

Protokoll

Versuch: Windows ans Netz

Datum: 15.11.2007

Gruppe: 1

Studiengang: Informationstechnik / Technische Informatik

Praktikanten: Linda Fröck
Karsten Wiedmann
Maik Gotzmann

Ort: Universität Rostock, Institut für Informatik, Raum D004

Benutze Geräte:

- Computer-Arbeitsplatz Nr. 1
- Cross-Patch-Kabel
- BS: MS Windows XP

Ziele:

Durch die Durchführung des Versuches sollen die Praktikanten folgende Fähigkeiten erwerben:

1. Integration eines MS Windows XP-Rechners in ein bestehendes TCP/IP-Netzwerk mittels Kommandokonsole
2. Integration eines MS Windows XP-Rechners in ein bestehendes TCP/IP-Netzwerk unter Zuhilfenahme der grafischen Benutzeroberfläche
3. Windows-Dienste zu aktivieren/deaktivieren

Aufgabe 1: Netzmaskenberechnung

1:

Netzmaske für Klasse B Netzwerke 255.255.0.0
Netzmaske für Klasse C Netzwerke 255.255.255.0

2:

Zerlegung des privaten C-Klasse Netzwerke

192.168.0.0/255.255.255.0	192.168.63.0
192.168.64.0/255.255.255.0	192.168.127.0
192.168.128.0/255.255.255.0	192.168.191.0
192.168.192.0/255.255.255.0	192.168.255.0

3:

192.168.0.0	255.255.255.0	192.168.0.255	192.168.0.1
10.128.0.0	255.128.0.0	10.127.255.255	10.128.0.1
139.30.3.0	255.255.255.192	139.30.3.63	139.30.3.1
192.168.255.16	255.255.255.31	192.168.255.31	192.168.255.1

4:

1 korrekt
2 nicht korrekt es müsste 10.127.65.31 sein
3 nicht korrekt es kann keine 257 in einer IP-Adresse stehen. Es darf nur ein Wert von maximal 255 angenommen werden
4 korrekt
5 korrekt

5:

Broadcast	Hostadresse
1 127.255.255.255	127.0.0.1
2 10.63.255.255	10.0.0.1
3 10.64.255.255	10.64.0.1
4 10.65.191.255	10.65.0.1
5 10.65.128.63	10.65.128.1
6 10.65.128.191	10.65.128.129
7 10.191.255.255	10.128.0.1
8 192.168.0.2	192.168.0.2

Aufgabe 2: Konfiguration über Komandozeile

Zunächst haben wir uns die aktuelle Netzwerkkonfiguration anzeigen lassen. Dazu haben wir den Befehl *ipconfig /all* eingegeben:

```
E:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : eins
    Primary Dns Suffix . . . . . : netprak.iuk.test
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : netprak.iuk.test
                                      informatik.uni-rostock.de
                                      uni-rostock.de

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : netprak.iuk.test
    Description . . . . . : Intel(R) PRO/1000 CT Network Connect
ion
    Physical Address. . . . . : 00-30-05-4F-EE-75
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IP Address. . . . . : 192.168.0.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
    DHCP Server . . . . . : 192.168.0.1
    DNS Servers . . . . . : 192.168.0.1
    Lease Obtained. . . . . : Donnerstag, 15. November 2007 09:55:
17
    Lease Expires . . . . . : Donnerstag, 15. November 2007 15:55:
17
```

Als Netzwerkgerät wird uns hier der Ethernet-Adapter angezeigt.

Als nächstes haben wir uns alle gestarteten Dienste mit dem Befehl *net start* anzeigen lassen.

```
E:\>net start
These Windows services are started:

    Application Layer Gateway Service
    Automatic Updates
    COM+ Event System
    Cryptographic Services
    DCOM Server Process Launcher
    DHCP Client
    Distributed Link Tracking Client
    DNS Client
    Error Reporting Service
    Event Log
    Fast User Switching Compatibility
    Help and Support
    IPSEC Services
    Logical Disk Manager
    MGABGEXE
    Network Connections
    Network Location Awareness (NLA)
    Plug and Play
    Print Spooler
    Protected Storage
    Remote Procedure Call (RPC)
    Remote Registry
    Secondary Logon
    Security Accounts Manager
    Security Center
    Server
    Shell Hardware Detection
    Simple TCP/IP Services
    SSDP Discovery Service
    System Event Notification
    System Restore Service
    Task Scheduler
    TCP/IP NetBIOS Helper
    Terminal Services
    Themes
    WebClient
    Windows Audio
    Windows Firewall/Internet Connection Sharing (ICS)
    Windows Image Acquisition (WIA)
    Windows Management Instrumentation
    Windows Time
    Wireless Zero Configuration
    Workstation

The command completed successfully.
```

Weiterhin sollen wir uns die Routingtabelle anzeigen lassen. Hierzu haben wir den Befehl *route print* in die Kommandozeile eingegeben. Auf der folgenden Abbildung ist die vollständige Routingtabelle zu sehen:

```
E:\>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x10003 ...00 30 05 4f ee 75 ..... Intel(R) PRO/1000 GT Network Connection
=====
Active Routes:
Network Destination        Netmask          Gateway       Interface    Metric
0.0.0.0                    0.0.0.0          192.168.0.1   192.168.0.11  20
127.0.0.0                  255.0.0.0        127.0.0.1     127.0.0.1     1
192.168.0.0                255.255.255.0    192.168.0.11  192.168.0.11  20
192.168.0.11              255.255.255.255  127.0.0.1     127.0.0.1     20
192.168.0.255             255.255.255.255  192.168.0.11  192.168.0.11  20
224.0.0.0                  240.0.0.0        192.168.0.11  192.168.0.11  20
255.255.255.255           255.255.255.255  192.168.0.11  192.168.0.11  1
Default Gateway:          192.168.0.1
=====
Persistent Routes:
None
```

Als nächstes haben wir die Netzwerk-Konfigurations-Konsole geöffnet und das Programm *netsh* geöffnet.

```
E:\>netsh
netsh>?

The following commands are available:

Commands in this context:
..          - Goes up one context level.
?           - Displays a list of commands.
abort      - Discards changes made while in offline mode.
add         - Adds a configuration entry to a list of entries.
alias      - Adds an alias.
bridge     - Changes to the 'netsh bridge' context.
bye        - Exits the program.
commit     - Commits changes made while in offline mode.
delete     - Deletes a configuration entry from a list of entries.
diag       - Changes to the 'netsh diag' context.
dump       - Displays a configuration script.
exec       - Runs a script file.
exit       - Exits the program.
firewall   - Changes to the 'netsh firewall' context.
help       - Displays a list of commands.
interface  - Changes to the 'netsh interface' context.
offline    - Sets the current mode to offline.
online     - Sets the current mode to online.
popd       - Pops a context from the stack.
pushd      - Pushes current context on stack.
quit       - Exits the program.
ras        - Changes to the 'netsh ras' context.
routing    - Changes to the 'netsh routing' context.
set        - Updates configuration settings.
show       - Displays information.
unalias    - Deletes an alias.
winsock    - Changes to the 'netsh winsock' context.

The following sub-contexts are available:
bridge diag firewall interface ras routing winsock

To view help for a command, type the command, followed by a space, and then
type ?.
```

Dann haben wir uns mit dem Befehl *show mode* in netsh den Status von netsh anzeigen lassen. Da der Status schon „online“ war, mussten wir ihn nicht noch auf online setzen.

```
netsh>show mode
online
```

Als nächstes haben wir in den Interface-Kontext mit dem Befehl *interface* gewechselt und haben uns mit dem Befehl *show interface* alle verfügbaren Netzwerkgeräte anzeigen lassen:

```
netsh>interface
netsh interface>show interface
```

Admin State	State	Type	Interface Name
Enabled		Dedicated	Local Area Connection
Enabled		Internal	Internal
Enabled		Loopback	Loopback

Dann haben wir in den Unterkontext ip gewechselt und mit dem Befehl *reset all* alle Einstellungen gelöscht. Weiterhin haben wir dann eine neue IP-Adresse mit *set address "Local Area Connection" static 192.168.0.21 255.255.255.0 192.168.0.1 1* gesetzt.

```
netsh interface ip>set address "Local Area Connection" static 192.168.0.21 255.255.255.0 192.168.0.1 1
Ok.
```

Nun haben wir den ersten DNS-Server mit *set dns "Local Area Connection" static 192.168.0.1* gesetzt, äquivalent verfahren wir mit dem WINS-Server.

```
netsh interface ip>set dns "Local Area Connection" static 192.168.0.1
Ok.
netsh interface ip>set wins "Local Area Connection" static 192.168.0.1
Ok.
```

Bei der Kontrolle der Netzwerkkonfigurationen erhielten wir die folgenden Angaben:

```
E:\>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : eins
Primary Dns Suffix . . . . . : netprak.iuk.test
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : netprak.iuk.test
                                   netprak.iuk.test
                                   iuk.test
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . : netprak.iuk.test
Description . . . . . : Intel(R) PRO/1000 CT Network Connect
ion
Physical Address. . . . . : 00-30-05-4F-EE-75
Dhcp Enabled. . . . . : No
IP Address. . . . . : 192.168.0.21
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
DNS Servers . . . . . : 192.168.0.1
Primary WINS Server . . . . . : 192.168.0.1
```

Wie man sieht haben die verschiedenen Parameter die manuell zugewiesenen Werte angenommen.

