5.2.2 Parameter für die Installation

Mit dem Aufrufen des Befehlsparameter „**Ultr@VNC-1.0.X-Setup_de.exe /silent /SP- /NORESTART“** wird die Installation im Silent-Mode aufgerufen. Damit kann das Programm sehr einfachund praxisgerecht in Installationsroutinen mit integriert werden. Beispiel hierfür sind: Der Aufruf in einer Batch-Datei, in der Verwendung in einer Betriebssystem Setup CD, eine Installationen in einer Server / Client Umgebung mit Hilfe eines Loginscripts[26] oder in einer Verwendung als Unterprogramm für Drittprogramme. Sie sehen, die vielfältigen Möglichkeiten den Ultr@VNC-„Silent-Mode“ der Installation zu verwenden sind umfangreich.

***.EXE Parameter**	**Erläuterung**
/dir=Verzeichnisname	Voller Verzeichnispfad, wohin installiert werden soll.
/log	Schreibt eine Log Datei ins temporäre Installationsverzeichnis.
/verysilent	Unterdrückt alle grafischen Anzeigefenster während der Installation.
/silent	Unterdrückt alle grafischen Anzeigefenster während der Installation. Entspricht dem vorangegangenen Parameter.
/norestart	führt keinen Neustart nach der Installation durch
/loadinf=Dateiname.inf	Mit Hilfe dieser Eingabe kann ein mit dem Parameter „**/saveinf**=Dateiname.inf“ erstellte Datei aufgerufen werden. Damit müssen die einzelnen Parameter nicht bei jeder Installation einzeln eingegeben werden.
/saveinf=Dateiname.inf	Automatische Scriptdateierstellung für eine spätere Zweitinstallation via **/loadinf**=Dateiname.inf Parameter.
/SP-	Nicht dokumentiert, evtl. Parameter vom eigentlichen Ultr@VNC Installationsprogramm und nicht von Ultr@VNC selbst.

[26] Mit Login-Scripts ist es möglich automatische Befehlsfolgen bei der Anmeldung eines Benutzers abzuarbeiten.

8.8 Die Toolbar im Ultr@VNC Viewer

Die Toolbar ist eine Art Symbolleiste, die dem Ultr@VNC Viewer zur Verfügung steht und sehr viele Bedienungen vereinfacht. Sie bildet das Herzstück für die leichte Administration von Ultr@VNC Servern.

Abbildung 57, neue Toolbar im Ultr@VNC Viewer 1.0.5

Wenn die Toolbar nach dem erfolgreichen Aufruf des Ultr@VNC Viewers erfolgreich gestartet ist, bekommen wird die Möglichkeit direkt über die Symbolleiste die Verbindung individuell zu administrieren. Die einzelnen Elemente an sich, sind selbsterklärend und werden, wenn man mit der Maus langsam über sie gleitet, auch mit einem Hinweistext angezeigt. Auf den nachfolgenden Seiten werden diese aber noch einmal ausführlich von mir erläutert. Aus diesem Grunde habe ich die Nummerierung in den Screenshot mit eingepflegt. Diese Nummerierung werden Sie sonst nirgends vorfinden.

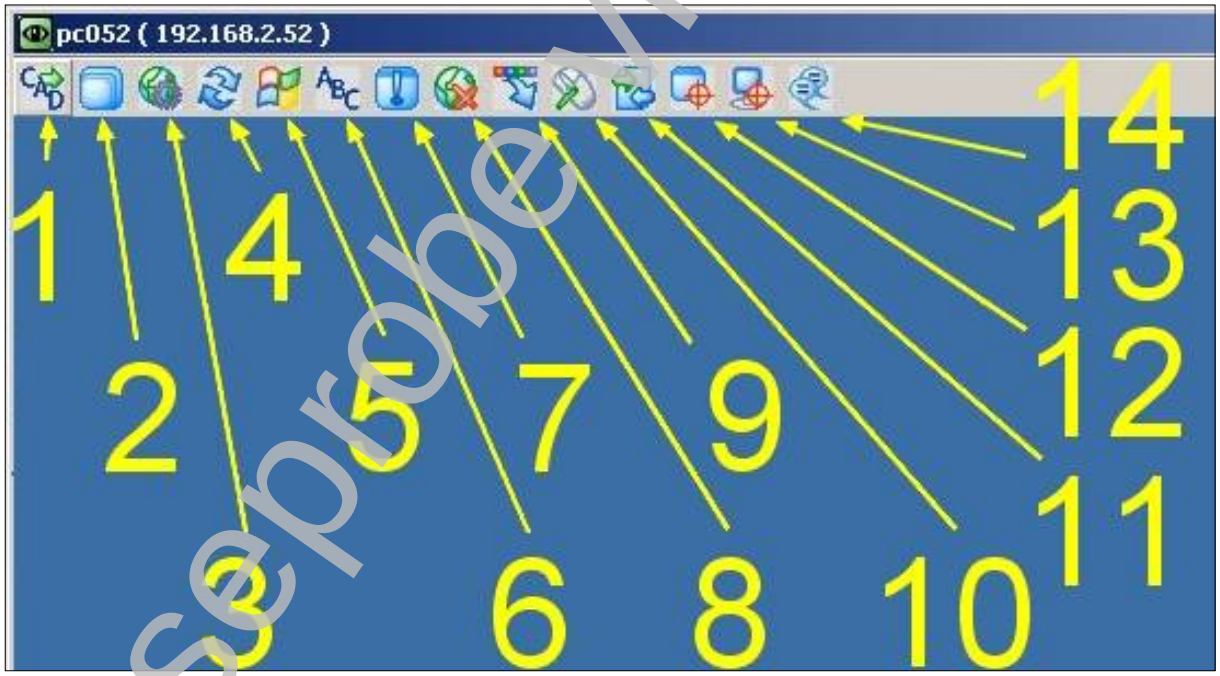


Abbildung 58, Toolbar aus Ultr@VNC 1.0.1 – mit Nummerierung

Nr. Beschreibung

1. „Sende STRG – ALT – ENTF zum Host“

Auf diese Weise besteht die Möglichkeit den Zielrechner neu zu starten oder, wenn Ultr@VNC Server als Dienst installiert ist, sich bei Microsoft Windows32 Betriebssystemen anzumelden.

2. „Vollbildmodus (An/Aus)“

Man bekommt das Gefühl, das man direkt vor dem Remotecomputer sitzt. Wenn man vorher in den Verbindungsoptionen noch die entsprechende Einstellung für das Viewerscaling vorgenommen hat, bekommt man auch keine Einschränkungen durch Bildlaufleisten oder zu kleinen Bildschirmdarstellungen geboten, wenn z.B. der Ultr@VNC Server und Ultr@VNC Viewer stark unterschiedliche Monitorauflösungen haben.

3. „Verbindungsoptionen anzeigen“

Es erfolgt die gleiche Anzeige des Bildschirms wie aus Kapitel 8.3. Die Daten werden übernommen und der Ultr@VNC Viewer neu gestartet. Je nachdem wie schnell der Computer ist, merkt der User der vor dem Ultr@VNC Viewer sitzt dies noch nicht einmal.

4. „Bildschirm aktualisieren“

Dieser Optionspunkt benötigt wenn man eine Aktualisierung braucht bzw. wenn der Datenverkehr im LAN allgemein zu hoch ist. (insbesondere bei A-DSL Verbindungen), keine ausreichenden Datensignale für den VNC Viewer mehr ankommen, das Bild eingefroren wirkt bzw. an einem Ultr@VNC Server aktiven Computer über einen längeren Zeitraum keine Veränderungen mehr vorgenommen wurden. Diese Option ist auch dann sehr sinnvoll, wenn beim plötzlichen Aktivwerden des VNC Servers, die Trägersignale vom Dienst nicht mehr angenommen und übertragen werden.

5. „Sende `Start` (STRG – ESC) zum Server“

Übermittelt einfach das Drücken der Windows Taste. Wichtig für alle die damit arbeiten. **J**

6. „Sende benutzerdefinierte Zeichen“

Oft gibt es Programme die mit Tastenkombinationen gesteuert werden, dabei kann es vorkommen, dass bestimmte Tastenkombinationen nicht übermittelt werden. Die Eingabe einer selbst gewählten Tastenkombination muss im ANSI-Code erfolgen. Diese gesamte Option ist zurzeit noch experimentell.

Abbildung 59, Toolbar - benutzerdefinierte Zeichen

7. „Zeige Statusfenster“.

Diese sehr wichtige Option eröffnet ein kleines Statusfenster in dem die sehr informativen Verbindungsdaten wie IP Adresse, Portangabe, Status, Encoding Format, Geschwindigkeit, etc. … angezeigt werden.

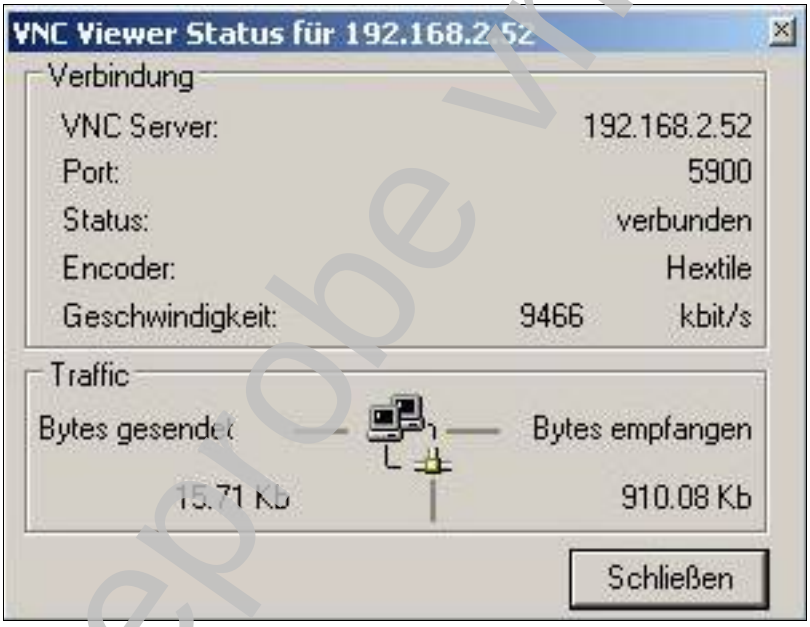


Abbildung 60, Toolbar - Statusfenster

8. „Schließe Verbindung“

Die aktuelle, aktive Verbindung wird beendet.

9. „Verstecke Toolbar“

Damit ist eine direkte Eingabe über die Symbolleisten auf dem Bildschirm nicht mehr möglich, ideal für Profis, die den Ultr@VNC Viewer über Tastenkombinationen steuern können. Siehe Kapitel 8.8.1 Aber wer ist den schon Profi? **J**

10. „**Remote Steuerung und Schwarzer Bildschirm aktivieren (An/Aus)**“ Der Remotecomputer wird Blank geschaltet. Der User vor dem anderen PC kann den Inhalt seines Monitors nicht mehr erkennen und auch keine Eingaben über Maus und Tatstatur vornehmen. Ideal für Serverüberwachungen oder z.B. der User vor dem anderen PC nicht das macht was Sie ihm sagen.

