Abschlussprojekt
im Modul
Netzwerk- und Betriebssysteme
FSIV 07

Thema:
Terminalserver am Beispiel von iTALC, TightVNC und RDP

Ausarbeitung von
Sabine Laubscher und
Orkun Akdeniz

Stand: 19.01.09

Inhaltsverzeichnis

1 Terminalserver....3
1.1 Vorteile eines Terminalservers:....3
1.2 Nachteile eines Terminalservers....4
2 Terminalserver anhand iTALC....4
2.1 Installation von iTALC auf Linux....5
2.1.1 Installationsanweisung....5
2.2 Konfigurationen für den Master PC....6
2.3 Konfigurationen für den Client PC....7
2.4 Grafische Darstellung des Programmes iTALC....8
2.5 Welche Protokolle werden im Hintergrund von iTALC verwendet und wie sicher werden die Daten über die Ports übertragen?....9
2.6 Einige Begriffsdefinitionen....11
2.6.1 Was bedeutet SSH „secure shell“ = sichere Shell....11
2.6.2 Was bedeutet VNC „Virtual Network Computing“ ?....11
2.6.3 Was bedeutet Remote Framebuffer Protocol (RFP)....11
2.6.4 Was bedeutet Plattformunabhängig....12
2.6.5 Was bedeutet Transmission Control Protocol?....12
2.6.6 Zugriffsverfahren bei Ethernet....12
2.6.7 Kollisionsdomäne....12
2.6.8 Logische Topologie (Weg der Daten)....13
2.6.9 Verbindung....13
2.6.10 Berücksichtigung der Firewall....13
2.6.11 Was bedeutet RDP „Remote Desktop Protocol“?....14
3 Terminalserver anhand Tight VNC....14
3.1 Installation unter Windows....14
3.2 Manueller Start des Programmes beim Terminalserver....14
3.3 Start des Programmes beim Client....15
3.4 Welche Protokolle werden im Hintergrund von Tight VNC verwendet und wie sicher werden die Daten über die Ports übertragen?....16
4 Terminalserver anhand Remote Desktop Control....17
4.1 Ausführen von Remotedesktop Control....17
4.2 Einrichten des Terminalservers....18
4.3 Einloggen des Clients auf den Terminalserver....18
4.4 Versteckte Datei Default.rdp....20
4.5 Definition der einzelnen Optionen in dieser Datei....21
4.6 Welche Protokolle werden im Hintergrund von einer Remote Desktop Verbindung verwendet und wie sicher werden die Daten über die Ports übertragen?....22
5 Fazit....24
6 Quellenangaben....25

1 Terminalserver

Ein Terminalserver ist ein Computer, der mehrere Terminals (PCs, Desktops) funktionell nachbilden kann. Das heißt, dass alle Daten sowie Programme, auf dem Terminalserver, wie auf dem Echtsystem abgebildet und bearbeitet werden können. Als Terminalserver wird daher auch die Software bezeichnet, die diese Funktionen ermöglicht. Ein Terminalserver kann ein separater Server sein, als auch ein ganz normaler Computer. Man kann vom Terminalserver zum Client werden und vom Client zum Terminalserver.

1.1 Vorteile eines Terminalservers:

- Die Anwendungsprogramme müssen nur auf dem Terminalserver installiert und gewartet werden
- Der Zugriff ist nicht lokal abhängig, d.h. der Client hat durch ein virtuelles privates Netzwerk weltweit Zugriff
- Unternehmen sparen Kapital durch Homeoffice-Arbeitsplätze.
- Bei Verlust des Clients gehen keine Daten verloren.
- Die Daten der Programme sind bei jedem Client auf dem aktuellsten Stand ohne überall aktualisiert werden zu müssen.
- Man spart Kosten für Administratoren, da diese auch bei räumlicher Entfernung Zugriff auf die Computer der Hilfesuchenden haben und Probleme lösen können.

1.2 Nachteile eines Terminalservers

- Bei einem Ausfall des Terminalservers sind die Programme und Dateien für die Clients nicht nutzbar.
- Man ist von einer funktionierenden Netzwerkverbindung vom Terminalserver abhängig
- Die Hardwarekosten eines Terminalservers sind wesentlich höher als

beim Client.

- Der Terminalserver muss über gute Antivirensofware verfügen
- Die Software muss für Terminalserver geeignet sein

2 Terminalserver anhand iTALC

iTALC wurde für Schulen entwickelt, um von einem Lehrercomputer auf bestimmte PC´s der Schüler (Clients) zugreifen und Hilfestellung leisten zu können. Man bildet einen virtuellen Klassenraum mit einem Lehrer und mehreren Schülern. Der Lehrer-PC kann sich den Desktop der Schüler ansehen oder sogar die Fernsteuerung dieses PC´s übernehmen. D.h.: man übernimmt die Tastatur und Maus des Clients und kann Programme und Dateien öffnen bzw. bearbeiten.
Der Lehrer kann die Aktivitäten der Schüler kontrollieren und den Schülern direkt die Ansicht seines Desktops auf die Schüler-Desktop dieses virtuellen Klassenraumes übertragen, um visuell Präsentationen bzw. Demonstrationen vorzuführen. Damit die Schüler diesen auch folgen, kann der Lehrer jeden einzelnen Schüler für Aktivitäten an dem Schüler-PC sperren. Der Lehrer kann auch einem Schüler die Fernsteuerung am Lehrer-PC kurzfristig übertragen, damit der Schüler Aktivitäten ausführen kann.
Voraussetzung ist, dass die Schülercomputer am Netzwerk angeschlossen sind und der Authentifizierungsschlüssel des Lehrercomputers auf den Schülercomputern hinterlegt ist.
Man sollte die Client-Nutzer informieren, dass auf dessen Computer der iTALC-Client im Autostart installiert ist, da man ohne Wissens des Nutzers seinen Desktop beobachten kann.

Siehe auch
http://italc.sourceforge.net/wiki/index.phpre?title=De:Handbuch#Was_ist_iTALC_und_was_kann_es.3F

2.1 Installation von iTALC auf Linux

Der Lehrercomputer wird als iTALC Master und der bzw. die Schülercomputer werden als iTALC Client eingerichtet.
Zuerst sucht man sich über das Internet eine geeignete Version unter Berücksichtigung des Betriebssystems der Computer von iTALC.
Dann wird über die Konsole die passende Version von iTALC auf beide Rechner heruntergeladen. Auf dem Lehrer PC muss der iTALC Master und der iTALC Client und auf dem Schüler PC darf nur der iTALC Client installiert sein.
Unter diesem Link, kann man sich die passende iTALC Version herunterladen.
http://sourceforge.net/project/showfiles.php?group_id=132465&package_id=145556

2.1.1 Installationsanweisung

herunterladen der Installationspakete auf Computer
~$ wget und dann der ausgewählte Link (copy and paste)

Danach beginnt man mit der Installation.

Auf dem Master (Lehrercomputer) mit dem Befehl:
~$ sudo apt-get install libitalc italc-client italc-master
(sudo = switch user and does; gehe zu root und führe aus)

und auf dem Client (Scülercomputer) mit dem Befehl:
~ $ sudo apt-get install italc-client

Nun führt man mit folgendem Befehl die GDM Konfiguration auf beiden Rechner aus, damit iTALC bereits beim Start ausgeführt wird.

„GDM (kurz für GNOME Display Manager) ist der Displaymanager der Desktopumgebung von GNOME und Xfce. Dieser ist dafür verantwortlich, dass Benutzer sich Einloggen und auch unterschiedliche Desktop-

umgebungen auswählen können." http://wiki.ubuntuusers.de/GDM 16.01.09;18:20 Uhr

Auszuführender Befehl:

$~ sudo gedit /etc/gdm/Init/Default /etc/gdm/PreSession/Default

2.2 Konfigurationen für den Master PC

Um von dem Master PC Zugriff auf den Client bekommen zu können, benötigt man diverse Authentifizierungsschlüssel, ansonsten würde man keinen Zugang auf die jeweiligen Rechner erhalten.

Zuerst Prozess stoppen mit dem Befehl:
~ $ killall ica /usr/local/bin/ica &
Verzeichnis anlegen mit dem Befehl:
~ $ sudo mkdir -p /etc/italc/keys/public/teacher/ /
/etc/italc/keys/private/teacher/
~ $ sudo ica -role teacher -createkeypair

Mit obigem Befehl wurden ein privater (private key) und ein öffentlicher Schlüssel (public key) erstellt. Damit nicht jeder über iTALC die Rechner kontrollieren kann, wird eine Gruppe erstellt auf die nur die berechtigten Benutzer Zugriff haben.