Anschließend haben wir uns mit den Befehlen *ping* und *tracert* vergewissert, dass die vorgenommenen Einstellungen auch korrekt sind.

```
E:\>ping 192.168.0.20

Pinging 192.168.0.20 with 32 bytes of data:

Reply from 192.168.0.20: bytes=32 time<1ms TTL=64
Reply from 192.168.0.20: bytes=32 time<1ms TTL=64
Reply from 192.168.0.20: bytes=32 time<1ms TTL=64
Reply from 192.168.0.20: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

E:\>tracert 192.168.0.20

Tracing route to 192.168.0.20 over a maximum of 30 hops
  0    1    <1 ms    <1 ms    <1 ms    192.168.0.20
Trace complete.
```

Wie man sieht, funktioniert sowohl der Befehl *ping* als auch *tracert*, denn wir erhalten ein Signal zurück.

Nun haben wir die Namensauflösung mit *nslookup* für drei Rechnernamen getestet:

```
> nslookup www.informatik.uni-rostock.de
Server: vesuv.informatik.uni-rostock.de
Address: 139.30.1.209
Aliases: www.informatik.uni-rostock.de

DNS request timed out.
    timeout was 2 seconds.
*** Request to www.informatik.uni-rostock.de timed-out
> nslookup labmaster.netprak.iuk.test
Server: labmaster.netprak.iuk.test
Address: 192.168.0.1

*** labmaster.netprak.iuk.test can't find nslookup: Non-existent domain
> nslookup google.de
Server: google.de
Addresses: 216.239.59.104, 66.249.93.104, 72.14.221.104
```

Wie zu sehen ist, haben wir zu den gegebenen Rechnernamen eine oder auch mehrere Adressen gefunden.

```
E:\>nbtstat -n

Local Area Connection:
Node IpAddress: [192.168.0.21] Scope Id: []

        NetBIOS Local Name Table

    Name                Type               Status
-----
EINS                    <00>    UNIQUE         Registered
EINS                    <20>    UNIQUE         Registered
INFORMATIK              <00>    GROUP           Registered

E:\>nbtstat -a labmaster

Local Area Connection:
Node IpAddress: [192.168.0.21] Scope Id: []

        NetBIOS Remote Machine Name Table

    Name                Type               Status
-----
MUNGO                   <00>    UNIQUE         Registered
MUNGO                   <03>    UNIQUE         Registered
MUNGO                   <20>    UNIQUE         Registered
...MSBROWSE...         <01>    GROUP           Registered
LABMASTER               <00>    UNIQUE         Registered
LABMASTER               <03>    UNIQUE         Registered
LABMASTER               <20>    UNIQUE         Registered
NETPRAK                  <00>    GROUP           Registered
NETPRAK                  <1B>    UNIQUE         Registered
NETPRAK                  <1C>    GROUP           Registered
NETPRAK                  <1D>    UNIQUE         Registered
NETPRAK                  <1E>    GROUP           Registered

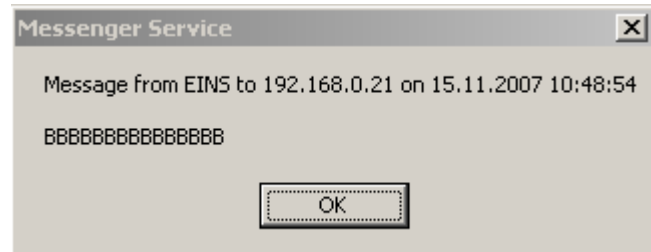
MAC Address = 00-00-00-00-00-00
```

Jetzt haben wir mit *nbtstat -n* die lokale Net-BIOS-Tabelle anzeigen lassen und anschließend haben wir *nbtstat -a labmaster* aufgerufen.

Nun haben wir uns mit *net send* selbst eine Nachricht geschickt.

```
E:\>net send 192.168.0.21 BBBBBBBBBBBBBBBB
The message was successfully sent to 192.168.0.21.
```

Wie man sieht, hat dies auch gut funktioniert.



Als Letztes haben wir uns noch mit *net name* die Liste der Namen ausgegeben lassen, die Nachrichten empfangen können.

```
E:\>net name
The Messenger service is not started.

Is it OK to start it? (Y/N) [Y]: y
The Messenger service is starting...
The Messenger service was started successfully.
```

Name

```
-----
EINS
ADMINISTRATOR
The command completed successfully.
```

```
E:\>nbtstat -n
```

```
Local Area Connection:
Node IpAddress: [192.168.0.21] Scope Id: []
```

NetBIOS Local Name Table

Name	Type	Status
EINS	<00> UNIQUE	Registered
EINS	<20> UNIQUE	Registered
INFORMATIK	<00> GROUP	Registered
EINS	<01> UNIQUE	Registered
EINS	<03> UNIQUE	Registered
ADMINISTRATOR	<03> UNIQUE	Registered

Es ist in beiden Abbildungen zu sehen, dass ich nur mit dem Administrator und mir selbst kommunizieren kann.

Aufgabe 3: Dekonfiguration über Kommandozeile

Zu Beginn des Versuches haben wir „netsh“ in den Offlinemodus gewechselt.

```
E:\>netsh
netsh>offline

netsh>show mode
offline
```

Diese Umstellung hat zur Folge, dass eingegebene Begriffe gesammelt werden und erst mit dem Befehl „commit“ ausgeführt werden. Im Onlinemodus werden sie dagegen sofort ausgeführt.

Anschliessend wechselten wir in den Interface- und dann in den IP-Kontext:

```
netsh>interface
netsh interface>ip
netsh interface ip>
```

In diesem Kontext haben wir dann den DNS-Server und dann den WINS-Server gelöscht:

```
netsh interface ip>del dns "Local Area Connection" 192.168.0.1
Ok.

netsh interface ip>del wins "Local Area Connection" 192.168.0.1
Ok.
```

Die Servernamen wurden somit aus der Namenliste der DNS und WINS gelöscht. Anschließend versuchten wir die IP-Adresse ebenfalls löschen:

```
netsh interface ip>del address "Local Area Connection" 192.168.0.21
An interface not using DHCP must have one or more static IP Addresses.
```

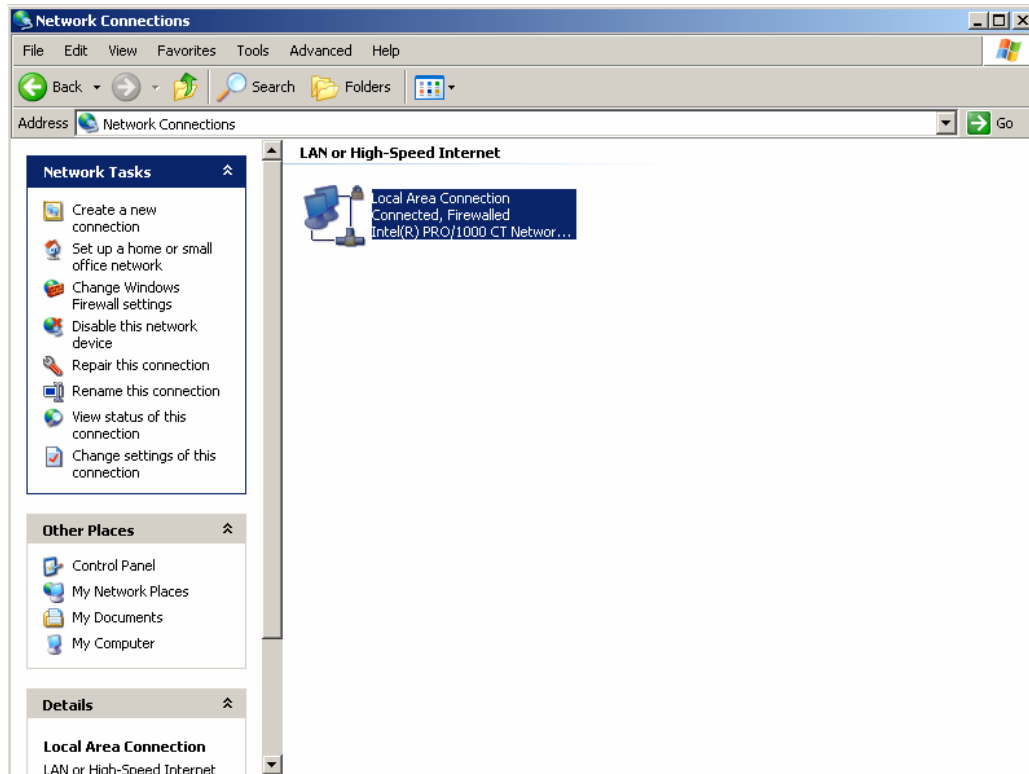
„Netsh“ brachte die Antwort, dass das Löschen der IP-Adresse unzulässig sei, weil die Zuweisung der IP-Adresse manuell geschieht. Löschen wäre nur möglich, wenn DHCP (Dynamic Host Configuration Protocol) aktiviert ist, da dieses die automatische Zuweisung der IP-Adresse übernimmt und nach einem Löschvorgang eine neue Adresse zuweisen würde.