11. „**Öffne Dateiübertragung**“

Hier wird ein zusätzliches Programmfenster geöffnet, das die Dateiübertragung über den VNC Kanal via Unicast[73] aufbaut. Ist die Ultr@VNC Verbindung verschlüsselt, wird während der Datenübertragung ebenfalls alles verschlüsselt und ein mithören bzw. mitschneiden des Datenstroms ist ausgeschlossen. Die Abbildung der Zweifenstertechnik stammt noch von der Ultr@VNC Version 1.0.1. Hier war das Dateiübertragungsfenster kleiner. Ab der Version 1.0.2 von Ultr@VNC wurde das Fenster der Auflösung 1024 auf 768 Pixel angepasst. Dies war deshalb notwendig, da das Dateiübertragungsfenster keine automatische Bildschirmanpassung bzw. Monitor-Scaling unterstützt. Also kann es sein, wenn Ultr@VNC auf einer Serverumgebung verwendet wird und ein 9`` oder eine 14- bzw. 15`` Monitor eingesetzt wird, das das Dateiübertragungsfenster nicht voll ersichtlich ist. Greifen Sie nur via Passwortauthentifizierung, also ohne MS Logon I oder MS Logon II, auf den Ultr@VNC Server zu, achten Sie darauf, dass in dem Bereich Dateiübertragung, bei den administrativen

[73] Im Gegensatz zu Broadcast wo in einem Computernetzwerk von einem Punkt aus an alle die Daten übertragen werden, wird bei Unicast nur eine Point-to-Point (PPP) Verbindung aufgebaut. Dritte sind dadurch ausgeschlossen. Die Gefahr beim Broadcast ist die, dass die Daten an alle Rechner geschickt werden, aber nur der Empfänger, der in der Empfängeradresse des Datenpaketes genannt sind, diese auch annimmt. Dadurch ist es aber möglich die Datenpakete aus dem LAN abzuhören und auszuwerten.

Einstellungen am Ultr@VNC Server, das Häkchen bei „Erlauben“ gesetzt und bei „Benutzer Identifikation (nur bei Service)“ nicht gesetzt ist, da sonst die Dateiübertragung nicht möglich ist.

Abbildung 61, Toolbar - Öffne Dateiübertragung

Gerade wenn man größere Dateien überträgt und dafür einige Zeit vergeht kommt man in die Versuchung zwischenzeitlich das Fenster des Ultr@VNC Viewers verwenden zu wollen. Dies funktioniert nicht. Es kann erst wieder verwendet werden, wenn das Dateiübertragungsfenster geschlossen ist. Also bitte daran denken!

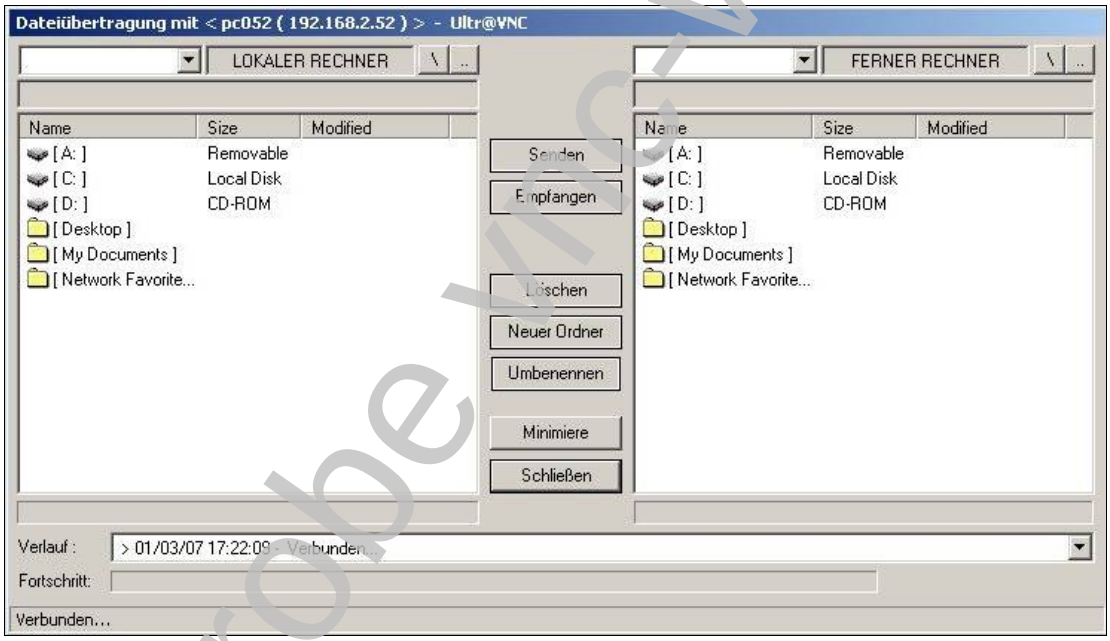


Abbildung 62, Dateiübertragungsfenster – alt – 600 auf 480 Pixel

12. „Wähle einzelnes Fenster“

Ist es gewünscht, das nur einzelne Anwendungsfenster an die Gegenstelle übermittelt werden sollen, kann man durch betätigen dieser Option die Maus einmalig in eine andere Funktion umstellen und das Anwendungsfenster auswählen, dass für die Übertragung zur Verfügung stehen soll. Dadurch wird auch der Datenverkehr stark reduziert und die Netzwerklast verringert. Dem Dozenten, Lehrer oder Präsentierenden wird dadurch auch die Möglichkeit geschaffen im Hintergrund, unbeobachtet von den Remotezuschauern, andere Arbeitsschritte am Computer durchzuführen.

13. „Wähle kompletten Desktop“

Hiermit wird die vorher ausgewählte Option „Wähle einzelnes Fenster“ zurückgenommen und der ganze Desktop wird wieder übertragen.

14. „Starte Chat“.

Gibt es für die User, die vor dem Ultr@VNC Server bzw. -Viewer sitzen keine Möglichkeit direkt oder über Telefon oder andere Möglichkeiten verbal miteinander zu kommunizieren ist bei Ultr@VNC auch der Chat möglich. Dies ist eine sehr interessante Funktion, da bei einer verschlüsselten Verbindung auch der Chat verschlüsselt wird.

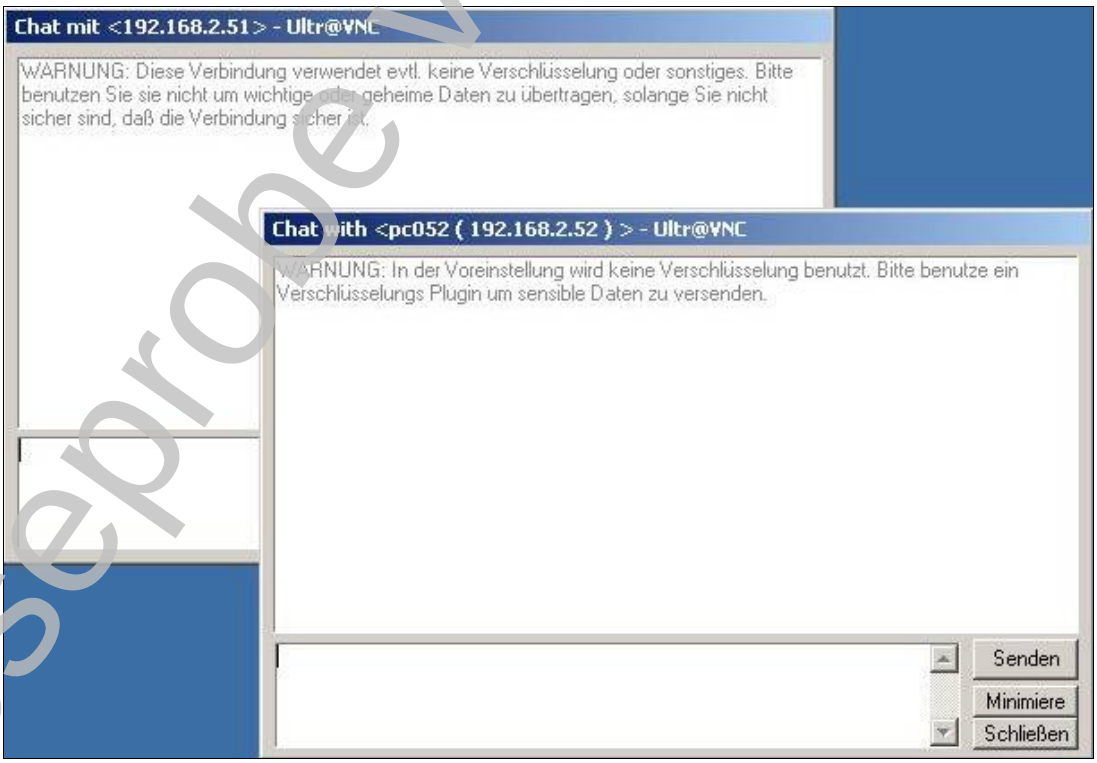


Abbildung 63, Toolbar - Chatclients

8.8.1 Tastenkombinationen in der Toolbar

Das unten aufgeführte Menü bekommen Sie angezeigt, wenn Sie mir der rechten Maustaste in der Toolbar ganz oben links auf das VNC Logo klicken. Ein wenig umständlich, aber wenn man weiß wie, ist das sehr sinnvoll.