Gruppe anlegen mit dem Befehl:
~ $ sudo addgroup italc
(Lege Gruppe italc an)
Benutzer anlegen
~ $ sudo adduser %trusted_user% italc
(Lege Benutzer an)
Gruppe dieser Datei verschieben
~ $ sudo chgrp -R italc /etc/italc/keys/private/
(Ändere Gruppe recursive von italc und verknüpfe sie in Verzeichnis /etc/italc/keys/private)

Der öffentliche Schlüssel muss nun zum Client kopiert werden, damit auch später der Zugriff von den berechtigten Benutzern zugelassen wird.

Befehl:

~ $ sudo scp -p /etc/italc/keys/public/teacher/key
sabine@192.168.2.103***:/tmp/***

(kopiere sicher über das Netzwerk das folgendes Verzeichnis und füge es in den Ordner tmp auf Computer sabine@192.168.2.103 ein)

Der Befehl **scp** erlaubt das sichere Kopieren von Dateien über das Netzwerk.

2.3 Konfigurationen für den Client PC

Für den öffentlichen Schlüssel wird noch ein Pfad für die Ablage auf dem Client-Rechner benötigt

Befehle:

~ $ sudo -s

(Wechsele auf Nutzer root)

~ $ mkdir -p /etc/italc/keys/public/teacher/

(lege folgendes Verzeichnis an)

~ $ mv /tmp/key /etc/italc/keys/public/teacher/

(verschiebe Schlüssel von Verzeichnis in Verzeichnis)

~ $ chown root:root /etc/italc/keys/public/teacher/key

(Berechtigung der Schlüssel an Root übergeben)

Nachdem alle Befehle ausgeführt wurden, starten wir jeweils den Master und Client neu.

Befehl:

~ $ reboot

(fahre Computer herunter und starte ihn erneut)

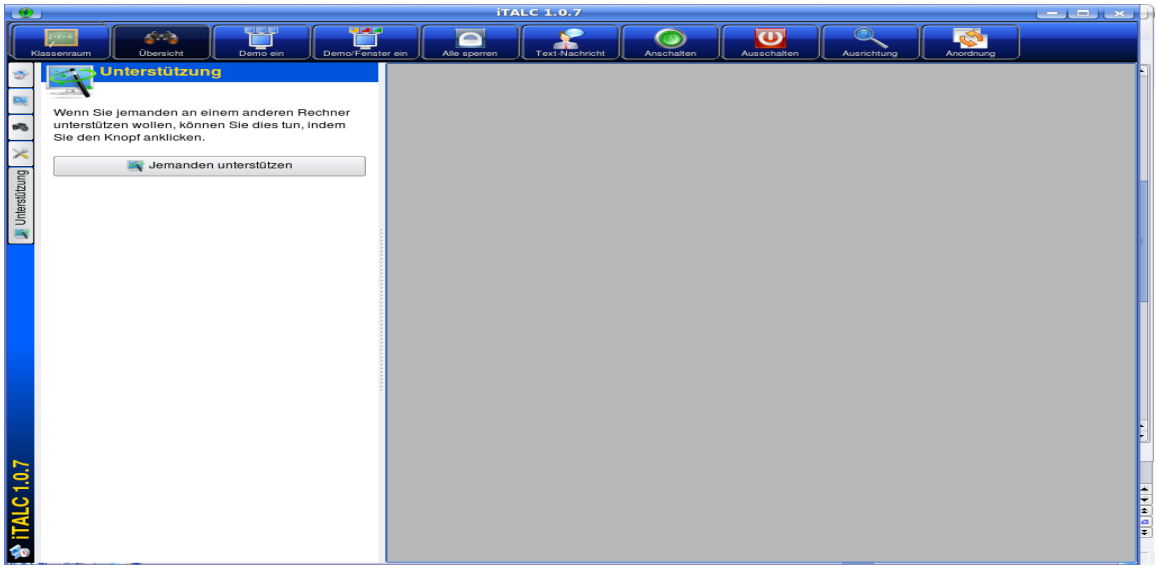
Von nun an ist iTALC nur noch als Root zu öffnen.

Auf dem Master wird zum Starten der Befehl

~ $ italc-launcher

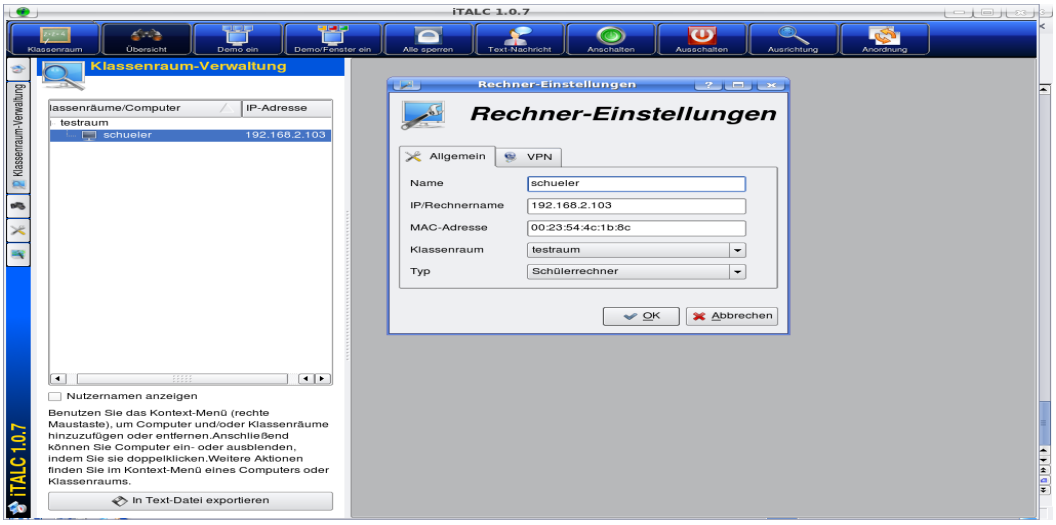
ausgeführt und man erhält die grafische Oberfläche von iTALC.

2.4 Grafische Darstellung des Programmes iTALC

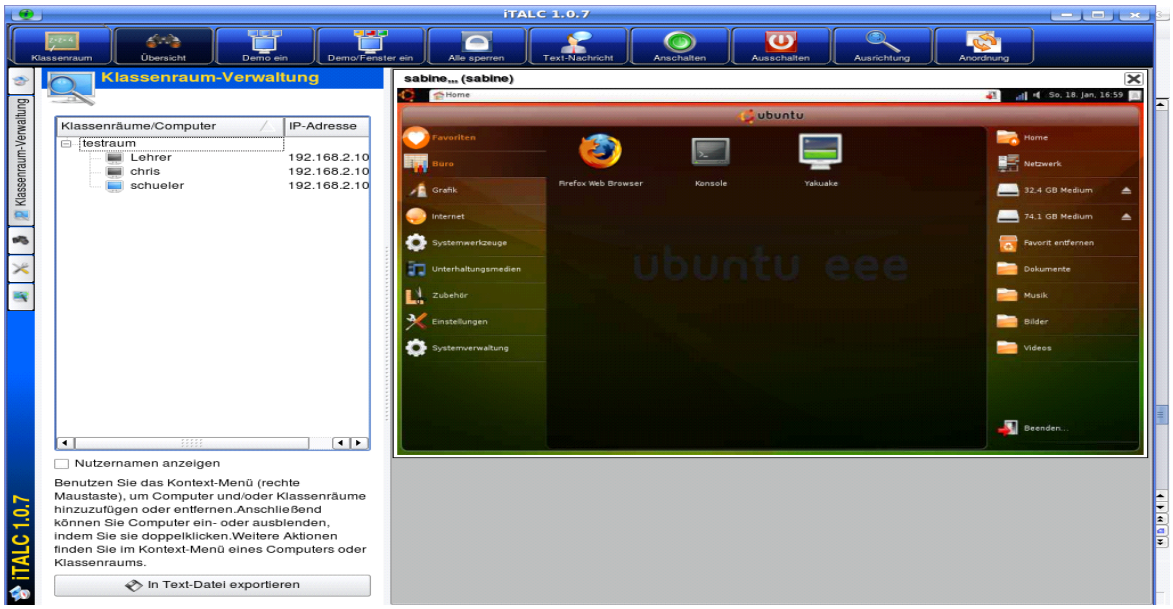


Hier können jeweils über die Einstellungen (Leiste links Symbol Werkzeug) die Klassenräume erstellt werden und darunter den jeweiligen Lehrer und die jeweiligen Schüler PCs.
Um den Lehrer- und die Schülercomputer einzurichten, benötigt man die IP sowie die MAC-Adresse der aktiven Ethernet-Karte (LAN oder WLAN) des jeweiligen PCs.

