium.
- **Klasse misc:** Microsoft Project, Microsoft Visio, (MiK)TeX, TeXnicCenter
  Verschiedene Programme, die nicht unbedingt auf jedem Rechner anzutreffen sind.
- ...

5.3 Handling

- Die maximale Bildschirmgröße (Auflösung) entspricht bei den normalen Desktop-Betriebssystemen der des Clients; bei den PDAs besteht die Möglichkeit, eine grössere Auflösung anzugeben als das Display wiedergeben kann. Dann kann man im Fenster des RD-Clients scrollen, wie man es z.B. beim Webbrowser gewöhnt ist. Dies funktioniert jedoch nur, wenn der RD-Client nicht im Vollbildmodus ausgeführt wird. Nicht alle Clients unterstützen jedoch den Wechsel der Auflösung.

- Eine Session entspricht einer normalen Windows-Session, wie man sie gewohnt ist. Man hat also sein eigenes Benutzerprofil mit der gewohnten Umgebung. Das Einloggen ist neben der Remote-Variante auch lokal möglich; man nutzt dann das gleiche Profil.

- Man kann eine Session 'parken' und jederzeit oder von jedem anderen Gerät aus weiter fortsetzen.

- Ein Nutzer kann sowohl eine lokale als auch eine remote-Session gleichzeitig offen haben. Dabei treten jedoch Probleme mit den Einstellungen und anderen gemeinsam genutzten Ressourcen auf - sowohl Windows als auch die Software von Drittanbietern fängt dies nur unzureichend ab; bei mehreren parallelen Sitzungen auf dem selben System ist daher mit Datenverlust zu rechnen.

- Bei den meisten PDAs/Laptops/Notebooks/WebPads usw. ist das Display nach wie vor sehr leuchtschwach und eignet sich nur bedingt bis gar nicht zum Einsatz in der freien Natur bzw. bei Sonneneinstrahlung.

- Je nach verwendetem Client hat man eine „Maus“ in Form des Zeigers oder aber es werden nur die „Clicks“ gewertet.

- Das on-screen-keyboard sowie die Funktion der Schrifterkennung (z.B. 'Transcriber') wirken sich nur lokal aus (d.h. sie können nicht für den Terminal Services Client genutzt werden) - daher empfiehlt sich für WebPads u.ä. dringend ein Gerät, welches eine rechte Maustaste hat (siehe oben - skeye.pad vs SIMpad).

- Die Akku-Laufzeiten von WebPads und PDAs sind in der Regel wesentlich besser als die von Notebooks - im Test konnten z.B. mit dem skeye.pad bis zu sieben Stunden erreicht werden.

- Dafür liegt der Preis eines solchen mobilen Gerätes in den gleichen Regionen wie der für ein gebrauchtes Notebook der vorletzten Generation (zur Zeit also so PII/PIII-Klasse).

- Verbindungabbrüche sind kein Problem; Sitzung kann später oder von einem anderen Gerät aus fortgesetzt werden

5.3.1 Was geht remote ...

- Windows kann im Großen und Ganzen normal innerhalb der Grenzen der Client-Hardware genutzt werden (Ausnahmen siehe nächster Abschnitt).

- Ist man mit den entsprechenden Rechten ausgestattet, kann der Rechner aus der Ferne verwaltet werden („remote management“), das heist, man kann Hardware-Treiber

und Software installieren oder entfernen, das System neu starten, Benutzer und andere Computereinstellungen verändern oder Laufwerke konfigurieren. Zu beachten ist jedoch, dass ein Neustart des Systems nicht immer problemlos von Statten gehen muss und man dann ggf. genau wie beim Herunterfahren des Systems physischen Zugang zum Server benötigt, damit man ihn wieder in einen netzwerkfähigen Zustand versetzen kann.

- Will man den Server herunterfahren oder neustarten, wird man darauf hingewiesen, wenn noch andere Anwender angemeldet sind.

5.3.2 ... und was nicht

- Als Desktophintergrund lassen sich per default weder ein Bild noch der ActiveDesktop verwenden. Dies kann zwar mit Hilfe der Gruppenrichtlinien wieder zugelassen werden; da dann der Desktophintergrund aber permanent mit übertragen werden muss, ist davon abzuraten.
- „Show window contents while dragging“ ist auch forciert deaktiviert; d.h. beim Verschieben von Fenstern ist nur der Rand zu sehen, wie man es von Windows 3.x her kennt.
- DirectX (TO-DO: detaillierter - WICHTIG! - einfach den Fehlermeldungsreport hier her)
- Multimedia-Daten wie Audio und/oder Video stellen hohe Ansprüche an die Übertragungsbandbreite und das Latenzverhalten, und sind daher via Terminal Services nur extrem eingeschränkt verwendbar.
- Je nach Ausstattung der Client-Hard- und Software gibt es evtl. keine rechte Maustaste (TO-DO: Emulation - a:moeglich?, b:wenn ja, wie?)
- Es lässt sich prinzipiell nur der komplette Desktop übertragen. Die Bereitstellung bzw. Übertragung nur einzelner Anwendung ist nur mit Hilfe des Citrix-Aufsatzes möglich.

5.3.3 Datenaustausch zwischen Client und Server

Copy'n'Paste funktionieren bei allen getesteten Clients.
(TO-DO: Umleitung von lokalen Ressourcen)

5.4 Performance

Die Anwendungen werden serverseitig ausgeführt. Die Anzeige sowie Eingabe erfolgen primär clientseitig (vgl. umgeleitete Geräte). Entsprechend ist auch die Performance. Was das Starten und die Ausführungsgeschwindigkeit der Anwendungen selber angeht, hängt diese also primär von der Leistung des Servers ab. Anders dagegen verhält es sich mit der Reaktionsgeschwindigkeit auf Benutzereingriffe, da diese erst vom Client verarbeitet und an den Server weitergereicht werden müssen. Die deutlichsten Einschnitte sind jedoch bei der Anzeige zu vermerken. Es war selbst bei Verwendung eines normalen PCs mit Fast Ethernet-Anschluß nicht möglich, ein Video mit halber PAL-Auflösung ruckelfrei zu übertragen. Selbst Anwendungen, die sog. „Skins“ zur Aufbesserung der Optik ihrer Benutzerschnittstelle nutzen, werden zwar gewohnt schnell ausgeführt, jedoch ist die Reaktion

der Anwendung nur stark zeitverzögert auf dem Client sichtbar und man kann teilweise beim Bildschirmaufbau zuschauen.
Sowohl der von Microsoft mitgelieferte 32 Bit-Client als auch die Clients für Linux verfügen über einen „Bitmap-Cache“, der Bildbereiche des zu übertragenden Desktops zwischenspeichern kann.
Negativ auf die Performance des Remote Desktops wirken sich also (u.a.) folgende Kriterien aus:

- Vorhandensein eines Hintergrundbildes („Wallpaper“)
- hohe Farbtiefe
- Übertragung von Multimedia-Datenströmen wie Audio oder Video
- „Skins“ bei Programmen
- Ein- und Überblendeffekte (z.B. bei älteren Installationsroutinen oben das Logo) (TO-DO: wie schaut das bei den Windows-eigenen Effekten aus fuer Menues etc.?)
- ...

