

Dienstprogramme zur TCP/IP-Fehlerbehebung

Christian Zahler

1. 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           UNIQUE      Registriert
R10           UNIQUE      Registriert
MCSE          GROUP       Registriert
MCSE          <1E> GROUP     Registriert
R10           UNIQUE      Registriert
MAC Adresse = 00-00-E8-83-3C-FC
```

2. IPCONFIG

Windows 2000-IP-Konfiguration

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-Auflösungscache.
/registerdns Aktualisiert alle DHCP-Leases und
          registriert DNS-Namen.
/displaydns Zeigt den Inhalt des
          DNS-Auflösungscaches 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,
                    ELINKi21karte usw.
```

Beispiel

```
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
```

3. 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

```
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 *.*
```



4. HOSTNAME

Zeigt den Hostnamen des lokalen Computers an.

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

5. ARP

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

```
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
        physikalische 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
        Hosteintrag. Die IP_Adr
        kann mit dem '*'-Platzhalter versehen
        werden, um alle Hosts zu löschen.
    -s Fügt einen Hosteintrag hinzu und ordnet die
        Internetadresse der physikalischen Adresse
        zu. Die physikalische Adresse wird
        durch 6 hexadezimale, durch Bindestrich
        getrennte Byte angegeben.
        Der Eintrag ist permanent.
    Eth_Adr Gibt eine physikalische Adresse
        (Ethernetadresse) an.
    Schnittst Gibt, falls vorhanden, die Internetadresse
        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 statischen
                                                Eintrag hinzu.
> arp -a Zeigt die ARP-Tabelle an.
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
```

6. PING

verwendet einen ICMP-Echo-Request - sendet IP-Paket an einen Rechner mit der Bitte um Rücksendung

```
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 sender 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 = 0
    (0% Verlust), Ca. Zeitangaben in Millisek.:
    Minimum = 20ms, Maximum = 30ms, Mittelwert = 25ms
```

7. ROUTE

Manipuliert die Netzwerkroutingtabellen.

```
ROUTE [-f] [-p] [Befehl [Ziel] [MASK Netzmaske] [Gateway]
[METRIC Anzahl] [IF Schnittstelle]
```

```
-f Löscht alle Gatewayeinträge in
Routingtabellen.
Wird der Parameter mit einem der Befehle
verwendet, werden die Tabellen vor der
Befehlsausführung gelöscht.
-p Wird der Parameter mit dem "ADD"-Befehl
verwendet, wird eine Route unabhängig von
Neustarts des Systems verwendet. Standard-
mäßig ist diese Funktion deaktiviert,
wenn das System neu gestartet wird.
Dies wird ignoriert für alle
anderen Befehle, die beständige Routen
beeinflussen. Diese Funktion wird
von Windows 95 nicht unterstützt.
Befehl Auswahlmöglichkeiten:
    PRINT Druckt eine Route
    ADD Fügt eine Route hinzu
    DELETE Löscht eine Route
    CHANGE Ändert eine bestehende Route
Ziel Gibt den Host an.
MASK Gibt an, dass der folgende Parameter ein
Netzwerkwert ist.
Netzmaske Gibt einen Wert für eine Subnetzmaske
für den Routeneintrag
an. Ohne Angabe wird die Standardeinstellung
255.255.255.255 verwendet.
Gateway Gibt ein Gateway an.
Schnittstelle Schnittstellenummer der angegebenen Route.
METRIC Gibt den Anzahl/Kosten-Wert für das Ziel an.
```

Alle symbolischen Namen, die für das Ziel verwendet werden, werden in der Datei der Netzwerkdatenbank NETWORKS angezeigt. Symbolische Namen für Gateway finden Sie in der Datei der Hostnamendatenbank HOSTS. Bei den Befehlen PRINT und DELETE können Platzhalter für Ziel und Gateway verwendet werden, (Platzhalter werden durch "*" angegeben), oder Sie können auf die Angabe des Gatewayparameters verzichten. Falls Ziel "*" or "?" enthält, wird es als Shellmuster bearbeitet und es werden nur übereinstimmende Zielrouten gedruckt. Der Platzhalter "*" wird mit jeder Zeichenkette überprüft, und "?" wird mit jedem Zeichen überprüft.

Beispiele: 157.*.1, 157.*, 127.*, *224*.

Diagnoseanmerkung

Eine ungültige MASK erzeugt einen Fehler unter folgender Bedingung: (DEST & MASK) != DEST.

Beispiel> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80. Die Route konnte nicht hinzugefügt werden: Der angegebene Maskenparameter ist ungültig. (Destination & Mask) != Destination.