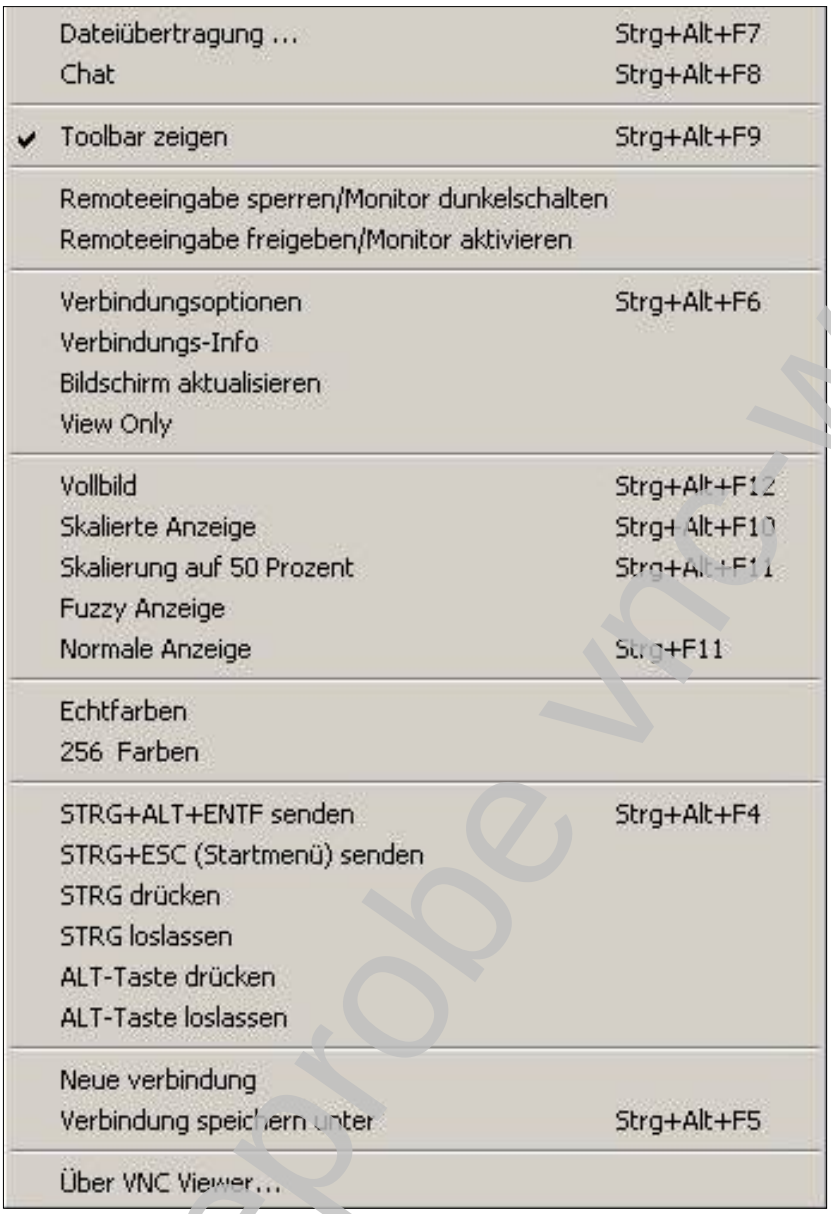


Abbildung 64, Toolbar - Menü

Tastenkombinationen innerhalb der Toolbar im Ultr@VNC Viewer.

Tastenkombination	**Erläuterung**
Strg – Alt – F1	Steht nicht zur Verfügung. Wird sehr oft von anderen Programmen verwendet.
Strg – Alt – F2	Steht nicht zur Verfügung. Wird sehr oft von anderen Programmen verwendet.
Strg – Alt – F3	Steht nicht zur Verfügung. Wird sehr oft von anderen Programmen verwendet.
Strg – Alt – F4	Strg – Alt – Entf Tastenkombination senden Anmeldebildschirm erscheint bzw. Sitzung wird beendet.
Strg – Alt – F5	Verbindung speichern unter . . . wird aufgerufen – Die Verbindungsparameter werden als *.vnc Datei abgespeichert.
Strg – Alt – F6	Verbindungsoptionen werden angezeigt
Strg – Alt – F7	„Dateiübertragung …“ Die Doppelfensteranzeige wird aufgebaut.
Strg – Alt – F8	Chatfunktion wird gestartet
Strg – Alt – F9	Toolbar wird angezeigt
Strg – Alt – F10	Skalierte Anzeige
Strg – Alt – F11	Skalierung auf 50 Prozent
Strg – Alt – F12	Vollbild – Ansicht wird aufgebaut
Strg – F11	Normale Anzeige

12.1.2 TightVNC - Die professionelle OpenSource-Lösung

Aus einer russischen Programmierschmiede stammt das kostenfreie[108] und universelle Programm TightVNC, das seit dem 08.05.2007 in der stabilen **Version 1.3.9** vorliegt und die stabile Version 1.2.9 aus 2003 ablöste. TightVNC gibt es auch eine Variante für das Betriebssystem LINUX / UNIX. Eine JAVA-Applet Viewer Umsetzung ist ebenfalls erhältlich und über den Download der Website www.tightvnc.com zu beziehen. Das große Plus was dieses Programm ausmacht ist die sehr gute Komprimierung der Grafiksignale eines einzelnen Bildes bzw. Frames[109]. Darin ist das Programm einfach unschlagbar. Aus diesem Grunde wurde dieses Encoding Format „TightVNC“ auch in Ultr@VNC mit übernommen. Dafür hat man die Dateiübertragungsfunktion in das TightVNC Programm aus Ultr@VNC heraus integriert. Eine Kooperation, die sich für beide Projekte gelohnt hat.

Die wesentlichen TightVNC Ausstattungsmerkmale:

- In der TightVNC Windowsversion ist seit der Version 1.3.9 ein Dateimanager für die Datenübertragung integriert, der in alle Verbindungsrichtungen vom TightVNC Server und zum TightVNC Viewer verwendet werden kann. In der Linuxversion von TightVNC kann die Funktion des Dateimanager nicht verwendet werden. Dies liegt an der Inkompatibilität von Microsoft Windows- und Linuxbetriebssysteme im Bezug auf die Zugriffsrechte der jeweiligen Dateien und Verzeichnisse.
- TightVNC unterstützt einen Video Mirror Driver ab Microsoft Windows 2000 Prof. Betriebssystemen und höher, insbesondere unterstützt die

[108] Auch wenn hier der Ausdruck kostenfrei verwendet wird, freuen sich die Entwickler immer über eine Spende. Gerade wenn dieses Programm in Unternehmen oder für den kommerziellen Einsatz von Ihnen verwendet werden sollte.

[109] Unter einem Frame versteht man ein einzelnes Bild, das durch eine schnellere Bildfolge zu einer animierten Darstellung des Bildschirminhaltes verwendet wird. Eine ideale Bildfolge bzw. Framerate ist 25-30 Frames pro Sekunde. Für administrative Zwecke ist aber auch eine Bildfolge von 4-5 Frames (pro Sekunde) schon ausreichend.

TightVNC Version 1.3.9 den Demoforge Mirage Treiber, der durch seine spezielle Aufnahmetechnik effizient die Prozessorlast beim TightVNC Server reduziert.

- Es ist eine freie Bildschirmauflösungsanpassung des TightVNC Viewers als auch des Java Viewers möglich.
- Volle Unterstützung der IPv6 Spezifikationen.[110]

Eine komplette Übersicht aller Eigenschaften von TightVNC finden wir unter: http://www.tightvnc.com/whatsnew.html. Das spezielle „Tight"-Encoding erlaubt es, auch Verbindungen die keinen hohen Datendurchsatz erlauben wie z.B. Modem- oder ISDN Verbindungen, sinnvoll und flüssig im Ablauf zu betreiben. Dabei ist der JPEG-Kompremierungsgrad und die damit verbundene Grafikqualität frei konfigurierbar. Siehe hier die Abbildung 83.

Auch der Zugriff über den Webbrowser mit JAVA Applet ist mit TightVNC umsetzbar, dabei kann eine Farbtiefe von bis zu 24-Bit umgesetzt werden. Dies entspricht einer Farbdarstellung von bis zu 16,7 Mio. Farben. Dabei kann das JAVA-Applet auch als HTTP-Server für die standardisierten VNC Versionen dienen.

Der TightVNC Server kann so konfiguriert werden, dass der Server über zwei verschiedene Passwörter angesprochen werden kann. Das eine Passwort für den Vollzugriff auf den Server und das zweite Passwort für die „Nur Lesefunktion". Sehr gut für die Administration in einem LAN. Bitte beachten Sie dazu die nachfolgende Abbildung 84 der TightVNC – Server Optionen.

In der UNIX Version von TightVNC können automatisch SSH Verbindungen mit unterstützt werden. Dabei wird auf das lokale SSH bzw. OpenSSH zurückgegriffen.

Dies sind die Highlights von TightVNC, weitere kleinere Spezifikationen können der Versionsdokumentation entnommen werden. In der vorliegenden Version von TightVNC stehen ebenfalls viele Optionen und Ausstattungsmerkmale von Ultr@VNC zur Verfügung. Wenn Sie sich alleine die folgenden Abbildungen einmal näher anschauen, werden Sie sehr viele parallelen zu anderen VNC Programmen oder zu Ultr@VNC selbst ziehen können.

[110] Ein sehr gute Umsetzung für eine IPv6 Netzwerkumgebung finden wir unter http://jungla.dit.upm.es/~acosta/paginas/vncIPv6.html .

