9 Internet Protocol Version 6 (IPv6)

Christian Zahler

Quelle: www.ipv6-net.de

Durch den rasch steigenden Bedarf an IP-Adressen ist absehbar, dass der nutzbare Adressraum von IPv4 früher oder später erschöpft sein wird. Vor allem aus diesem Grund wurde IPv6 (Version 6 des Internet Protokolls, auch: IPng für „*next generation*“) entwickelt. Es verwendet 128 Bit zur Speicherung von Adressen, damit sind

$2^{128} = 256^{16}$ (= 340.282.366.920.938.463.463.374.607.431.768.211.456 ≈ 3,4 10^{38})

Adressen darstellbar. Diese Zahl reicht aus, um für jeden Quadratmeter der Erdoberfläche mindestens 665.570.793.348.866.943.898.599 (6,65.10^{23}) IP-Adressen bereitzustellen. Damit sollten in absehbarer Zukunft keine Adressraumprobleme bei der Verwendung von IPv6 zu befürchten sein.

Windows Server 2003 unterstützt bereits IPv6. Der neue TCP/IP-Stack in den Betriebssystemen Windows Vista/Windows 7 und Windows Server 2008 (R2) beinhaltet IPv6, das somit nicht mehr deinstalliert werden kann.

IPv6 verwendet zur Darstellung seiner IP-Adressen das Hexadezimalsystem in einer Adresslänge von 128 Bit. Eine solche IPv6-Adresse könnte beispielsweise so aussehen:

```
3ffe:400:89AB:381C:7716:AA91:0000:0001
```

Ein derartiger vierstelliger Block steht dabei für einen 16 bit-Wert.

Um eine IPv6-Adresse wie die angegebene verkürzt darzustellen, kann man auf die Nullen in einer Gruppe verzichten:

```
3ffe:400:89AB:381C:7716:AA91::1.
```

Beachten Sie aber, dass ein doppelter Doppelpunkt nur ein einziges Mal pro IPv6-Adresse vorkommen darf.

Für Adressbereiche verwendet man – ähnlich wie bei IPv4 – den ersten Teil der IPv6-Adresse. IPv6 unterstützt keine Kennungen für Subnetze variabler Länge; der Netzwerkanteil beträgt immer 64 bit.

Statt

```
3ffe:400:89AB:381C:7716:AA91::1/64
```

schreibt man einfach

```
3ffe:400:89AB:381C:7716:AA91::1
```

9.1 IPv6-Adresstypen

- **Unicast-Adresse**: stellt eine einzelne Schnittstelle dar.
  - **Globale Unicast-Adressen**: sind im Internet eindeutig, stellen also die Nachfolger der öffentlichen IPv4-Adressen dar.
  - **Link-Local Unicast Addresses**, deutsch: **Verbindungslokale Unicast-Adressen**: werden mit Hilfe der IPv6-Autokonfiguration zugewiesen und verlassen die lokale Verbindung nicht. Sie entsprechen daher den IPv4-APIPA-Adressen (169.254.0.0/16). Die ersten 64 bit sind fix vorgegeben, die hinteren 64 bit geben eine eindeutige Schnittstelle in der lokalen Verbindung an. Verbindungslokale Adressen können wiederverwendet werden, das bedeutet, dass zwei verschiedene Schnittstellen auf unterschiedlichen Verbindungen dieselbe Adresse haben können. Deshalb wird eine zusätzliche Kennung angegeben (Zonen-ID), die angibt, welcher Verbindung die Adresse zugewiesen ist.
  - **Unique Local Unicast Addresses (ULAs)**, deutsch: **Eindeutige lokale Unicast-Adressen (RFC 4193):** Solche Adressen entsprechen den privaten Adressen von IPv4.Dabei wird zwischen lokal generierten ULA mit dem Präfix fd und global zugewiesenen eindeutigen ULA mit dem Präfix fc unterschieden. Struktur:
    - 8 bit: vorgegeben
    - 40 bit: globale ID (zufällig generierter Wert, der einen Standort innerhalb der Organisation repräsentiert)
    - 16 bit: Subnet-ID
    - 64 bit: Host-ID
- **Multicast-Adresse:** IPv6-Pakete mit Multicast-Adresszielen werden an alle Schnittstellen ausgeliefert, die diese Adresse annehmen (also funktioniert Multicasting in IPv6 praktisch genau so wie in IPv4.)
- **Anycast-Adresse:** identifiziert mehrere Schnittstellen; Pakete mit Anycast-Zieladressen werden an die am nächsten gelegene Schnittstelle (gemessen als Routingabstand) gesendet. Momentan werden solche Adressen nur Routern zugewiesen, und auch dort nur als Zieladressen.