Beispiele

```
> route PRINT
> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1
METRIC 3 IF 2
                Ziel^      ^Maske      ^Gateway
Metric^
Schnittstelle^
Sollte "IF" nicht angegeben sein,
wird versucht die beste
Schnittstelle für das angegebene Gateway zu finden.
```



```
> route PRINT
> route PRINT 157*   Zeigt passende Adressen mit 157* an.
> route DELETE 157.0.0.0
> route PRINT
```

8. TRACERT

Zur Routenverfolgung im Internet.

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
```

```
C:\>tracert www.wienerwald.org
Routenverfolgung zu www.wienerwald.org [216.218.196.178]
über maximal 30 Abschnitte:
  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.

9. NSLOOKUP

Beispiel 1

```
C:\>nslookup
*** Der Servername für die Adresse 194.96.13.3 konnte nicht
gefunden werden:
Server failed
*** Die Standardserver sind nicht verfügbar.
Standardserver: UnKnown
Address: 194.96.13.3
> www.noe.wifi.at.
Server: UnKnown
Address: 194.96.13.3
Name: www.noe.wifi.at
Address: 194.96.13.5
> set type=any          Damit können erweiterte Informationen
                        abgerufen werden!
> www.noe.wifi.at
Server: UnKnown
Address: 194.96.13.3
www.noe.wifi.at internet address = 194.96.13.5
noe.wifi.at     nameserver = ns.noe.wifi.at
noe.wifi.at     nameserver = ns1.via.at
ns.noe.wifi.at  internet address = 194.96.13.3
ns1.via.at      internet address = 194.
```

Beispiel 2

```
Beachten Sie den Punkt am Ende der Adresse (Root Domain!)
C:\>nslookup www.microsoft.com.
*** Der Servername für die Adresse 194.96.13.3 konnte nicht
gefunden werden:
Server failed
*** Die Standardserver sind nicht verfügbar.
Server: UnKnown
Address: 194.96.13.3
Nicht autorisierte Antwort:
Name: microsoft.com
Addresses: 207.46.130.149, 207.46.130.45, 207.46.131.137,
207.46.131.30
207.46.130.14
Aliases: www.microsoft.com
```

Beispiel 3

```
> www.sbg.wifi.at
Server: UnKnown
Address: 194.96.13.3
Nicht autorisierte Antwort:
www.sbg.wifi.at canonical name = WEBWIFI.sbg.wifi.at
sbg.wifi.at     nameserver = ns2.sbg.wifi.at
sbg.wifi.at     nameserver = ns.sbg.wifi.at
ns2.sbg.wifi.at internet address = 193.83.60.252
ns.sbg.wifi.at  internet address = 193.83.60.251
> WEBWIFI.sbg.wifi.at
Server: UnKnown
Address: 194.96.13.3
Nicht autorisierte Antwort:
WEBWIFI.sbg.wifi.at internet address = 193.83.60.233
sbg.wifi.at     nameserver = ns2.sbg.wifi.at
sbg.wifi.at     nameserver = ns.sbg.wifi.at
ns2.sbg.wifi.at internet address = 193.83.60.252
ns.sbg.wifi.at  internet address = 193.83.60.251
```

Beispiel 4: www.via.at

```
C:\>nslookup
> set type=any
> www.via.at
Server: UnKnown
Address: 194.96.13.3
Nicht autorisierte Antwort:
www.via.at internet address = 194.96.203.221
via.at     nameserver = ns1.via.at
via.at     nameserver = ns2.via.at
ns1.via.at internet address = 194.41.60.10
ns2.via.at internet address = 194.41.60.16
> 221.203.96.194.in-addr.arpa.  Achtung: Man muss die
gefunden Adresse
von hinten eingeben!
Server: UnKnown
Address: 194.96.13.3
Nicht autorisierte Antwort:
```

```
221.203.96.194.in-addr.arpa name = www.via.at
203.96.194.in-addr.arpa nameserver = ns1.via.at
203.96.194.in-addr.arpa nameserver = ns2.via.at
ns1.via.at internet address = 194.41.60.10
ns2.via.at internet address = 194.41.60.16
```

Beispiel 5: Auflistung aller Rechner in einer Zone

```
C:\>nslookup
> ls noe.wifi.at
[UnKnown]
noe.wifi.at. NS server = ns.noe.wifi.at
noe.wifi.at. NS server = ns1.via.at
ls215510 A 194.96.13.135
ls215508 A 194.96.13.133
ls215511 A 194.96.13.136
ls215509 A 194.96.13.134
ls215512 A 194.96.13.137
ls215513 A 194.96.13.138
www2 A 194.96.13.3
ls216601 A 194.96.13.139
ls216602 A 194.96.13.140
ls216603 A 194.96.13.141
ls216604 A 194.96.13.142
...
```

Den kompletten Ausdruck der Ausgabe von `nslookup` für den Name-Server `noe.wifi.at` finden Sie bei der Web-Version dieses Artikels.