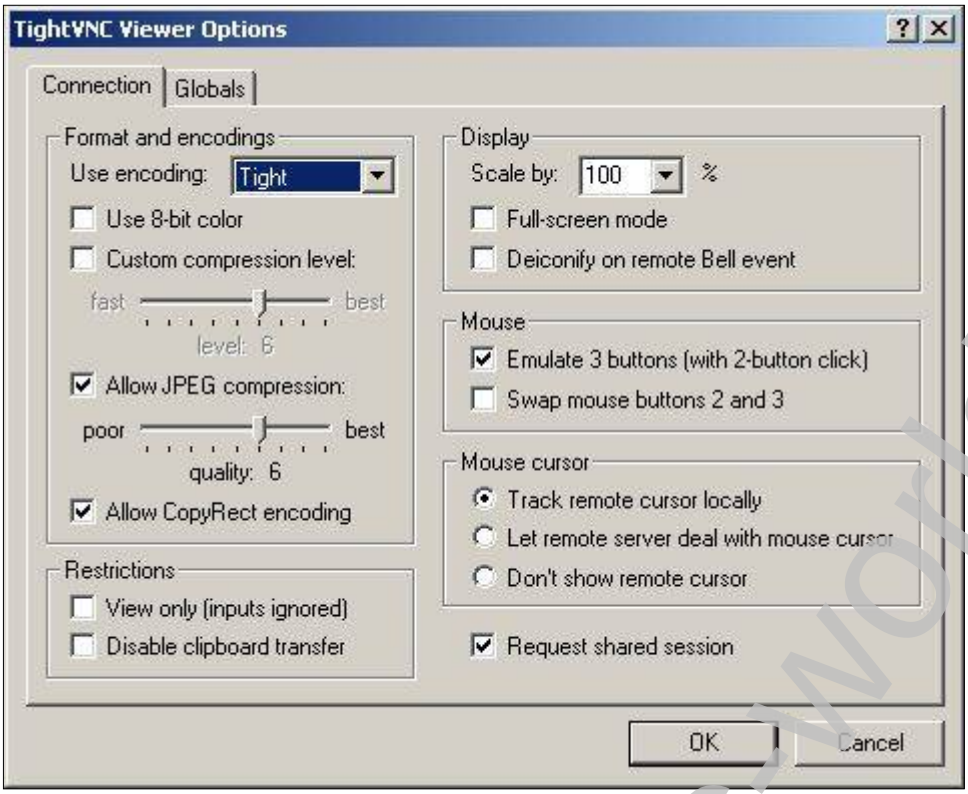


Abbildung 83, TightVNC - Viewer Optionen

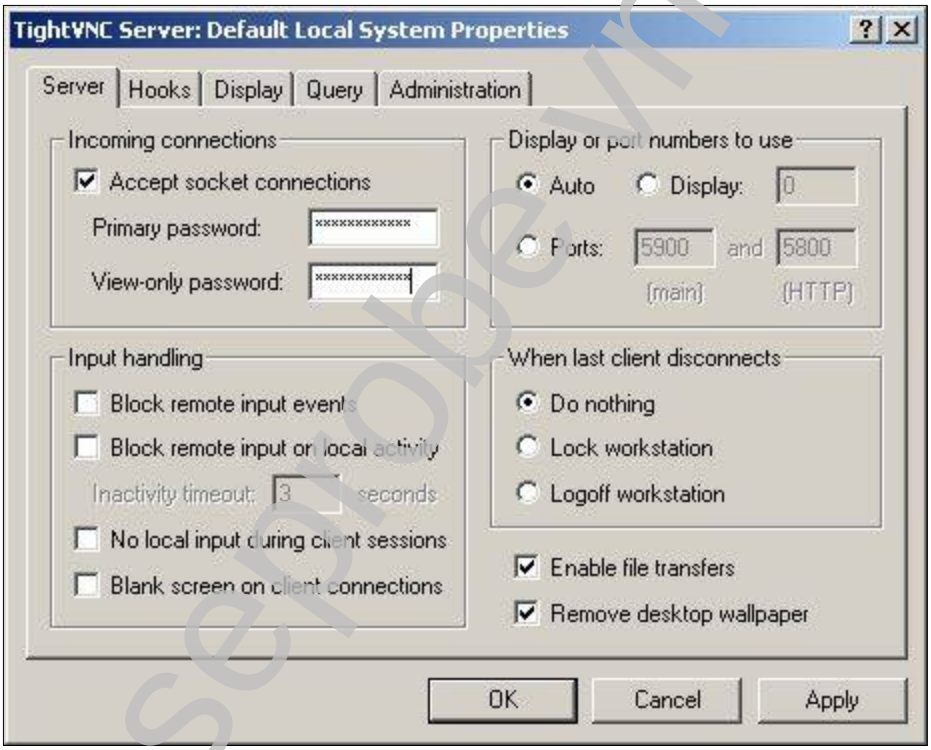


Abbildung 84, TightVNC - Server Optionen

16.5 DHCP Server – dynamische IP Vergabe leicht gemacht

Mithilfe dieses Freewareprogramms in der **Version 1.6.4** (Stand 07.2008) lassen sich sehr einfache Lösungen für das administrieren eines dynamischen Netzwerkbereichs umsetzen. Es kann über die Website http://ruttkamp.gmxhome.de/dhcpsrv/dhcpsrv.htm bezogen werden. Und für seine gute Arbeit kann man Ihm gerne mal über seine E-Mailadresse uwe.ruttkamp@gmx.net ein Dankeschön zukommen lassen. Das Programm hält sich streng an die bekannten und veröffentlichten RFCs 1541 und 1533 für DHCP Server. Der DHCP Server von Uwe Ruttkamp startet auch auf allen MS-Windows32 Clients und kann zusätzlich auf den NT Betriebssystemen als Dienst eingerichtet werden. Damit wird bei NT Betriebssystemen keine Anmeldung eines Benutzers am System notwendig. Er benötigt keine spezielle Serverbetriebssystemversion eines Drittanbieters. Der dhcpsrv.exe-Datei wird eine gleichlautende INI-Datei zur Seite gestellt. Das Programm kann auch ohne Installation als „portable“ Anwendung verwendet werden. Jeder einzelnen Netzwerkkarte kann via MAC Adresse eine feste IP-Adresse zugeordnet werden. Meldet sich nun ein Computer mit der entsprechenden MAC Adresse an, wird ihm automatisch durch den DHCP Dienst die vordefinierte IP zugewiesen. Die MAC Adresse kann man durch Eingabe „ipconfig /all“ in der Befehlszeilenkonsole an jedem Computer abfragen.

Die nachfolgenden Parameter einer INI-Datei, erweitern die möglichen Optionen des DHCP Servers ungemein. Aus einem IP-Adresspool können die entsprechenden IPs auch an nicht bekannte oder eingetragene MAC Adressen verteilt werden. Gleichzeitig können auch Angaben zu DNS Server, Router, Subnetmaske, Domänenname, WINS Server, etc. … bei der Zuweisung der IP-Adresse übermittelt werden. Damit werden sehr viele mögliche Bereichsoptionen abgedeckt. Selbst kommerzielle Server unterstützen meist nicht mehr Bereichsoptionen als dieses kleine Programm und sind dabei wesentlich umständlicher und intensiver zu administrieren. Der einzige „Nachteil“, der Administrator muss wissen was er tut und er muss die theoretischen Grundlagen eines DHCP Servers beherrschen. **J**

Übersicht der möglichen Einstellungen der „dhcpsrv.ini“ Konfigurationsdatei:

[General]; Bereichsdeklaration, Einstellungen, die für alle Clients gelten.

; Auch andere individuell eingerichtete Subnetmasken sind zulässig.
SUBNETMASK=255.255.255.0

; es sind die 10 Bereiche von ROUTER_0 bis ROUTER_9 möglich
ROUTER_0=192.168.54.1
;ROUTER_9=192.168.23.101

; es sind die 10 Bereiche von DNS_0 bis DNS_9 möglich
DNS_1=208.67.220.220
;DNS_2=208.67.200.200

; es sind die 10 Bereiche von WINS_0 bis WINS_9 möglich
WINS_1=192.168.54.253
;WINS_2=192.168.54.252

; Mit diesem Parameter wird die Art des Knotentyps definiert. Hier haben wir
; einen Hybridknotentyp.
NODETYPE=8

; Die Leasedauer in Sekunden seit dem Dienststart, hier z. B. 1 Tag.
LEASETIME=86400

; Domänennamen, der allen Verbindung zugeordnet werden soll
DOMAINNAME=mydomain.local

; Hier wurden für Netzwerkkarten, die eine bestimmte MAC Adresse haben,
; eine IP Adresse reserviert.
[00-23-A2-45-B4-78]
IPADDR=192.168.54.12

; Diese Option wird leider von Windows PCs nicht unterstützt. Hiermit
; kann ein Computername eines PCs bezogen auf die IP-Adresse,
; während des laufenden Betriebes umbenannt werden.
NAME=ClientPC

; Für TFTP Server kann eine Bootdatei hinterlegt werden die aufgerufen wird, wenn
; ein TFTP Client startet und versucht den Bootvorgang zu initiieren.
BOOTFILE=bootimage.bin

; Auf diese Weise kann auf einen anderen TFTP Server im Rahmen der BootTP
; Spezifikationen hingewiesen werden.
NEXTSERVER=192.168.21.2

; Hier kann die absolute Dauer bis zum Ablauf einer Lease in Sekunden seit dem
; 1.1.1970 00:00:00 eingegeben werden. Nach diesem Zeitraum hat der Client keine
; Möglichkeit mehr sich anzumelden. Die Leasedauer ist am 01.01.2008 abgelaufen.
LeaseEnd=1199145699

[Settings] ; Bereichsdeklaration, Einstellungen, die für alle Clients gelten.

; Ist kein „TraceFile“ gesetzt, gilt das Verzeichnis in der sich der DHCP Server
; befindet. Auch UNC Pfade sind möglich. Die Textdateien werden
; unter Umständen sehr lang. Um die Logdatei zu betrachten verwenden
; Sie einen einfachen Texteditor. Das betriebssysteminterne Notepad
; gibt je nach Größe der Logdatei dabei sehr schnell auf. Ich empfehle hier den
; freien PSPAD 4.5.3 Editor BUILD 2298 (Stand 11.2007),
; der über www.pspad.com bezogen werden kann.
Trace=1 ; 1= aktiviert, 0= deaktiviert (Standard)
TraceFile=c:\temp\dhcptrc.txt ; Der Pfad für die Verlaufsdaten des Servers

; IPPOOL_0= . . . bis IPPOOL_9= . . . , 10 IP Adresspool`s sind möglich
; Im ersten Beispiel werden 90 PCs neue IP-Adressen zugeordnet.
IPPOOL_0=192.168.54.11-100
;IPPOOL_1=192.168.55.11-160

; Hiermit kann der DHCP Server an best. Netzwerkkarten gebunden werden.
; IPBIND_0= . . . . IPBIND_9= können als Scriptanweisung verw. werden,
; damit werden max. 10 NIC`s unterstützt. Wenn keine genannt wird,
; gilt der DHCP Server für alle Netzwerkkarten.
IPBIND_1=194.168.123.132

; 1 = keine Antwort bei unbekannten Clients geben, entspricht dem statischen
; DHCP Server und sollte damit nur in Verbindung mit der MAC Adresse der
; Netzwerkkarte verwendet werden.
; 0 = antworten auf Anfragen von unbekannten Clientsanfragen, Standard
IgnoreUnknownClients=1

; Ermöglicht beim automatischen Start als Dienst, das die Abfrage „Don`t ask
; this question again“ nicht den Start des DHCP Servers verhindert.
InstallAsService=2

; Auf diese Weise kann man die minimalste PAcketgröße einstellen, 300 Byte
; ist Standard. Dieser Parameter wird vor allem dann gebraucht, wenn einige
; Clients Probleme haben diese zu handhaben.
MINPACKETLENGTH=300

; Mit diesem Parameter kann eine bestimmten Bind Bereich ein
; gleicher IPPOOL Bereich zugeordnet werden. Sie Beispiel 3.
AssociateBindsToPool=1

Notizen:

Anwendungsbeispiele

1. Ein DHCP Server mit einer Netzwerkkarte, 192.168.10.1, muss ein Subnetz mit IP Adressen versorgen. Die Konfigurationsdatei müsste wie folgt aussehen:

   [General]
   SUBNETMASK=255.255.255.0
   ROUTER_1=192.168.10.1
   DNS_1=192.168.10.1
   [Settings]
   IPPOOL_1=192.168.10.2-49

   Alle Computer im Subnetz werden mit IP Adressen aus dem Bereich 192.168.10.2 bis 192.168.10.49 versehen und bekommen als Gateway 192.168.10.1 und als DNS Eintrag 192.168.10.1 zugewiesen.

2. Der DHCP Server besitzt 2 Netzwerkkarten, eine davon, die 192.168.10.1, soll das angeschlossene Subnetz entsprechend versorgen.

   [General]
   SUBNETMASK=255.255.255.0
   ROUTER_1=192.168.10.1
   DNS_1=192.168.10.1
   [Settings]
   IPBIND_1=192.168.10.1
   IPPOOL_1=192.168.10.2-100

   Alle Computer im Subnetz werden mit IP Adressen aus dem Bereich 192.168.10.2 bis 192.168.10.100 versehen und bekommen als Gateway 192.168.10.1 und als DNS Eintrag 192.168.10.1 zugewiesen. Das zweite angeschlossene Subnetz bleibt unberücksichtigt.