Abschließend wurden die eingegebenen Befehle ausgeführt:

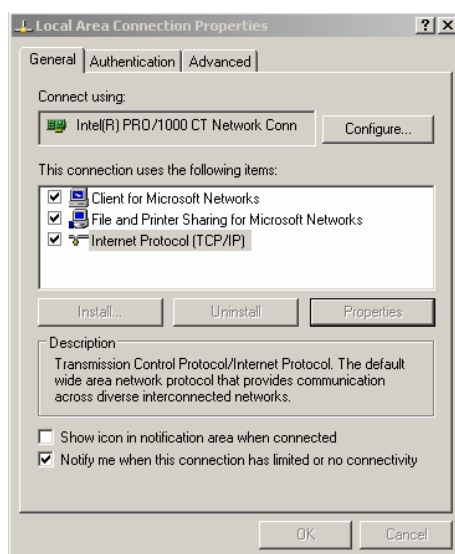
```
netsh interface ip>commit
```

Aufgabe 4: Konfiguration über die Grafische Oberfläche

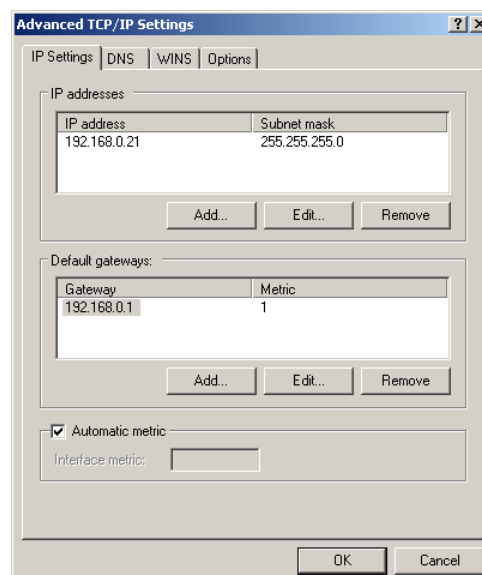
Um unter Windows XP die Netzwerkeinstellungen mittels grafischer Oberfläche durchzuführen, haben wir unter „Network Connection“ (Aufruf über Startmenü) die verfügbaren Netzwerkverbindungen aufgerufen:



Um die IP- Einstellungen zu ändern haben wir unter „local Area Connection“ mittels rechter Maustaste im Kontextmenü die Eigenschaften des Protokolls aufgerufen (Properties -> This Connection uses following Item -> Internet Protocol (TCP/IP)).

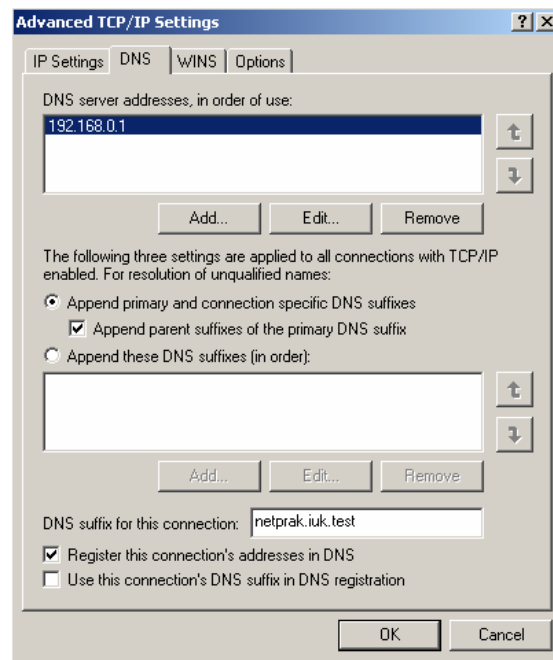


Im erscheinenden Dialog wählten wir „Advanced“ um die Einstellungen der IP-Adresse, Netzmaske, Gateway, Domainnamen, DNS- und WINS-Server einzutragen:

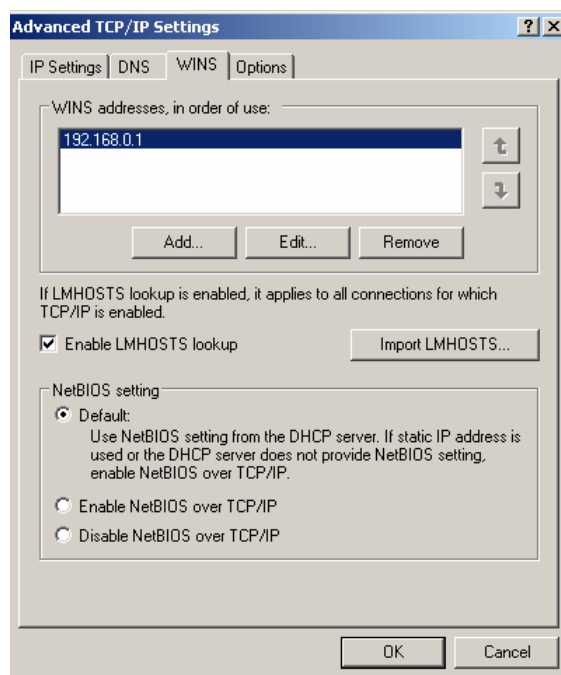


IP-Adresse, Netzmaske, Gateway:

DNS-Server:



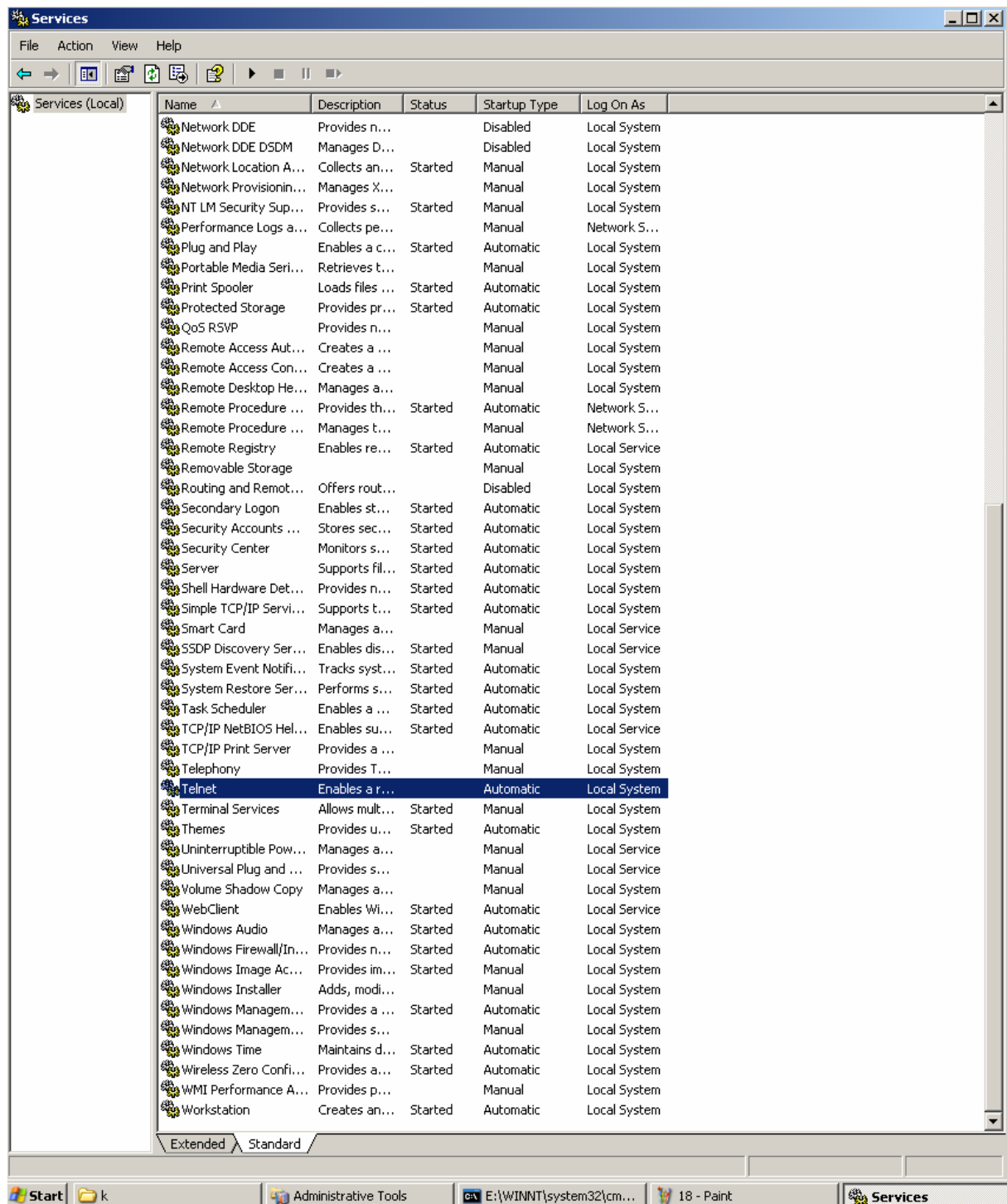
WINS-Server:



Die Änderungen wurden abschließend mit OK bestätigt.