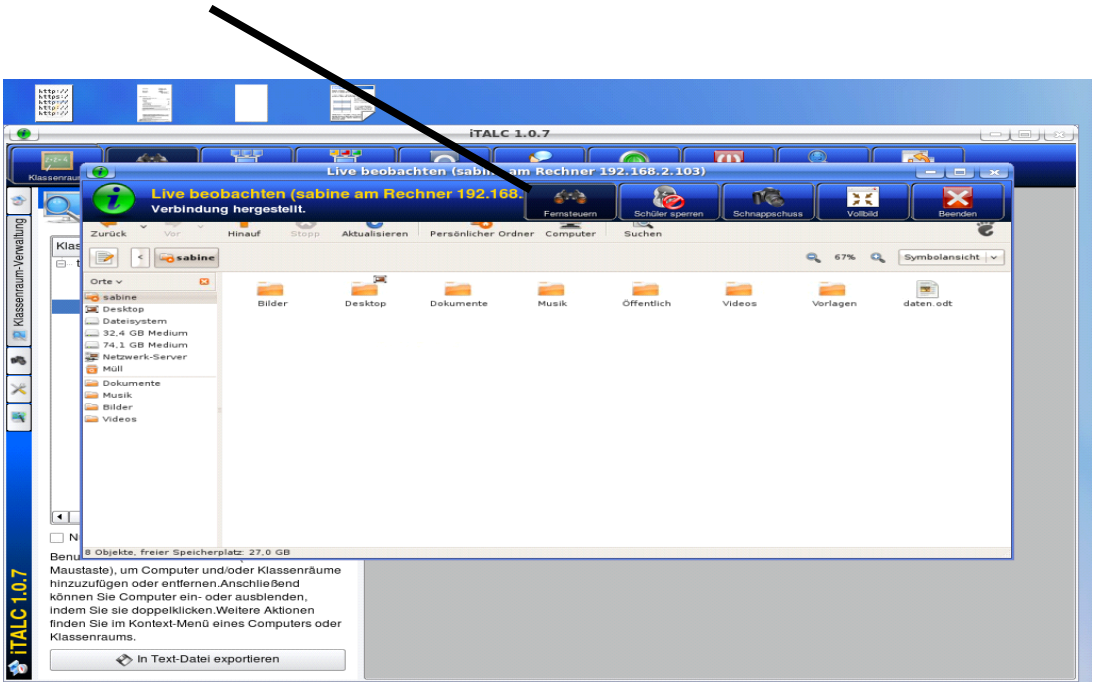
Diese Informationen erhält man durch den Befehl
$~ sudo ifconfig
Natürlich benötigt man für diesen Befehl das Root-Passwort des jeweiligen Rechners.



Nachdem die Einrichtung des Lehrers und der Schüler dieses Klassenraumes erfolgt ist, kann man mit Doppelklick auf den Schüler dessen Desktop beobachten.



Mit diesem Button, können wir den Schüler beobachten oder fern steuern, falls Hilfestellung benötigt wird.

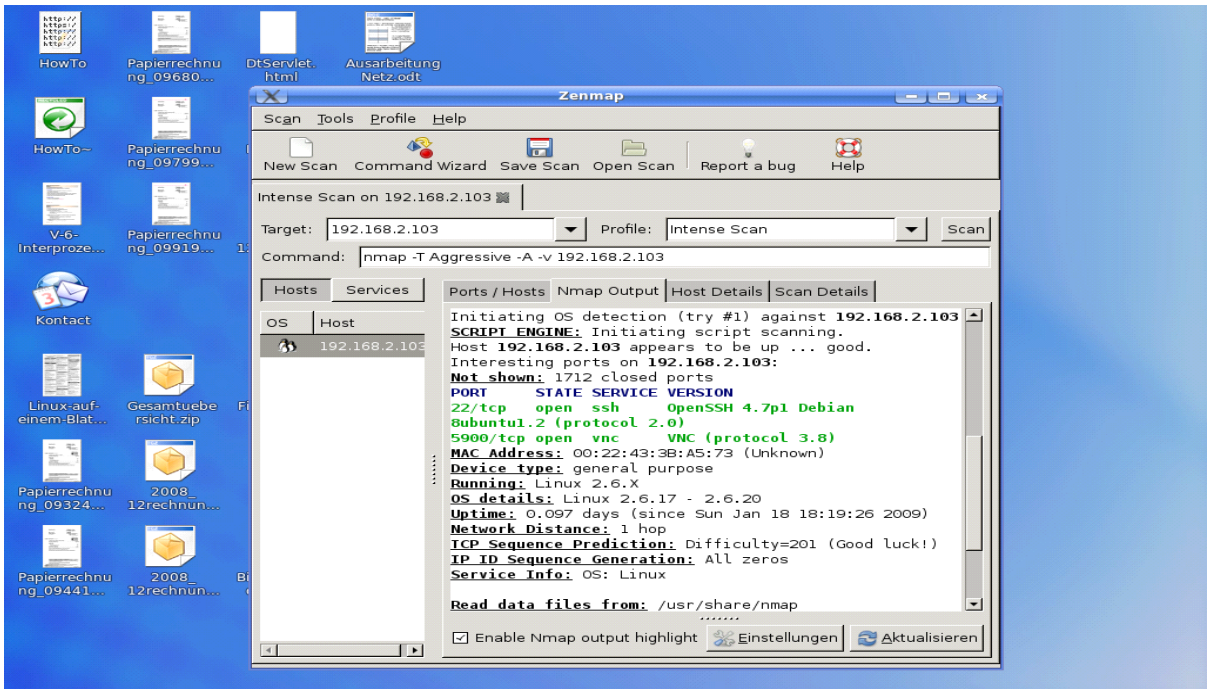


2.5 Welche Protokolle werden im Hintergrund von iTALC verwendet und wie sicher werden die Daten über die Ports übertragen?

Mit dem Sniffer nmapfe haben wir die Ports mit dem User „Root“ ausgelesen.

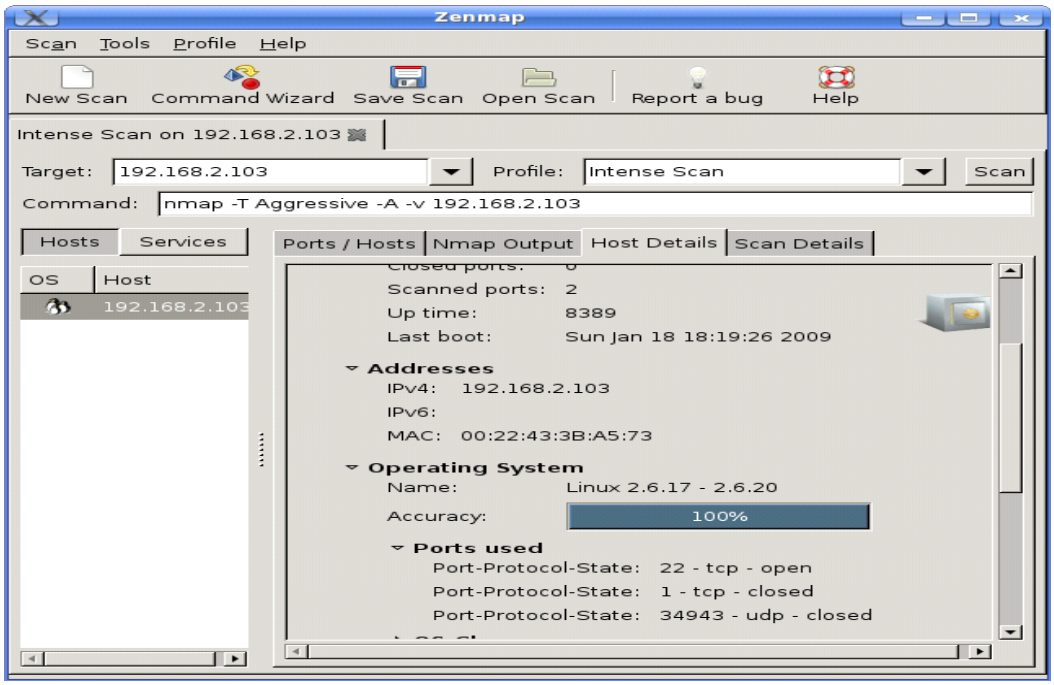
Befehl des bereits installierten Tools:
~ $ nmapfe

Man erkennt die beiden Ports, die durch iTALC genutzt werden.



Einmal Port 22 per ssh; Protokolle tcp, der für eine sichere Verbindung sorgt.

und Port 5900 per vnc; Protokolle tcp, der für die Übertragung des Desktops und die Steuerungskontrolle des entfernten Pc' s sorgt.