3. Der DHCP Server besitzt 2 Netzwerkkarten, 192.168.10.1 und 192.168.11.1, er soll das jeweils angeschlossene Subnetz entsprechend versorgen.

```
[General]
SUBNETMASK=255.255.255.0
ROUTER_1=192.168.10.1
DNS_1=192.168.10.1
[General_1]
LEASETIME=3600
[General_2]
LEASETIME=86400
[Settings]
AssociateBindsToPools=1
IPBIND_1=192.168.10.1
IPBIND_2=192.168.11.1
IPPOOL_1=192.168.10.2-100
IPPOOL_2=192.168.11.51-80
```

Alle Computer im Subnetz 192.168.10.1 werden mit IP Adressen aus dem Bereich 192.168.10.2 bis 192.168.10.100 versehen und bekommen als Gateway 192.168.10.1 und als DNS Eintrag 192.168.10.1 zugewiesen und hat eine Leasedauer von 1 Stunde (3600 Sekunden). Alle Computer im zweiten angeschlossenen Subnetz 192.168.11.1 werden mit IP Adressen aus dem Bereich 192.168.11.51 bis 192.168.11.100 versehen und bekommen als Gateway 192.168.10.1 und als DNS Eintrag 192.168.10.1 zugewiesen und haben eine Leasedauer von einem Tag (86400 Sekunden).

Mit Hilfe des Bereichnamens General_1 und General_2 sind nicht nur unterschiedliche Leasezeiten zuzuordnen, sondern auch unterschiedliche Subnetmask-, DNS-, Router-(Gateway-), WINS-Einträge, etc. . . … zuzuordnen.

4. Ein DHCP Server mit einer Netzwerkkarte, 192.168.10.1, muss ein Subnetz mit IP Adressen versorgen. Die Konfigurationsdatei müsste wie folgt aussehen:

   [General]
   SUBNETMASK=255.255.255.0
   LEASETIME=32000000
   ROUTER_1=192.168.10.1
   DNS_1=192.168.10.1
   [Settings]
   IPBIND_1=192.168.10.1
   IgnoreUnknownClients=1
   [00-E0-00-1C-AB-68]
   IPADDR=192.168.10.50
   [00-E0-00-1C-AB-62]
   IPADDR=192.168.10.11

   Der DHCP Serverdienst ist deaktiviert und weist nur den beiden Netzwerkkarten bzw. den beiden PCs, die über die oben aufgeführten MAC Adressen verfügen, die entsprechenden IP Adressen zu. Andere Clients werden nicht bedient. So macht zwar der DHCP Server keinen Sinn, aber auf diese Weise können zentral die Angaben für Gateway, DNS Server, WINS Server und vieles mehr administriert werden.

Notizen:

17.10 Einrichten eines Klassenraums mit iTALC

iTALC habe ich im Kapitel 14.9 schon einmal vorgestellt. Da aber die Praxis gezeigt hat, dass immer mehr Schulen und Ausbildungseinrichtungen eine leichte und sichere Administration wünschen, die die interaktive Darstellung von Unterrichtsthemen unterstützt, möchte ich auf Installation und Administration von iTALC hier noch einmal eingehen.

Der große Vorteil von iTALC ist die Unterstützung von Microsoft Windows (ab MS Windows 2000 Prof. und höher) und Linux Betriebssystemen. Auf diese Weise ist keine Schule oder Bildungseinrichtung bei der strategischen Überlegung für die Verwendung an ein bestimmtes Betriebssystem gebunden.

Kommen wir nun zur Installation von iTALC in Ihrem Klassenraum-Netzwerk. Da in den meisten öffentlichen Schulen das Microsoft Windows Betriebssystem verwendet wird, wollen wir an einem Beispiel unter Microsoft Windows Betriebssystemen die Installation praxisnah durchführen. Das für Ihr Betriebssystem zutreffende Dateipaket von iTALC ist im Internet unter http://italc.sourceforge.net/ über Download auf Ihre Festplatte herunterzuladen. Nach dem Download entpacken Sie das ZIP Archiv in ein Verzeichnis Ihrer Wahl und führen die sich in dem Archiv befindliche **SETUP.EXE**-Datei aus. Für die Installation benötigen Sie ein Administratorkonto bzw. ein Benutzerkonto, dass über Administratorrechte verfügt. In unserem ersten Schritt der Installationsroutine wird ein laufender iTALC Dienst (ICA.EXE) auf dem Lehrer PC eingerichtet. Bei der Erstinstallation werden neue DSA 1024-Bit Schlüssel erzeugt. Diese bestehen aus einem öffentlichen und privaten Schlüsselteil und dienen nur zur Authentifizierung der jeweiligen Gegenstelle. Der öffentliche Schlüssel des LehrerPCs muss bei der Installation der SchülerPCs integriert werden. Aus diesem Grunde ist es immer zu empfehlen, die LehrerPCs als erstes zu installieren und den dabei neu zu generierenden öffentlichen DSA Authentifizierungsschlüssel über das Netzwerk oder USB Stick auf die ebenfalls neu zu installierenden SchülerPCs zu integrieren. In der Installationsroutine von iTALC finden Sie dazu eine spezielle Auswahloption. Sie werden gefragt ob ein öffentlicher Schlüssel schon vorhanden ist und von welchem Datenträger und Verzeichnis er kopiert werden soll. Mit Hilfe dieser Schlüsselzuordnung von SchülerPCs zu LehrerPCs ist es auch möglich unabhängige Schulklassen in gleichen TCP / IP Subnetz zu erstellen. Damit hat der zuständige Lehrer nur Zugriff auf seine Schüler (SchülerPCs) und nicht auf

die SchülerPCs im Nachbarklassenraum. Auf diese Weise ist es aber auch möglich dass alle Schüler über nur einen Internetzugang (Proxy) ins Internet können, ohne dabei einen oder mehrere Router im Schulnetzwerk installieren und administrieren zu müssen. Dieser Lösungsansatz würde auch die Installation von nur einem besseren Drucker für mehrere Klassen ermöglichen. Der Drucker kann über ein Subnetz von allen Lehrern und Schülern im gleichen Maße angesprochen werden.
Damit noch einmal der Sachverhalt klar ist. Mit diesen Schlüsseln kann keine Verschlüsselung der Verbindung untereinander generiert werden. Er dient lediglich der Authentifizierung zweier Partner für die Verbindung über iTALC.
Grundsätzliches zum Verständnis dieses Programms. iTALC baut auf TightVNC auf. Nach Auskunft von Tobias Doerffel, dem Entwickler von iTALC, wird die zukünftige Entwicklung von iTALC sich eher an Ultr@VNC orientieren. Für die Zukunft sind auch kostenpflichtige Verschlüsselungen zwischen den Clients geplant und auch sonstige Erweiterungen werden von Drittanbietern möglich sein.
Das Programm iTALC wird beim SchülerPC als Dienst installiert. Da man Schüler grundsätzlich keine Administrationsrechte in ihren Benutzerkonten geben sollte, **J** sind die Schüler auch nicht in der Lage den iTALC Dienst zu deaktivieren. Auf diese Weise ist sichergestellt, dass ein Zugriff eines Lehrers bzw. Dozent zu jeder Zeit gewährleistet ist. Auch auf dem LehrerPC wird der iTALC Dienst ebenfalls installiert. Mit dem kleinen Unterschied, dass der Lehrer auf diesen aktiven Dienst zugreifen kann und seinen Monitor oder ein einzelnes Fenster als Demonstration im „Demo"-Modus an die Schüler übermitteln kann. Der Lehrer ist in der Lage die einzelnen Bildschirme der jeweiligen Schüler gleichzeitig zu überwachen, einzugreifen, zu sperren oder zur Beweissicherung Bildschirmfotos von einzelnen SchülerPCs zu machen. Auf diese Weise ist der Lehrer auch in der Lage einen Schülermonitor über einen am LehrerPC angeschlossenen Beamer an der Leinwand der Klasse vorzuführen. Die didaktische Unterstützung des Lehrers ist so sehr umfangreich.

Kurze Exkursion: Zurzeit ist es noch ein wenig problematisch mit der Einrichtung eines Fileservers für Schüler in den Schulklassen. Fileserver sind teuer, schwerfällig und meist für die zuständigen Lehrer sehr schwer einzurichten und zu administrieren. Ich empfehle Ihnen eine NAS[206] Station ab einer Größe von 120 – 160 GB Festplattenspeicher zu verwenden. Sie ist nur so groß wie zwei nebeneinander

[206] NAS = **N**etwork **A**ttached **S**torage

liegende CD Hüllen, einfach über ein Webinterface (Browser) eines angeschlossenen PCs über ein TCP / IP Netzwerk zu administrieren. Sie kann mit Benutzerkonten[207] für die einzelnen Schüler oder jeweiligen PC Konten sehr leicht eingerichtet werden, benötigt wenig Energie, ist sehr leise, isehr preiswert[208], meist noch als Druckserver für USB Drucker zu verwenden und kann im Notfall in einer Schreibtischschublade eingeschlossen werden.

Der Einsatz von Gruppenrichtlinien in einem Windows Servernetzwerk ermöglicht eine starre und für den Anwender sehr restriktive Einsatzmöglichkeit. Die Nachteile liegen aber auch auf der Hand. Die Windows Server sind sehr preisintensiv, setzen ein umfassendes Serverfachwissen voraus und sind im Einsatz sehr unflexibel im Einsatz bzw. auf die Projekte der unterschiedlichen Klassen nur sehr schwerfällig neu zu konfigurieren.

Die ganze Klassenraumkonfiguration von iTALC wird abgerundet durch die Verwendung von PC Wächter[209] Netzwerkkarten. Diese besonderen PCI Steckkarten ermöglichen einen Netzwerkaufbau, der beim jeweiligen Start des PCs alle Einstellungen von der Ursprungskonfiguration übernimmt. Alle Änderungen von Einstellungen, selbst Veränderungen durch Viren oder sonstigen Schadprogrammen, können nur mit einem Passwort abgespeichert werden. Wird dieses Passwort am Ende eine Arbeitssitzung nicht gesetzt, startet der Computer beim neuerlichen Start von der Ursprungskonfiguration, dann auch wieder ohne Viren und Schadprogramme. Der Vorteil dabei ist der geringe Administrationsaufwand für den Lehrer, gerade unter Microsoft Windows Betriebssystemen. Diese speziellen Karten sind auch für Linux Betriebssysteme verwendbar und haben dort die gleiche Auswirkung. Der Einsatz auf PCs mit beiden Betriebssystemen gleichzeitig st ebenfalls möglich. Man kann die Karten auch so konfigurieren, dass alle Änderungen abgespeichert werden und erst beim Setzen eines Administratorpasswortes für die PC Wächter Netzwerkkarte alle Änderungen wieder rückgängig gemacht werden. Auf

[207] Achten Sie beim Kauf der NAS darauf, dass der installierte SAMBA Fileserver auch ausreichend Accounts zur Verfügung stellt. Es gibt leider NAS Stationen die bieten nur die Möglichkeit 8 Benutzerkoneten anzulegen. Für zu Hause ist diese Lösung noch zu gebreauchen aber für eine Schulklasse ist diese wenig sinnvoll. Die ALLNET 6250 bietet eine Benutzerkontenverwaltung von bis zu 50 Konten, von denen 32 Benutzer gleichzeitig auf die NAS zugreifen können.