Services:

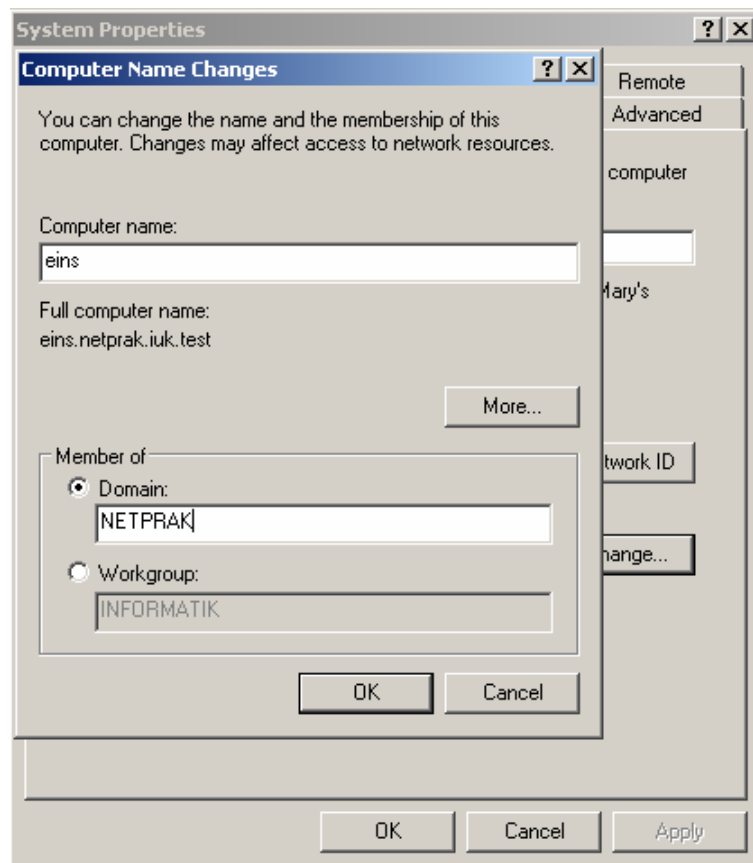
Anschließend ließen wir uns die Netzwerkdienste anzeigen (Control Panel -> Administrative Tools -> Services).



Dort starteten wir den „telnet“-Dienst und den Simple TCP/IP-Services-Dienst.

Domaine „netprak“

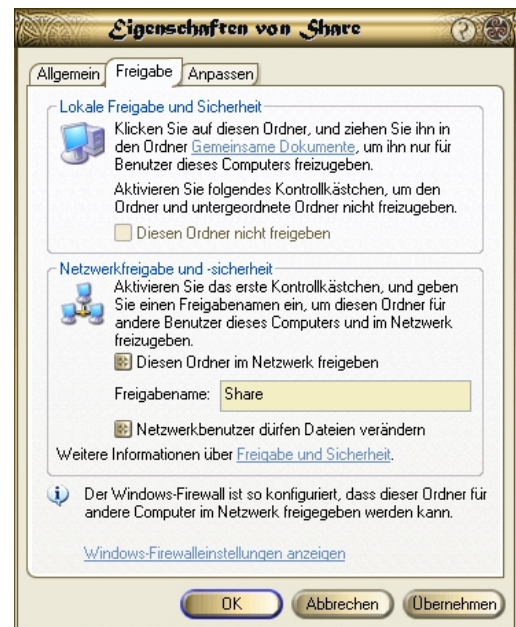
Weiterhin meldeten wir den Computer in der Domaine „netprak“ an, indem wir Dialog „System“ öffneten (Systemsteuerung -> System). Dort änderten wir unter „Computer Name“ den korrekten Rechnernamen („eins“) und den Domainnamen („netprak“):



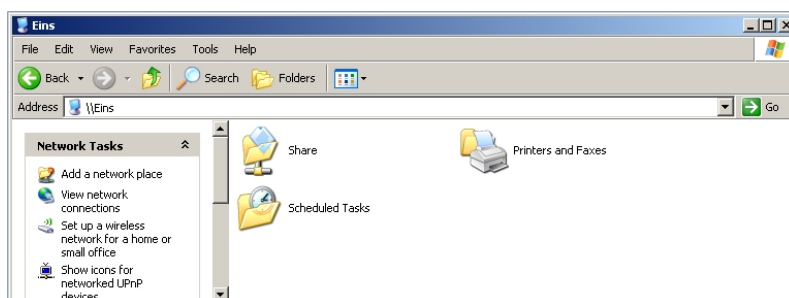
Zum Schluss bestätigten wir die Eingaben und starteten den Computer neu.

Aufgabe 5: Freigabe eines Verzeichnisses

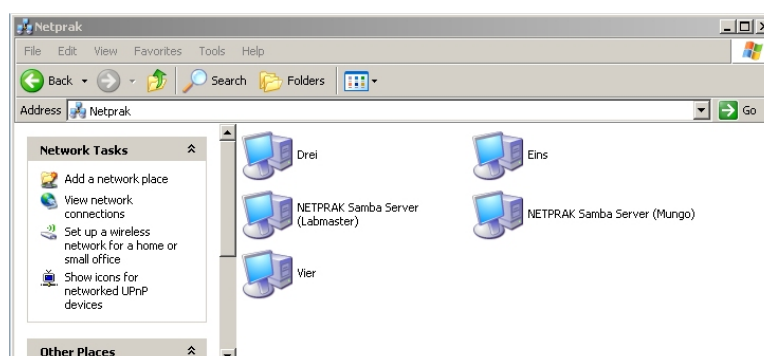
Als erstes erstellen wir ein Verzeichnis mit dem Namen „Share“ auf der lokalen Festplatte und kopierten wahllos ein paar Dateien hinein. Mittels rechtem Mausklick auf den Dateiordner -> „Properties“ (Eigenschaften) -> „Sharing and Security“ (Freigabe) gelangen wir in das Kontextmenü, und mit Setzen des Häkchens im Kontrollkästchen „Diesen Ordner im Netzwerk freigeben“ wird dann auch die allgemeine Freigabe dieses Ordners für das Netzwerk erteilt. Standardmäßig wird der Datei-/Ordnername als Freigabename vorgeschlagen, den wir hier auch so belassen, und aktivieren ebenfalls noch die Option „Netzwerkbenutzer dürfen Dateien verändern“, womit alle Benutzer des Netzwerkes volle Lese- und Schreibrechte für diesen Ordner besitzen. Mit Klick auf „Übernehmen“ werden die so gemachten Einstellungen wirksam, und der Ordner wird freigegeben.



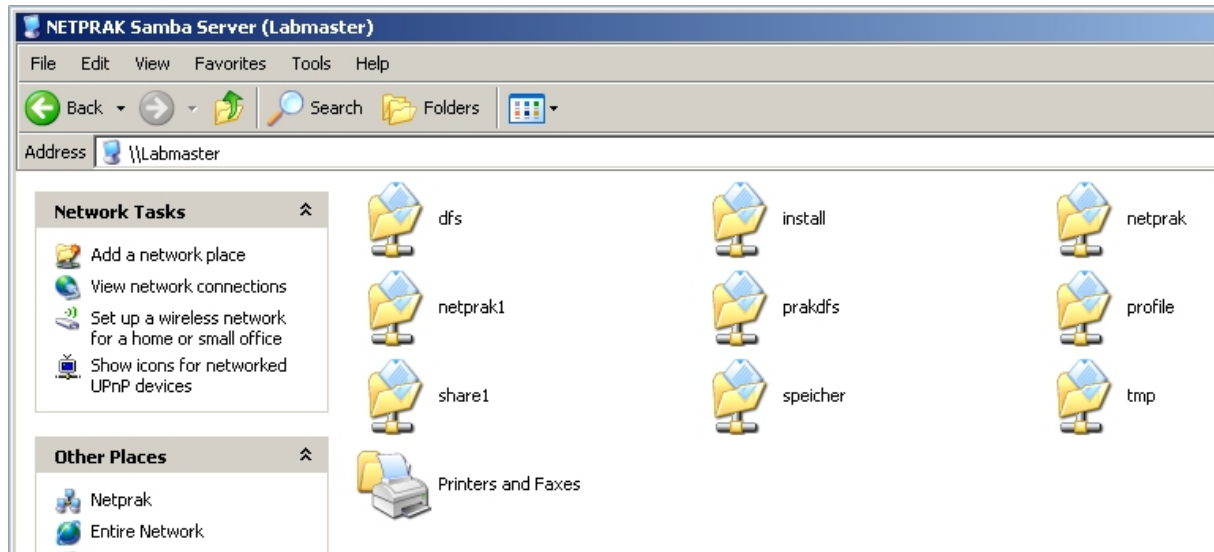
Um die Wirksamkeit unserer eben gemachten Freigabe zu kontrollieren, gehen wir über „Arbeitsplatz“ -> „Netzwerkumgebung“ -> wählen unser Netz „Netprak“ -> wählen unseren eigenen Rechner „eins“ und alle für diesen Rechner bestehenden Freigaben werden nun angezeigt: Neben dem Drucker-/Faxfreigabe-Ordner und dem Task-Ordner, ist nun auch der eigene Ordner „Share“ freigegeben und für jedermann im eigenen Netz sichtbar.



