# 12 Diagnose und Konfiguration

***Christian Zahler***

## 12.1 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 Computername, besteht unter Umständen ein Namenauflösungsproblem. 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-UNTRBR 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 WS01IS07.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
```

```
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 Ab-
schnitte:

  1   <10 ms    10 ms   <10 ms  172.16.200.1
  2   <10 ms    10 ms   <10 ms  vianet-stpolten-gw01.via.at [194.96.211.18]
  3   <10 ms    10 ms    10 ms  vianet-stpolten-gw00.via.at [194.96.211.17]
  4    10 ms    20 ms    20 ms  vianet-head-gw04.via.at [194.96.210.5]
  5    70 ms    30 ms    31 ms  vianet-vix-gw01-s1-0.via.at [194.96.160.2]
  6    50 ms    30 ms    50 ms  vix.above.net [193.203.0.45]
  7   320 ms   100 ms    90 ms  core1-vix-stm-1.vie.above.net [208.184.102.49]
  8    40 ms    40 ms    60 ms  fra-vie-stm1-1.fra.above.net [208.184.102.130]
  9    60 ms    90 ms    60 ms  lhr-fra-stm-1.lhr.above.net [208.184.102.134]
 10    50 ms    70 ms   110 ms  core1-linx-oc3-1.lhr.above.net [216.200.254.81]
 11   130 ms   130 ms   140 ms  iad-lhr-stm4.iad.above.net [216.200.254.77]
 12   210 ms   230 ms   221 ms  mae-west-iad-oc3.above.net [216.200.0.69]
 13   220 ms   231 ms   230 ms  mae-west-core1-oc3-1.maew.above.net
[209.133.31.178]
 14   361 ms   230 ms   220 ms  100tx-f6-1.mae-west.he.net [207.126.96.98]
 15   210 ms   231 ms   220 ms  gige-g9-0.gsr12012.sjc.he.net [216.218.130.1]
 16   221 ms   230 ms   220 ms  launch.server101.com [216.218.196.178]

Ablaufverfolgung beendet.
```

kann er nun als erreichbar markiert werden und die Pakete, auf die er verweist, können ausgelöst werden.

Der Knoten antwortet in diesem Beispiel mit seiner MAC-Adresse 02-BF-C0-A8-0A-80. Die Zuordnung IPv6/MAC-Adresse wird nun im Neighbor Cache gespeichert.

Der Neighbor Cache kann folgendermaßen angezeigt werden:

```
C:\>Netsh interface ipv6 show neighbors
Internetadresse              Physische Adresse   Typ
-------------------------------------------  -----------
fe80::1c0:3453:e3c3:98d9     00-18-f3-b3-c6-cd  Abgelaufen
fe80::d36:c38d:9570:d45      00-18-f3-b3-c7-43  Abgelaufen
fe80::11bd:89f9:ea3f:d482    00-18-f3-a0-bb-e8  Test
fe80::61d1:85a:19f2:f41b     00-00-00-00-00-00  Nicht erreichbar
fe80::cd58:3ef9:3dc3:d355    00-1b-fc-dc-9b-4c  Abgelaufen (Router)
fe80::d852:e5bc:859b:585b    02-bf-c0-a8-0a-80  Abgelaufen
fe80::f148:7657:2901:9a6a    00-1b-fc-dc-9a-d4  Abgelaufen
ff02::2                      33-33-00-00-00-02  Permanent
ff02::c                      33-33-00-00-00-0c  Permanent
ff02::16                     33-33-00-00-00-16  Permanent
ff02::1:2                    33-33-00-01-00-02  Permanent
ff02::1:3                    33-33-00-01-00-03  Permanent
ff02::1:ff01:9a6a            33-33-ff-01-9a-6a  Permanent
ff02::1:ff3f:d482            33-33-ff-3f-d4-82  Permanent
ff02::1:ff64:4bb2            33-33-ff-64-4b-b2  Permanent
ff02::1:ff70:d45             33-33-ff-70-0d-45  Permanent
ff02::1:ff9b:585b            33-33-ff-9b-58-5b  Permanent
ff02::1:ffac:4579            33-33-ff-ac-45-79  Permanent
ff02::1:ffac:da00            33-33-ff-ac-da-00  Permanent
ff02::1:ffc3:98d9            33-33-ff-c3-98-d9  Permanent
```

Löschen des Nachbarn-Caches:

```
C:\>Netsh interface ipv6 delete neighbors
```

Das **ping**-Tool steht auch unter Linux zur Verfügung, unterstützt jedoch andere Optionen und Parameter.

## 12.2 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 folgenden 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 verwerfen jedoch Pakete mit abgelaufenen TTL-Werten ohne Warnung und sind nicht sichtbar für tracert.

Das **tracert**-Tool steht auch unter Linux zur Verfügung, unterstützt jedoch andere Optionen und Parameter.

## 12.3 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.

## 12.4 arp

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

***Beispiel:***