Eine Broadcast-Übertragung gibt es bei IPv6 nicht mehr; diese Funktion wird von Multicast übernommen.

- **Präfixe siehe Tabelle oben.**
- **Wohlbekannte Multicast-Adressen (siehe Tabelle auf der nächsten Seite).**

Ein weiterer Vorteil von IPv6 ist die gegenüber IPv4 stark vereinfachte Headerstruktur, die eine merkbar schnellere Bearbeitung am den Router ermöglicht.

Die Loopback-Adresse lautet ::1.

Adresstyp	Hexadezimal	Binärer Präfix
Globale Unicastadresse	2000::/3	001
Globale Unicastadresse, die an Provider vergeben werden; diese delegieren Subnetze daraus an ihre Kunden	2001::	001
6to4-Adressen	2002::	001
Verbindungslokale Unicastadresse	fe80::/64	1111 1110 0100 0000 0000 0000 0000 0000 0000 0000 0000 0000
Standortlokale Unicastadresse (veraltet, werden nun als globale Unicasts behandelt)	fec0::/10	1111 1110 11
Eindeutige lokale Unicastadresse	fc00::/7 (also: fc00::/8 und fd00::/8)	1111 110
IPv4-mapped IPv6 (die letzten 32 bits enthalten die IPv4-Adresse)	0:0:0:0:0:ffff::/96	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1111 1111 1111 1111

Übersicht über Adresstypen und ihre Präfixe

Multicast-Bereich	Hexadezimal	Gültigkeitsbereich	Verwendungszweck
Alle Knoten	FF01::1	Schnittstellenlokal	Entspricht dem IPv4-Broadcast
Alle Knoten	FF02::1	Verbindungslokal	Entspricht dem IPv4-Broadcast
Alle Router	FF01::2	Schnittstellenlokal	Adressiert alle Router in einem Bereich
Alle Router	FF02::2	Verbindungslokal	Adressiert alle Router in einem Bereich
Alle Router	FF05::2	Standortlokal	Adressiert alle Router in einem Bereich

Tabelle: Übersicht über Adresstypen und ihre Präfixe:

9.2 Statische Konfiguration von eindeutigen lokalen IPv6-Adressen

Windows

Konfiguration in der grafischen Oberfläche **siehe Bild rechts**.

Die Konfiguration erfolgt unter der Command Shell wie folgt:

IPv6-Konfiguration:

```
netsh interface ipv6 add address interface=LAN-Verbindung
address=FC00:1::4A type=unicast

netsh interface ipv6 add route prefix=::/0 interface=LAN-
Verbindung address=FC00:1::21b8

netsh interface ipv6 add dnsserver interface=LAN-Verbindung
address=FC00:1::47
```

Kurzschreibweise:

```
netsh interface ipv6 add address LAN-Verbindung FC00:1::4A

netsh interface ipv6 add route ::/0 LAN-Verbindung FC00:1::21b8

netsh interface ipv6 add dnsserver LAN-Verbindung FC00:1::47
```

Linux

Analog zur IPv4-Konfiguration.

9.3 Anzeigen von IPv6-Konfigurationen

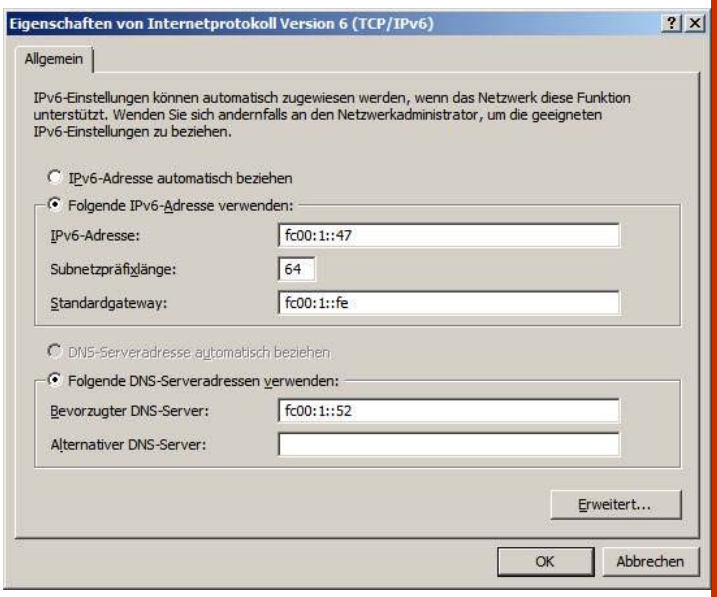
Die Anzeige der aktuellen Konfiguration erfolgt unter Windows mit dem ipconfig-Tool, unter Linux mit ifconfig oder ip.

```
C:\>ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter LAN-Verbindung:

   Verbindungsspezifisches DNS-Suffix: zahler.at
   Verbindungslokale IPv6-Adresse  . : fe80::b91b:f8f0:ccbe:4723%11
   IPv4-Adresse  . . . . . . . . . . : 192.168.3.117
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : 192.168.3.14
```

Hier sieht man, dass der Ethernet-Netzwerkkarte eine verbindungslokale IPv6-Adresse über Autokonfiguration zugewiesen wurde. Interessant ist der Zusatz `%11`, der die Zonen-ID darstellt. Die Zonen-ID gibt an, zu welcher Netzwerkschnittstelle diese Adresse gehört. Eine Liste aller Netzwerkschnittstellen mit den zugehörigen IDs lässt sich folgendermaßen ermitteln:

```
C:\>netsh interface ipv6 show interface

Idx     Met         MTU          State                Name
---  ----------  ----------  ------------  ---------------------------
  1          50  4294967295  connected     Loopback Pseudo-Interface 1
 12          50        1280  disconnected  isatap.zahler.at
 11          20        1500  connected     LAN-Verbindung
 14          50        1280  disconnected  isatap.{B78FCE4F-8FA1-467A-9A17-
A610E11014D8}
```

Aus der hier angeführten Liste kann man ersehen, dass `%11` sich auf die Schnittstelle `"LAN-Verbindung"` bezieht.



9.4 Aufbau des IPv6-Headers

Version (4 Bits): Enthält immer den Wert '6' bei IPv6. Dieses Feld dient der Software zur Unterscheidung verschiedener IP-Versionen.

Class (8 Bits): Gibt die Priorität der zu übermittelnden Daten an.

Flow-Label (20 Bits): Dieses Feld kennzeichnet einen Datenstrom zwischen Sender und Empfänger. Alle Pakete die zu einem bestimmten Datenstrom gehören, tragen in diesem Feld den gleichen Wert.

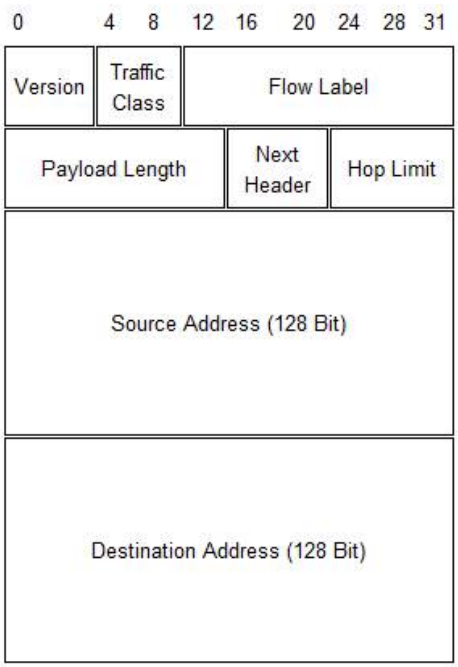
Payload Length (16 Bits): Hier wird die Länge des Datenpakets (nach dem ersten Header) angegeben.

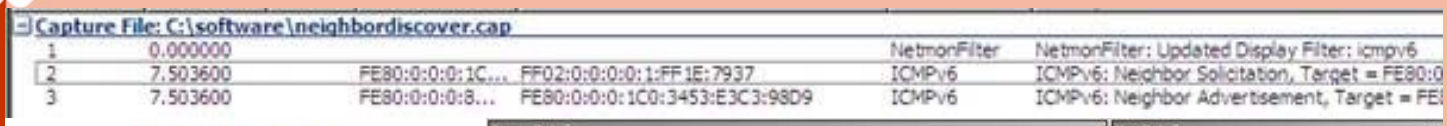
Next (8 Bits): Gibt den Typ des nächsten Headers an. Der Wert '59' signalisiert, dass keine weiteren Header bzw. Daten folgen.

Hop-Limit (8 Bits): Legt fest, nach wie vielen Durchgängen das Paket vom Router, zur Vermeidung von Schleifen, verworfen werden soll.

Source Address (128 Bits): Beinhaltet die Absenderadresse.

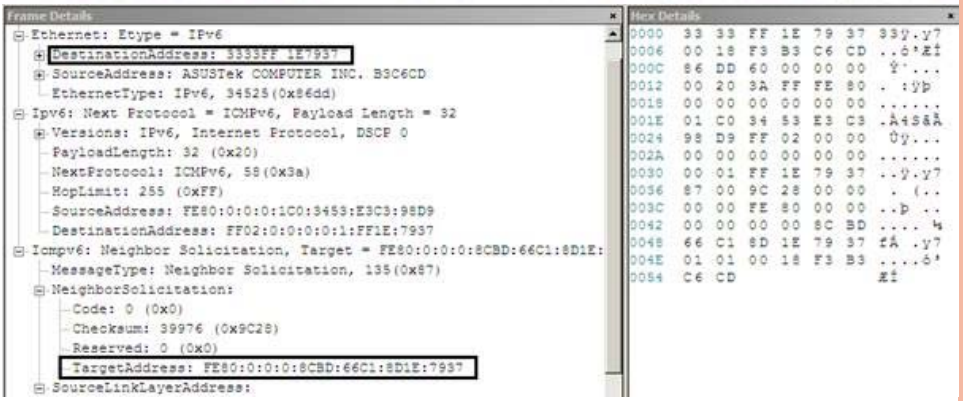
Destination Address (128 Bits): Beinhaltet die Empfängeradresse. IPv6-Header (Abbildung: Wikipedia)





Neighbor-Solicitation-Schema

+	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
0	Type	Code	Prüfsumme	
32	Reserviert			
64	Zieladresse			
96				
128				
160				
...	Optionen			



Im Moment unterstützen besonders europäische und asiatische Institutionen und Firmen die Entwicklung und Verbreitung von IPv6. Das ist wohl mit der Tatsache, dass etwa 75% des IPv4-Adressraums den USA zugeteilt wurde, zu erklären. Im Moment unterstützen zwar nur wenige Dienste das Internet Protokoll der Zukunft, aber gerade bei der Entwicklung neuer Dienste in diesem Bereich wird es in den nächsten Jahren einen enormen Zuwachs geben.

9.5 Neighbor Discovery Protocol (NDP)

Zur Ermittlung der MAC-Adresse kann IPv6 nicht mehr ARP *(Address Resolution Protocol)* verwenden, da ARP auf Broadcasts aufbaut und Broadcasts in IPv6 nicht mehr vorgesehen sind.

Stattdessen wird das *Neighbor Discovery Protocol* verwendet, das auf ICMPv6 beruht.

Für NDP muss der Knoten für jedes Interface folgende Informationen verwalten:

- Im **Neighbor Cache** werden Adressen verwaltet, an die etwas gesendet wurde und die sich im selben Netzwerk befinden. Zu jedem Eintrag einer IPv6-Adresse steht ihre Link-Layer-Adresse. Auch weitere Informationen werden hier verwaltet, wie zum Beispiel Pointer auf Pakete, die auf die Adressauflösung warten, Informationen für die Erreichbarkeitsprüfung oder ob es ein Router ist.
- Im **Destination Cache** werden Adressen verwaltet, an die etwas gesendet wurde. Für jeden Eintrag wird, per Link auf den Neighbor Cache, gespeichert, welches der nächste Hop ist, den ein Paket nehmen soll.
- In der **Prefix List** werden die Präfixe verwaltet, die auf dem selben Netz gültig sind. Jeder Eintrag, außer der zur link-lokalen Adresse, hat ein Ablaufdatum. Somit bleiben nur Netze in der Liste, die von einem Router verkündet werden.

Neighbor-Advertisement-Schema

+	Bits 0–7				Bits 8–15	Bits 16–23	Bits 24–31
0	Type				Code	Prüfsumme	
32	R	S	O	Reserviert	Reserviert		
64	Zieladresse						
96							
128							
160							
...	Optionen						

- In der **Default Router List** werden alle Router verwaltet, die für das Interface bekannt sind. Die Einträge verweisen auf Einträge im *Neighbor Cache*. Zusätzlich haben sie ein Ablaufdatum, sodass alte Router verschwinden und nur die erhalten bleiben, die ihre Anwesenheit verkünden.

Die Informationen zum Erstellen dieser Listen werden per ICMPv6 *(Internet Control Message Protocol V6)* ausgetauscht. NDP definiert zu diesem Zweck fünf ICMPv6-Typen.

Ermittlung von MAC-Adressen, wenn sich der Zielknoten im selben Netz befindet

Grober Ablauf: Eine Anfrage-ICMPv6-Nachricht *(Neighbor Solicitation)* wird an eine spezielle Multicast-Adresse des Zielknotens gesendet; dieser sendet als Antwort eine *Neighbor Advertisement*-Nachricht, die seine MAC-Adresse enthält.

Im Detail: Um die MAC-Adresse eines Knotens zu ermitteln, wird eine *Neighbor-Solicitation*-Nachricht per IPv6-Multicast an die sog. *Solicited Nodes*-Adresse des Ziels versendet. Anzumerken ist, dass auf OSI Schicht 2-Ebene ebenfalls Multicast genutzt wird - jeder IPv6-Knoten muss also auf MAC-Ebene nicht nur auf seine originäre feste Adresse (z.B. Ethernet) hören, sondern auch auf einer für seiner MAC-Adresse beruhenden spezifischen Multicast-MAC-Adresse. Im *Neighbor-Solicitation*-Paket ist dann die vollständige gesuchte IPv6-Adresse in den Nutzdaten enthalten, und nur der Knoten mit der gleichen Adresse antwortet darauf.

Beispiel: Die MAC-Adresse des Knotens mit der link-lokalen Adresse

`FE80::8CBD:66C1:8D1E:7937`

soll ermittelt werden, da Frames an diesen Knoten gesendet werden sollen.

Es wird daher zunächst die *„solicited-node multicast address“* dieses Empfängers ermittelt. Dazu nimmt man die letzten drei Oktette der IPv6-Adresse und stellt FF02::1:FF00:0000/104 voran.

Also ergibt sich als *„solicited-node multicast address“* von

`FE80::8CBD:66C1:8D1E:7937`

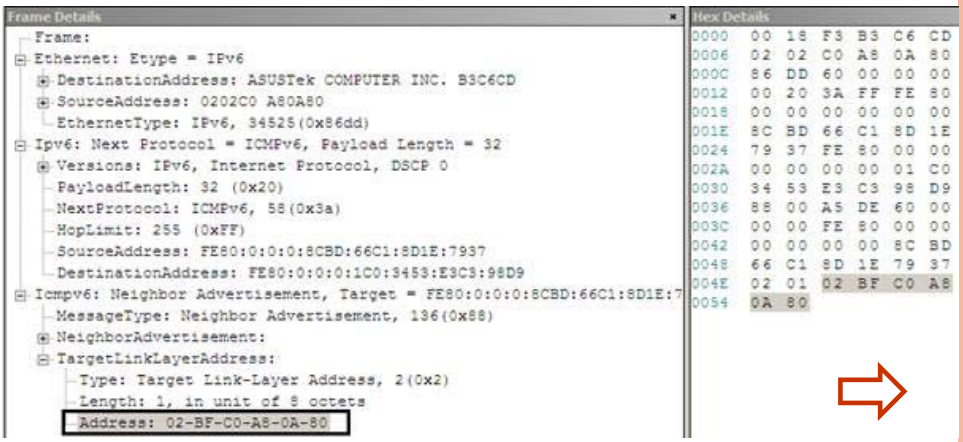
der Wert

`FF02::1:FF1E:7937`.

An diese Multicast-Adresse wird nun eine Neighbor Solicitation Nachricht versendet. Die Chance, dass sich mehrere Knoten betroffen fühlen, ist sehr gering. Trotzdem wird im ICMPv6-Feld *„TargetAddress“* auch noch die komplette IPv6-Adresse mitgeschickt, damit auch wirklich nur ein einziger Knoten antwortet.

Auch die Multicast-MAC-Ziel-Adresse wird ähnlich ermittelt. Auch hier nimmt man die letzten 3 Oktette der Ethernet-MAC-Adresse (diese stellen die eigentliche Multicast-Gruppe dar) und stellt `33:33:FF` voran. Als Ziel-MAC wird also `33:33:FF:1E:79:37` verwendet.

Der angesprochene Knoten verschickt als Antwort eine Neighbor-Advertisement-Nachricht. Die darin enthaltenen Informationen werden im Neighbor Cache gespeichert. Wenn ein Eintrag noch unfertig war,



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
```