Nebenbei kann man mit dem nmapfe noch andere Informationen wie z.B. die Mac-Adresse herausfinden und mit Kenntnissen evt. sogar die Daten. Dieses Programm haben wir nur in unserem eigenen Netzwerk genutzt, denn in einem öffentlichen Netzwerk Ports und Protokolle und evt. Daten zu sniffen ist strafbar und wird auch verfolgt.

Das Programm ITALC kann auch über das eigene Netzwerk hinaus über VPN (Virtual Private Network) genutzt werden. Hierzu sind ausser der IP- und MAC-Adresse auch noch die Subnetmaske und die Hostadresse erforderlich.

Mit diesem Programm sind Lehrer und Schüler nicht mehr lokal abhängig, sondern können zu einer festgelegten Zeit die berechtigten Schüler am Unterricht teilnehmen.

2.6 Einige Begriffsdefinitionen

2.6.1 Was bedeutet SSH „secure shell“ = sichere Shell

Secure **Sh**ell ist ein Netzwerkprotokoll, das die gesicherte (verschlüsselte) Anmeldung an einen Computer bzw. an ein Netzwerk ermöglicht. Sie bietet drei wichtige Eigenschaften:

- Authentifizierung der Gegenstelle
- Verschlüsselung der Datenübertragung, einschließlich der Anmelde-Informationen
- Datenintegrität, also Schutz vor Manipulation der Übertragung.

2.6.2 Was bedeutet VNC „Virtual Network Computing“ ?

VNC ist eine Software, die den Desktop eines entfernten Terminalservers auf einem Client anzeigt und im Gegenzug Tastatur- und Mausbewegung des Clients an den Terminalserver sendet. Damit kann man auf einem entfernten Rechner (Client) arbeiten, als säße man direkt davor. VNC implementiert das Remote Framebuffer Protocol und ist damit, im Gegensatz zu anderer Fernwartungssoftware, plattformunabhängig benutzbar.

2.6.3 Was bedeutet Remote Framebuffer Protocol (RFP)

Das **Remote Framebuffer Protocol** ist ein Netzwerkprotokoll für den Zugriff auf die grafischen Benutzungsoberflächen anderer Computer. Es wird von VNC zur Übertragung von Bildschirminhalten und Benutzereingaben verwendet.

2.6.4 Was bedeutet Plattformunabhängig

*„**Plattformunabhängigkeit** ist die Eigenschaft eines Programms, auf verschiedenen Computersystemen mit Unterschieden in Architektur, Prozessor, Compiler, Betriebssystem und weiteren Dienstprogrammen, die zur Übersetzung notwendig sind, lauffähig zu sein.“*

http://de.wikipedia.org/wiki/Plattformunabh%C3%A4ngigkeit

2.6.5 Was bedeutet Transmission Control Protocol?

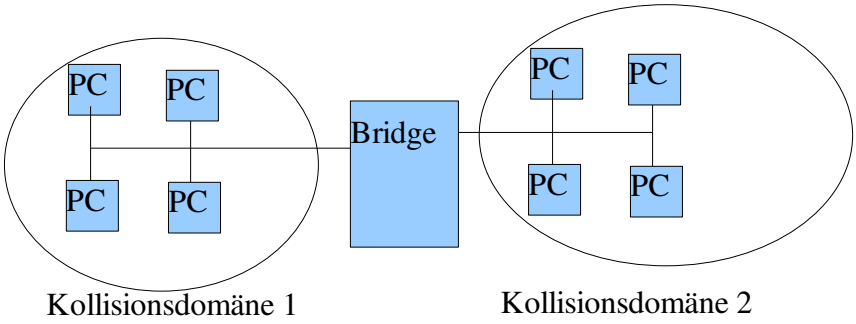
Das **Transmission Control Protocol** TCP = Übertragungssteuerungs-protokoll definiert, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden. Dieses Protokoll bewegt sich auf der Transportschicht Layer vier des OSI-Modells.
Norm: ISO 8073/X.224,ISO 8602 TCP

2.6.6 Zugriffsverfahren bei Ethernet

Das Zugriffsverfahren ist CSMA/CD (Carrier Sense Multiple Access / Collision Detection), Standard bei Ethernet.
(Leitung abhören, wenn frei senden, bei Kollision sendet die erste Station, die es bemerkt ein „jam“ Signal, alle hören sofort auf zu senden ,dann warten auf eine zufällige Zeit, dann erneut senden innerhalb der Kollisionsdomäne. Die Adressierung erfolgt mittels der MAC-Adresse.)

2.6.7 Kollisionsdomäne

Zeichnung Kollisionsdomäne



Die PC' s links und rechts der Bridge befinden sich jeweils in einer eigenen Kollisionsdomäne. D.h. Wenn die PC' s links bzw. rechts der Bridge gleichzeitig in ihrem Segment (Kollisionsdomäne) kommunizieren, entstehen Kollisionen.Wenn ein PC von links nach rechts der Bridge kommunizieren will, wird das Datenpaket erst im Bridge zwischengespeichert und dann in das rechte Segment versendet. Falls in diesem Moment jeweils ein weiterer PC links und rechts sendet, entsteht

nur in dem rechten Segment eine Datenkollision.
In größeren Netzen nutzt man Switch' s (Multiportbridges), da ist jeder PC direkt an den Switch angeschlossen und es entsteht nur zwischen dem Switch und dem jeweiligen PC eine Kollision.

2.6.8 Logische Topologie (Weg der Daten)

Broadcast, d.h. Jeder PC innerhalb der Domäne kann sofort senden, ohne eine feste Reihenfolge zu berücksichtigen.

2.6.9 Verbindung

PPP Point to Point bis zum Router und über das Internet PPPOE Point to Point over Ethernet.
Durch die Adressierung Mac-Adresse und IP-Adresse, wird der Frame (Datenpaket) nur an diese Adresse übergeben.
Die im eigenen Netz bekannte IP-Adresse wird nicht über den Router hinaus über das Internet versendet. Der Router des Empfängers wandelt die IP-Adresse wieder mit seinem Default Gateway und seiner Subnetmaske wieder um.

2.6.10 Berücksichtigung der Firewall

Da die meisten Rechner eine Firewall besitzen, wird das Protokoll FTP (File Transfer Protocol) per Passive Mode ausgeführt. Der Client baut die Verbindung über den Port 21 des Servers auf und der Server sendet dem Client eine Portnummer, mit der die Datenverbindung aufgebaut werden kann. Der weitere Zugriff erfolgt mit Protokollen der Anwendungsschicht wie RDP „Remote Desktop Protocol“, das zum Darstellen und Steuern von Desktops auf entfernten Rechnern dient.

2.6.11 Was bedeutet RDP „Remote Desktop Protocol“?

Das Netzwerkprotokoll RDP das im TCP/IP Modell unter der Anwendungs-schicht angeordnet ist, dient zur Steuerung und Darstellung von Desktops

entfernter Rechner.
Es ist eine Terminaldienst-Sitzung für Einzelbenutzer. Da nur die Tastatur- und Mauseingaben sowie die Bildschirmausgaben übertragen werden, wird die Bandbreite effizient genutzt. Die Verbindung über den Remotedesktop ist daher von der Verbindungsgeschwindigkeit unabhängig.
Siehe auch:

3 Terminalserver anhand Tight VNC

Das Programm TightVNC dient zur Nutzung eines Terminalservers durch einen Client. Es ist eine Opensource-Version, d.h. man kann sie kostenlos aus dem Internet beziehen.

3.1 Installation unter Windows

Unter folgendem Link kann man sich das Programm downloaden:
http://www.netzwelt.de/software/4455-tightvnc.html

Für den Terminalserver lädt man das komplette Programm herunter.
Diese .exe kann man gleich ausführen.

Für den Client lädt man nur den Tight VNC Viewer herunter. Hier kann ebenfalls die .exe gleich ausgeführt werden.