Im folgendem lassen wir uns die Freigaben des Computers „Labmaster“ anzeigen, indem wir wiederum über „Arbeitsplatz“ -> „Netzwerkumgebung“ -> wählen unser Netz „Netprak“ -> den Rechner „Labmaster“ auswählen:



Und nach erfolgreicher Anmeldung mit Nutzernamen und Passwort (hier beides „netprak“), werden die nachfolgenden 9 Ordner des Rechners „Labmaster“ als freigegeben angezeigt:



Wir werfen noch einen kurzen Blick in den Ordner „share1“ und finden dort eine einzige Datei:



In der Kommandokonsole von Windows ist es ebenso möglich, sich die Freigaben einzelner Rechner anzeigen zu lassen. Dazu verwenden wir den Befehl „*net view <Rechnername>*“.

Mit „*net view eins*“ werden die freigegebenen Ordner unseres eigenen Rechners, hier also nur „Share“, ausgegeben, und mit „*net view labmaster*“ werden alle 9 freigegebenen Ordner des Rechners „Labmaster“ angezeigt. Was im Unterschied zur grafischen Anzeige hier nicht dargestellt wird, sind die Druckerfreigaben und der Task-Ordner des eigenen Rechners.

```
E:\Documents and Settings\Administrator>net view eins
Shared resources at eins

Share name  Type  Used as  Comment
-----
Share       Disk
The command completed successfully.

E:\Documents and Settings\Administrator>net view labmaster
Shared resources at labmaster

NETPRAK Samba Server
Share name  Type  Used as  Comment
-----
dfs         Disk
install    Disk
netprak     Disk          Heimatverzeichnis
netprak1    Disk
prakdfs     Disk
profile     Disk
share1      Disk
speicher    Disk
tmp         Disk
The command completed successfully.
```

Aufgabe 6: Sicheres Windows

In dieser Aufgabe spüren wir mit Hilfe des Programmes „nmap“ (gehört nicht zum Lieferumfang von MS Windows) Sicherheitslücken beim Betreiben von Windows XP in offenen Netzen auf. Mit Hilfe der beiden Testverfahren TCP Connect-Scan und TCP SYN-Scan werden wir den eigenen Rechner auf offene Ports hin untersuchen.

TCP Connect-Scan: „nmap“ verhält sich dabei wie ein normaler Client, d.h., es versucht über den zu scannenden Port eine vollständige TCP-Verbindung aufzubauen. Kommt eine Verbindung zustande, so ist der Port offen. Dieser Port-Angriff ist jedoch einfach zu entdecken und wird von den meisten Betriebssystemen protokolliert.

TCP SYN-Scan: „nmap“ scannt die Ports durch senden eines Syn-Signals, dabei wird jedoch keine vollständige TCP-Verbindung aufgebaut: sobald nmap ein „SYN/ACK“ als Antwort des Ports vom Zielrechner erhält, sendet es an ihn ein „RST“-Signal und beendet umgehend diese halb-offene Verbindung wieder. Mit dieser Methode kann unter Umständen eine Erkennung des Portscans durch den Zielrechner vermieden werden.

Leider konnten wir in unserem Versuch den TCP SYN-Scan mit Ziel eigener Rechner nicht durchführen, da dieser angeblich nicht von unserem Betriebssystem unterstützt wird.

Nach Eingabe des entsprechenden Befehls: `nmap -sS 192.168.0.21` erhielten wir folgende Fehlermeldung:

```
E:\Documents and Settings\Administrator>nmap -sS 192.168.0.21
Starting Nmap 4.20 ( http://insecure.org ) at 2007-11-15 11:20 W. Europe Standard Time
Skipping SYN Stealth Scan against 192.168.0.21 because Windows does not support scanning your own machine (localhost) this way.
All 0 scanned ports on 192.168.0.21 are
Nmap finished: 1 IP address (1 host up) scanned in 13.015 seconds
```

Wie gehen daher nahtlos zum TCP-Connect-Test über. Durch Eingabe des Befehls:
`nmap -v -sT 192.168.0.21`
(die Option -v macht nmap nur ein wenig „gesprächiger“, zeigt also schon während des testens was an) erhalten wir nebenstehendes Testergebnis:

```
E:\Documents and Settings\Administrator>nmap -v -sT 192.168.0.21
Starting Nmap 4.20 ( http://insecure.org ) at 2007-11-15 11:27 W. Europe Standard Time
Initiating Parallel DNS resolution of 1 host. at 11:27
Completed Parallel DNS resolution of 1 host. at 11:28, 13.00s elapsed
Initiating Connect() Scan at 11:28
Scanning 192.168.0.21 [1697 ports]
Discovered open port 3389/tcp on 192.168.0.21
Connect() Scan timing: About 12.26% done; ETC: 11:32 (0:03:35 remaining)
Discovered open port 3462/tcp on 192.168.0.21
Discovered open port 139/tcp on 192.168.0.21
Increasing send delay for 192.168.0.21 from 0 to 5 due to 11 out of 13 dropped probes since last increase.
Discovered open port 445/tcp on 192.168.0.21
Discovered open port 135/tcp on 192.168.0.21
Discovered open port 9/tcp on 192.168.0.21
Discovered open port 13/tcp on 192.168.0.21
Discovered open port 7/tcp on 192.168.0.21
Discovered open port 19/tcp on 192.168.0.21
Discovered open port 17/tcp on 192.168.0.21
Completed Connect() Scan at 11:32, 254.42s elapsed (1697 total ports)
Host 192.168.0.21 appears to be up ... good.
Interesting ports on 192.168.0.21:
Not shown: 1687 filtered ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-term-serv
3462/tcp  open  track

Nmap finished: 1 IP address (1 host up) scanned in 273.188 seconds
Raw packets sent: 0 (0B) ; Rcvd: 0 (0B)
```

In diesem Test wurden die wichtigsten 1697 Ports von insgesamt ca. 65500 auf ihre Verbindungsfreundlichkeit hin untersucht. Dabei wurden uns von nmap insgesamt 10 offene Ports gemeldet.

Das sind zum Beispiel:

Port 135: MS-RPC (Remote Procedure Call)

Gehört seit Windows 2000 zum MS Windows-Netzwerkdienst. Mit dessen Hilfe lassen sich andere entfernte Rechner administrieren (fernsteuern). So lassen sich Netzwerkfreigaben konfigurieren, Systemdienste können gestartet und beendet werden, selbst ein Abschalten oder Neustart des Zielrechners ist damit möglich.

Port 139: NetBIOS Session Service

NetBIOS ist Bestandteil des MS Windows-Netzwerkdienstes und wird überwiegend zum Datentransfer (Dateien/Drucker) genutzt. Der Authentifizierungsmechanismus wird als nicht besonders sicher eingestuft, und oftmals erfolgen Netzwerkfreigaben ohne Passwort.

Port 3389: Remote Desktop

Dieser Port ist für den Terminalserver von Microsoft zuständig. Dieser sollte bei Servern, die diesen Dienst anbieten auch offen bleiben.

Nun Deaktivieren wir die beiden Dienste „Server“ und „Workstation“. Dazu starten wir die „Microsoft Management Console“ („MMC.EXE“ über Ausführen, oder die Verwaltung aus der Systemeinstellungen), fügen nötigenfalls noch das entsprechende Snap-In „Dienste“ hinzu und deaktivieren die Dienste über das Kontextmenü, welches nach anklicken mit der rechten Maustaste auf den entsprechenden Dienst hin erscheint: „Microsoft DS“ und „track“ (die sollten den Port 445 und 3462 beanspruchen).

Nun führen wir den TCP Connect-Scan ein weiteres mal aus und erhalten nebenstehendes Resultat:

Es werden nunmehr nur noch 8 offene Ports gemeldet, Port 445 und 3462 sind aus der Liste durch Beendigung der entsprechenden Dienste verschwunden.

```
E:\Documents and Settings\Administrator>nmap -v -sT eins
Starting Nmap 4.20 ( http://insecure.org ) at 2007-11-15 11:44 W. Europe Standard Time
Initiating Parallel DNS resolution of 1 host. at 11:44
Completed Parallel DNS resolution of 1 host. at 11:44, 13.00s elapsed
Initiating Connect() Scan at 11:44
Scanning 192.168.0.21 [1697 ports]
Discovered open port 3389/tcp on 192.168.0.21
Connect() Scan Timing: About 8.69% done; ETC: 11:50 (0:05:16 remaining)
Discovered open port 9/tcp on 192.168.0.21
Discovered open port 17/tcp on 192.168.0.21
Discovered open port 135/tcp on 192.168.0.21
Stats: 0:02:50 elapsed; 0 hosts completed (1 up), 1 undergoing Connect() Scan
Connect() Scan Timing: About 44.23% done; ETC: 11:50 (0:03:18 remaining)
Discovered open port 139/tcp on 192.168.0.21
Discovered open port 7/tcp on 192.168.0.21
Discovered open port 13/tcp on 192.168.0.21
Discovered open port 19/tcp on 192.168.0.21
Completed Connect() Scan at 11:50, 364.36s elapsed (1697 total ports)
Host 192.168.0.21 appears to be up ... good.
Interesting ports on 192.168.0.21:
Not shown: 1689 closed ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
3389/tcp  open  ms-termin-serv

Nmap finished: 1 IP address (1 host up) scanned in 377.390 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

Mit Aktivierung des TelNet-Dienstes gesellt sich Port 23 zur Liste der offenen Ports hinzu. Über diese unverschlüsselte Datenverbindung ist das Ausführen von Befehlen und Programmen direkt auf dem Zielrechner möglich.

Und hier kommt der Beweis:

TCP Connect-Test nach Aktivierung des TelNet-Dienstes:

```
Starting Nmap 4.20 ( http://insecure.org ) at 2007-11-22 19:01 Westeuropäische Normalzeit
Initiating Parallel DNS resolution of 1 host. at 19:01
Completed Parallel DNS resolution of 1 host. at 19:01, 0.00s elapsed
Initiating Connect() Scan at 19:01
Scanning privat-ab211cd5 (192.168.178.21) [1697 ports]
Discovered open port 23/tcp on 192.168.178.21
Discovered open port 445/tcp on 192.168.178.21
Connect() Scan Timing: About 9.10% done; ETC: 19:06 (0:04:59 remaining)
Discovered open port 135/tcp on 192.168.178.21
Discovered open port 139/tcp on 192.168.178.21
Completed Connect() Scan at 19:06, 340.05s elapsed (1697 total ports)
Host privat-ab211cd5 (192.168.178.21) appears to be up ... good.
Interesting ports on privat-ab211cd5 (192.168.178.21):
Not shown: 1693 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap finished: 1 IP address (1 host up) scanned in 340.140 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

TCP Connect-Test nach Deaktivierung des TelNet-Dienstes:

```
Starting Nmap 4.20 ( http://insecure.org ) at 2007-11-22 18:52 Westeuropäische Normalzeit
Initiating Parallel DNS resolution of 1 host. at 18:52
Completed Parallel DNS resolution of 1 host. at 18:52, 0.02s elapsed
Initiating Connect() Scan at 18:52
Scanning privat-ab211cd5 (192.168.178.21) [1697 ports]
Connect() Scan Timing: About 8.99% done; ETC: 18:58 (0:05:04 remaining)
Discovered open port 135/tcp on 192.168.178.21
Discovered open port 445/tcp on 192.168.178.21
Discovered open port 139/tcp on 192.168.178.21
Completed Connect() Scan at 18:58, 340.05s elapsed (1697 total ports)
Host privat-ab211cd5 (192.168.178.21) appears to be up ... good.
Interesting ports on privat-ab211cd5 (192.168.178.21):
Not shown: 1694 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap finished: 1 IP address (1 host up) scanned in 340.563 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```



Aufgabe 7: Automatische Konfiguration

In dieser Aufgabe werden wir uns mit der automatischen Konfiguration der Netzwerkeinstellungen vertraut machen.

Dazu starten wir unter der Windows-Kommandokonsole das Programm netsh, wechseln in den Kontext interface und anschließend ip, und mit der Eingabe der folgenden drei Befehle wird die Netzwerkkarte automatisch konfiguriert:

set address „Local Area Connection“ dhcp

Der Netzwerkkarte des eigenen Rechners wird automatisch vom DHCP-Server die IP-Adresse, die Netzmaske und ein Default-Gateway zugewiesen.

set dns „Local Area Connection“ dhcp

set wins „Local Area Connection“ dhcp

Die Server zur Namensauflösung werden ebenfalls durch den DHCP-Server bestimmt.

```
E:\Documents and Settings\Administrator>netsh
netsh>ip
The following command was not found: ip.
netsh>interface
netsh interface>ip
netsh interface ip>set address "Local Area Connection" dhcp
The following command was not found: set address "Local Area Connection" dhcp.
netsh interface ip>set address "Local Area Connection" dhcp
Ok.

netsh interface ip>set dns "Local Area Connection" dhcp
Ok.

netsh interface ip>set wins "Local Area Connection" dhcp
Ok.
```

Alle drei Befehle wurden von netsh akzeptiert und so mit einem „Ok.“ quittiert. Um nun die neu gemachte Netzwerkkonfiguration ohne Neustart des PC's zu aktivieren, beenden wir netsh und geben den Befehl *ipconfig /renew* ein. Mit *ipconfig /all* lassen wir uns nun die Netzwerkkonfiguration anzeigen:

```
E:\Documents and Settings\Administrator>ipconfig /renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : netprak.iuk.test
    IP Address. . . . . : 192.168.0.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

E:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration

    Host Name . . . . . : eins
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : netprak.iuk.test

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : netprak.iuk.test
    Description . . . . . : Intel(R) PRO/1000 CT Network Connect
ion
    Physical Address. . . . . : 00-30-05-4F-EE-75
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.0.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
    DHCP Server . . . . . : 192.168.0.1
    DNS Servers . . . . . : 192.168.0.1
    Lease Obtained. . . . . : Donnerstag, 15. November 2007 11:54:
16
    Lease Expires . . . . . : Donnerstag, 15. November 2007 17:54:
16
```

Vom DHCP-Server wurde uns nun folgende Konfiguration zugewiesen:

IP-Adresse:	192.168.0.11
Netzmaske:	255.255.255.0
Default-Gateway:	192.168.0.1
DNS-Server:	192.168.0.1
DHCP-Server:	192.168.0.1

Nun geben wir die IP-Adresse unseres Rechners mit dem Befehl *ipconfig /release* wieder frei und schauen uns das Resultat mittels *ipconfig /all* an:

```
E:\Documents and Settings\Administrator>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : netprak.iuk.test
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . :

E:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : eins
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : netprak.iuk.test
    Description . . . . . : Intel(R) PRO/1000 CT Network Connect
ion
    Physical Address. . . . . : 00-30-05-4F-EE-75
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . :
    DHCP Server . . . . . : 255.255.255.255
```

Alle vom DHCP-Server zugewiesenen Adressen wurden aus der Netzwerkconfiguration entfernt. Die hier eingetragene IP-Adresse: 0.0.0.0 ist eine Ungültige und weist normalerweise auf eine nicht bestehende Netzwerkverbindung oder eine nicht funktionierende Netzwerkkarte hin.

Aber da die automatische Netzwerkconfiguration noch aktiviert ist, reicht ein *ipconfig /renew*, damit die Netzwerkkarte eine Zuweisungsanfrage an den DHCP-Server sendet und alle notwendigen Adressen von ihm wiederum zugewiesen bekommt. Die nun zugewiesenen Adressen sollten identisch mit den Vorherigen sein, lediglich die IP-Adresse könnte sich ändern, da sie vielleicht zwischenzeitlich vom DHCP-Server an einem anderen Rechner vergeben wurde.

Zum Abschluss versuchen wir noch zwei PC's direkt miteinander zu verbinden. Dazu geben wir erstmal die bestehenden Adressen mit *ipconfig /release* wieder frei. Anschließend trennen wir die Verbindung zum Netzwerk, indem wir das Kabel der Netzwerkkarte ziehen und unseren PC mit dem PC der Praktikumsgruppe 2 mit einem Cross-Patch-Kabel verbinden. Dieses ist notwendig, da eine Direktverbindung zweier Netzwerk-Endgeräte nur über ein Kabel mit gekreuzten Leitungen (RX und TX

sind einmal vertauscht) funktioniert. Nach ca. einer Minute weist sich der eigene Rechner selbst eine entsprechende Netzwerkkonfiguration mit der IP-Adresse: 169.254.142.14 zu.