```
Microsoft Windows 2000 [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-lo1.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  c76wrdh2-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.cr1.vie2.at.mfnx.net [208.184.231.93]
  7  so-7-0-2.cr1.lhr3.uk.mfnx.net [208.184.231.37]
  8  so-7-0-0.cr1.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                                          zahler1.zahler.intern [212.152.140.14]        0/ 100 =  0%   |
  1   47ms     0/ 100 =  0%     0/ 100 =  0%  c58wmichu2-lo1.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%  c76wrdh2-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.cr1.vie2.at.mfnx.net [208.184.231.93]
                                 0/ 100 =  0%   |
  7  135ms     0/ 100 =  0%     0/ 100 =  0%  so-7-0-2.cr1.lhr3.uk.mfnx.net [208.184.231.37]
                                 0/ 100 =  0%   |
  8  206ms     1/ 100 =  1%     1/ 100 =  1%  so-7-0-0.cr1.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.
```

**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 Netzwerk-
                schnittstelle 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       Physikal. Adresse     Typ
  172.16.200.7          00-00-e8-83-6c-a5     dynamisch
```

## 12.5 netstat

Zeigt Protokollstatistik und aktuelle TCP/IP-Netzwerkverbindungen an.

```
Syntax:
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 angege-
                benen 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         *:*
```

## 12.6 nbtstat

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

```
Syntax:
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
```

## 12.7 hostname

Zeigt den Hostnamen des lokalen Computers an.➪

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

# 13 Netzwerkanalyse

*Christian Zahler*

**Sniffer** erstellen Kopien von Frames (Pakete auf OSI-Schicht 2), um deren Header bzw. Inhalt analysieren zu können.

### Marktübersicht

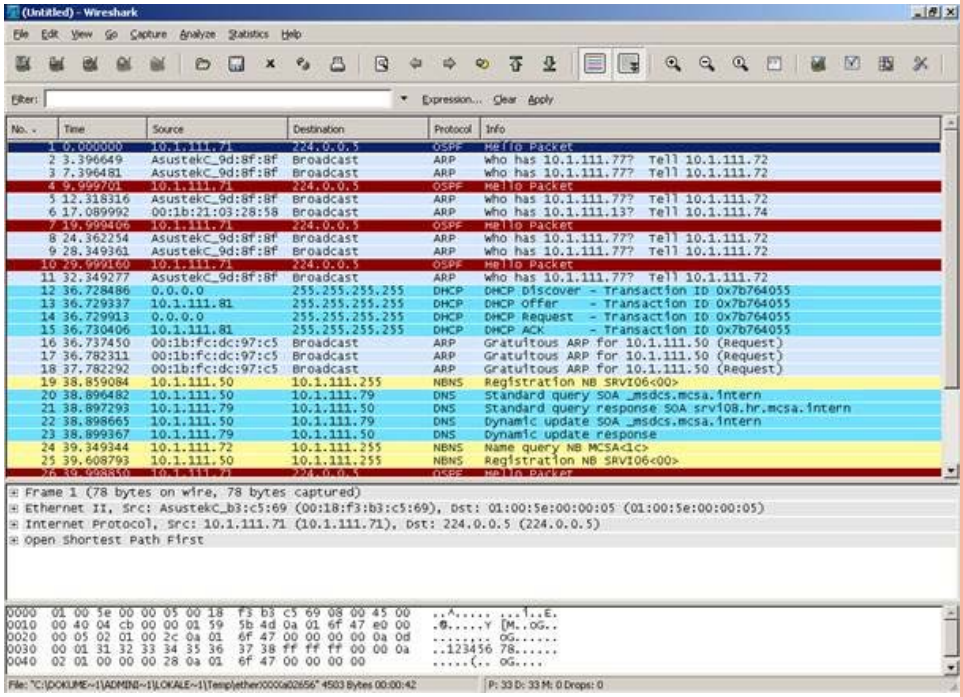
**Freie Produkte**

- Wireshark (ehemals: ethereal; oft mit Treiber WinPCap kombiniert)
- Ettercap
- NETCORtools (TCP Trace basierend)
- Tcpdump

**Proprietäre Produkte**

- Microsoft Network Monitor(Bestandteil von Microsoft Windows Server)
- Clearsight Analyzer (Clearsight Networks)
- EtherPeek, OmniPeek, GigaPeek (WildPackets)
- LANdecoder32 (Triticom)
- NetSpector (INAT)
- NetVCR (Niksun)
- NetworkActiv PIAFCTM
- Observer (Network Instruments)
- OptiView (Fluke Networks)
- Sniffer (Network General)
- TraceCommander (Synapse Networks)
- webSensor und webProbe (Moniforce)

Sehr gerne wird Wireshark eingesetzt.




## ⇨12.8 Bindung von Netzwerkprotokollen an die Netzwerkkarte unter Windows

Damit Netzwerkkartentreiber und Netzwerkprotokoll ordnungsgemäß zusammenarbeiten, müssen die Protokolltreiber (zum Beispiel für TCP/IP) an den Netzwerkkartentreiber **gebunden** werden. Diese Bindung kann folgendermaßen angezeigt und geändert werden:

Öffnen Sie das Systemsteuerungs-Objekt „Netzwerkverbindungen“ und wählen Sie den Menüpunkt **Erweitert** – **Erweiterte Einstellungen** (gegebenenfalls drücken Sie bei Vista die ALT-Taste, um die Pulldown-Menüs anzuzeigen).