[208] Eine gute NAS Station bekommen sie incl. Festplatte zu einem Preis ab € 150,00. Die ALLNET 6250 ist zurzeit für ca. € 90,00 zu bekommen. Mit einer IDE Festplatte in der oben aufgeführten Größe für € 40,00 --€ 50,00 lässt sich schon ein sehr guter Fileserver aufbauen.

[209] Nähere Informationen finden Sie unter http://www.dr-kaiser.eu/pc-waechter.0.html

diese Weise kann eine Klasse über mehrere Tage oder Wochen an einem Projekt arbeiten und nach dessen Beendigung kann der zuständige Lehrer durch Passworteingabe die Ursprungskonfiguration aufrufen und den EDV Klassenraum in einer Grundkonfiguration an seinen Kollegen übergeben. Der einigste Nachteil dieser Lösung, die Karte ist mit € 77,00 je Stück relativ teuer. Die Softwarelösung, die nur für Microsoft Windows Betriebssysteme verwendbar ist, schlägt immerhin noch mit über € 35,00 je Lizenz zu Buche. Die Kosten sind aber sehr schnell wieder erwirtschaftet und die meisten EDV Klassenräume, die ich kenne und in denen diese PC Wächterkarte eingesetzt wird, setzen diese Technik schon mehr als 5 Jahre erfolgreich ein. Über diese Zeitspanne hat sich die Investition für jeden nachvollziehbar amortisiert. Hier wird die Exkursion beendet.

Aber kommen wir wieder zu iTALC zurück. Nach der Installation auf den SchülerPCs, die auf den DAS Authentifizierungsschlüssel des LehrerPCs verweisen, ist auf den SchülerPCs nur ein grünes iTALC Icon unten rechts im Infobereich des Schülerdesktops zu erkennen. Auf dem LehrerPC ist dieses Icon auch im Infobereich zu erkennen und deutet darauf hin, dass der iTALC Dienst und ICA Authentifizierungsdienst aktiv ist. Bei beiden Installationsarten befindet sich das Programm im Verzeichnis **C:\PROGRAMME\iTALC**. In diesem Verzeichnis befindet sich auch die Datei **iTALC.exe**. Wenn Sie wollen, können Sie auch eine Verknüpfung mit dieser Datei auf den Desktop des LehrerPCs erstellen. Auf diese Weise kann iTALC vom jeweiligen Lehrer leichter gestartet werden. Sie werden auf dem LehrerePC den Programmaufruf auch in der Startmenüleiste finden. Beim ersten Start von iTALC auf dem LehrerPC wird eine fehlende Konfigurationsdatei angemahnt. Bestätigen Sie die Vorgabe mit `OK` und die Konfigurationsdatei wird unter **C:\DOKUMENTE UND EINSTELLUNGEN\ <Benutzerkonto>\ ANWENDUNGSDATEN\iTALC** abgespeichert. Beim zweiten Start des iTALC Programms ist dies schon nicht mehr der Fall, da die Konfigurationsdaten beim ersten Start erstellt und abgespeichert wurden.

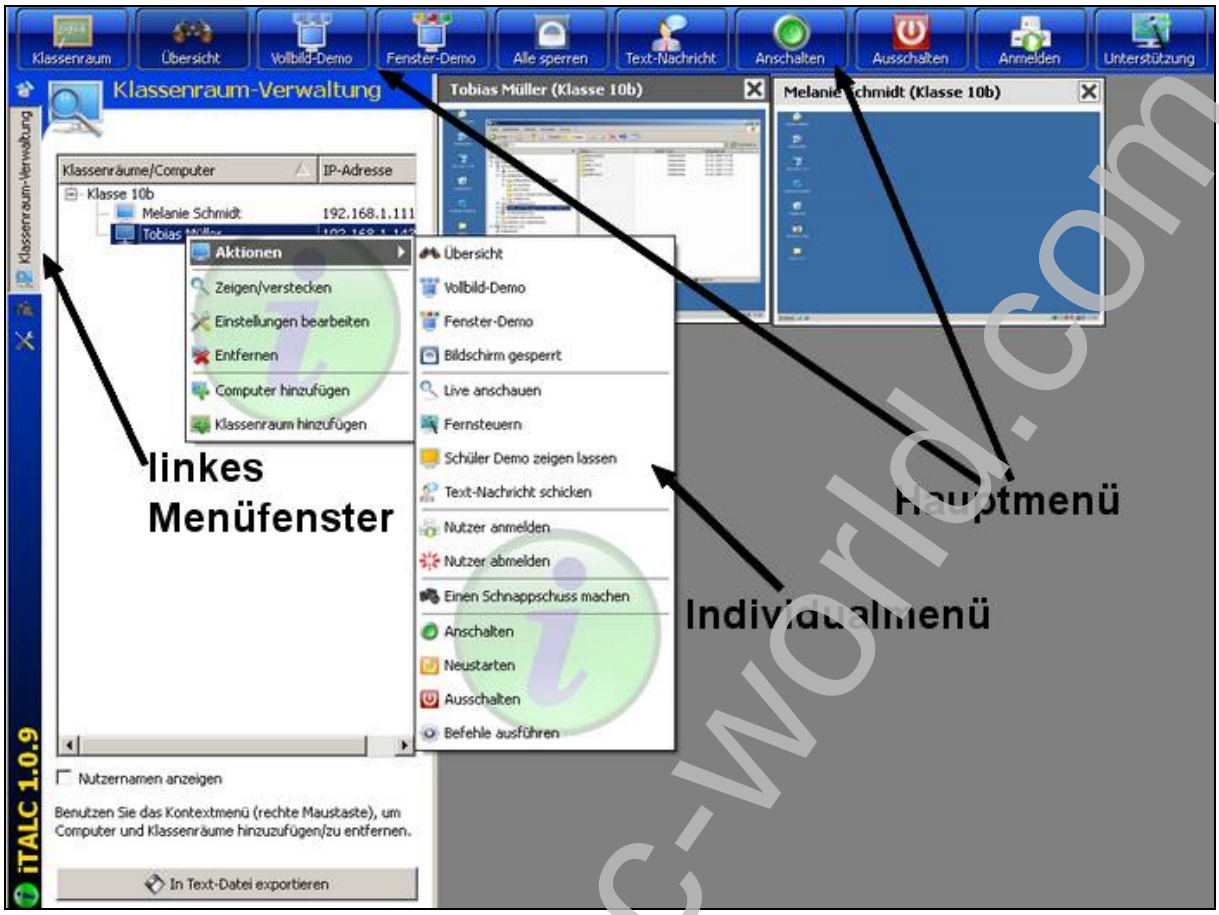


Abbildung 191, iTALC - LehrerPC - Ansicht

Über das Hauptmenü kann man Befehle eingeben, die sich auf die gesamte Klasse auswirken. Alles was dort eingestellt wird, wirkt sich auf alle PCs aus. Für jede Klasse muss eine Klasse im linken Hauptmenü definiert werden. Danach müssen die SchülerPC hinzugefügt werden. Mit Hilfe der rechten Maustaste können alle wie in Abbildung 191 gezeigten Befehle für den einzelnen PC ausgeführt werden.

Die eine oder andere Übungseinheit für den Lehrer ist hier von Vorteil. **J** In der Praxis hat sich gezeigt, dass die Schüler mit der Technik meist besser zu recht kommen als die Lehrer. Deshalb meine wiederholte Bitte an die entsprechenden Lehrer vor dem effektiven Einsatz ein wenig die Handhabung z. B. in einem Workshop mit Kollegen zu üben.

Im linken Menüfenster stehen zusätzliche Befehle zur Verfügung, die sich auf die Konfiguration wie Datenübermittlung, die Schnappschussverwaltung, die Klassenverwaltung und der Willkommensbildschirm beziehen. Mit einem Doppelklick können Sie sich den Bildschirm des einzelnen Schülers betrachten. Das Hauptmenü am oberen Rand des Monitors blendet sich nach einigen Sekunden wieder aus und wird erst wieder aktiv, wenn Sie mit der Maus in den Kopfbereich des Hauptmenüs

verweilen. Für die Netzwerkadministration müssen auf den einzelnen lokalen PCs die Ports 5800 und 5900 freigegeben sein. Zusätzlich wird z. B. für die Verbindungsaufnahme im Netzwerk iTALC spezifische Port 5858 verwendet und der iTALC Dienst greift zusätzlich auf die TCP / IP Ports 1165 und 1174 zu, um eine Remoteverbindung zu unterstützen.

Für mich ist iTALC nicht nur für Schulen und Bildungseinrichtungen interessant, sondern auch für Administratoren eines LAN, die auf diese Weise sich ständig ändernde Rechnerkonfigurationen einfach überwachen und administrieren können und dies auch in einem Firmennetzwerk. Der einzige Schwachpunkt ist die fehlende Verschlüsslung zwischen den Verbindungen. Gerade für Verbindungen die in ihrer Tragweite nicht überschaubar sind ist das ein wesentlicher Nachteil. Sollten Sie doch eine Verbindung über eine unbekannte Netzwerkverbindung z. B. das Internet aufbauen wollen, können Sie gerne auf Hamachi zurückgreifen. Dieses Programm habe ich im Workshop in Kapitel 17.8 bereits vorgestellt. Auch die Anbindung über eine SSH via freeSSHd ist vorstellbar. Abschließend sei die Kostenersparnis durch iTALC von mehr als € 1.200,00 je Klassenraum mit max. 15 PC SchülerPC Plätzen an dieser Stelle nur einmal am Rande erwähnt.

Notizen:

21 TCP / IPv4 Grundlagen

21.1 Das Protokoll allgemein

Im Gegensatz zum UDP ist das TCP Protokoll ist in der Lage einen zusammenhängenden Datenstrom in kleine Datenpakete zu teilen. Dies verlangt von allen beteiligten Komponenten, wie z.B. CPU des Hostsystems, NIC Chips[224] und PCinternen BUS Systemen[225] sehr viele Leistungsressourcen ab. Bei der Leistungsfähigkeit der heutigen Computer spielt dies keine so große Rolle mehr, vor einigen Jahren, als die PC Systeme bei weitem noch nicht so leistungsfähig waren wie heute, wäre das jedoch noch ein Thema gewesen. TCP- und UDP-Protokolle arbeiten in der 4. Schicht des OSI Referenzmodells. Beide Protokolle sind die eigentlichen Träger der zu übermittelnden Informationen. Sie stellen eine Art Lore[226] dar, in denen die Daten transportiert werden. Beide Protokolle nutzen das IP-Protokoll lediglich für die Adressierung der Daten, um zu bestimmen woher und wohin die Daten transportiert werden sollen. Das IP-Protokoll arbeitet auf der 3. Schicht des OSI Referenzmodells. Jetzt stellt sich die Frage, welchen Vorteil wir dadurch haben, dass die Daten gestückelt werden. Relativ einfach. Bei der Übermittlung der Daten kann es immer wieder zu Fehlern oder Störungen kommen. Dies lässt sich grundsätzlich nicht vermeiden. Wenn jedoch die zu übermittelnden Informationen in Datenpakete gestückelt werden, müssen nur die Datenpakete die defekt oder nicht angekommen sind neu eingelesen werden und neu übermittelt werden. Das UDP übermittel die gesamten Daten und fragt erst am Ende der Übermittlung nach ob diese komplett angekommen sind. Eine Überprüfung ob die Daten in sich auch korrekt übertragen wurden findet nicht statt.. Ist bei der Übertragung ein Fehler aufgetreten müssen die gesamten Daten noch einmal neu eingelesen und übermittelt werden. Beim TCP-Protokoll werden die Daten in Datenpakete aufgeteilt und übertragen. Kommt es bei der einen oder anderen

[224] Diese Verarbeitungsprozessoren finden wir direkt auf den Netzwerkkarten. Zu den Klassikern gehören zum Beispiel die RealTEK Chipsätze RTL 8139D oder die Chipsätze von 3CM 3COM905. Dies ist nicht immer so von Bedeutung, soll aus diesem Grunde auch hier nicht weiter ausgeführt werden.