5.5 Mögliche Ereignisse

In diesem Kapitel sollen einige Ereignisse aufgezeigt werden, mit denen sich der Anwender während der Nutzung der Terminal Services konfrontiert sehen könnte. Diese Liste erhebt jedoch nicht den Anspruch der Vollständigkeit. Im Zweifelsfall sollte der Nutzer immer bei seinen zuständigen Administrator nachfragen, ob und welche Auswirkungen dies oder jenes auftretende Ereignis auf ihn und seine Daten hat.

5.5.1 Kein Verbindungsaufbau möglich

Kommt es bereits beim Aufbau einer Terminalserververbindung zu Problemen, wird der Nutzer vom Microsoft-Client mit der Meldung in Abb. 5.4 konfrontiert.

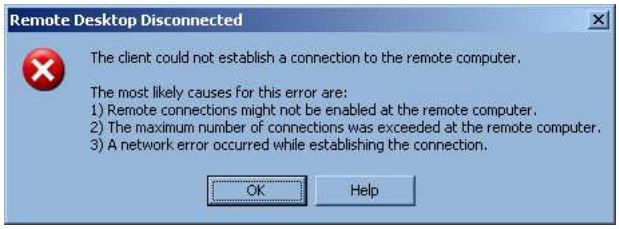

Abbildung 5.4: Kein Verbindungsaufbau möglich

Dieses Problem kann mehrere Ursachen haben:

- der Server ist noch nicht vollständig hochgefahren
- der Server ist gerade am Herunterfahren
- der Server akzeptiert keine remote-Verbindungen
- die Höchstanzahl der zulässigen Verbindungen am Server ist erreicht
- Netzwerkprobleme (TO-DO: bei welchen kommt das und bei welchen nicht?)

5.5.2 Lizenzprobleme

Abbildung 5.5: Ablaufen der temporären Client-Lizenz

Diese Meldung erscheint beim Anmeldevorgang, wenn der Server für den Client nur eine temporäre Lizenz ausgestellt hat. Nach Ablauf der in der Meldung jeweils angegebenen Zeit ist von diesem Client aus nur noch eine Verbindung zur Console des Servers möglich, nicht jedoch der Neubeginn und auch nicht die Wiederaufnahme einer Terminalsitzung. Stattdessen wird dem Nutzer bereits vor der Anmeldung die in Abb. 5.6 dargestellte Meldung präsentiert.

Abbildung 5.6: Keine Client-Lizenz vorhanden

5.5.3 Trennung der Sitzung

Eine Terminalsitzung kann nicht nur durch den Benutzer beendet werden. Ebenso ist es möglich, dass ein Administrator die Sitzung beendet (Abb. 5.7) oder der genutzte Server heruntergefahren wird (Abb. 5.8). Im Falle des Heruntefahrens des Servers - gleich ob Windows XP oder Windows Server - ist ein Fortsetzen der Sitzung zu einem späteren Zeitpunkt nur dann möglich, wenn der Server nur in den StandBy- oder Hibernate-Modus heruntergefahren wurde.

Abbildung 5.7: Sitzung wurde durch einen Administrator beendet

Ausserdem existiert noch die Möglichkeit, dass eine Sitzung von einem anderen Nutzer oder Administrator übernommen (und damit im Regelfall von einem anderen Client oder dem Server aus weitergeführt) wird. Auch dies bedeutet eine Trennung der Terminalsitzung. Dabei wird der Benutzer davon ohne die nähere Spezifikation von Details in Kenntnis gesetzt, wie in Abb. 5.9 zu sehen ist.

Abbildung 5.8: Sitzung wurde durch Herunterfahren des Servers beendet

Abbildung 5.9: Sitzung wurde beendet, weil sie übernommen wurde

Aber nicht nur vorsätzliche Verbindungsabbrüche können auftreten. So sind z.B. auch ein Absturz des Servers oder Netzwerkprobleme als Ursachen möglich. In diesen Szenarios, über die sich Client und Server nicht verständigen können, wird die Session temporär inaktiv geschaltet und im Hintergrund versucht, diese fortzusetzen, sobald die Verbindung zwischen Client und Server wiederhergestellt ist. Im Fall eines Serverabsturzes funktioniert dies nicht, wohl aber z.B. beim kurzzeitigen Verlust einer Drahtlosverbindung oder dem Reset eines Netzwerkswitches.
Beim Windows-Client wird dem Nutzer der Konnektivitätsverlust optisch durch ein Abdunkeln der Sitzung, wie man es z.B. beim Beenden einer XP-Workstation kennt, und der Darstellung eines blinkenden „disconnected“-Symbols wie in Abb. 5.10 signalisiert.

Abbildung 5.10: Temporäre Unterbechung der Terminalverbindung

6 Verschiedenes

6.1 Sicherheit

(TO-DO: aus dem bhv-Buechlein ziemlich am Anfang zitieren) Auch wenn es oft gerne vernachlässigt wird, so ist Sicherheit ein Aspekt, der immer wichtiger wird. Gerade wenn es um gemeinsam genutzte Ressourcen wie z.B. drahtlose Medien oder Server geht. Zu den üblichen Sicherheitsproblematiken (vgl. auch [IT-security]) kommen hier noch Aspekte wie z.B. Transaktionsmanagement, da es bei mobilen Verbindungen öfter zu Verbindungsabbrüchen kommt als bei kabelgebundenen Verbindungen. Neben dieser vertikalen Beobachtungsweise gliedern sich die horizontale Aspekte in vier Gruppen:

1. Sicherheit rund um den Server
2. Sicherheit der Netzinfrastruktur / des Backbone
3. Sicherheit der Funkstrecke
4. Sicherheit des Clients

- Security Configuration and Analysis-Tool
- Plugins in der MMC
- ATguard geht nicht mehr mit SP1, wg. Windows-Firewall (analog zu XP w/ SP2)
(Punkt 3 enfällt natürlich bei einer rein kabelgebundenen Verbindung.)
(TO-DO: security beim Verbinden lokaler Ressourcen mit dem Server, Policy - vgl. Kapitel 3)

6.2 Vergleiche mit verwandten Technologien

Wie schon am Anfang der Arbeit erwähnt, hat Microsoft mit seinen Terminal Services keine neue Erfindung getätigt, wenngleich auch die Qualität des Produktes (z.B. in Hinblick auf die Integration in die Microsoft-eigenen Standards) sich durchaus von anderen Produkten unterscheidet. Es seien daher hier stellvertretend einige andere, verwandte Produkte aufgelistet:

- **Apples Remote Desktop (ARD)**: Wie der Name schon andeutet, handelt es sich hierbei um eine spezielle Lösung für Apple's MacOS ab Version 8. Nähere Informationen gibt es beim Hersteller unter `http://www.apple.com/de/remotedesktop` oder z.B. in [iX 02/2004, Seite 59].
- **Citrix MetaFrame/Presentation Server:** Wie bereits in Abschnitt Abschnitt 2.1 „Geschichte“ auf Seite 3 erwähnt, gingen die Microsoft Terminal Services ursprünglich aus dieser Technologie hervor. Auch heute bietet Citrix weiterhin seine Software an, die sich als Erweiterung zu den Microsoft Terminal Services versteht. Unter anderem seien hier folgende Vorteile aufgezählt:

  - WebAccess nicht auf den IE/ActiveX beschränkt, sondern dank Java-Applet plattformübergreifend
  - Möglichkeit der Veröffentlichung nur einzelner Applikationen statt des gesamten Desktops
  - besseres Kompressionsverfahren bei der Übertragung
  - hochskalierbare Lastverteilung

  Da sich das auch auf die Kosten auswirkt, sei für einen eventuellen Entscheidungsfindungsprozess auf den Artikel in [iX 02/2004, Seite 78ff.] und einen darauf folgenden Leserbrief, den ich in Abschnitt 6.4 „Praxisaussagen“ auf Seite 54 aufgreife, verwiesen.