```
E:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : eins
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : netprak.iuk.test
    Description . . . . . : Intel(R) PRO/1000 CT Network Connect
ion
    Physical Address. . . . . : 00-30-05-4F-EE-75
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Autoconfiguration IP Address. . . : 169.254.142.14
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :
```

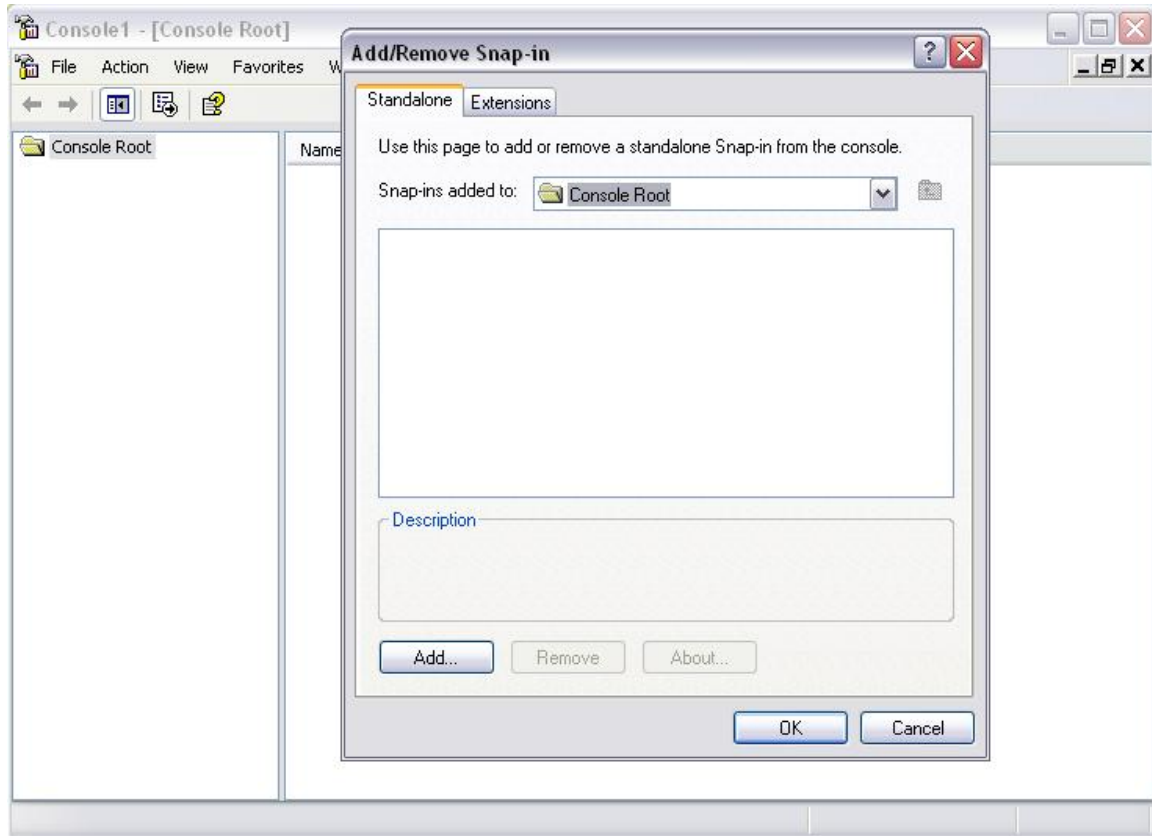
An den ersten beiden Bytes der neu zugewiesenen IP-Adresse (also 169.254) ist zu erkennen, dass sich unser Rechner in einer Direktverbindung mit einem anderen PC befindet: Er befindet sich nun in einem sogenannten zeroconf (Zero Configuration Networking)-Modus. Dieser Modus erlaubt ein konfigurationsfreies Betreiben von Netzwerkgeräten innerhalb eines lokalen Netzwerkes mit Direktverbindungen mit dem IP-Internetprotokoll. Da in einem solchem Netzwerk kein DHCP-Server existiert, weist sich ein jeder Rechner selbst eine IP-Adresse nach folgendem Schema zu:

Mithilfe eines Zufallsgenerators wird eine IP-Adresse zwischen 169.254.1.0 und 169.254.254.255 vom Rechner generiert. Diese ist jedoch nur pseudozufällig: rechnerspezifische Informationen, wie etwa die Physikalische Adresse der Netzwerkkarte, fließen in die Bestimmung dieser Link-Local-IP Adresse mit ein, um die Chance zur Bestimmung einer bereits vergebenen IP-Adresse zu minimieren. Nach Bestimmung dieser Adresse, wird diese für sich beansprucht und im lokalen Netzwerk getestet, um Adressenkonflikte zu vermeiden; Ist sie wider Erwarten doch bereits vergeben, wird der gesamte Vorgang zur Bestimmung wiederholt. Dieser Vorgang nennt sich Automatische IP-Allokation.

Zusatzaufgabe 1: IPSec

In diesem Versuch bauen wir eine verschlüsselte Verbindung zwischen zwei XP-Rechnern mit Hilfe des Programms „mmc“ auf:

Dazu starten wir „mmc“ und wählen dort unter „File“ -> „Add Snap-In“:



Dort führen wir den Add- Dialog aus, und wählen „Services“ aus:



Im anschließenden Dialog wählen wir unseren Rechner („Local computer“):

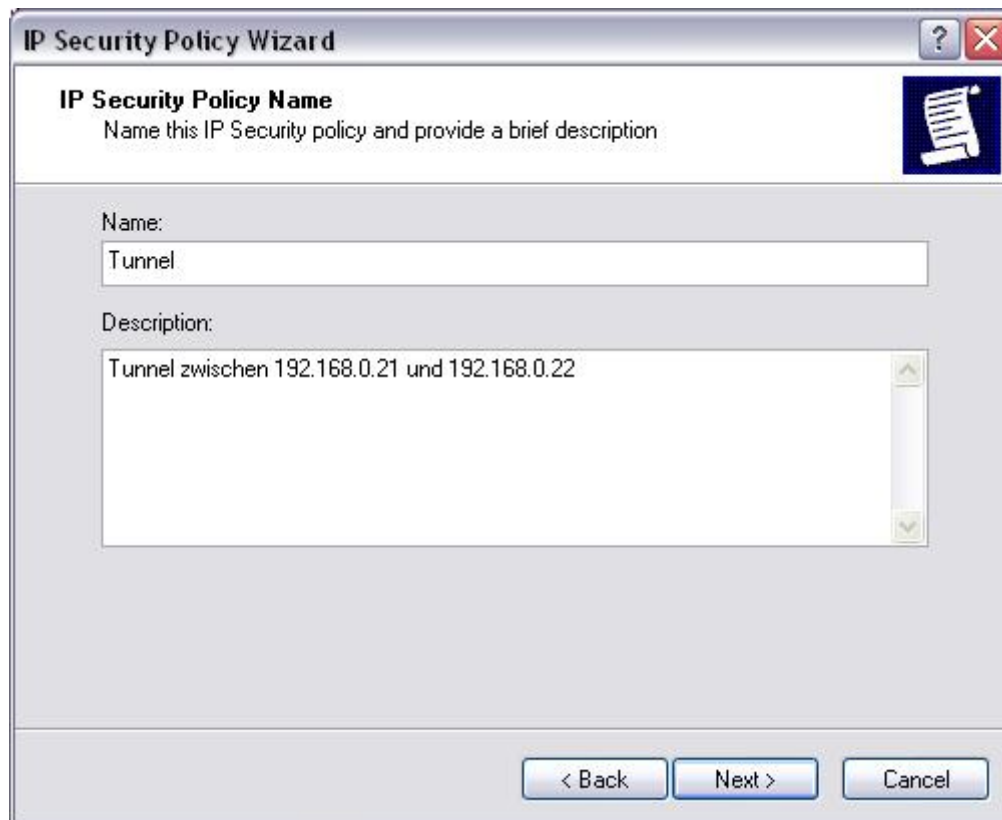


Der Vorgang wird für den „IP Sec polices“- Dienst wiederholt:

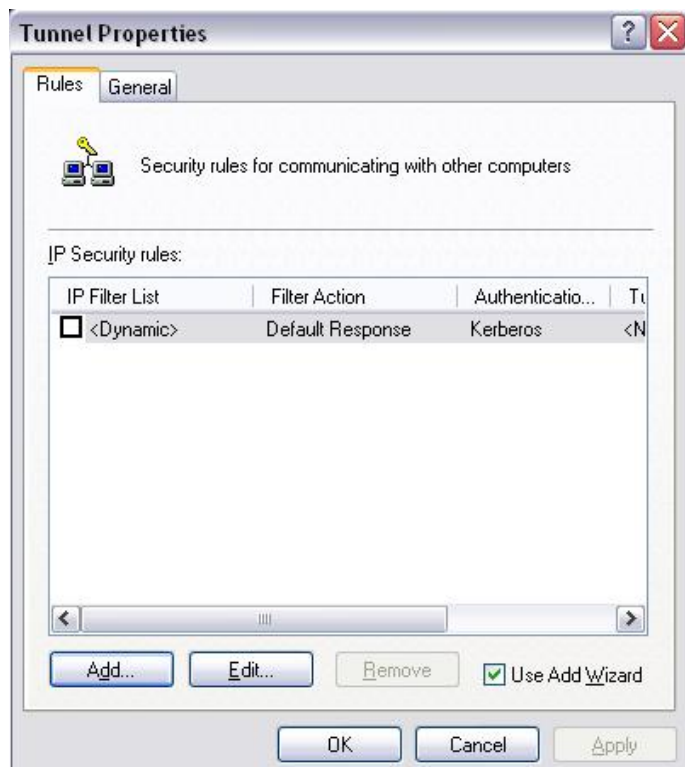


Sollte der Dienst „IP Sec polices“ nicht gestartet sein, muss dieser nun gestartet werden.

Im Kontextmenü von „IP Sec polices“ (rechte Maustaste) wird nun ein Tunnel zwischen den Rechner eins (192.168.0.21) und Rechner zwei (192.168.0.22) erstellt:



Anschließend werden zwei Regeln mittels Add- Dialog hinzugefügt:



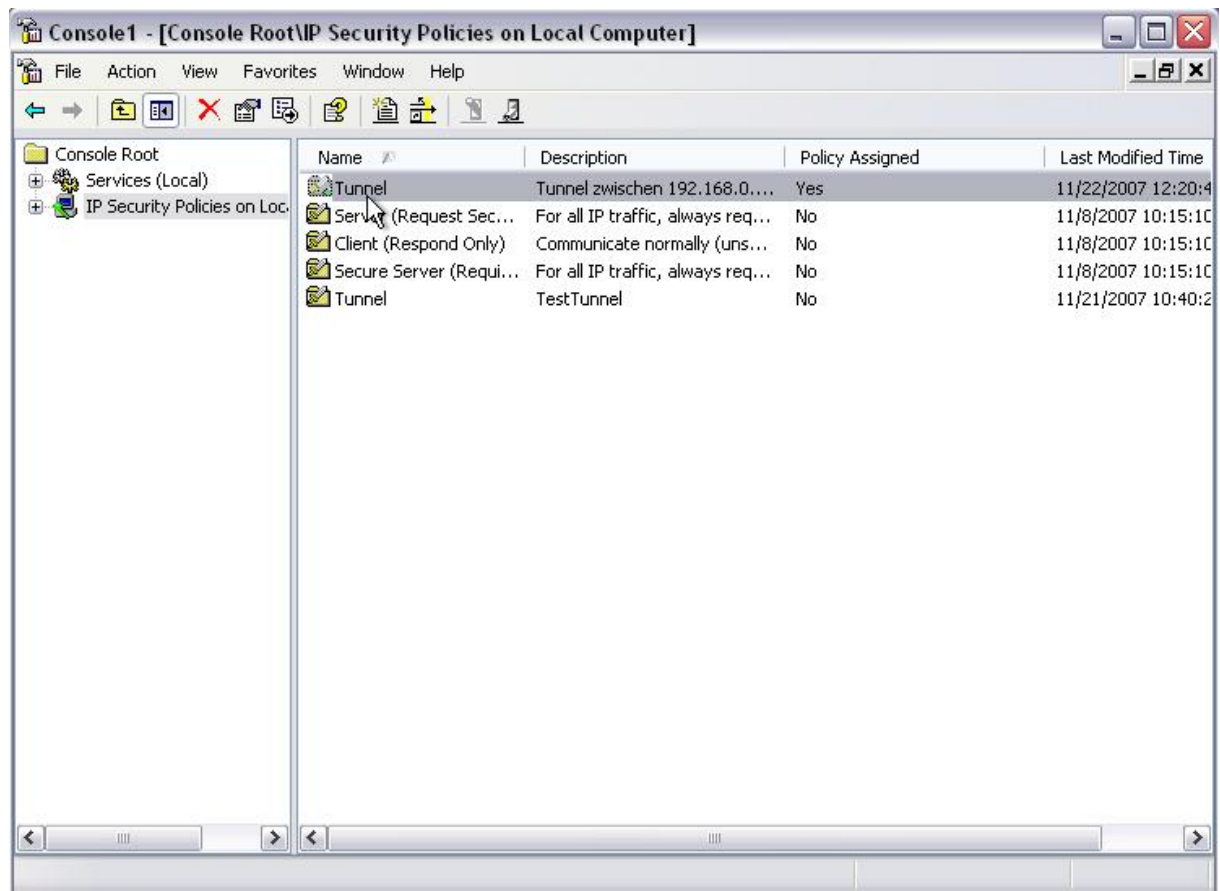
Der Endpunkt der ersten Regel wird auf Rechner „zwei“ gelegt:



Als Überwachungsmethode wird sämtlicher Verkehr über die IP- Adresse bestimmt:



Nach Erstellung des zweiten Tunnels (analog zu Tunnel 1) wird die Sicherheitsrichtlinie im Kontextmenü von „mmc“ zugewiesen:



Die verschlüsselte Verbindung sollte somit hergestellt sein.

Zusatzaufgabe 2: Firewall

In diesem Versuch wird eine Portbasierte Firewall eingerichtet, welche auf dem „IP-Sicherheitsrichtliniendienst“ basiert. In unserem Beispiel soll der TCP- Port 23 gesperrt werden.

Dazu wird unter „mmc“ wieder eine neue IP- Sicherheitsrichtlinie erschaffen (siehe Zusatzaufgabe 1) und dort eine neue Regel:



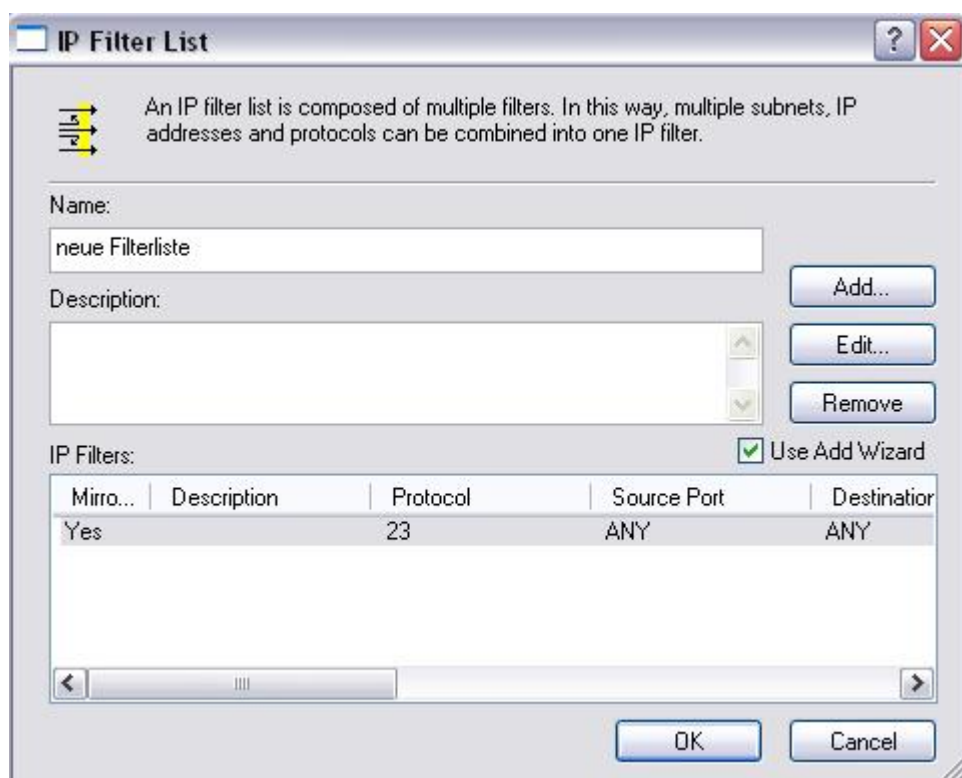
neue Regel (Add- Dialog):



kein Tunnel -> gesamte Verbindungen -> neue IP- Filterliste:



Im Edit- Dialog werden die Einstellungen auf den TCP- Port 23 gelegt:



Um den Port 23 hinzuzufügen muss der Add- Dialog geöffnet werden:
z.B.:



Anschliessend wird der Ursprung festgelegt. In unserem Fall sollen alle Eingänge zu unserer IP- Adresse gesperrt:

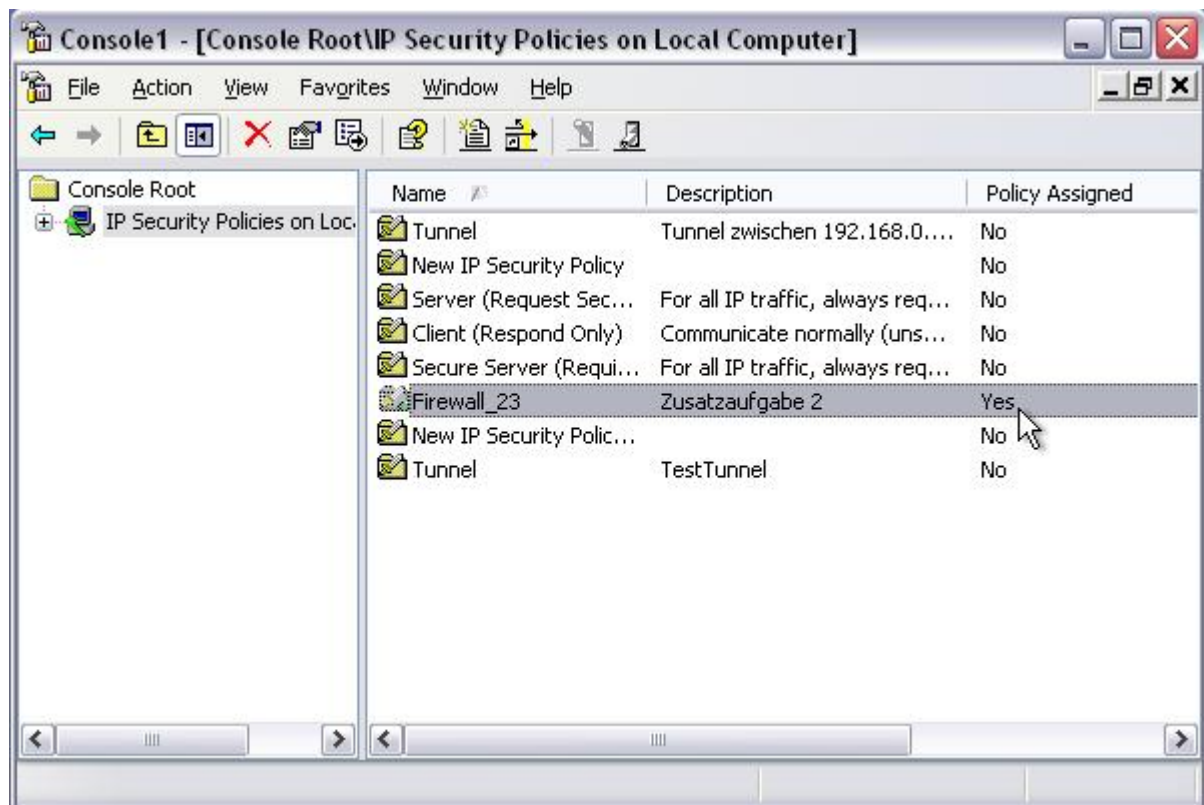


Im anschliessenden Dialog wird die Zieladresse auf „My IP Address“ gelegt.

Im nächsten Schritt wird die Sperrung auf den Port 23 gesetzt:



Der Konfigurationsdialog wird nun beendet und abschliessend muss die Überwachung nur noch gestartet werden:
(rechte Maustaste -> Assign)



Nun ist die Überwachung für den TCP- Port 23 aktiviert.