[225] Zu diesen zählen ISA, EISA, VLB, PCI, AGP und PCI Express.

[226] Eine Lore ist ein oben offener Güterwagon der Eisenbahn bzw. ein Beförderungsmittel im unterirdischen Kohlebergbau.

Übertragung eines Datenpaketes zu einer Störung, muss auch nur dieses eine Datenpaket neu eingelesen und wieder übermittelt werden. Das TCP/IP hat einen eigenen Fehlerkorrekturdienst, der unter anderem durch Prüfsummenverfahren feststellen kann, ob die Datenpakete in der richtigen Reihenfolge vorliegen, als auch vom Inhalt vollständig sind.

21.2 Spezifikationen und RFCs

Das TCP Protokoll ist nach der RFC 793 spezifiziert. Die RFC 791 wird für das IP Protokoll herangezogen.[227] Für den weiterführenden Bereich des Umgangs mit den TCP/IP Protokollen können Sie sich gerne folgende RFC`s noch anschauen:
RFC 1122 - Fehlerbehebungen und Fehlerkorrekturverfahren bei TCP
RFC 1323 - Erweiterungen bei TCP Protokollen
RFC 2581 – TCP - Ueberlastungs- und Korrekturkontrolle

21.3 Aufbau der IPv4 Adressierung

Eine IPv4 Adresse besteht aus vier Oktetten. Jedes einzelne Oktett wird durch ein Byte, das wiederum aus 8 Bit besteht, gebildet. Somit stehen uns 32 Bit für die Adressierung zur Verfügung. Jedes einzelne Oktett kann einen Dezimalwert von 0-255 haben. Damit haben wir 256 verschiedene Vergabewerte für ein einzelnes Oktett. Der Wert eines Oktetts wird aus dem dualen Werten des jeweiligen Bytes gebildet. Das hört sich kompliziert an ist aber in der Praxis halb so wild. Um nun eine gewisse Struktur aufbauen zu können, wird jedem Computer, bzw. jeder Netzwerkkarte eine IPv4 Adresse zugewiesen. Nehmen wir einfach einmal eine solche Adresse 210.45.212.34. Sie sehen wir haben 4 Oktette = 4 Dezimalwerte, die zwischen 0 und 255 liegen. Diese IPv4 Adresse könnte ich auch im Rahmen der dualen Zahlensysteme binär schreiben, dies würde dann so aussehen.
11010010.00101101.11010100.00100010 Mit dieser Zahl arbeitet der Computer. Diese Zahl ist für den Menschen nur sehr schwer werthaltig zu erfassen, aus diesem Grunde arbeiten wir bei der IPv4 Adressierung nur mit den Dezimalwerten. Die IP Adresse 210.45.212.34 wird z.B. bei der Einwahl ihres Computers ins Internet von

[227] Zu dem Thema finden Sie auch unter http://edocs.tu-berlin.de/diss/2004/savoric_michael.htm eine sehr gute und sehenswerte Dissertation.

ihrem Internet Service Provider[228] zugewiesen. Damit ist Ihr PC während der gerade vorhandenen Onlineverbindung unter dieser IP Adresse weltweit für alle, die sich im Internet befinden, erreichbar. Diese Adresse ist eineindeutig und wird es ein zweites Mal nicht geben. Wenn Sie die Verbindung zu Ihrem ISP beenden, wird die IPv4 Adresse freigegeben und kann dann einem anderen Kunden Ihres ISP`s bei dessen Einwahl ins Internet neu zugewiesen werden. Da das IP Protokoll routingfähig[229] ist, müssen wir einen bestimmten hierachichen Aufbau beachten. Jeder öffentlichen IP Adresse ist einem bestimmten regionaler Bereich auf der Erde zugewiesen, diesen Aufbau darzustellen würde den Rahmen des Buches bei weitem überschreiten. Aus diesem Grunde widmen wir uns lieber der hierachichen IPv4 Adressierung in unserem eigenen oder firmeninternen Netzwerk. Um die einzelnen Computer logisch zu öffentlichen Netzen abzugrenzen, verwendet man IPv4 Adressbereiche, die man im öffentlichen Netzen im Internet nicht finden würde. Diese Adressbereiche werden für die lokale Adressierung reserviert.

Klasse	IP Range	mögliche Netze	mögliche Hosts
A	**10**.0.0.0 – **10**.255.255.255	1	16.777.216
B	**172.16**.0.0 – **172.31**.255.255	16	65.536
C	**192.168.0.**0 – **192.168.255.**255	256 (s. 3. Oktett)	256(s. 4. Oktett)

Die jeweils fett hervorgehobenen IPv4 Adresse klassifizieren die jeweiligen Netzbezeichnungen und die nicht hervorgehobenen IP Adresswerte klassifizieren die möglichen Adressierungen für die einzelnen Netzwerkhosts. Jedem Netzwerkhost kann man einen Computer gegenüberstellen. Also ein Klasse A-Netz hat als Netzwerkkennung nur die „10“, für die möglichen Computer in diesem Netzwerk stehen dann 256 x 256 x 256 = 16.777.216[230] möglichen IPv4 Adresswerte zur Verfügung. Damit wären 16,7 Mio. Computer in diesem Netzwerk möglich.
In einem Klasse B Netzwerk stehen uns in dem ersten möglichen Netzwerk von 172.16.0.0 – 172.16.255.255 insgesamt 256 x 256 = 65.536 Netzwerkhost zur

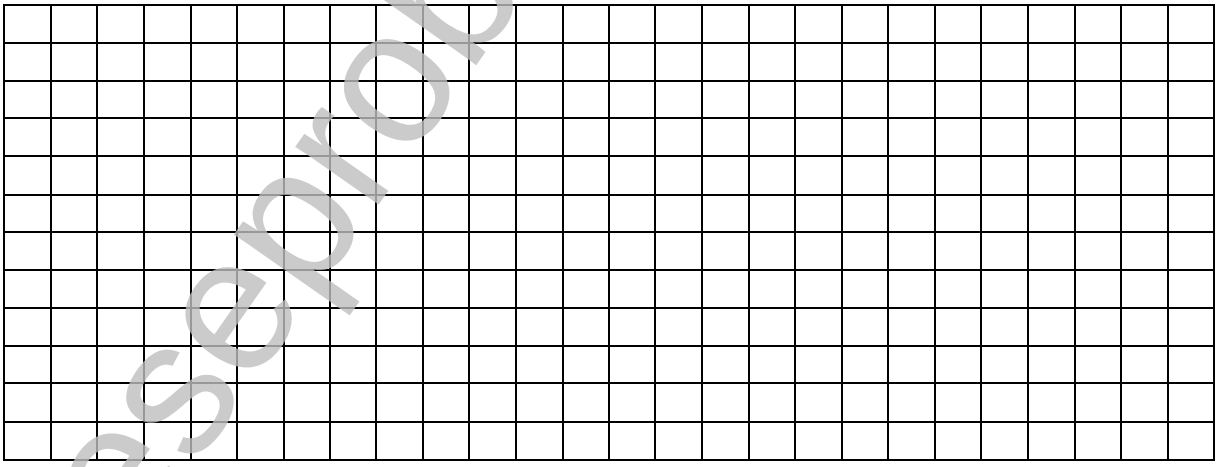
[228] Unter Internet Service Provider (ISP) versteht man Unternehmen die entgeltlich den technischen Zutritt zum Internet ermöglichen.

[229] Unter der Routingfähigkeit versteht man die Möglichkeit einen Zielrechner mit Hilfe anderer im Netz befindlichen Verbindungsknoten, die ebenfalls durch IP Adressen gekennzeichnet sind, zu erreichen.

[230] Warum verwenden wir die 256 und nicht die 255. Weil es hier um die Anzahl der möglichen Werte geht und in einem Oktett sind 256 Werte, incl. dem Wert „0“, möglich.

Verfügung. Gleichzeitig stehen uns aber von 172.16.x.x bis 172.31.x.x 16 von einander unabhängige Netzwerksegmente mit jeweils 65.536 möglichen Netzwerkhosts zur Verfügung. Dies entspricht immerhin einer Gesamtanzahl von 1.048.576 möglichen Netzwerkhosts. Bei einem Klasse C-Netz haben wir durch die Deklaration von 192.168.0.0 bis 192.168.0.255 die Möglichkeit 256 Computern eine Netzwerkadresse zu vergeben. Aber auch in diesem Klasse C Netz haben wir die Möglichkeit 256 unabhängige Segmente zu bilden. Dies würde bei 256 Netzen x 256 Host ein Netzwerk von 65.536 möglichen Computern (Hosts) ergeben.
Ist für eine Netzwerkkarte keine IPv4 Adresse festgelegt und ist die Netzwerkkarte in der Lage eine IP Adresse nach den Spezifikationen für BooTP oder DHCP von einem DHCP Server selbst anzufordern, muss eine manuelle IP Adressvergabe nicht durchgeführt werden, dies erleichtert nicht nur die Administration in einem Netzwerk, sondern sorgt auch für eine gewisse Flexibilität im Ausbau und Betrieb des LAN. Was ist aber wenn der DHCP Server ausfällt. Dann würden die Hosts keine IPv4Adresse beziehen können und wären nicht in der Lage eine Netzwerkverbindung aufzubauen. Aus diesem Grunde kommen dann die APIPA Spezifikationen[231] zum Tragen und der einzelne Host würde sich automatisch eine einzelne IP Adresse aus dem Bereich von 169.254.1.0 bis 169.254.254.255 in Rahmen eines Klasse B Netzwerkes zuordnen. Aus diesem Grund ist auch der IPv4 Bereich 169.254.x.x für die IP Adressvergabe in der Praxis nicht geeignet und auch nicht zu verwenden.

Notizen:



[231] APIPA = **A**utomatic **P**rivate **IP A**dressing. Hier werden gem. Spezifikationen RFC 3330 per Zufallsgenerator die benötigten Adresswerte erstellt und den einzelnen NIC (Network Interface Controller) zugeordnet.