- **Linux Terminal Server Project (LTSP):** `http://ltsp.sourceforge.net` bzw. `http://www.ltsp.org`, (TO-DO - WICHTIG!)

- **PC-AnyWhere:** PC-AnyWhere[PC-AnyWhere] von Symantec[Symantec] war früher - neben VNC - eine der Möglichkeiten, auf einem NT-Server remote zu arbeiten. Mittlerweile klassifiziert die Firma ihr Produkt selber als „the world's leading remote control solution“ und sieht sie als „fast and secure problem resolution for remote workstations and servers“. Die Stärken des Produktes liegen laut Herstellerangaben u.a. in Sicherheitsfeatures.

- **screen:** Dabei handelt es sich um eine rein textbasierte Lösung für die Unix-Shell. Neben dem großen Anwendungsgebiet des Parkens einer Sitzung, welches auch eine Absicherung bei Verbindungsabbrüchen leistet, bietet dieses Tool auch die Möglichkeit, mehrere logische Sitzungen innerhalb einer physischen Sitzung aufzunehmen.

- **VNC:** VNC (mittlerweile „RealVNC“) [realVNC] ist ein Spross von AT&T Laboratories, Cambridge. Es steht unter der GNU public license (GPL)[GPL]. Seine Stärke liegt in der cross-platform-Technologie (Windows [32 Bit only], Linux und Solaris verfügbar und gegenseitig verbindbar) sowie in der geringen Größe des Clients (ca. 150KB), die es u.a. für Thin Clients - und damit gerade für mobile Endgeräte - attraktiv macht. Mehrere Nutzer können sich eine Session teilen (z.B. für classroom-applications interessant). Full Screen möglich. Protokoll: RFB. Connection via TCP Port 5900. Schwächen u.a.: Sicherheit nur durch Passwort, keine Regionalisierung („localisation“). Nur KVM. Getestete Version: v3.3.7. VNC ist auch in einer Version für mobile Endgeräte bzw. Thin Clients erhältlich - und zwar als PocketVNC[pocket-VNC] von SmartLab. Zahlreiche weitere Software rund um VNC - z.B. einen Client für MacOS - gibt es im Open Source Development Network (OSDN)[OSDN], z.B. bei FreshMeat[freshmeat] oder SourceForge[sourceforge] unter dem Stichwort „VNC“. (TO-DO: wird viel verwendet unter Linux - testen und drauf eingehen! - WICHTIG!)

- **X11-forwarding:**

6.3 Virtuelle Maschinen

Einen anderen Ansatz verfolgen Produkte wie „VirtualPC“, „VirtualServer“ (beides mittlerweile aus dem Hause Microsoft), „VMware“ oder „WinE“. Dort liegt das Ziel nicht in der Steuerung oder Nutzung eines entfernten Rechners (z.B. zwecks Ressourcennutzung),

sondern hier werden die Ressourcen des eigenen Rechners auf mehrere sog. „virtuelle Maschinen“ aufgeteilt. Diese Vorgehensweise ist - u.a. aus sicherheitstechnischen Gründen - im MainFrame-Bereich bereits lange bekannt. Mit den oben genannten Produkten hält diese Technologie auch Einzug in den PC-Bereich. Zumeist wird sie eingesetzt, um an einer physischen Workstation mehrere verschiedene Client-Betriebssysteme zu betreiben (z.B. eine Linux-Box mit Windows „im Fenster“ bzw. auf einer anderen Console) oder einfach mehrere (virtuelle) Rechner parallel zu betreiben, um z.B. ein Netzwerk zu simulieren. Man kann aber auch hier den Server mit mehreren virtuellen Maschinen betreiben. Insbesondere, wenn Cluster oder Grids physische Ressourcen wieder zusammenfassen, könnte das wieder interessant werden. (...)
WinE unterscheidet sich von den anderen beiden dadurch, dass es keinen vollständigen PC emuliert, sondern nur ein Windows-System. Damit ist es möglich, auf einem Unix(derivat)-Desktop einzelne Windows-Applikationen auszuführen, was in dieser Form beim Remote Desktop via Terminal Services ja nicht möglich ist.

6.4 Praxisaussagen

(TO-DO: die Aussagen von Siemens und der Thueringer Firmen: F-F, agenos, eMail JFMM)

Das Rechenzentrum (RZ) der TU Ilmenau sieht momentan keinen Bedarf der Einführung einer zentralen Terminal Services-Infrastruktur. Dies ist wohl hauptsächlich den bereits vorhandenen Rechnerpools, die an der Universität nicht nur im Rechenzentrum selber existieren, geschuldet. Einem Pilotprojekt zum Aufbau einer Struktur zur Nutzung von mobilen Clients über das bereits vorhandene und gut ausgebaute WLAN steht das RZ jedoch offen gegenüber.

Sehr oft traf ich auf die Meinung, dass ohne den Citrix-Aufsatz kein vernünftiges Arbeiten möglich wäre. Stellvertretend dafür möcht ich hier aus einem Leserbrief aus [iX 03/2004, Seite 9, Leserbriefe, „Citrix wahre Stärken“] zitieren:

> Durch den universellen Druckertreiber und das automatische „Client-Druckermapping“ ist es bei Citrix möglich, ohne „Tricks“ und administrativen Aufwand „alle“ Clientdrucker aus allen Betriebssystemwelten zu verbinden; sowohl lokale als auch Netzwerkdrucker. Dies wird Ihnen jeder Admin bestätigen, der schon mal versucht hat, von Windows 9x, Mac OS oder Linux über einen TS zu drucken.Mit reinen Terminalserverdiensten ist dies fast unmöglich. Siehe auch `download2.citrix.com/files/client_feature.xls`
> Ans Terminalfenster vom RDP-Client konnten sich unsere Mitarbeiter nie gewöhnen. Sie klickten die Anwendungen mit „X“ zu. Dadurch wurden diese nicht ordentlich beendet, und Folgefehler waren vorprogrammiert. Durch die Seamless-Anwendung [von Citrix] haben wir in diesem Bereich keine Probleme mehr. Auch die Desktop- und Startmenü-Integration tut ihr Übriges.
> Außerdem sind Features wie NFuse oder das Citrix Secure Gateway kostenlos zu haben. Diese erleichtern den administrativen Aufwand nochmal um ein Vielfaches. Das automatische Update der Clients gar nicht zu erwähnen.
> Citrix spielt seine Stärken im administrativen Bereich aus. Mit Citrix muss der Admin nur dafür sorgen, dass der User an den Client kommt, egal ob über NFuse oder Nativ installiert. Der Rest ist über Richtlinien und die Citrix Ma-

nagement Console zu steuern.
Es gibt nur ein Problem an MF [MetaFrame] XP: der hohe Preis von Citrix täuscht über diese Features hinweg. Die Admins müssen es dann eben wieder ausbaden!

6.5 noch zu klärende Fragen

Folgende Fragen könnten oder müssten noch geklärt werden; manche davon eignen sich evtl. für weiterführende Arbeiten:

- Unter welchen Umständen reichen die integrierten Dienste von Microsoft nicht aus und man benötigt zusätzlich den Citrix-Aufsatz Metaframe? Detailliertere Gegenueberstellung ... (vgl. z.B. iX-Artikel 2?/2004)
- Clustering von Servern, Lastverteilung/load-balancing (siehe z.B. LANline 1/2004, S.76 & 77)
- Wie verhält es sich mit der Standard Edition des Microsoft Windows Servers 2003? (resp. Win2k-Server etc.)
- Welche Änderungen sind bei zukünftigen Windows-Versionen zu erwarten (aktuell z.B. Longhorn)?
- Einfluss von DRM & Co. auf die Terminal Services
- Nutzung(smöglichkeiten) der Terminal Services unter weiteren Betriebssystemen wie z.B. MacOS
- Hier nicht bzw. nicht tiefgründig untersuchte Clients, wie z.B. Win 3.11
- Wie sieht es mit Clients für Geräte wie den Compaq iPAQ aus?
- Ist es bei Handhelds/Palms möglich, den Bildschirm um 90° zu drehen? -> Geht z.B. bei OPIE
- ganz andere Ansätze: VirtualPC & VMware, WinE
- Betrachtung sicherheitstechnischer Aspekte
- Wie genau funktioniert die bei der Installation auszuwählende Lizensierung?
- Wird die Installations-CD vom Server 2003 später noch mal benötigt?
- Ist das Dateisystem NTFS zwingend nötig? [TO-DO: Vor- und Nachteile]
- Schattenkopien ... ;-)
- Design eines geeigneten UI
- weitere Forschung an alternativen Ein-/Ausgabeverfahren (z.B. Sprache)
- Weitere Artikel etc. von der Microsoft-Website
- Vergleiche: PC-Anywhere, VNC, Citrix Metaframe, X11-forwarding - auch mit aktuellen Versionen

- Einbindung in Netzwerke mit (P)DCs und AD/DS
- Genaue Darstellung der Unterschiede zwischen MSDN-Version und Volumenlizenz (außer Aktivierung)
- Sind MSDN und MSDNAA-Versionen identisch?
- Vergleiche mit aelteren Versionen? -> eigentlich obsolet ...
- Lizenzen: normale Session vs /console
- Lizenzen: Standard vs volume license vs MSDN
- SUS und WUS
- Weitere Implikationen bei Einbindung in ein Active Directory
- Apple's Client genauer untersuchen
- die Funktionen, die ActiveSync fuer den Benutzer bringt, genauer untersuchen
- DirectX
- Verwaltung aktiver RDP-Connections auf dem Server durch den Administrator (Task Manager, MMC usw.)

7 Zusammenfassung & Ausblick

(TO-DO: hier muss noch n Text hin :-)

- Heutige Applikationen lassen sich in der Regel ohne Maus, rechte Maustaste und ordentliche Tastatur kaum sinnvoll bedienen
- Geräte ohne Maus und Tastatur sind daher für heutige Applikationen nur sehr bedingt geeignet; ein anderes UI-Design ist notwendig; insb. auf Rechts- und Doppel„klick“ verzichten
- Diese Szenarien verstärken den Wunsch nach einer alternativen Ein-/Ausgabe (z.B. via Sprache)
- Die Wiedergabe von Multimedia-Daten über den Terminal Service ist bei Thin Clients nur bei sehr geringen Datenraten möglich
- Ein Teil der Windows-Software heutzutage ist noch nicht mal auf die Strukturen von Windows NT oder auch deren Nachfolger - sprich: die Mehrbenutzerfähigkeit (auch seriell, parallel meist gleich gar nicht) - eingestellt. Diese Situation bessert sich jedoch momentan.

Ausblick:

> Ab SP2 [für Windows Server 2003] sollen Funktionen wie Anwendungsveröffentlichung, Zusammenarbeit (verschiedene Anwender können in einer Sitzung von verschiedenen Standorten aus arbeiten) und Multimedia dazukommen. [iX 02/2004, Seite 82]

Auf Client-Seite ist dagegen mit Windows Longhorn bisher weder an Hand des verfügbaren Client-Previewnoch der Microsoft-Websites viel Neues zu erwarten. Eine Integration weiterer Client-Hardware wie z.B. der USB-Schnittstellen erscheint zwar logisch, dafür ließ sich jedoch bisher keine Bestätigung finden.
Wünschenswert wäre auf jeden Fall eine kontinuierliche Anpassung des Clients und des Übertragungsprotokolls an jeweils aktuelle Sicherheitsstandards, sowohl zur Authentifikation als auch zur Übertragung.

Insgesamt ist festzustellen, dass nicht nur ein Teil der angebotenen Windows-Software heutzutage noch nicht einmal an die Strukturen von Windows NT (bzw. dessen Nachfolger) angepasst ist, sondern dies auch teilweise bei Microsoft selber der Fall ist. Echte Multi-User-Fähigkeit kann damit sowohl weder in Hinblick darauf, dass mehrere Nutzer verwaltet werden können, noch im Hinblick darauf, dass mehrere Nutzer gleichzeitig auf einem System oder mit einer bestimmten Software arbeiten, vorbehaltlos bescheinigt werden. Jede eingesetzte Software muß bezüglich dieser Aspekte getestet werden, bevor sie in den Produktionsbetrieb überführt werden kann. Unix-basierte Anstze sind hier klar überlegen, da Unix von Haus aus eine strikte Trennung der Daten des Systems und der einzelnen Nutzer fordert. Hier ist in der Microsoft-Welt noch Entwicklungsarbeit gefordert.

Gerade im Umfeld einer Mehrbenutzer-Umgebung wäre es wünschenswert, wenn der Administrator bei zu treffenden Einstellungen klarer ersichtlich wäre, welche Einstellungen sich nur auf ein Benutzerprofil beziehen, und welche global sind.

A Abkürzungen & Begriffe

(TO-DO: Streichen aller nicht WTS-gebundenen Abkuerzungen)
Weitere Abkürzungen & Begriffe gibt es auf meiner Internetseite unter `http://www.zeropage.de/it`.

CAL Client Access License: Lizenz pro Client zum Zugriff auf die Terminal Services

CCM Client Connection Manager: Verwaltung der Verbindungsprofile bei der 16bit-Version des Microsoft Terminal Services Clients

CE „Consumer Electronics“ oder „Compact Edition“ oder „Compact Embedded“; Compactness, Compatiblity, Companion and Efficiency: Windows-Version für den Einsatz in embedded oder mobile Geräten. Über die genaue Bedeutung der Abkürzung gibt es unterschiedliche Aussagen, u.a. auch die, dass es sich um keine Abkürzung handelt. Aus den Quellen bei Microsoft war dazu nichts Verbindliches zu entnehmen. (`http://msdn.microsoft.com/embedded/windowsce`)

CIFS Common Internet File System

CLI Command Line Interface: die Kommandozeile, auch als Shell oder Eingabeaufforderung bekannt

GPL GNU public license: Lizenzmodell vieler openSource-Projekte (`http://www.gnu.org/copyleft/gpl.html`)

GPO Group Policy Objects

GSM Global System for Mobile communication: digitaler Standard für Mobiltelefonie der 90er Jahre

HPC ...

IANA Internet Assigned Numbers Authority

IE Microsoft Internet Explorer

IETF Internet Engineering Task Force: `http://www.ietf.org`

IIS Microsoft Internet Information Server

MANIAC Munich Administration aNd Internet Access Control for MSDN Academic Alliance

MMC Microsoft Management Console

MSDN Microsoft Developer Network

MSDNAA Microsoft Developer Network Academic Alliance

MUI Multilanguage User Interface: Erweiterung der englischen Windows-Versionen, um die Sprache der Windows-Komponenten für jeden Nutzer einzeln einstellen zu können. Verfügbar für Windows XP und Windows Server 2003.

NT New/Next Technologie: Microsoft-Bezeichnung für eine neue Basis ihres Windows-Betriebssystems, die ohne den MS-DOS-Untersatz auskommt. Seit Windows XP sind der DOS-basierte und der eigenständige NT-Ansatz vereint und werden nicht mehr als getrennte Zweige weitergeführt.

OS Operating System: das Betriebssystem

OSDN Open Source Development Network: Entwickler- und Entwicklungsnetzwerk der openSource-Gemeinde

PC Personal Computer: privat nutzbarer Computer (im Vergleich z.B. zu MainFrames), ursprünglich die Bezeichnung für IBMs Desktop-Computer, heute üblicherweise Bezeichnung für x86-Systeme, oft auch für MacIntosh, Commodore, Apple & Co.

PCMCIA Personal Computer Memory Card International Association

PDA Personal Digital Assistant: Kleincomputer, in der Regel ungefähr in der Größe einer Hand und mit TouchScreen

PDC Primary Domain Controller: spezieller Server im Verwaltungskonzept von Windows-NT-Netzwerken

PPC ...

RD Remote Desktop: hier wirklich als reine Abkürzung

RDC Remote Desktop Connection

RDP Remote Desktop Protocol

RFC Request for comments: `http://www.ietf.org/rfc`
Diskussionsgrundlage der Internet Engineering Task Force (IETF), offen für Vorschläge und Diskussionen; diese Papiere stellen keine Standards im eigentlichen Sinne, sondern nur Quasi-Standards dar; dienen jedoch durch ihre offene Struktur einem Großteil der Hard- und Software, die das Internet ausmacht, als Grundlage.

SBC Server Based Computing

SP ServicePack: kumulative Sammlung von Microsoft-(Sicherheits-)updates

SUS System Update Service

TLS Terminal License Server

TS Terminal Services

TSAC Terminal Services Advanced Client

TUI TU Ilmenau

TUILAN TU Ilmenau-LAN

UI User Interface: die Benutzerschnittstelle eines Systems; ihre Eingabemöglichkeiten, Ausgaben und Dialoge.

UMTS Universal Mobile Telecommunications System: kommender bzw. teilweise schon aktueller digitaler Standard für Mobiltelefonie

WILNET „Wireless Ilmenau Network“: WLAN der TU Ilmenau

WLAN Wireless Local Area Network: drahtloses Netzwerk mit beschränkter Reichweite (z.B. Campus)

WUS Windows Update Service

B Ports & Protokolle

Alleine bei den bei IP üblichen Layer-4-Protokollen TCP und UDP gibt es jeweils 65536 mögliche Ports. Üblich ist die Trennung, bei der die Ports bis 1024 als sogenannte „priviligierte Ports“ und die darüber als „unpriviligierte Ports“ bezeichnet werden. Hinter den priviligierten Ports stehen meistens Systemdienste, die ein normaler User nicht starten oder beenden kann. Im Gegensatz zum (auch wesentlich größeren Bereich der unpriviligierten Ports) sind sehr viele davon als „well-known“ bekannt. Die Zuordnung zwischen Port und Dienst ist jedoch keine Pflicht. Daher beschränke ich mich hier auf die Wichtigsten im Zusammenhang mit dieser Arbeit. Eine aktuelle Liste gibt es bei der Internet Assigned Numbers Authority (IANA) [IANA] unter `http://www.iana.org/assignments/port-numbers`.

(TO-DO: IPsec (inkl. IKE), Kerberos)

Port	**Dienst**	**Beschreibung**
135	epmap	DCOM / RPC
137	netbios-ns	NETBIOS Name Service
138	netbios-dgm	NETBIOS Datagram Service
139	netbios-ssn	NETBIOS session service
445	microsoft-ds	Common Internet File System (CIFS) [TO-DO: stimmt so nicht genau]
3389	ms-wbt-server	Terminal Services

Tabelle B.1: Ports & Protokolle

C Windows 16 Bit (v3.x)

Hier nur ein kurzer Abriss des Verbindungsaufbaus der 16bit-Version des Terminal Server Clients.

Nach der Installation findet man In der Programmgruppe „TSClient“ sowohl den sogenannten „Client Connection Manager“, als auch die zugehörigen, benutzerdefinierten Konfigurationsdateien (`*.CNS`).

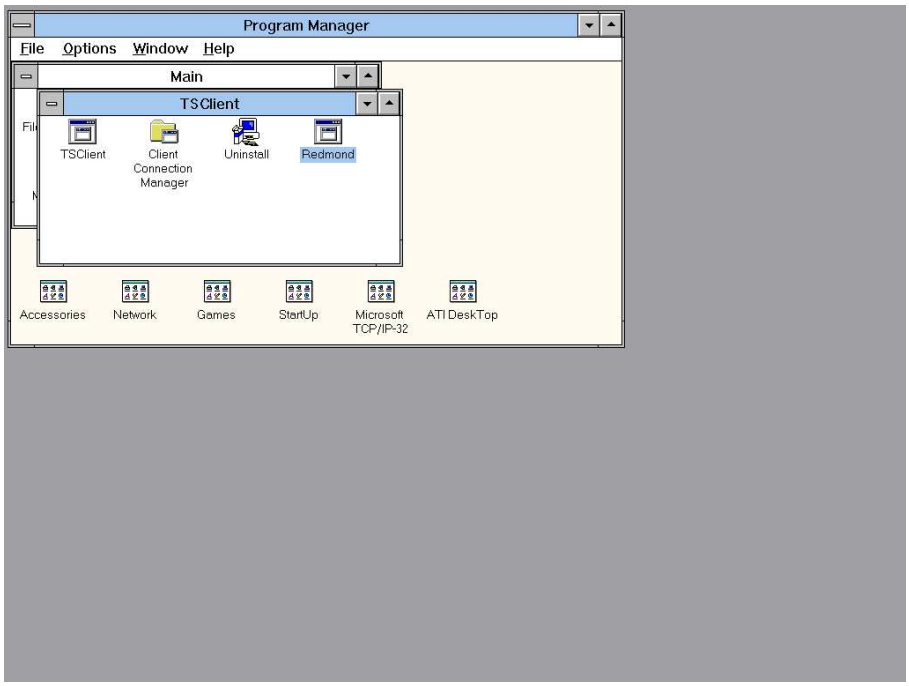

Abbildung C.1: Programmmanager mit Gruppe „TS-Client“

Startet man einen Verbindungseintrag (hier im Beispiel „redmond“, benannt nach dem Namen meines Testservers), so erscheint ein kurzer Dialog, während versucht wird, eine Verbindung zum Server aufzubauen.

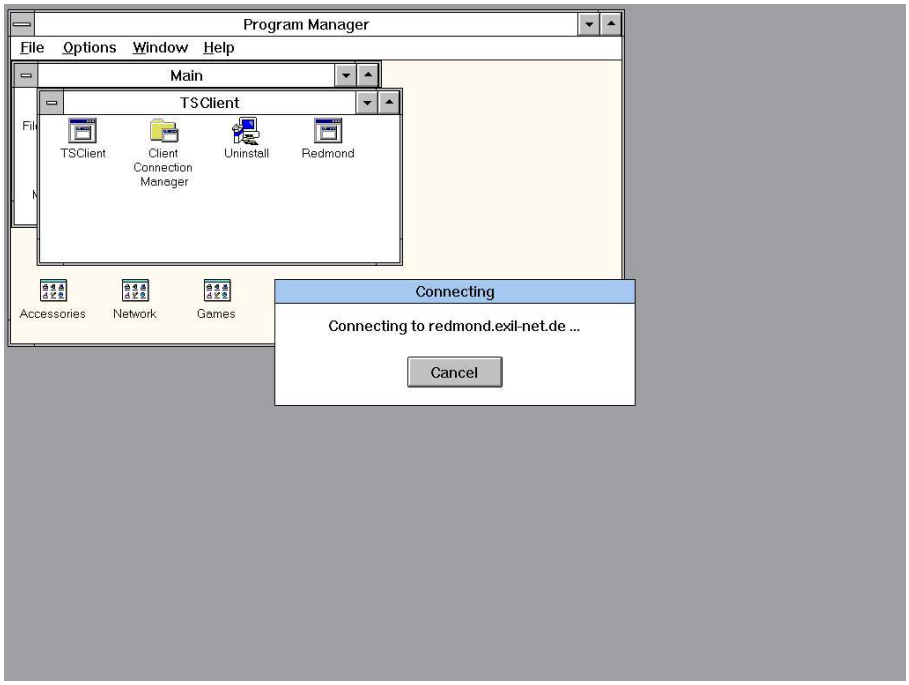

Abbildung C.2: TSClient: Verbindungsaufbau

Bei erfolgreicher Verbindung wird anschliessend der bekannte Anmelde-Bildschirm präsentiert. Am Beispiel des Screenshots kann man die Beschränkung der Farbtiefe des TerminalServerClients auf 16 Farben erkennen.

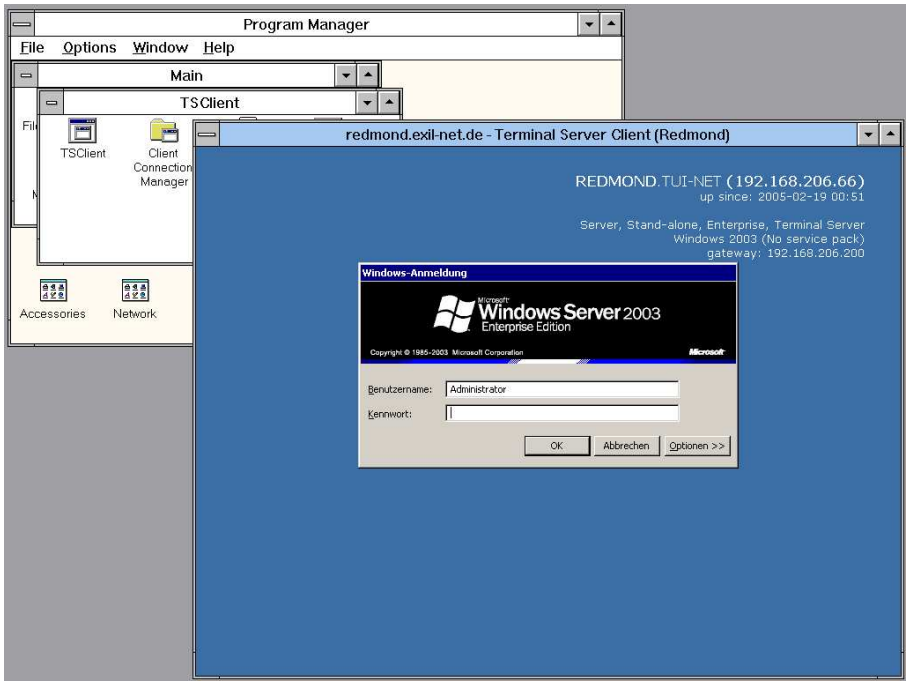

Abbildung C.3: TSClient: Anmelde-Bildschirm

Nach dem Einloggen kann man dann wie gewohnt arbeiten. Es existiert jedoch weder eine Hilfsleiste im Vollbildmodus, noch sind Zusatzoptionen wie Audio-Übertragung oder gar umgeleitete Client-Laufwerke verfügbar.

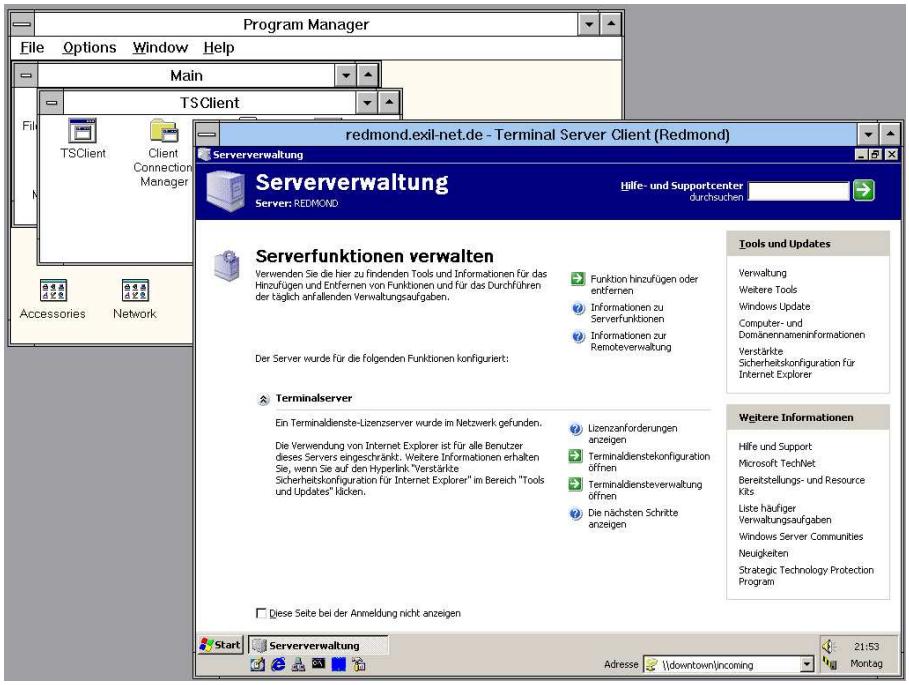

Abbildung C.4: TSClient: angemeldet

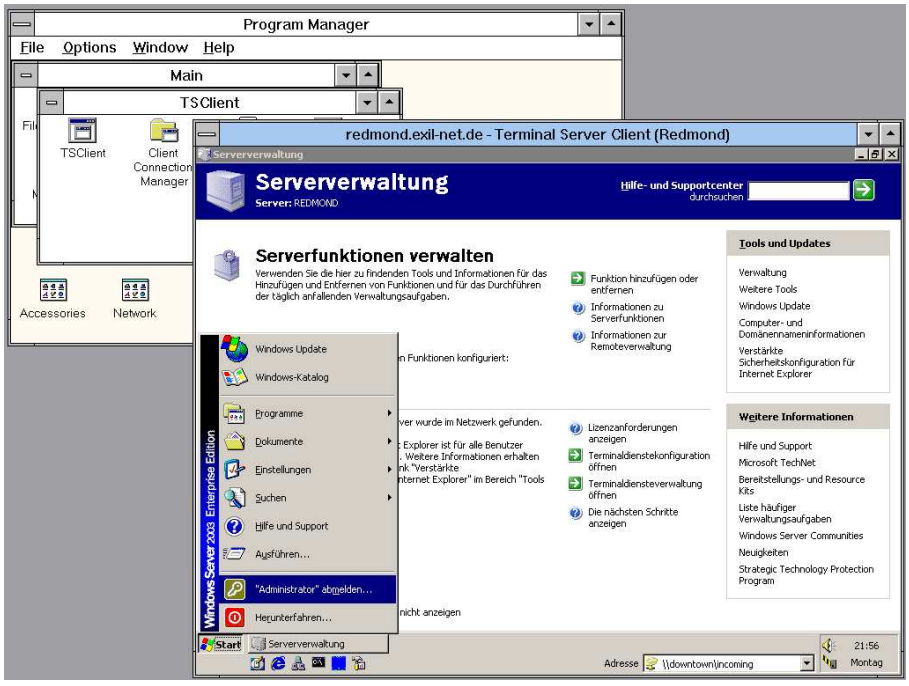

Abbildung C.5: TSClient: remote arbeiten

Zur Verwaltung der Verbindungsprofile kommt bei der 16bit-Version der sogenannte „Client Connection Manager“ (CCM) zum Einsatz.

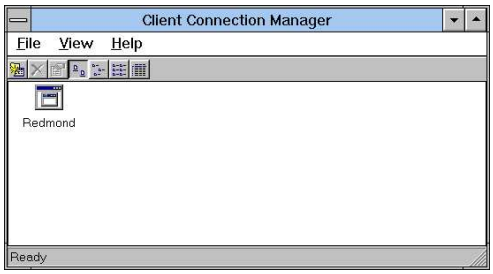

Abbildung C.6: Client Connection Manager

Abbildung C.7: Client Connection Manager: about

Für die Verbindungsprofile gibt es noch die folgenden Optionen:

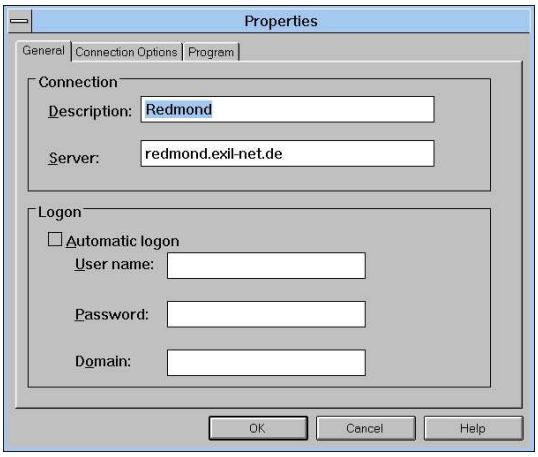

Abbildung C.8: Client Connection Manager: Generelle Optionen

Abbildung C.9: Client Connection Manager: Verbindungsoptionen

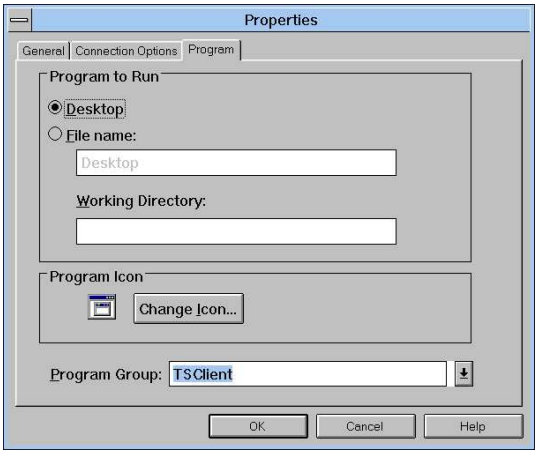

Abbildung C.10: Client Connection Manager: Programmoptionen

D Microsoft Windows Server 2003

Hier einige der Aspekte, die mir bei der Installation von Windows Server 2003 aufgefallen sind:

- CD-ROM auf HDD kopieren: wie schon bei vorhergehenden Versionen kann das Kopieren der CD (Verz. i386) auf die Festplatte beim Installieren Geschwindigkeitsvorteile bringen (wichtig: Cache-Programm - z.B. smartdrv - nicht vergessen ;-), Verzeichnis muss i386 heissen; Unterverzeichnisse sind [nicht] notwendig!). Mindestgröße: 900MB (i386-Verz. [... MB] + temp. Platz [453MB laut Microsoft] zum Installieren) - empfohlen: 2GB FAT16 mit MS-DOS 6.22. Lohnt sich besonders dann, wenn mehrfache nicht automatisierbare Installationen durchzuführen sind oder man Windows nicht auf Laufwerk C: installieren will (siehe nächster Punkt). Bisher wurde die CD nach der Installation jedoch noch nicht wieder benötigt (vielleicht ändert sich das ja noch).

- Laufwerksbuchstaben: leider besitzt auch Windows 2003 Server - wie schon die Vorgänger aus der NT-Reihe - die unangenehme Eigenschaft, Wechseldatenträger bei der Installation automatisch und manuell nicht eingreifbar in die Laufwerksbuchstabennamensvergabe mit einzubeziehen (ein weiterer Punkt, der für das Kopieren der CD auf die Festplatte spricht), so dass es passieren kann, dass Volumes auf Festplatten (z.B. erweiterte Partitionen) hinter CD-ROM-Laufwerken plaziert werden. Dies lässt sich nachträglich für den Systemdatenträger leider nicht mehr ändern.

- ACPI (Advanced Configuraion and Power Interface): ist das System nicht ACPI-konform oder das ACPI-BIOS broken, kann ACPI bei der Installation mittels F7 (an der Stelle, wo nach F6 für third-party-storage-drivers gefragt wird) deaktiviert werden. Auf ATX-Systemen empfiehlt sich dann die Installation des NT/APM-Legacy-Nodes, damit der Rechner automatisch ausgeschaltet wird nach dem Herunterfahren. Dieser scheint jedoch bei Win2003Server nicht mehr vorhanden zu sein

- Dateisystem: angeboten wird FAT12, 16, 32 und NTFS. FAT12 scheidet wegen der maximal adressierbaren Grösse (32MB) aus; auch FAT16 mit seinen max. 4GB [2GB unter DOS und Windows != NT] dürfte fast immer ungeeignet sein. Von den noch verbleibenden ist NTFS der FAT32 vorzuziehen, da sonst keine Verwaltung von Rechten für Dateien und Verzeichnisse im Dateisystem verankert werden können. (Anm.: die nächsten Versionen von Windows werden ein neues Filesystem mitbringen. Der Support für FAT und NTFS wird aber trotzdem weiterhin erwartet.).

- Hardware: Benötigter Speicherplatz auf HDD nach Grundinstallation: 1.5GB (FAT32), 1.3GB (NTFS) - tatsächliche Belegung je nach gewählter Clustergröße des Dateisystems

- Hardware: Mit 128MB RAM läuft das Grundsystem.

- Aktivierung: auch bei Win2003Server ist die von Windows XP schon bekannte Produktaktivierung nötig, auch bei der via MSDN bezogenen Versionen; die Ausnahme

bilden auch hier wieder nur die Volumenlizenzen. Die Aktivierung sollte gleich nach erfolgter Installation (inkl. Sicherheitspatches) und Netzwerkanbindung durchgeführt werden, wenn man die Aktivierung über das Internet machen will - nach 30 Tagen kann man sich nämlich nicht mehr anmelden, um ggf. noch eine NIC zu installieren (auch nicht im abgesicherten Modus und auch nicht mit BIOS-Datum zurückstellen). Unser Microsoft Student Consultant lieferte mir noch den Link zur TÜViT: „Studie zur Microsoft Produktaktivierung“ (`http://www.tuvit.de/?content=000203&sprache=DE`). Wichtig: die MANIAC-Images fallen unter den Lizenzvertrag der MSDNAA und nicht unter die Volumenlizenzen und müssen somit aktiviert werden.

- Hardware: Für 3com-Karten scheint kein Support mehr dabei zu sein.
- Ein (versehentliches oder vorsätzliches) Vertauschen der Product-Keys für Standard- und Enterprise-Version des Servers scheint nicht möglich zu sein.
- Filesystem: Der Systemdatenträger lässt sich im laufenden System nicht auf Konsistenz prüfen - dazu ist ein Neustart des Servers erforderlich, bei welchem dann der Filesystem-Check durchgeführt wird, wie man es schon von ScanDisk unter Windows 9x her kennt. Bisher hat sich das beim Windows Server 2003 verwendete NTFS v5 als relativ robust erwiesen, so dass auch nach forciertem Systemabsturz der Check keine negativen Ergebnisse brachte. Bei einem Absturz des Servers auf Grund eines Hardwareausfalls kann dies zwar anders aussehen, in diesem Fall ist jedoch sowieso meistens noch mehr Arbeit notwendig als das bloße Neustarten des Servers.
- Freigaben: Leider sind auch bei der neuesten Version der NT-Reihe per default wieder die Laufwerke komplett R/W freigegeben über die Standardfreigaben C$, D$ usw. - wenngleich auch durch Login geschützt.
- Hardware: der Testserver besitzt einen Standard-onBoard-Soundchip: ESS1371 aka SoundBlaster PCI 64/128. Dieser wird nicht unterstützt; von Creative Labs gibt es nur Treiber für Win2k & XP (WDM), die nicht funktionieren. Da für unseren Anwendungsfall auch keine Soundkarte im Server benötigt wird, ist dies hier jedoch nicht ausschlaggebend.
  update: Mittlerweile existiert im Windows-Update ein entsprechender Treiber.
- Aktivierung: leider erfordern auch kleinere Hardwareänderungen eine Produktneuaktivierung (Bsp.: Tausch des Promise-IDE-Controllers gegen ein aktuelleres Modell). Für diese Re-Aktivierung stehen jedoch nur 3 Tage zur Verfügung!
- Dienste: wie immer bei WinNT sollte man auch hier die laufenden Dienste prüfen; so kann es z.B. sinnvoll sein, Dienste wie automatic updates, computer browser, DHCP client, remote registry und auch wireless configuration abzuschalten (siehe dazu [hardening])

E Linksammlung & downloads

(TO-DO: Uebernahme von `http://www.zeropage.de/it/terminal-services/appendix.html\#links`)
(TO-DO: Trennen in Info-Websites und Software-downloads - WICHTIG!) Nach Abschluß dieser Arbeit gewonnene Informationen gibt es auf meiner Internetseite unter `http://www.zeropage.de/it`.

Quellen

[Schiller2003] Jochen Schiller (`http://www.jochenschiller.de`): *Mobilkommunikation* 2., überarbeitete Auflage 2003, Addison-Wesley/Pearson-Studium (`http://www.pearson-studium.de`), ISBN 3-8273-7060-4

[Bartenstein2005] Uwe Bartenstein: *Realisierung einer PDA-Testumgebung für Ad-hoc-Netze*, Studienarbeit an der TU Ilmenau

[Dreyer2002] Dreyer: *Citrix MetaFrame und Windows Terminal Services*, 1. Auflage 2002, mitp, ISBN 3-8266-0766-X

[Harwood2002] Harwood: *Inside Citrix(R) Metaframe XP[TM]*, Addison-Wesley, ISBN 0-735-71192-5

[KaplanMangus2000] Kaplan, Mangus: *MetaFrame[TM] for Windows(R) Terminal Services*, Osborne, ISBN 0-07-212443-1

[KretschmerHerkert2001] Kretschmer, Herkert: *Windows 2000 Terminaldienste - Windows 2000 Application Services zentral bereitstellen*, Addison-Wesley, ISBN 3-8273-1585-9)

[Spealman2003] Spealman, Hudson, Craft: *Microsoft Windows Server 2003 - Active Directory-Infrastruktur*, Microsoft Press 2003, ISBN 3-86063-932-3

[Tritsch2004] Bernhard Tritsch: *Microsoft Windows Server 2003 Terminaldienste* 2. Auflage 2004, Microsoft Press, ISBN 3-86063-656-1

[iX 02/2004] iX 2/2004, Seite 78ff., „Mit oder ohne Aufsatz - Microsoft Windows 2003 vs. Citrix Metaframe XPe“, Heise-Verlag

[iX 03/2004] iX 3/2004, Seite 9/10, Leserbriefe, Heise-Verlag

[LANline spezial III/2005] LANline spezial III/2005, konradin-Verlagsgruppe

[tec 04/2004] PC-Welt Sonderheft - *tecchannel compact* (`http://www.tecchannel.de`), Juli/August/September 04/2004

[freshmeat] `http://www.freshmeat.net`

[GPL] `http://www.gnu.org/copyleft/gpl.html`

[hardening] `http://www.zeropage.de/it/security/hardening.html`

[IANA] `http://www.iana.org`

[IT-security] `http://www.zeropage.de/it/security`

[MANIAC] http://maniac.rz.tu-ilmenau.de: (Munich Administration aNd Internet Access Control for MSDN Academic Alliance)

[Microsoft] http://www.microsoft.com

[MSDNAA] http://www.msdnaa.org

[OSDN] http://www.osdn.com

[PC-AnyWhere] http://www.symantec.com/pcanywhere

[pocket-VNC] http://www.pocketvnc.com

[rdesktop.org] http://www.rdesktop.org

[SIMpad] http://www.my-siemens.com/simpad

[skeye.pad] http://www.hoeft-wessel.com/de/produkte/skeyepad.htm http://forum.skeye.com/load.php?id=14

[sourceforge] http://www.sourceforge.net

[Symantec] http://www.symantec.com

[realVNC] http://www.realvnc.com

[Win2003-Editionen] http://www.microsoft.com/windowsserver2003/evaluation/features/compareeditions.mspx

[Windows-wishlist] http://www.zeropage.de/it/windows/wishlist.html

Stichwortverzeichnis