

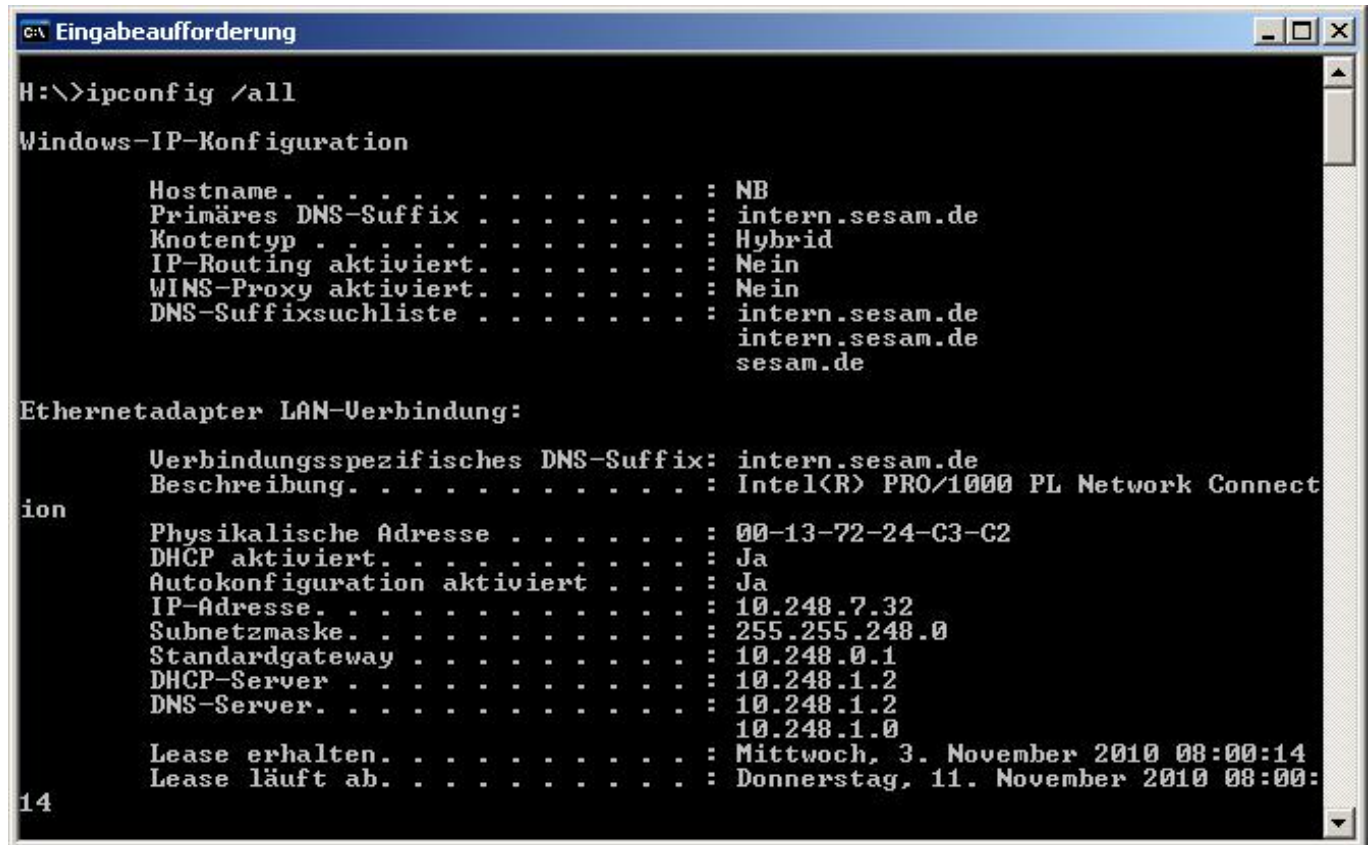
Netzwerk-Analysewerkzeuge

Aufruf der Kommandozeile:

Startmenü -> Eingabeaufforderung oder Ausführen **cmd** [Enter]

ipconfig

zeigt Informationen zu Netzwerkadaptern, IP-Adressen, IP-Einstellungen etc.



```
C:\>ipconfig /all

Windows-IP-Konfiguration

        Hostname. . . . . : NB
        Primäres DNS-Suffix . . . . . : intern.sesam.de
        Knotentyp . . . . . : Hybrid
        IP-Routing aktiviert. . . . . : Nein
        WINS-Proxy aktiviert. . . . . : Nein
        DNS-Suffixsuchliste . . . . . : intern.sesam.de
                                         intern.sesam.de
                                         sesam.de

Ethernetadapter LAN-Verbindung:

        Verbindungsspezifisches DNS-Suffix: intern.sesam.de
        Beschreibung. . . . . : Intel(R) PRO/1000 PL Network Connect
ion
        Physikalische Adresse . . . . . : 00-13-72-24-C3-C2
        DHCP aktiviert. . . . . : Ja
        Autokonfiguration aktiviert . . . . . : Ja
        IP-Adresse. . . . . : 10.248.7.32
        Subnetzmaske. . . . . : 255.255.248.0
        Standardgateway . . . . . : 10.248.0.1
        DHCP-Server . . . . . : 10.248.1.2
        DNS-Server. . . . . : 10.248.1.2
                               10.248.1.0
        Lease erhalten. . . . . : Mittwoch, 3. November 2010 08:00:14
        Lease läuft ab. . . . . : Donnerstag, 11. November 2010 08:00:
14
```

ping

testet Verbindung und löst Namen zu IP-Adressen auf



```
C:\>ping google.de

Ping google.de [66.249.92.104] mit 32 Bytes Daten:

Antwort von 66.249.92.104: Bytes=32 Zeit=27ms TTL=55
Antwort von 66.249.92.104: Bytes=32 Zeit=26ms TTL=55
Antwort von 66.249.92.104: Bytes=32 Zeit=26ms TTL=55
Antwort von 66.249.92.104: Bytes=32 Zeit=27ms TTL=55

Ping-Statistik für 66.249.92.104:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 26ms, Maximum = 27ms, Mittelwert = 26ms

H:\>
```

netstat

zeigt momentane Netzwerkverbindungen und geöffnete Ports des Rechners

```
C:\>Eingabeaufforderung
H:\>netstat -a

Aktive Verbindungen

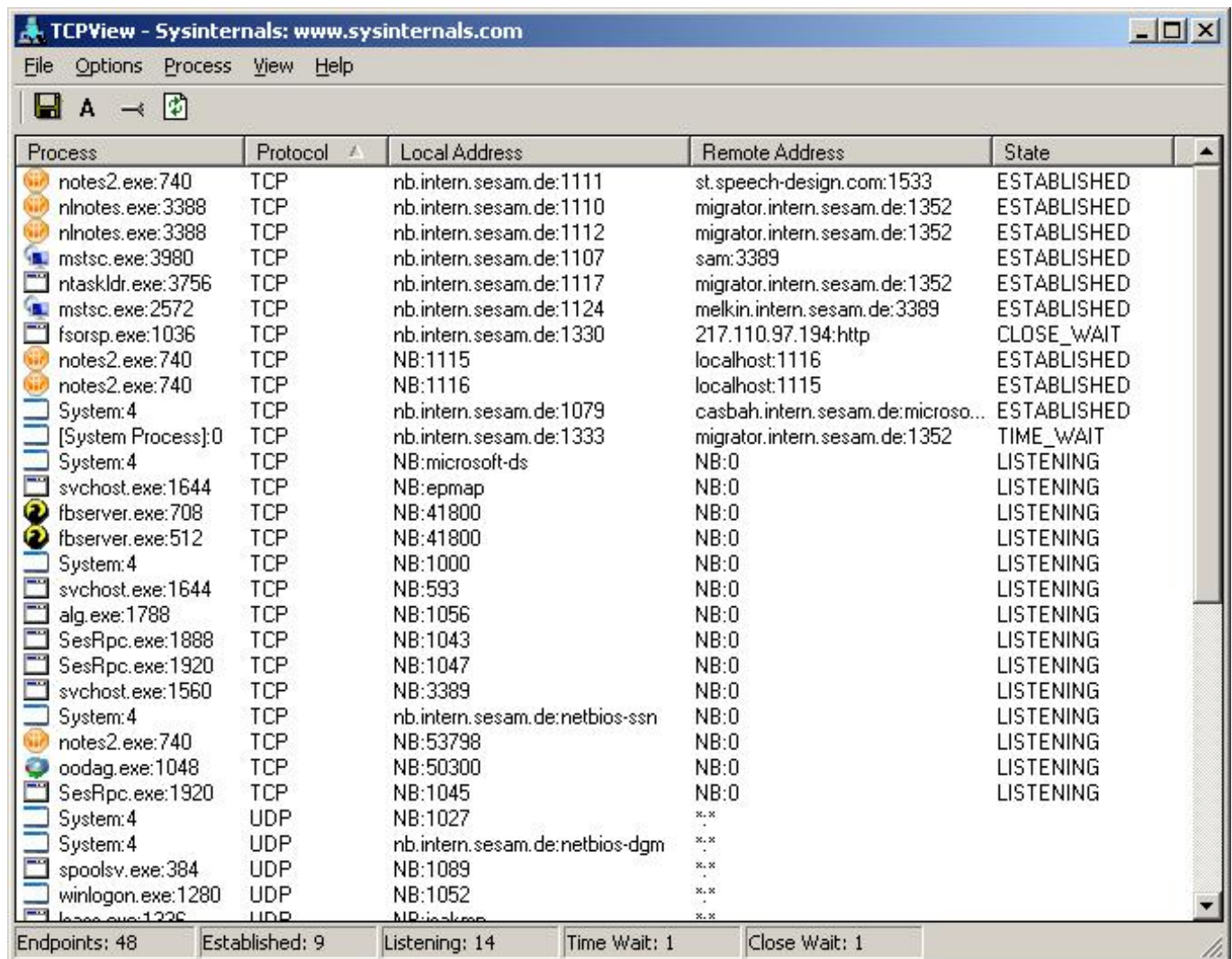
Proto Lokale Adresse Remoteadresse Status
TCP NB:epmap NB.intern.sesam.de:0 ABHÖREN
TCP NB:microsoft-ds NB.intern.sesam.de:0 ABHÖREN
TCP NB:593 NB.intern.sesam.de:0 ABHÖREN
TCP NB:1000 NB.intern.sesam.de:0 ABHÖREN
TCP NB:1043 NB.intern.sesam.de:0 ABHÖREN
TCP NB:1045 NB.intern.sesam.de:0 ABHÖREN
TCP NB:1047 NB.intern.sesam.de:0 ABHÖREN
TCP NB:3389 NB.intern.sesam.de:0 ABHÖREN
TCP NB:41800 NB.intern.sesam.de:0 ABHÖREN
TCP NB:41800 NB.intern.sesam.de:0 ABHÖREN
TCP NB:50300 NB.intern.sesam.de:0 ABHÖREN
TCP NB:nethios-ssn NB.intern.sesam.de:0 ABHÖREN
TCP NB:1079 casbah.intern.sesam.de:microsoft-ds HERGESTELLT
TCP NB:1107 sam:3389 HERGESTELLT
TCP NB:1110 migrator.intern.sesam.de:1352 HERGESTELLT
TCP NB:1111 st.speech-design.com:1533 HERGESTELLT
TCP NB:1112 migrator.intern.sesam.de:1352 HERGESTELLT
TCP NB:1117 migrator.intern.sesam.de:1352 HERGESTELLT
TCP NB:1124 melkin.intern.sesam.de:3389 HERGESTELLT
TCP NB:1189 sam:nethios-ssn HERGESTELLT
TCP NB:1203 217.110.97.194:http ZULETZT_ACK
TCP NB:1285 217.110.97.194:http SCHLIESSEN_WARTEN
TCP NB:1056 NB.intern.sesam.de:0 ABHÖREN
TCP NB:1115 localhost:1116 HERGESTELLT
TCP NB:1116 localhost:1115 HERGESTELLT
TCP NB:53798 NB.intern.sesam.de:0 ABHÖREN
UDP NB:epmap ***
UDP NB:microsoft-ds ***
UDP NB:isakmp ***
UDP NB:1025 ***
UDP NB:1027 ***
UDP NB:1044 ***
UDP NB:1046 ***
UDP NB:1089 ***
UDP NB:4500 ***
UDP NB:20830 ***
UDP NB:20831 ***
UDP NB:20832 ***
UDP NB:20833 ***
UDP NB:41799 ***
UDP NB:ntp ***
UDP NB:nethios-ns ***
UDP NB:nethios-dgm ***
UDP NB:1900 ***
UDP NB:ntp ***
UDP NB:1028 ***
```

Suche nach speziellem Port:
netstat -a | find "41800"

```
C:\>Eingabeaufforderung
H:\>netstat -a | find "41800"
TCP NB:41800 NB.intern.sesam.de:0 ABHÖREN
TCP NB:41800 NB.intern.sesam.de:0 ABHÖREN
```

Alternative zu netstat:
TCPView (www.sysinternals.com)

zeigt auch die Programme übersichtlich an, die Ports geöffnet haben



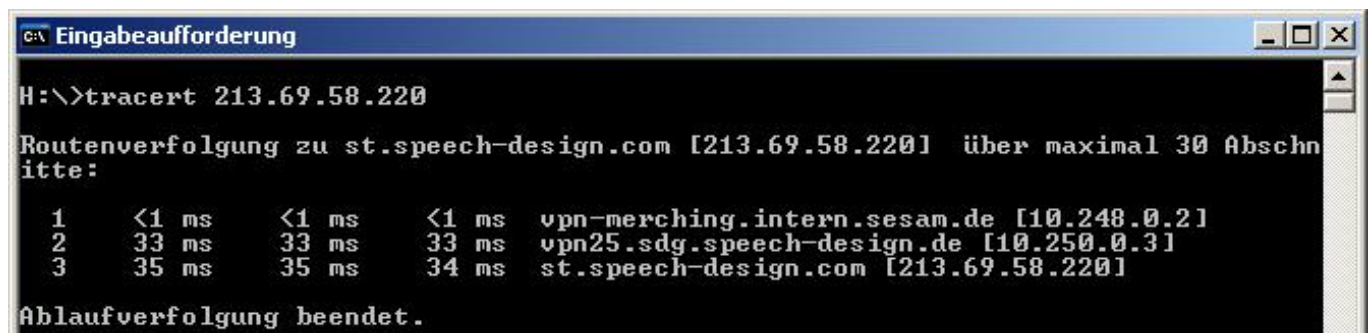
The screenshot shows the TCPView application window with the title bar "TCPView - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Options", "Process", "View", and "Help". The main window displays a table of active network connections. The table has five columns: "Process", "Protocol", "Local Address", "Remote Address", and "State". The "Process" column lists various system and user processes along with their port numbers. The "Protocol" column shows the transport protocol used (TCP or UDP). The "Local Address" and "Remote Address" columns show the IP addresses and port numbers involved in the connection. The "State" column indicates the current state of the connection (e.g., ESTABLISHED, LISTENING, CLOSE_WAIT). At the bottom of the window, there are summary statistics: "Endpoints: 48", "Established: 9", "Listening: 14", "Time Wait: 1", and "Close Wait: 1".

Process	Protocol	Local Address	Remote Address	State
notes2.exe:740	TCP	nb.intern.sesam.de:1111	st.speech-design.com:1533	ESTABLISHED
nlnotes.exe:3388	TCP	nb.intern.sesam.de:1110	migrator.intern.sesam.de:1352	ESTABLISHED
nlnotes.exe:3388	TCP	nb.intern.sesam.de:1112	migrator.intern.sesam.de:1352	ESTABLISHED
mstsc.exe:3980	TCP	nb.intern.sesam.de:1107	sam:3389	ESTABLISHED
ntaskldr.exe:3756	TCP	nb.intern.sesam.de:1117	migrator.intern.sesam.de:1352	ESTABLISHED
mstsc.exe:2572	TCP	nb.intern.sesam.de:1124	melkin.intern.sesam.de:3389	ESTABLISHED
fsorpc.exe:1036	TCP	nb.intern.sesam.de:1330	217.110.97.194:http	CLOSE_WAIT
notes2.exe:740	TCP	NB:1115	localhost:1116	ESTABLISHED
notes2.exe:740	TCP	NB:1116	localhost:1115	ESTABLISHED
System:4	TCP	nb.intern.sesam.de:1079	casbah.intern.sesam.de:microso...	ESTABLISHED
[System Process]:0	TCP	nb.intern.sesam.de:1333	migrator.intern.sesam.de:1352	TIME_WAIT
System:4	TCP	NB:microsoft-ds	NB:0	LISTENING
svchost.exe:1644	TCP	NB:epmap	NB:0	LISTENING
fbserver.exe:708	TCP	NB:41800	NB:0	LISTENING
fbserver.exe:512	TCP	NB:41800	NB:0	LISTENING
System:4	TCP	NB:1000	NB:0	LISTENING
svchost.exe:1644	TCP	NB:593	NB:0	LISTENING
alg.exe:1788	TCP	NB:1056	NB:0	LISTENING
SesRpc.exe:1888	TCP	NB:1043	NB:0	LISTENING
SesRpc.exe:1920	TCP	NB:1047	NB:0	LISTENING
svchost.exe:1560	TCP	NB:3389	NB:0	LISTENING
System:4	TCP	nb.intern.sesam.de:netbios-ssn	NB:0	LISTENING
notes2.exe:740	TCP	NB:53798	NB:0	LISTENING
oodag.exe:1048	TCP	NB:50300	NB:0	LISTENING
SesRpc.exe:1920	TCP	NB:1045	NB:0	LISTENING
System:4	UDP	NB:1027
System:4	UDP	nb.intern.sesam.de:netbios-dgm
spoolsv.exe:384	UDP	NB:1089
winlogon.exe:1280	UDP	NB:1052
lsass.exe:1228	UDP	NB:1052

Endpoints: 48 Established: 9 Listening: 14 Time Wait: 1 Close Wait: 1

trace route (tracert)

verfolgt Routen zu einem Ziel und zeigt die "Hops" an



The screenshot shows a Windows command prompt window titled "Eingabeaufforderung". The user has entered the command "H:\>tracert 213.69.58.220". The output shows the route from the local host to the destination IP address 213.69.58.220 (st.speech-design.com) over a maximum of 30 hops. The output is as follows:

```
H:\>tracert 213.69.58.220

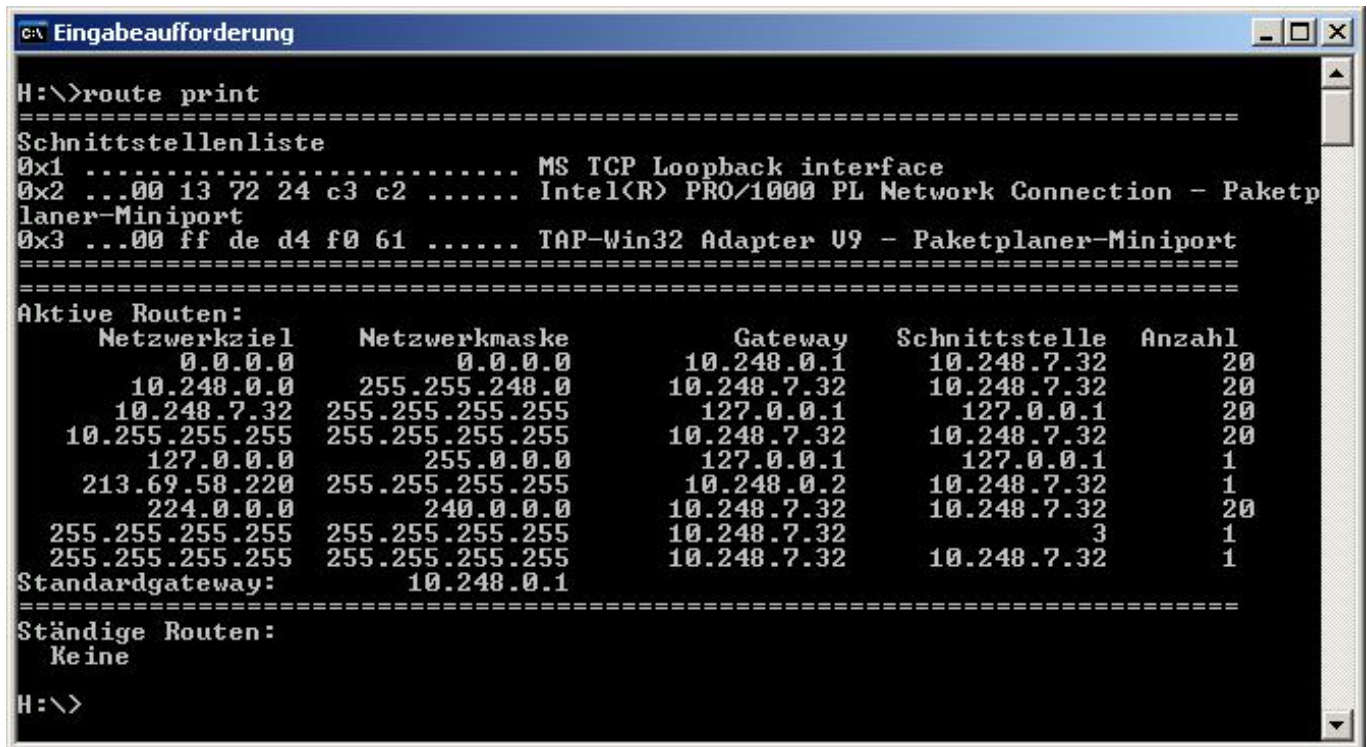
Routenverfolgung zu st.speech-design.com [213.69.58.220] über maximal 30 Abschn
itte:

 1  <1 ms    <1 ms    <1 ms    vpn-merching.intern.sesam.de [10.248.0.21]
 2  33 ms     33 ms     33 ms     vpn25.sdg.speech-design.de [10.250.0.3]
 3  35 ms     35 ms     34 ms     st.speech-design.com [213.69.58.220]

Ablaufverfolgung beendet.
```


route

zeigt und bearbeitet Routen



```
H:\>route print

=====
Schnittstellenliste
0x1 ..... MS TCP Loopback interface
0x2 ...00 13 72 24 c3 c2 ..... Intel(R) PRO/1000 PL Network Connection - Paketp
laner-Miniport
0x3 ...00 ff de d4 f0 61 ..... TAP-Win32 Adapter V9 - Paketplaner-Miniport
=====

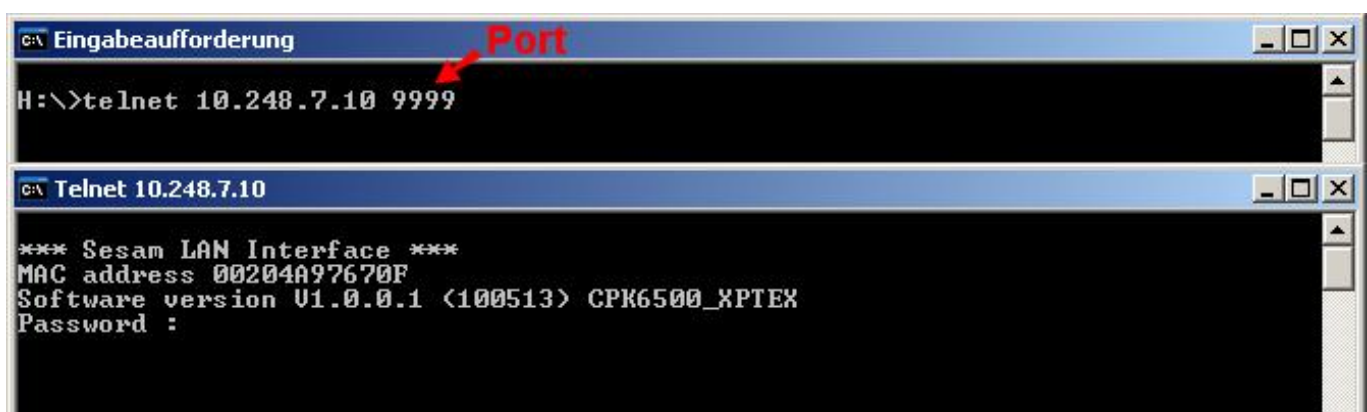
Aktive Routen:
      Netzwerkziel      Netzwerkmaske      Gateway      Schnittstelle      Anzahl
      0.0.0.0           0.0.0.0           10.248.0.1   10.248.7.32        20
      10.248.0.0       255.255.255.0     10.248.7.32  10.248.7.32        20
      10.248.7.32      255.255.255.255   127.0.0.1   127.0.0.1          20
      10.255.255.255   255.255.255.255   10.248.7.32  10.248.7.32        20
      127.0.0.0        255.0.0.0        127.0.0.1   127.0.0.1          1
      213.69.58.220    255.255.255.255   10.248.0.2   10.248.7.32        1
      224.0.0.0        240.0.0.0        10.248.7.32  10.248.7.32        20
      255.255.255.255   255.255.255.255   10.248.7.32  3                  1
      255.255.255.255   255.255.255.255   10.248.7.32  10.248.7.32        1
Standardgateway:      10.248.0.1
=====

Ständige Routen:
Keine

H:\>
```

telnet

textbasiertes Internetprotokoll, oft als Remote-Konsole verwendet
Gut um offene TCP-Ports zu prüfen



```
H:\>telnet 10.248.7.10 9999

C:\ Telnet 10.248.7.10

*** Sesam LAN Interface ***
MAC address 00204A97670F
Software version V1.0.0.1 <100513> CPK6500_XPTX
Password :
```

Offene TCP-Ports mit Telnet prüfen (Test ob Verbindung möglich):

telnet [IP-Adresse] [Port]

Wenn Port offen, bleibt Telnet mit leerem Fenster offen.

Wenn Port geschlossen oder nicht erreichbar, wird Telnet sofort beendet.