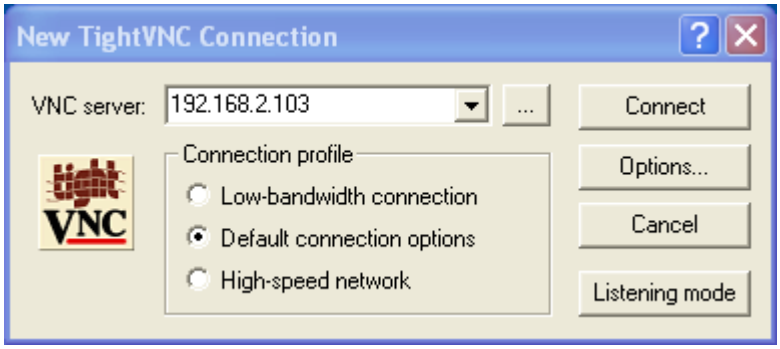
3.2 Manueller Start des Programmes beim Terminalserver

Unter Menü: Programme → TightVNC → Launch TightVNC-Server wird das Programm gestartet.
Ob das Programm gestartet ist, erkennt man dem Button in der Taskleiste rechts.
Beim ersten Öffnen muss man noch die Einrichtung eines Passwortes vergeben, damit nur autorisierte Benutzer mit dem Client Zugriff auf den

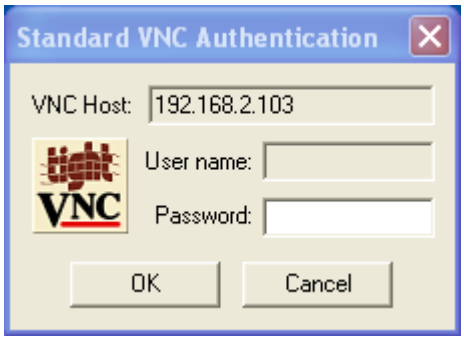
Terminalserver haben.
Damit der Terminalserver dieses Programm gleich ausführt, sollte man es dem Autostart hinzufügen.

3.3 Start des Programmes beim Client

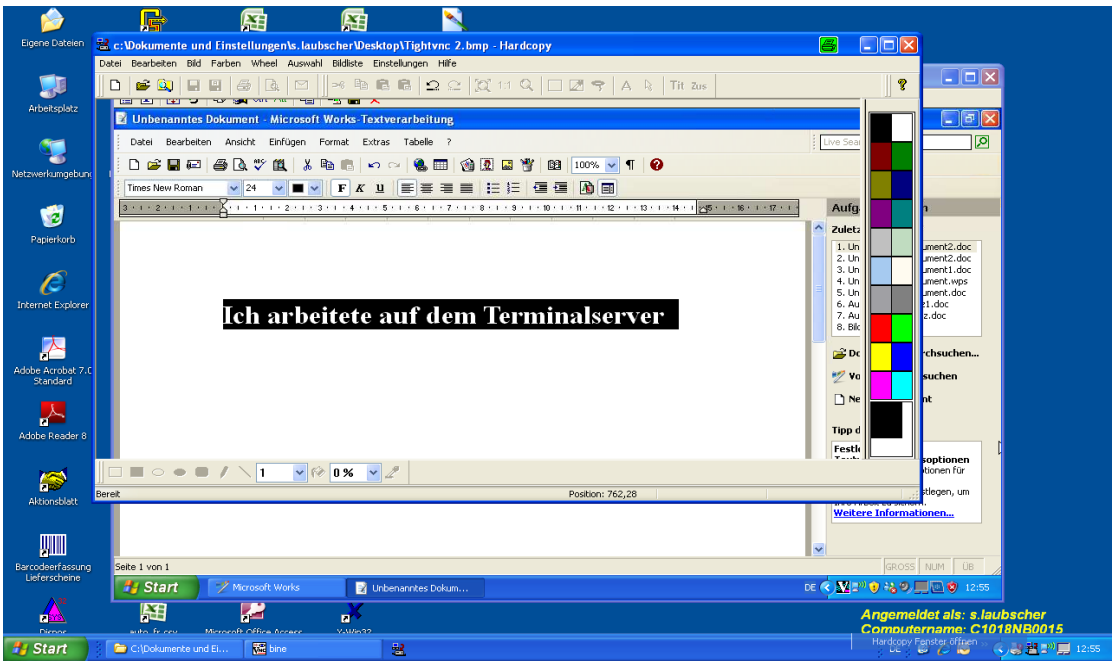
Menü: Programme → TightVNC → TightVNC Viewer
Es erscheint folgender Bildschirm:



Nun kann man die IP-Adresse des Terminalserves eingeben und auf den Button „Connect“ drücken eine Verbindung herstellen.
Es erscheint folgender Bildschirm:



Hier ist die Eingabe des Passwortes für den Zugriff auf den Terminalserver erforderlich. Autorisierten Benutzern wird dieses Passwort durch den Administrator bekannt gegeben.
Nach Eingabe des richtigen Passwortes ist man mit dem Terminalserver verbunden und kann mit Programmen und Dateien arbeiten, als wäre man auf seinem eigenen Computer. Je nach Übertragungsgeschwindigkeit kann es zu leichten Verzögerungen kommen.



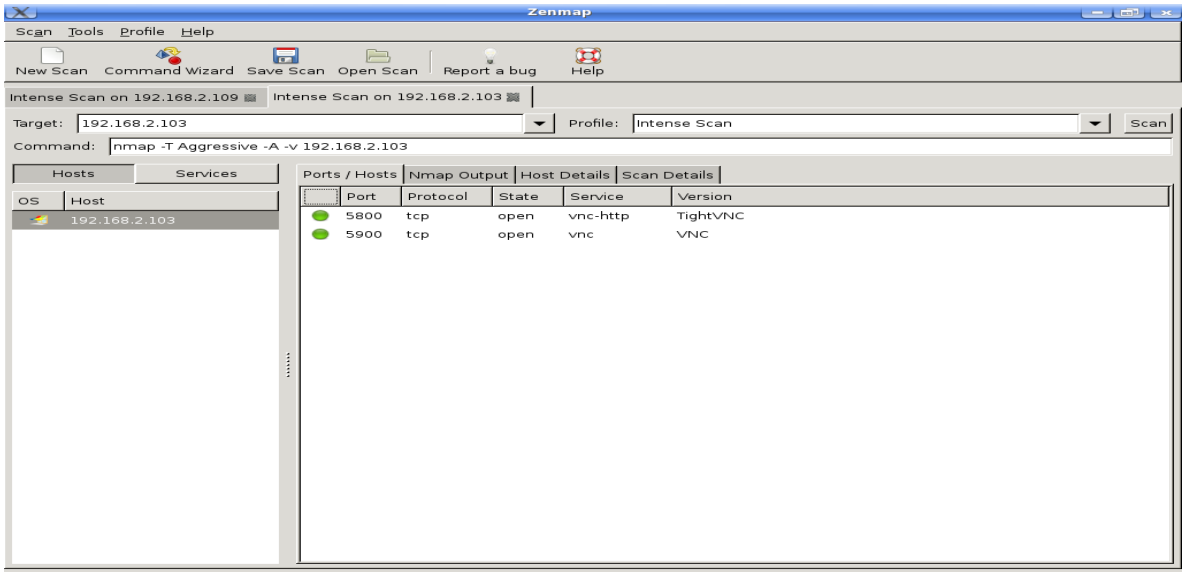
Um diese Verbindung zu trennen, schliesst man mit dem X oben rechts die Verbindung oder unter Datei → Verbindung trennen.

Man sollte auf dem Terminalserver keinesfalls unter Start den Terminalserver beenden, da sonst kein Fernzugriff mehr möglich ist.

Man muss erst vor Ort den Terminalserver wieder starten.

3.4 Welche Protokolle werden im Hintergrund von Tight VNC verwendet und wie sicher werden die Daten über die Ports übertragen?

Mit dem Sniffer nmapfe haben wir die Ports mit dem User „Root“ ausgelesen.



Auf dem Terminalserver sind zwei Ports offen.

- Port 5800, genutzt von vnc http tight VNC, Protokoll tcp, der den sicheren Zugriff auf den Terminalserver gewährleistet und
- Port 5900, genutzt von vnc, Protokoll tcp, der die Übernahme von der Desktopsteuerungskontrolle gewährleistet.

4 Terminalserver anhand Remote Desktop Control

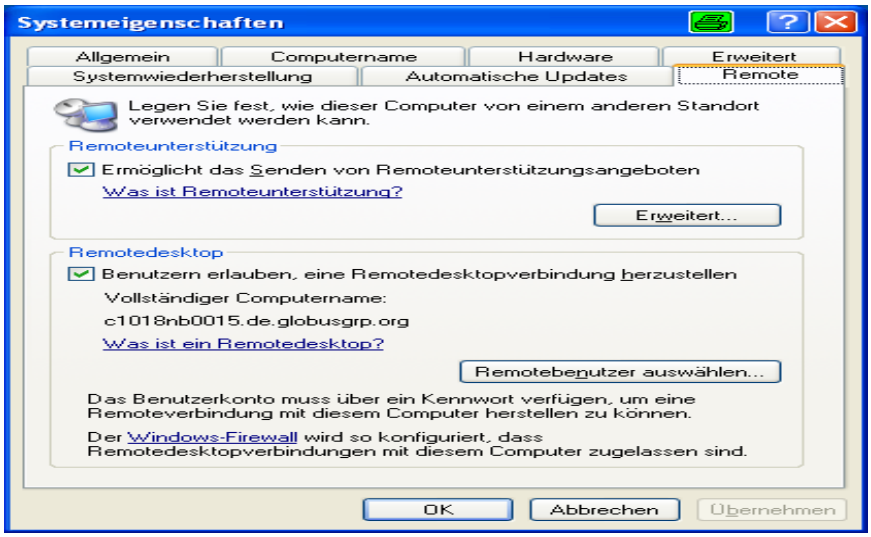
Das Tool Remote Desktop wird von den Systemen Windows 2000, Windows ME, Windows XP, Windows NT und sogar von Windows 9x unterstützt. Meist ist das Programm auch vorinstalliert und falls nicht, ist kann es unter dem folgenden Link heruntergeladen werden.
http://www.microsoft.com/downloads/details.aspx?FamilyID=80111f21-d48d-426e-96c2-08aa2bd23a49&DisplayLang=en

4.1 Ausführen von Remotedesktop Control

Ausgeführt wird das Tool
beim Client unter
Start --> Programme --> Zubehör --> Kommunikation --> Remotedesktopverbindung
oder unter
dem Menü „Ausführen“ mit dem Befehl „mstsc“.

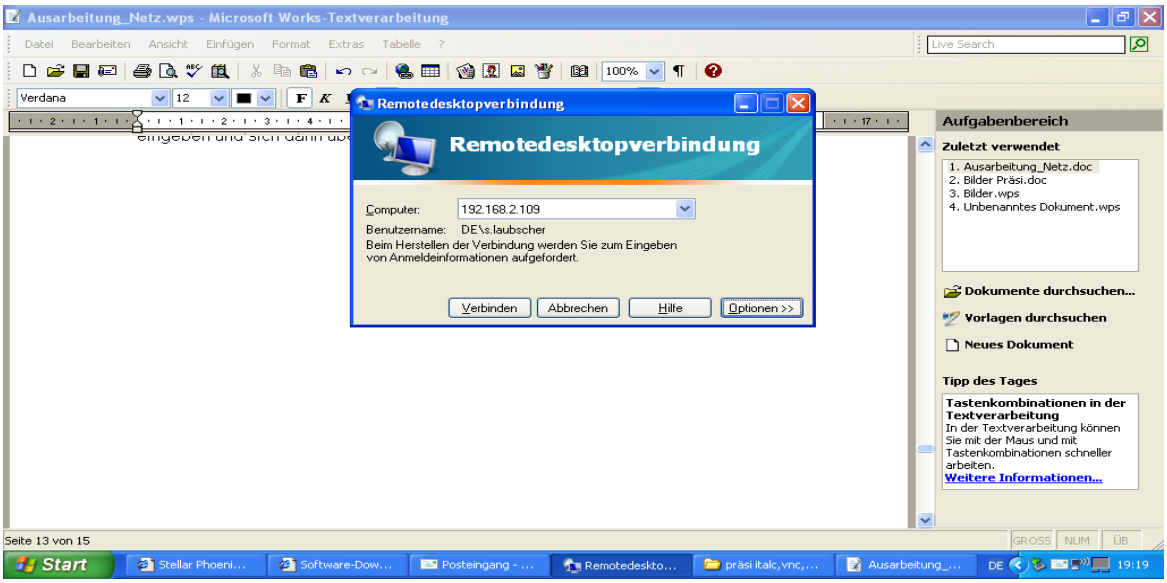
4.2 Einrichten des Terminalservers

Auf dem Computer, auf dem Unterstützung bzw. Hilfe geleistet werden soll, muss unter dem Menü → Systemeinstellungen, → System, → Reiter Remote folgende Häkchen gesetzt werden.



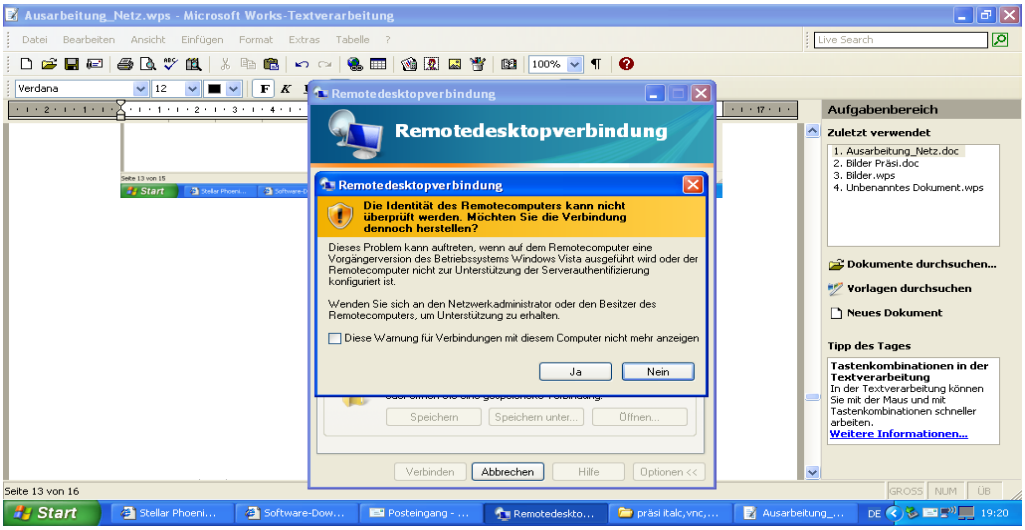
4.3 Einloggen des Clients auf den Terminalserver

Nach Ausführen des Tools erscheint das folgende Fenster, in dem man die IP-Adresse des zu unterstützenden Remote- Computers eingeben und die via Telefon übermittelte Anmeldeinformation, damit man sich auf dem entfernten Computer einloggen kann. Administratoren sind in einem Netzwerk als Benutzer angelegt und können sich auch mit ihrem Admin-Login anmelden.

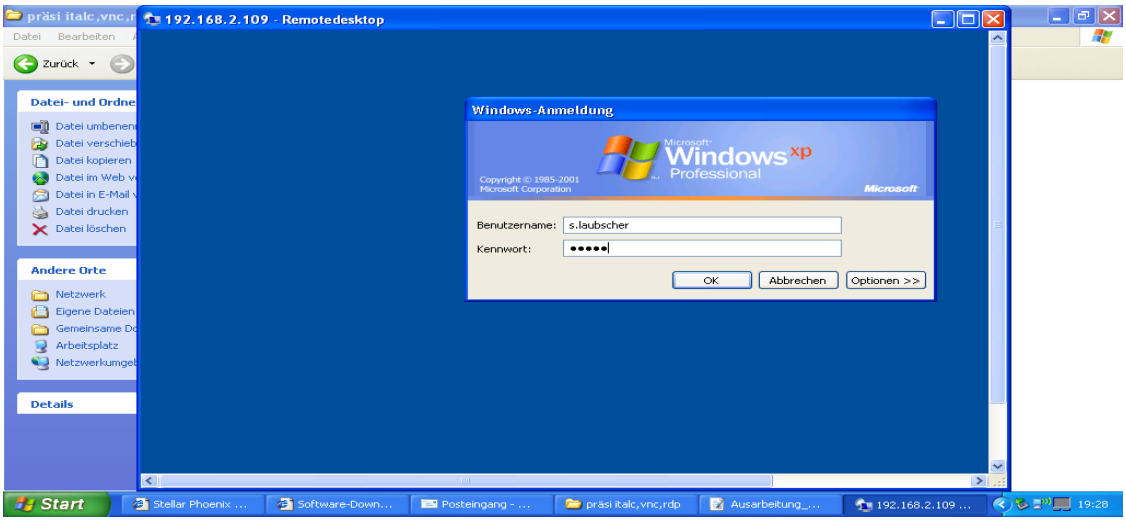


Es kommt bei der Verbindung evt. eine Warnmeldung, die darauf hinweist, dass die Identität des Remotecomputers nicht geprüft werden kann. Dies

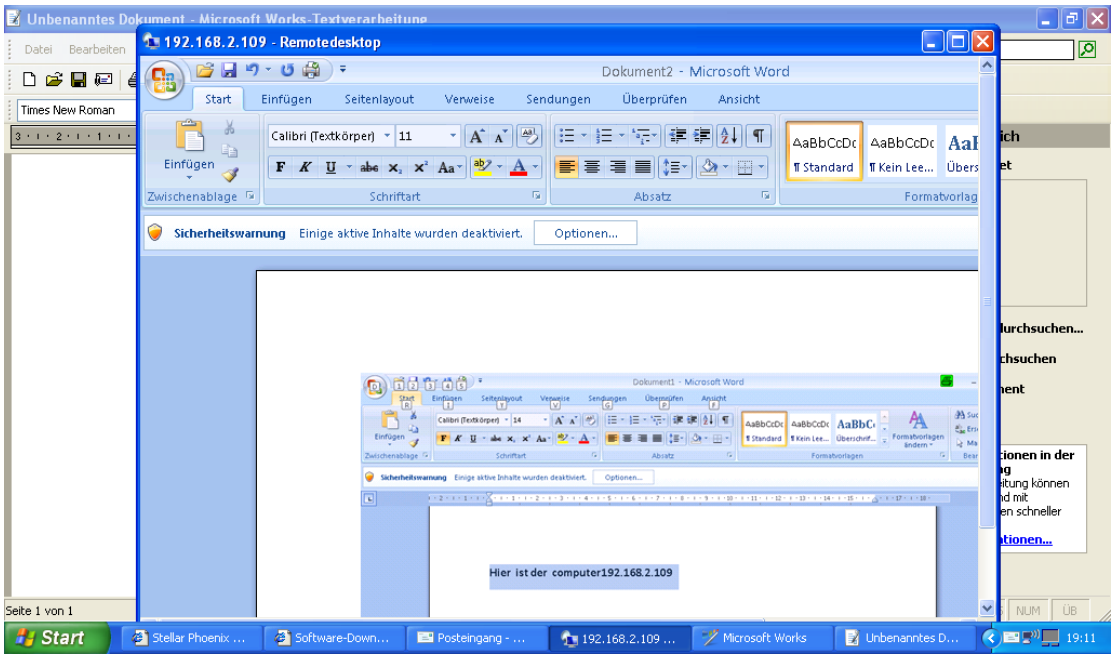
kann in einer sicheren Netzwerkumgebung mit OK bestätigt werden.



Nun befindet man sich auf dem Remotedesktop und kann sich mit dem übermittelten Benutzername und Passwort des entfernten Computers einloggen.



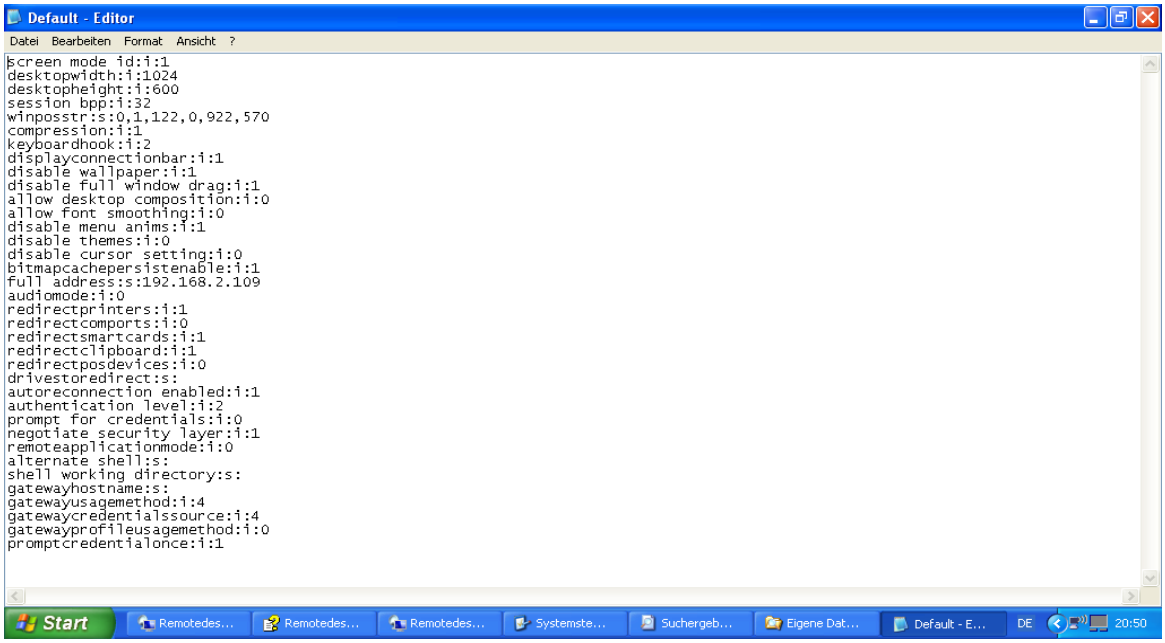
Nach erfolgreichem Login kann man auf Programme und Dateien des entfernten Computers zugreifen. Auf dem entfernten Computer kann man auch definieren, auf welche Programme und Dateien zugegriffen werden darf.



Die Remoteverbindung kann mit mit dem X oben rechts oder unter Datei Remotedesktop verbinden.

4.4 Versteckte Datei Default.rdp

Der zugreifende Computer speichert eine versteckte Datei unter → Eigene Dateien mit dem Namen Default.rdp, in denen folgende Eigenschaften der Remoteverbindung definiert sind.



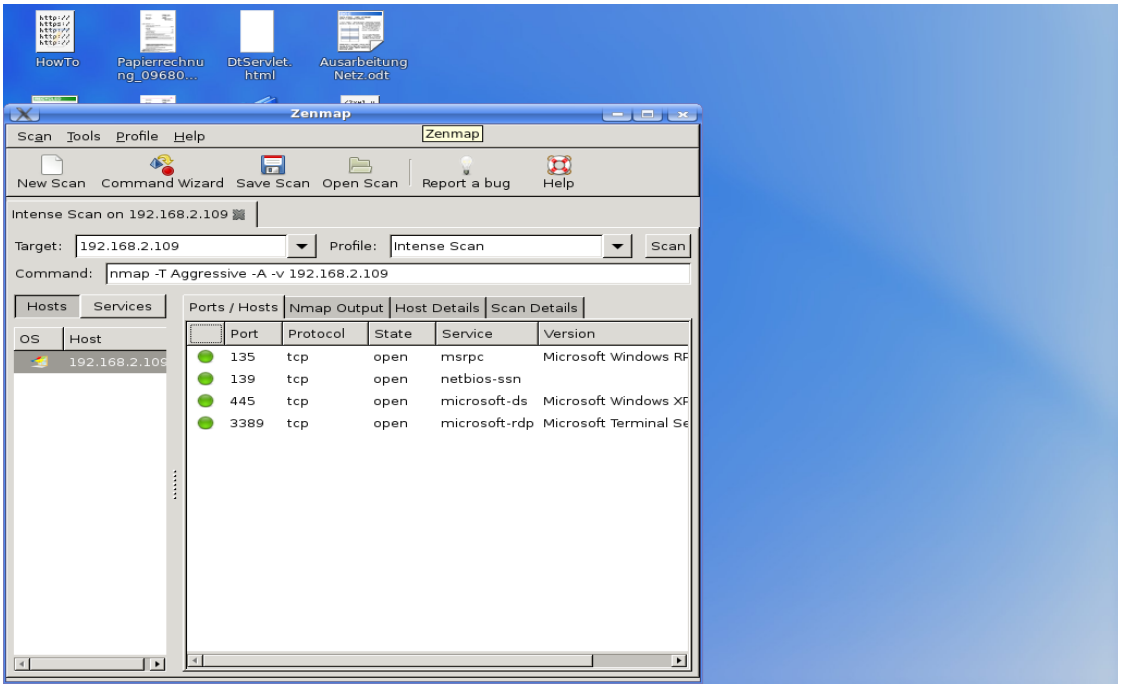
4.5 Definition der einzelnen Optionen in dieser Datei

Option	Beschreibung
Screen mode id:i:1	Dieser Wert bestimmt ob die Remoteverbindung in einer bestimmten Auflösung, oder als Vollbild gestartet wird. 1: Vorgegebene Auflösung 2: Vollbildmodus
desktopwidth:i:1024	Breite des Remote Desktops, wobei auch andere Werte als die Standard-Werte (640, 600, 1024) zugelassen sind
desktopheight:i:768	Höhe des Remote Desktops, wobei auch andere Werte als die Standard-Werte (480, 600, 768) zugelassen sind
session bpp:i:16	Bestimmt die Farbtiefe in Bits, mögliche Werte sind: 8, 15, 16, 24
winposstr:s:0,3,0,0,800,600	Bestimmt die Position und die Grösse des Clientfensters: Werte 3 und 4 definieren die Position der linken oberen Ecke; Werte 5 und 6 die rechte untere
full address:s:sbs.unterwegs-im.net	Adresse des Remote Systems, wobei die Adresse der DNS Name, oder die IP-Adresse sein kann
compression:i:1	Ist der Wert, der die bestimmt, ob Daten komprimiert zum Client gesendet werden: 0: Compression ist aus; 1: Compression ist an
keyboardhook:i:2	Dieser Wert gibt an, wo die Windows-Tastatureingaben erfolgen: 0: Auf dem lokalem System 1: Auf dem Remote System 2: Nur im Vollbildmodus anwenden
displayconnectionbar:i:1	Dieser Wert bestimmt, ob die Verbindungsleiste im Vollbildmode angezeigt wird: 0: Nein; 1: Ja
disable wallpaper:i:1 **disable full window drag:i:**1 allow desktop composition:i:0 allow font smoothing:i:0 **disable menu anims:i:**1 **disable themes:i:**0 **disable cursor setting:i:**0	Optionen die zur Optimierung der Netzwerkleistung deaktiviert werden können. Das betrifft den Desktophintergrund, das Anzeigen des Fensterinhalts beim Ziehen, Menü und Fenster Animationen, Designs und die Bitmapzwischenspeicherung 0: zulassen der Option; 1: Deaktivieren der Option
bitmapcachepersistenable:i:1	Dieser Wert bestimmt, ob zwischengespeicherte Bitmaps persistent, also auf der lokalen Festplatte gelagert werden. Somit können diese bei der nächsten Sitzung wieder verwendet werden. 0: Nein; 1: Ja
Full adress:s.:192.168.2.109	Adresse des Remote Systems, wobei die Adresse der DNS Name, oder die IP-Adresse sein kann
audiomode:i:0	Wie werden Sound abgespielt:0: Auf dem lokalem System 1: Nicht wiedergeben 2: Auf dem Remote System
redirectprinters:i:1 **redirectcomports:i:**0 **redirectsmartcards:i:**1 redirectclipport:i:1 redirctpostdiveces:i:0 drivestoreredirect:s:	Diese Werte geben an, ob lokale Laufwerke, Drucker, serielle Anschlüsse und Smartcards automatisch eine Verbindung zum zur Session auf dem Remote Computer herstellen 0: Nein; 1: Ja
autoreconnection enabled:i:1	Ob eine Verbindung automatisch wieder hergestellt wird, falls sie getrennt wurde, definiert dieser Wert: 0: Nein; 1: Ja
alternate shell:s:	Wenn man ein Programm bei der Verbindung starten will, kann man das dort mit dem komplettem Pfad angeben
shell working directory:s:	Gibt für das mit dem obigem Parameter gestartetem Programm das Arbeitsverzeichnis an
auto connect:i:	Automatische Anmeldung des Benutzers: 0: Nein; 1: Ja
connect to console:i:	Wert bestimmt, ob eine Konsolen Sitzung, oder eine Benutzer Sitzung geöffnet wird. Diese Zeile wird nicht automatisch im .rdp File gespeichert und muss bei Bedarf nachgetragen werden. 0: Benutzersitzung (default); 1: Konsolensitzung

siehe: http://support.microsoft.com/kb/885187/de

4.6 Welche Protokolle werden im Hintergrund von einer Remote Desktop Verbindung verwendet und wie sicher werden die Daten über die Ports übertragen?

Mit dem Swiffer Nmapfe haben wir die Ports mit dem User „Root“ ausgelesen.
Man erkennt die Ports, die durch Remote Desktop genutzt werden.



Es werden auf dem zugegriffenen Computer vier Ports verwendet.

- Port 135 von msrpc, Protokoll tcp

„Die dynamische RPC-Portzuweisung (RPC = Remote Procedure Call) wird von Remoteverwaltungsanwendungen wie DHCP Manager (DHCP = Dynamic Host Configuration Protocol), WINS Manager (WINS = Windows Internet Name Service) usw. verwendet. Die dynamische RPC-Portzuweisung weist das RPC-Programm an, einen bestimmten zufälligen Port oberhalb von 1024 zu verwenden.“
http://support.microsoft.com/kb/154596/de

- Port 139 von netbios.ssn, Protokoll tcp

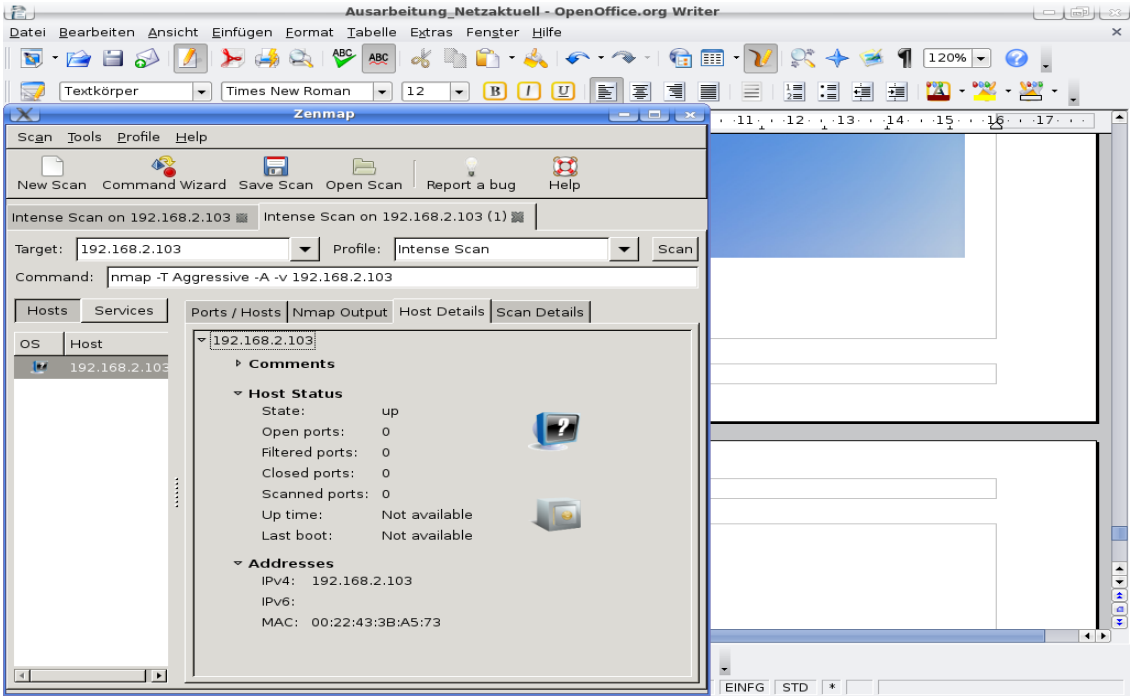
Die NETBIOS Pakete werden über diese Portnummer sicher verschickt.

- Port 445 von ms-ds, Protokoll tcp

Über diesen Port findet die Namensauflösung, login und browsing wie beim 'normalen' NetBios statt.

- Port 3389 von ms-rdp, Protokoll tcp.
-

Über diesen Port wird das Remote Desktop Protokoll gesendet, d.h. mit diesem Protokoll übernimmt man die Steuerungskontrolle.



Von dem zugreifenden Computer kann man keine offene Ports erkennen. Ausser man hätte spezielle Kenntnisse, die uns fehlen.

Bei dieser Sitzung gibt es nur einen Server (erlaubt Zugriff) und einen bzw. mehrere Clients (Zugriff).
Man kann auf dem Server arbeiten und dessen Programme nutzen ohne diese auf dem eigenen Computer installiert zu haben. Der Server kann aber nicht auf dem Client arbeiten und kann dessen Desktop nicht sehen.

5 Fazit

Es gibt noch viele weitere kostenpflichtige und kostenfreie Programme, die zur Verbindung zwischen Terminalserver und Clients dienen.
Je nach Bedarf und Übertagungsgeschwindigkeit kann man sich für ein bestimmtes Programm entscheiden.
Entscheidend für die Nutzung ist, wie werden die Daten verschlüsselt und sicher übertragen.
Vor allem wie schützt man unerlaubten Zugriff von Dritten.

6 Quellenangaben

http://wiki.ubuntuusers.de permanent genutzt im Projektzeitraum
http://de.wikipedia.org permanent genutzt im Projektzeitraum
http://microsoft.com/germany ab_und zu genutzt im Projektzeitraum
http://www.netzmafia.de/skripten/netze/index.html
Schulunterlagen des Unterrichtsfaches Netzwerk- und Betriebssystem
http://de.opensuse.org/Willkommen_auf_openSUSE.org
http://www.unterwegs-im.net/content/view/30/8/
http://www.tomsnetworking.de/content/tipps_tricks/j2005a/workshop_fernzugriff_mit_windows_xp_pro/index.html
und die bei den einzelnen Themen direkt aufgeführten Links

Vielen Dank auch für die freundliche Unterstützung von

Alexander Scheib,
Manuel Heinrich, der uns immer das Internet freigeschaltet hat,
und vielen mehr