Die Netzwerke werden von Ihrer Zugehörigkeit nicht alleine durch die IPv4 Adresse definiert, sondern vor allem durch den Aufbau der Subnetmaske. Die Subnetmaske bzw. Subnetadresse ist ebenfalls binär aufgebaut und gibt durch die XOR Verknüpfung zur IPv4 Adresse eine Prüfsumme wieder, um festzustellen, ob zwei Computer dem gleichen logischen Netzwerksegment zugehörig sind. Ist dies der Fall können Sie eine Verbindung miteinander aufnehmen. Ist dies nicht der Fall können beide Computer keine Verbindung miteinander aufnehmen, auch wenn sie physisch mit Switch[232] und Twisted Pair Verkabelung miteinander verbunden wären.

Kurze Exkursion:

Unter der **T**wisted **P**air Verkabelung versteht man die 8adrige bzw. 4paarige Verkabelung in Stern- und Mischnetztopologien. Dabei ist es für die Qualität der Verbindung sehr wichtig, ob die Verkabelung geschützt (**S**hielded **T**wisted **P**air) oder ungeschützt ist. (**U**nshielded **T**wisted **P**air). Bei UTP Verkabelungen kann es in Kabelkanälen, mit stromführenden Kabeln aus dem Stromversorgungsnetz eines Hauses, zu störenden elektromagnetischen Feldern kommen, die zu nicht immer direkt nachvollziehbaren Störungen im Netzwerkbetrieb führen können. Für die Spezifikationen für die Datenübertragungskapazitäten gilt folgendes:

Kategorie – CAT	max. Datendurchsatz	MB/Sekunde	MB/Sekunde/praktisch
3, veraltet	30 Mbit	3,75	ca. 1,60
5	100 Mbit	12,50	ca. 8,50
5e	(duplex) 2 x 100 Mbit	25,00	ca. 13,00
6	250 Mbit	31,25	ca. 16,00
7 (Gigabit Ether.)	650 Mbit	81,25	ca. 50,00

[232] Eine Switch ist ein Verteiler, der nicht nur die Signale verstärkt, sondern die Daten von Host zu Host auf der Basis der MAC Adressen (Adressen der Netzwerkkarten) auf der 2. Schicht des OSI Referenzmodells vermittelt und zuordnet. Aus diesem Grunde übernehmen die meisten guten Switch`s auch die Aufgaben einer Bridge. Die Daten werden dabei nicht im Rahmen einer Broadcastmeldung an alle angeschlossenen Host verteilt, wie bei einem HUB, sondern ausschließlich an den definierten bestimmten Empfänger übertragen. Aus diesem Grunde ist mit guten und hochwertigen Verteilern auch der Aufbau von „managed Switches“ und VLANs möglich. Diese sorgen durch ihre Arbeitsweise für geringe Datenkollisionen und optimierte Direktverbindungen.

Kommen wir aber wieder zu unseren Subnetmasken zurück. Um einen kleinen Überblick zu bekommen, hab ich nachfolgend eine klassische Zuordnung der einzelnen Subnetmasken einmal aufgeführt:

Klasse	IP Range	Subnetmaske	mögliche Hosts
A	**10**.0.0.0 – **10**.255.255.255	**255**.0.0.0	16.777.216
B	**172.16**.0.0 – **172.31**.255.255	**255.255**.0.0	65536
C	**192.168.0**.0 – **192.168.0**.255	**255.255.255.**0	256

In dieser Gegenüberstellung kann man sehr gut erkennen wie die Subnetmaskendeklaration die Netzzugehörigkeit und Hostzugehörigkeit definiert ist. Beachten Sie dabei den Fettdruck.

Bei der IP Adressevergabe ist grundlegend zu berücksichtigen, dass aus einem Netzwerksegment immer die erste und die letzte IP Adresse nicht verwendet werden sollten, deshalb muss man bei allen Berechnungen im 2 Hosts abziehen. Die erste Iv4P Adresse ist die Netzwerk ID und die letzte IPv4 Adresse ist die Broadcastadresse unter der alle vorhanden Host in dem entsprechenden Netzwerksegment angesprochen werden können. Über die Broadcastadresse wird in einem Netzwerksegment festgestellt welche Clients aktiv und vorhanden sind. Die Zuordnung IPv4 Adresse zu MAC Adresse einer Netzwerkkarte wird für 120 - 240 Sekunden im ARP Cache gespeichert. Die Einträge im ARP Cache können mit dem Befehl „arp –a“ abgefragt werden. Auf diese Weise nehmen die einzelnen PCs Verbindung zueinander auf und stellen die Verbindung sicher. Wenn die im ARP Cache befindliche MAC Adresse nicht mehr vorhanden ist muss sie mit Hilfe einer Broadcastmeldung wieder neu erfragt werden. Sie auch Abbildung 192.

Notizen:

21.4 Die Konfiguration der Subnetmask

Wie wir gehört haben ist die IPv4 Adresse nicht alleine maßgebend für die vollständige Adressierung von Netzwerkverbindungen. Zusätzlich zu einer IPv4 Adresse wird immer auch eine Subnetmaske mit angegeben. Aufgrund dieser Subnetmaske wird definiert in welchem Netzwerksegment man sich die befindet. Da nur die Adressen, die sich im gleichen Netzwerksegment befinden, auch eine Verbindung miteinander aufnehmen können ist es immer sehr wichtig auch die gleiche Subnetmaske zu der entsprechenden IPv4 Adressen mit einzugeben. Schauen wir uns dies an einem Beispiel an. Sie haben 4 Computer in einem Netwerk. Alle 4 Computer befinden sich im Netzwerksegment „23“ und haben die gleiche Subnetmaske.

Computer 1	Computer 2	Computer 3	Computer 4
192.168.**23**.45	192.168.**23**.62	192.168.**23**.131	192.168.**23**.237
255.255.255.0	**255.255.255.**0	**255.255.255.**0	**255.255.255.**0

Alle 4 Computer können sich sehen und miteinander arbeiten. Mit Hilfe eines Ping Befehls (Start – Ausführen –„command“ eingeben – ENTER – „ping <IP Zieladresse>) kann man dies sehr leicht nachprüfen[233]. Daraus ergeben sich für dieses Netzwerksegment folgende Kenndaten.

Beschreibung	Werte	
IP Adressrange	**192.168.23**.0	bis **192.168.23**.255
Netzwerk ID	192.168.23**.0**	
Broadcastadresse	192.168.23**.255**	
Subnetmaske	255.255.255.0	Klasse C-Netz
mögliche Hostanzahl	256 – 2 = **254**	**254** mögl. Hosts
Verwendbare IP Adressen	192.168.**23**.1	bis 192.168.**23**.254

Alle Computer die eine Adresse zwischen 192.168.23.1 und 192.168.23.254 mit einer Subnetmask von 255.255.255.0 eine Verbindung miteinander aufnehmen

[233] Mit „arp –a“ kann man sich die zugehörigen MAC Adressen der jeweiligen PCs anzeigen lassen.

Neben den schon vier verwendeten Adressen können 250 weitere vergeben werden. Gehen wir jetzt aber einmal von einem anderen Beispiel aus. Wir haben wieder 4 Computer von denen sich zwei im ersten Segment eines Netzwerkes befinden sollen und die beiden anderen in einem 2. Netzwerksegment sein sollen.

Computer 1	Computer 2	Computer 3	Computer 4
192.168.23.45	192.168.23.62	192.168.23.131	192.168.23.237
255.255.255.128	255.255.255.128	255.255.255.128	255.255.255.128

Wir müssen uns vorstellen, dass für den Dezimalwert 255 in der Subnetmaske jeweils 8-mal der Binärwert „1“ vergeben wird. Die ersten 3 Oktette sind mit dem Wert 255 vergeben, also haben wir binär 24-mal den Wert „1“ in unserer Subnetmaske. Aus diesem Grunde gibt man hier sehr oft die CIDR-Notation an. Diese würde dann so aussehen 192.168.23.63/24 für eine 255.255.255.0 Subnetmask und 192.168.23.63/25 für eine 255.255.255.128 Subnetmask. Wie Sie erkennen können haben wir in unserem Beispiel nun an der ersten Stelle im 4 Oktett der Subnetmaske eine führende „1“ gesetzt und damit die Netzwerkdeklaration anstatt auf 24-mal Wert „1“ auf 25-mal Wert „1“ gesetzt. Für das 4. Oktett ergibt sich „10000000“ binär und „128“ dezimal. Aus diesem Grunde 255.255.255.128 für die Subnetmask. Die Computer haben ihre IPv4 Adressen beibehalten, nur deren Subnetmaske hat sich geändert. Aus dieser einfachen Änderung ergib sich aber folgende Netzwerksegmentkonfiguration und Zuordnung:

Beschreibung	Werte	Netzwerksegment 1
IP Adressrange	**192.168.23**.0	bis **192.168.23**.127
Netzwerk ID	192.168.23.**0**	
Broadcastadresse	192.168.23.**127**	
Subnetmaske	255.255.255.128	Klasse C Netz
mögliche Hostanzahl	128 – 2 = **126**	126 mögl. Host
Verwendbare IP Adressen	192.168.**23**.1	bis 192.168.**23**.126

Beschreibung	Werte	Netzwerksegment 2
IP Adressrange	**192.168.23.**128	bis **192.168.23**.255
Netzwerk ID	192.168.23.**128**	
Broadcastadresse	192.168.23.**255**	
Subnetmaske	255.255.255.128	Klasse C Netz
mögliche Hostanzahl	128 – 2 = **126**	126 mögl. Host
Verwendbare IP Adressen	192.168.**23**.128	bis 192.168.**23**.254

Durch diese einfache Neuordnung der Subnetmaske befinden sich Computer 1 und Computer 2 im Netzwerksegment 1 und Computer 3 und Computer 4 im Netzwerksegment 2. Beide Segmente können keine Verbindung zueinander aufbauen und die jeweiligen Freigaben, Drucker oder andere Netzwerkressourcen nutzen. Bei Microsoft Windows Betriebssystemen kann, wie auch in anderen Betriebssystemen üblich, die Netzwerkkonfiguration nur durch Benutzer mit Administratorrechten geändert werden, aus diesem Grunde ist es für den normalen Benutzer sehr schwer die Netzwerkkonfiguration selbst zu ändern.

Aber halten wir jetzt einmal vor Augen welche Vorteile diese Konfiguration hat. Auf diese weise können sichere Segmente gebildet werden. Viren, Trojaner, Hackerangriffe und unberechtigte Zugriffe durch Dritte können stark reduziert werden. Durch die verringerte Subnetmaske wird der allgemeine Broadcast Netzwerkverkehr drastisch reduziert. Evtl. vorhandene Switch müssen weniger ungeordneten Netzwerkverkehr herausfiltern und die allgemeine Netzwerklast und das Kollisionsverhalten kann spürbar reduziert werden.

Beide Netzwerksegmente sind nur mit Hilfe eines PCs mit 2 Netzwerkkarten wieder zusammenzuführen. Dieser PC muss dann die Aufgaben eines Router übernehmen und über die entsprechende Protokolltechnik verfügen. Jede Netzwerkkarte muss dabei für eins der beiden Netzwerksegmente entsprechend konfiguriert sein.

Notizen: