

Netzwerktechnik-6

Christian Zahler

6 Das Transfer/Transmission Control Protocol (TCP)

Das TCP ist ein verbindungsorientiertes Protokoll; es bildet die Verbindung zwischen IP und Anwendung.

Aufgaben

- garantiert den sicheren Transport von Daten im Netz
- gewährleistet, dass kein Datenpaket verlorengeht und dass alle Pakete in der richtigen Reihenfolge ankommen

Merkmale

- voll duplex, bidirektionale (virtuelle) Verbindung
- Benutzer sieht Datenstrom, keine Pakete
- Zuordnung der Pakete zur entsprechenden Anwendung
- geregelter Verbindungsauf-/abbau

Der TCP-Header: Natürlich fügt auch das TCP-Protokoll spezielle Daten hinzu – wieder in Form eines Headers – der wie folgt aufgebaut ist:

| | | | |
|-----------------|------------|----------------|--------------|
| Sender-Port | | Empfänger-Port | |
| Sequenznummer | | | |
| Quittungsnummer | | | |
| Datenabstand | Reserviert | Flags | Fenstergröße |
| Prüfsumme | | Urgent-Zeiger | |
| Optionen | | Füllzeichen | |

TCP-Header

- **Sender/Empfänger-Port** (je 16 Bit): Endpunkte der Verbindung
- **Sequ./Quitt.nummer** (32 Bit): Synchronisation der Daten
- **Datenabstand** (4 Bit): Länge des Headers in 32 Bit
- **Flags** (6 Bit): Aktionen (Aufbau, Ende, ...)
- **Fenstergröße** (16 Bit): Größe des verfügbaren Empfängerbuffers (bei Stop des Senders)
- Prüfsumme (16 Bit): Korrektheit des Headers
- Urgent-Zeiger (16 Bit): zur Verarbeitung von wichtigen Daten
- Optionen (24 Bit), Füllzeichen (6 Bit)

Ports

Auf TCP/IP basieren viele verschiedene Dienste wie FTP, Mail, News, DNS, etc. Um nun diese Dienste innerhalb der Protokollfamilie TCP/IP voneinander abzugrenzen, werden diese Dienste den sogenannten Ports zugewiesen. Ein Port ist nichts anderes als eine zusätzliche Kennung, die durch das TCP-Protokoll übertragen wird. Derzeit sind rund 65.536 Ports definiert, welche sich auf verschiedene Bereiche aufteilen.

Well known Ports 0 - 1023 festgelegt in RFC 1340 (Request for Comment, „Bitte um Kommentar“, de facto eine „Internet-Norm“)

Registered Ports 1024 - 49151
Dynamic and/or private Ports 49152 - 65535

Im Verzeichnis c:\winnt\System32\etc (Linux: /etc) befindet sich eine Datei mit dem Namen SERVICES, in der die Portnummern für bekannte Dienste gemäß IANA abgelegt in Server sind:

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Diese Datei enthält die Portnummern für bekannte Dienste gemäß IANA.
#
# Format:
#
# <Dienstname> <Portnummer>/<Protokoll> [Alias...] [#<Kommentar>]
#
echo 7/tcp
echo 7/udp
discard 9/tcp sink null
discard 9/udp sink null
sysstat 11/tcp users #Active users
sysstat 11/tcp users #Active users
daytime 13/tcp
daytime 13/udp
qotd 17/tcp quote #Quote of the day
qotd 17/udp quote #Quote of the day
chargen 19/tcp ttytst source #Character generator
chargen 19/udp ttytst source #Character generator
ftp-data 20/tcp #FTP, data
ftp 21/tcp #FTP. control
telnet 23/tcp
smtp 25/tcp mail #Simple Mail Transfer Protocol
time 37/tcp timeserver
time 37/udp timeserver
rlp 39/udp resource #Resource Location Protocol
nameserver 42/tcp name #Host Name Server
nameserver 42/udp name #Host Name Server
nicname 43/tcp whois
domain 53/tcp #Domain Name Server
domain 53/udp #Domain Name Server
bootps 67/udp dhcps #Bootstrap Protocol Server
bootpc 68/udp dhcps #Bootstrap Protocol Client
tftp 69/udp #Trivial File Transfer
gopher 70/tcp
finger 79/tcp
http 80/tcp www www-http #World Wide Web
kerberos 88/tcp krb5 kerberos-sec #Kerberos
kerberos 88/udp krb5 kerberos-sec #Kerberos
hostname 101/tcp hostnames #NIC Host Name Server
iso-tsap 102/tcp #ISO-TSAP Class 0
rlogin 107/tcp #Remote Telnet Service
pop2 109/tcp postoffice #Post Office Protocol - Version 2
pop3 110/tcp #Post Office Protocol - Version 3
sunrpc 111/tcp rpcbind portmap #SUN Remote Procedure Call
sunrpc 111/udp rpcbind portmap #SUN Remote Procedure Call
auth 113/tcp ident tap #Identification Protocol
uucp-path 117/tcp
nntp 119/tcp usenet #Network News Transfer Protocol
ntp 123/tcp #Network Time Protocol
epmap 135/tcp loc-srv #DCE endpoint resolution
epmap 135/udp loc-srv #DCE endpoint resolution
netbios-ns 137/tcp nbname #NETBIOS Name Service
netbios-ns 137/udp nbname #NETBIOS Name Service
netbios-dgm 138/udp nbdatagram #NETBIOS Datagram Service
netbios-ssn 139/tcp nbssession #NETBIOS Session Service
imap 143/tcp #Internet Message Access Protocol
pcmail-srv 158/tcp #PCMail Server
snmp 161/udp #SNMP
snmptrap 162/udp snmp-trap #SNMP trap
print-srv 170/tcp #Network PostScript
bgp 179/tcp #Border Gateway Protocol
irc 194/tcp #Internet Relay Chat Protocol
ipx 213/udp #IPX over IP
ldap 389/tcp #Lightweight Directory Access Protocol
https 443/tcp MCom
https 443/udp MCom
microsoft-ds 445/tcp
microsoft-ds 445/udp
kpasswd 464/tcp # Kerberos (v5)
kpasswd 464/udp # Kerberos (v5)
ike 500/udp #Internet Key Exchange
exec 512/tcp #Remote Process Execution
biff 512/udp #Remote Login
login 513/tcp #Remote Login
who 513/udp whod
cmd 514/tcp shell
syslog 514/udp
printer 515/tcp spooler
talk 517/udp
ntalk 518/udp
efs 520/tcp #Extended File Name Server
router 520/udp route routed
timed 525/udp timeserver
tempo 526/tcp newdate
courier 530/tcp rpc
conference 531/tcp chat
netnews 532/tcp readnews
netwall 533/udp #For emergency broadcasts
uucp 540/tcp
klogin 543/tcp #Kerberos login
kshell 544/tcp #Kerberos remote shell
new-rwho 550/udp new-who
remotefs 556/tcp rfs rfs_server
rmonitor 560/udp rmonitord
monitor 561/udp
ldaps 636/tcp #LDAP over TLS/SSL
doom 666/tcp #Doom Id Software
doom 666/udp #Doom Id Software
kerberos-adm 749/tcp #Kerberos administration
kerberos-adm 749/udp #Kerberos administration
kerberos-iv 750/udp #Kerberos version IV
kpop 1109/tcp #Kerberos POP
phone 1167/udp #Conference calling
ms-sql-s 1433/tcp #Microsoft-SQL-Server
ms-sql-s 1433/udp #Microsoft-SQL-Server
ms-sql-m 1434/tcp #Microsoft-SQL-Monitor
ms-sql-m 1434/udp #Microsoft-SQL-Monitor
wins 1512/tcp #Microsoft Windows Internet Name Service
wins 1512/udp #Microsoft Windows Internet Name Service
ingres 1524/tcp ingres
l2tp 1701/udp #Layer Two Tunneling Protocol
pptp 1723/tcp #Point-to-point tunnelling protocol
radius 1812/udp #RADIUS authentication protocol
radacct 1813/udp #RADIUS accounting protocol
nfsd 2049/udp nfs #NFS server
knetd 2053/tcp #Kerberos de-multiplexor
man 9535/tcp #Remote Man Server
```

Wenn nötig, ist die Portnummer auch anzugeben (mit einem Doppelpunkt nach der eigentlichen Adresse). Ein Beispiel ist der bekannte Ö3-Chat:



Die Syntax in der URL-Zeile lautet allgemein:

Servertyp://servername.domain.tld:portnummer

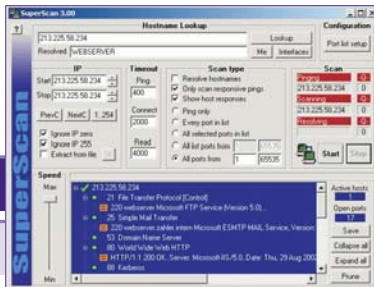
Die IP-Adresse gemeinsam mit der Portnummer (diese Kombination wird auch als „Socket“

bezeichnet) gestattet die eindeutige Identifikation eines Dienstes, der auf einem PC läuft. So hätte also der WWW-Dienst auf einem Server mit der IP 203.225.56.204 mit der TCP-Anschlussnummer 80 die komplette Identifikation 203.225.56.204:80.

Die genaue Kenntnis der TCP-Ports ist vor allem auch wichtig, um die Sicherheit eines Netzwerkes zu gewährleisten. Mit sogenannten „Port-Scannern“ ist es leicht möglich, herauszufinden, welche TCP-Ports auf einem Rechner oder Router freigegeben sind. Dies wiederum ermöglicht Hackern den unerwünschten Zugriff auf Firmennetze.

Beispiel für einen Port-Scanner: „Superscan“

Download von Superscan zum Beispiel unter <http://www.foundstone.com/>



7 TCP/IP-Diagnose- und Konfigurationsprogramme

7.1 ping ("Packet Internet Groper")

Versucht, vier IP-Pakete an einen Host-Rechner zu senden. Zweck: Überprüfung der Funktionsfähigkeit von Netzwerkverbindungen. Die PING-Anforderung wird vom ICMP (Internet Control Message Protocol) durchgeführt.

Der Befehl ping arbeitet wie folgt:

Die Netzwerkverbindungen zu einem oder mehreren Remotecomputern werden überprüft, indem ICMP-Echopakete an den Host gesendet und Echo-Antwortpakete als Antwort erwartet werden.

Nach dem Senden jedes Pakets wird eine Sekunde gewartet.

Die Anzahl der empfangenen und übertragenen Pakete wird ausgegeben.

Jedes empfangene Paket wird mit der übertragenen Nachricht verglichen. Standardmäßig werden vier Echopakete mit je 32 Byte Daten (eine sich wiederholende Großbuchstabenfolge) übertragen.

Mit ping können Sie den Computernamen und die IP-Adresse des Computers überprüfen. Wenn die IP-Adresse bestätigt wird, nicht aber der Computernamen, besteht u. U. ein Namensauflösungsproblem. Prüfen Sie in diesem Fall, ob sich der abgefragte Hostname in der lokalen Hostsdatei oder in der DNS-Datenbank befindet.

Syntax

```
ping [-t] [-a] [-n Anzahl] [-l Größe] [-f] [-i Gültigkeitsdauer]
[-v Diensttyp] [-r Anzahl] [-s Anzahl] [[-j Hostliste]
[-k Hostliste]] [-w Zeitlimit] Zielliste
Optionen:
-t Sendet fortlaufend Ping-Signale zum angegebenen Host.
Geben Sie STRG-UNTERR ein, um die Statistik anzuzeigen.
Geben Sie STRG-C ein, um den Vorgang abzubrechen.
-a Löst Adressen in Hostnamen auf.
-n n Anzahl Anzahl zu sendender Echoanforderungen
-l Länge Pufferlänge senden
-f Setzt Flag für "Don't Fragment".
-i TTL Gültigkeitsdauer (Time To Live)
-v TOS Diensttyp (Type Of Service)
-r Anzahl Route für Anzahl der Abschnitte aufzeichnen
-s Anzahl Zeiteintrag für Anzahl Abschnitte
-j Hostliste "Loose Source Route" gemäß Hostliste
-k Hostliste "Strict Source Route" gemäß Hostliste
-w Zeitlimit Zeitlimit in Millisekunden für eine Rückmeldung
```

Beispiel

```
C:\>ping www.aon.at
Ping WS011507.highway.telekom.at [195.3.96.73] mit 32 Bytes Daten:
Antwort von 195.3.96.73: Bytes=32 Zeit=30ms TTL=248
Antwort von 195.3.96.73: Bytes=32 Zeit=20ms TTL=248
Antwort von 195.3.96.73: Bytes=32 Zeit=20ms TTL=248
Antwort von 195.3.96.73: Bytes=32 Zeit=30ms TTL=248
Ping-Statistik für 195.3.96.73:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 20ms, Maximum = 30ms, Mittelwert = 25ms
```

7.2 ipconfig

Gibt Informationen über die Windows IP-Konfiguration aus.

Syntax

```
ipconfig [/? | /all | /release [Adapter] | /renew [Adapter]
| /flushdns | /registerdns
| /showclassid Adapter
| /setclassid Adapter [Klassenkennung] ]
Adapter: Ganzer Name oder Zeichen mit "*" und "?", wobei
"*" für beliebig viele und "?" für ein Zeichen steht.
Optionen
/? Zeigt diesen Hilfetext an.
/all Zeigt die vollständigen Konfigurationsinformationen an.
/release Gibt die IP-Adresse für den angegebenen Adapter frei.
/renew Erneuert die IP-Adresse für den angegebenen Adapter.
/flushdns Leert den DNS-Auflösungs-cache.
/registerdns Aktualisiert alle DHCP-Leases und registriert DNS-Namen.
/displaydns Zeigt den Inhalt des DNS-Auflösungs-caches an.
/showclassid Zeigt alle DHCP-Klassenkennungen an, die für diesen Adapter zugelassen sind.
/setclassid Ändert die DHCP-Klassenkennung.
```

Standardmäßig wird nur die IP-Adresse, die Subnetzmaske und das Standardgateway für jeden an TCP/IP gebundenen Adapter angezeigt.

Wird bei /RELEASE oder /RENEW kein Adaptername angegeben, so werden die IP-Adressen von allen an TCP/IP gebundenen Adapter freigegeben oder erneuert.

Wird bei /SETCLASSID keine Klassenkennung angegeben, dann wird die Klassenkennung gelöscht.

Beispiele

```
> ipconfig ... Zeigt Informationen an.
> ipconfig /all ... Zeigt detaillierte Informationen an.
> ipconfig /renew ... Erneuert IP-Adressen für alle Adapter.
> ipconfig /renew EL* ... Erneuert IP-Adressen für Adapter mit Namen EL...
> ipconfig /release *ELINK*21*... Gibt alle entsprechenden Adapter frei, z.B. ELINK-21, ELINK121karte usw.
```

Beispiel 1: Ausgabe ohne Parameter /all

```
C:\>ipconfig
Windows 2000-IP-Konfiguration
Ethernetadapter "LAN-Verbindung":
Verbindungsspezifisches DNS-Suffix:
IP-Adresse. . . . . : 172.16.200.210
Subnetzmaske. . . . . : 255.255.255.0
Standardgateway. . . . . : 172.16.200.1
```

Beispiel 2: Ausgabe mit Parameter /all

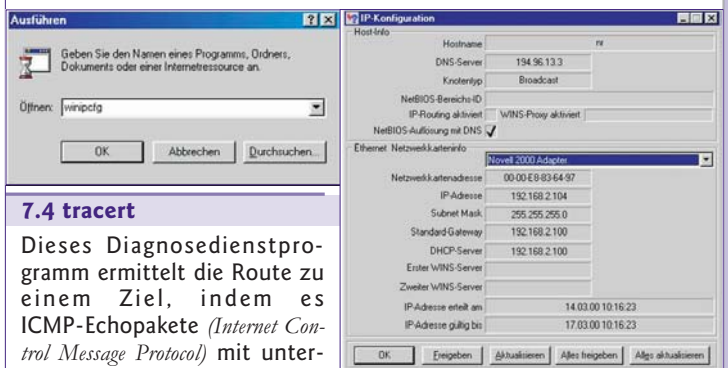
```
Windows XP-IP-Konfiguration
Hostname. . . . . : zahler1
Primäres DNS-Suffix. . . . . : zahler.at
Knotentyp. . . . . : Broadcastadapter
IP-Routing aktiviert. . . . . : Ja
WINS-Proxy aktiviert. . . . . : Nein
DNS-Suffixsuchliste. . . . . : zahler.at
Ethernetadapter "LAN-Verbindung":
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : 3Com EtherLink XL 10/100 PCI-TX-NIC (3C905B-X)
Physische Adresse. . . . . : 00-50-04-81-70-9C
DHCP-aktiviert. . . . . : Nein
IP-Adresse. . . . . : 213.225.58.236
Subnetzmaske. . . . . : 255.255.255.248
Standardgateway. . . . . : 213.225.58.233
DNS-Server. . . . . : 213.225.58.235
Ethernetadapter "LAN-Verbindung 2":
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : AVN FRITZ!web PPP over ISDN
Physische Adresse. . . . . : 00-07-77-64-09-32
DHCP-aktiviert. . . . . : Nein
IP-Adresse. . . . . : 192.168.120.254
Subnetzmaske. . . . . : 255.255.255.0
Standardgateway. . . . . :
DNS-Server. . . . . : 192.168.120.252 192.168.120.253
```

7.3 winipcfg

Dieses Programm stellt eine grafische Variante von IPCONFIG dar und ist in folgenden Windows-Versionen enthalten:

- Windows 95
- Windows 98
- Windows ME

Am besten über [Start] – [Ausführen] aufrufen.



7.4 tracert

Dieses Diagnosedienstprogramm ermittelt die Route zu einem Ziel, indem es ICMP-Echopakete (Internet Control Message Protocol) mit unterschiedlichen TTL-Werten (Time-To-Live) sendet. Von jedem Router auf dem Pfad wird erwartet, dass er den TTL-Wert für ein Paket vor dem Weiterleiten um mindestens 1 verkleinert; so dass der TTL-Wert die Anzahl der Abschnitte angibt. Wenn der TTL-Zähler für ein Paket den Wert Null erreicht, sendet der Router eine "ICMP-Zeitüberschreitung"-Nachricht zur Quelle zurück. Tracert ermittelt die Route, indem es das erste Echopaket mit dem TTL-Wert 1 sendet und den TTL-Wert bei jeder folgen-

den Übertragung um Eins erhöht, bis das Ziel antwortet oder der TTL-Höchstwert erreicht ist. Die Route wird durch Prüfen der "ICMP-Zeitüberschreitung"-Nachrichten ermittelt, die von den dazwischenliegenden Routern zurückgesendet werden. Einige Router werfen jedoch Pakete mit abgelaufenen TTL-Werten ohne Warnung und sind nicht sichtbar für `tracert`.

Syntax

```
tracert [-d] [-h Abschnitte max] [-j Hostliste] [-w Zeitlimit] Zielname
Optionen:
-d Adressen nicht in Hostnamen auflösen
-h Abschnitte max Max. Anzahl an Abschnitten bei Zielsuche
-j Hostliste "Loose Source Route" gemäß Hostliste
-w Zeitlimit Zeitlimit in Millisekunden für eine Antwort
```

Beispiel

```
C:\>tracert www.wienerwald.org
Routenverfolgung zu www.wienerwald.org [216.218.196.178] über maximal 30 Abschnitte:
 0 <10 ms 10 ms <10 ms 172.16.200.1
 1 <10 ms 10 ms <10 ms vianet-stpolten-gw01.via.at [194.96.211.18]
 2 <10 ms 10 ms 10 ms vianet-stpolten-gw00.via.at [194.96.211.17]
 3 <10 ms 10 ms 20 ms vianet-head-gw04.via.at [194.96.210.5]
 4 10 ms 20 ms 31 ms vianet-vix-gw01-s1-0.via.at [194.96.160.2]
 5 70 ms 30 ms 50 ms vix.above.net [193.203.0.45]
 6 50 ms 30 ms 90 ms core1-vix-stm-1.vie.above.net [208.184.102.49]
 7 320 ms 100 ms 60 ms fra-vie-stm1-1.fra.above.net [208.184.102.130]
 8 40 ms 40 ms 60 ms lhr-fra-stm-1.lhr.above.net [208.184.102.134]
 9 60 ms 90 ms 110 ms core1-linx-oc3-1.lhr.above.net [216.200.254.81]
10 50 ms 70 ms 140 ms iad-lhr-stm.iad.above.net [216.200.254.77]
11 130 ms 230 ms 221 ms mae-west-1ad-oc3.above.net [216.200.0.69]
12 210 ms 230 ms 230 ms mae-west-core1-oc3-1.mae.above.net [209.133.31.178]
13 220 ms 231 ms 220 ms 100tx-f6-1.mae-west.he.net [207.126.96.98]
14 361 ms 230 ms 220 ms gige-g9-0.gsr12012.sjc.he.net [216.218.130.1]
15 210 ms 231 ms 220 ms launch.server101.com [216.218.196.178]
16 221 ms 230 ms 220 ms
Ablaufverfolgung beendet.
```

7.5 pathping

Kombination der Befehle `PING` und `TRACERT`; steht nur in Windows-Betriebssystemen ab Windows 2000 zur Verfügung.

Ein Tool zum Verfolgen von Routen, das neben Features der Befehle `ping` und `tracert` weitere Informationen bietet, die durch diese Befehle nicht zur Verfügung gestellt werden. Der Befehl `pathping` sendet über einen gewissen Zeitraum Datenpakete an jeden Router auf dem Pfad zu einem Ziel. Anhand der von jedem Abschnitt zurückübermittelten Datenpakete werden dann bestimmte Statistiken berechnet. Da der Befehl `pathping` den Paketverlust bei jedem Router und jeder Verbindung anzeigt, können Sie feststellen, welche Router oder Verbindungen Netzwerkprobleme verursachen.

Beispiel

```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>pathping www.wienerwald.org
Routenverfolgung zu www.wienerwald.org [216.218.210.195] über maximal 30 Abschnitte:
0 zahler1.zahler.intern [212.152.140.14]
1 c58wmichu2-1o1.net.uta.at [212.152.140.1]
2 c72wmich10-f0-0.net.uta.at [212.152.150.2]
3 c120wmich1-g0-0.net.uta.at [62.218.1.93]
4 c76wrdrh2-g2-2.net.uta.at [212.152.192.14]
5 uta0001-p116-sw1.vie1-p7-2-bgp2.abovenet.at [212.69.161.4]
6 so-2-3-0.crl.vie2.at.mfnx.net [208.184.231.93]
7 so-7-0-2.crl.lhr3.uk.mfnx.net [208.184.231.37]
8 so-7-0-0.crl.dca2.us.mfnx.net [64.125.31.186]
9 so-3-0-0.mpr3.sjc2.us.mfnx.net [208.184.233.133]
10 pos5-0.mpr1.pao1.us.mfnx.net [208.184.233.142]
11 209.249.24.136.he.net [209.249.24.136]
12 gige-g9-0.gsr12012.sjc.he.net [216.218.130.1]
13 fe0-0-bordercore0.SJC.server101.com [216.218.132.34]
14 .scorpion.server101.com [216.218.210.195]
Berechnung der Statistiken dauert ca. 350 Sekunden...
Quelle zum Abs. Knoten/Verbindung
Abs. Zeit Verl./Ges. % Verl./Ges. % Adresse
0 0 0/100=0% 0/100=0% zahler1.zahler.intern [212.152.140.14] 0/100=0%
1 47ms 0/100=0% 0/100=0% c58wmichu2-1o1.net.uta.at [212.152.140.1] 0/100=0%
2 45ms 0/100=0% 0/100=0% c72wmich10-f0-0.net.uta.at [212.152.150.2] 0/100=0%
3 45ms 0/100=0% 0/100=0% c120wmich1-g0-0.net.uta.at [62.218.1.93] 0/100=0%
4 48ms 0/100=0% 0/100=0% c76wrdrh2-g2-2.net.uta.at [212.152.192.14] 0/100=0%
5 47ms 0/100=0% 0/100=0% uta0001-p116-sw1.vie1-p7-2-bgp2.abovenet.at [212.69.161.4] 0/100=0%
6 48ms 0/100=0% 0/100=0% so-2-3-0.crl.vie2.at.mfnx.net [208.184.231.93] 0/100=0%
7 135ms 0/100=0% 0/100=0% so-7-0-2.crl.lhr3.uk.mfnx.net [208.184.231.37] 0/100=0%
8 206ms 1/100=1% 1/100=1% so-7-0-0.crl.dca2.us.mfnx.net [64.125.31.186] 0/100=0%
9 275ms 0/100=0% 0/100=0% so-3-0-0.mpr3.sjc2.us.mfnx.net [208.184.233.133] 1/100=1%
10 270ms 3/100=3% 2/100=2% pos5-0.mpr1.pao1.us.mfnx.net [208.184.233.142] 0/100=0%
11 219ms 1/100=1% 0/100=0% 209.249.24.136.he.net [209.249.24.136] 1/100=1%
12 219ms 2/100=2% 0/100=0% gige-g9-0.gsr12012.sjc.he.net [216.218.130.1] 1/100=1%
13 220ms 3/100=3% 0/100=0% fe0-0-bordercore0.SJC.server101.com [216.218.132.34] 0/100=0%
14 220ms 3/100=3% 0/100=0% scorpion.server101.com [216.218.210.195]
Ablaufverfolgung beendet.
```

7.6 arp

Ändert und zeigt die Übersetzungstabellen für IP-Adressen/physische Adressen an, die vom ARP (*Address Resolution Protocol*) verwendet werden.

Parameter

```
ARP -s IP_Adr Eth_Adr [Schnittst]
ARP -d IP_Adr [Schnittst]
ARP -a [IP_Adr] [-N Schnittst]
```

-a Zeigt aktuelle ARP-Einträge durch Abfrage der Protokoll-daten an. Falls IP Adr angegeben wurde, werden die IP- und physische Adresse für den angegebenen Computer angezeigt. Wenn mehr als eine Netzwerkschnittstelle ARP verwendet, werden die Einträge für jede ARP-Tabelle angezeigt.
-g Gleiche Funktion wie -a.
IP_Adr Gibt eine Internet-Adresse an.
-N Schnittst Zeigt die ARP-Einträge für die angegebene Netzwerkschnittstelle an.
-d Löscht den durch IP_Adr angegebenen Host-Eintrag.
-s Fügt einen Host-Eintrag hinzu und ordnet die Internet-Adresse der physischen Adresse zu. Die physische Adresse wird durch 6 hexadezimale, durch Bindestrich getrennte Bytes angegeben. Der Eintrag ist permanent.
Eth_Adr Gibt eine physische Adresse (Ethernet-Adresse) an.
Schnittst Gibt, falls vorhanden, die Internet-Adresse der Schnittstelle an, deren Übersetzungstabelle geändert werden soll.
Sonst wird die erste geeignete Schnittstelle verwendet.

Beispiel

```
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Fügt einen statischen Eintrag hinzu.
> arp -a ..... Zeigt die Arp-Tabelle an.
Beispiel:
C:\>arp -a
Schnittstelle: 172.16.200.210 on Interface 0x1000003
Internetadresse Physisk. Adresse Typ
172.16.200.7 00-00-e8-83-6c-a5 dynamisch
```

7.7 netstat

Zeigt Protokollstatistik und aktuelle TCP/IP-Netzwerkverbindungen an.

```
NETSTAT [-a] [-e] [-n] [-s] [-p Proto] [-r] [Intervall]
-a Zeigt den Status aller Verbindungen an. (Verbindungen des Servers werden normalerweise nicht angezeigt).
-e Zeigt die Ethernetstatistik an. Kann mit der Option -s kombiniert werden.
-n Zeigt Adressen und Portnummern numerisch an.
-p Proto Zeigt Verbindungen für das mit Proto angegebene Protokoll an. Proto kann TCP oder UDP sein. Bei Verwendung mit der Option -s kann Proto TCP, UDP oder IP sein.
-r Zeigt den Inhalt der Routingtabelle an.
-s Zeigt Statistik protokollweise an. Standardmäßig werden TCP,UDP und IP angezeigt. Mit der Option -p können Sie dies weiter einschränken.
Intervall Zeigt die gewählte Statistik nach der mit Intervall angegebenen Anzahl von Sekunden erneut an. Drücken Sie STRG+C zum Beenden der Intervallanzeige. Ohne Intervallangabe werden die aktuellen Konfigurationsinformationen einmalig angezeigt.
```

Beispiel für netstat

```
C:\>netstat -a
Aktive Verbindungen
Proto Lokale Adresse Remoteadresse Status
TCP r10:epmap r10:0 ABHÖREN
TCP r10:microsoft-ds r10:0 ABHÖREN
TCP r10:1025 r10:0 ABHÖREN
TCP r10:1027 r10:0 ABHÖREN
TCP r10:netbios-ssn r10:0 ABHÖREN
UDP r10:epmap *.*
UDP r10:microsoft-ds *.*
UDP r10:1026 *.*
UDP r10:netbios-ns *.*
UDP r10:netbios-dgm *.*
UDP r10:isakmp *.*
```

7.8 nbtstat

Zeigt Protokollstatistik und aktuelle TCP/IP-Verbindungen an, die NBT (NetBIOS über TCP/IP) verwenden.

```
NBTSTAT [-a Remotename] [-A IP-Adresse] [-c] [-n] [-r] [-R] [-RR] [-s] [Intervall] ]
-a Zeigt die Namentabelle des mit Namen angegebenen Remotecomputers an.
-A Zeigt die Namentabelle des mit IP-Adressen angegebenen Remotecomputers an.
-c Zeigt Inhalt des Remotenamencache mit IP-Adressen an.
-n Zeigt lokale NetBIOS-Namen an.
-r Zeigt mit Broadcast und WINS aufgelöste Namen an.
-R Lädt Remotecache-Namentabelle neu.
-S Zeigt Sitzungstabelle mit den Ziel-IP-Adressen an.
-s Zeigt Sitzungstabelle mit Computer NetBIOS-Namen an, die aus den Ziel-IP-Adressen bestimmt wurden.
-RR (ReleaseRefresh) Sendet Namensfreigabe-Pakete an WINS und startet die Aktualisierung.
Remotename Name des Remotehosts
IP-Adresse Punktierte Dezimalschreibweise einer IP-Adresse
Intervall Zeigt die ausgewählte Statistik nach der angegebenen Anzahl Sekunden erneut an. Drücken Sie STRG+C zum Beenden der Intervallanzeige.
```

Beispiel

```
C:\>nbtstat -A 172.16.200.210
LAN-Verbindung:
Knoten-IP-Adresse: [172.16.200.210] Bereichskennung: []
NetBIOS-Namentabelle des Remotecomputers
Name Typ Status
-----
R10 <00> UNIQUE Registriert
R10 <20> UNIQUE Registriert
MCSE <00> GROUP Registriert
MCSE <1E> GROUP Registriert
R10 <03> UNIQUE Registriert
```

7.9 hostname

Zeigt den Hostnamen des lokalen Computers an.

Beispiel

```
C:\>hostname
r10
```