Tools bei Netzwerkproblemen

Dinge die zu Problemen bei der Netzwerkanbindung führen können, sind z.B.:

- Hardwareprobleme (defektes Kabel, defekte Netzwerkkarte),
- Treiberprobleme (der Treiber passt nicht zur verwendeten Netzwerkkarte),
- Einrichtungsprobleme (Angabe einer falscher IP, einer falschen Netmask oder ein falsch vergebenes Default Gateway) oder
- IP Probleme (falsche MTU, Routing funktioniert nicht).

Die folgende Auflistung einiger TCP/IP-Diagnosebefehle, soll einen ersten Anhaltspunkt geben, mit welchen Befehlen man Probleme im IP Umfeld eingrenzen kann.

	Linux / Unix	Windows
IP-Konfiguration	ifconfig ipconfig,	winipcfg, ipconfig
Konnektivitätstest	ping	ping
ARP-Cache	arp	arp
Routenermittlung	traceroute	tracert
Routing-Tabelle	route	route
Netzstatistik	netstat	netstat
DNS-Diagnose	nslookup	nslookup

ping:

ping ist normalerweise **der erste Befehl** zum Testen einer Verbindung:

- ob ein anderer Rechner erreichbar ist.
- ob es bei einer Verbindung zu einem Rechner zu hohen Paketausfällen kommt (was ein Hinweis darauf wäre, dass irgend etwas auf der ”Leitung” nicht richtig funktioniert oder konfiguriert ist).
- ob man nicht evtl. ein lokales Problem hat (ping auf die eigene IP-Adresse)
- ob man TCP/IP ”sauber” verwenden kann (ping localhost (127.0.0.1))

Funktionsweise:

Der Name “ping” stammt aus der Marine. Zum Aufspüren eines U-Boots wird hier ein Schallsignal (Sonar) ausgesendet, welches vom U-Boot reflektiert wird. Im U-Boot hört sich dieses Schallsignal wie ein hohes Klopfgeräusch, ein “Ping” an.

Das Netzwerkkommando Ping sendet ein ICMP-“Echo-Request”-Paket (ping) an die Zieladresse und wartet auf ICMP “Echo-Reply” (pong). Ist der Zielrechner nicht erreichbar, antwortet der zuständige Router: “Network unreachable” oder “Host unreachable”. Da manche Hosts so konfiguriert sind, dass sie ICMP-Pakete ignorieren und verwerfen, kann aus einer fehlenden Antwort nicht zwangsläufig geschlossen werden, dass die Gegenstelle nicht erreichbar wäre.

traceroute / tracert:

Falls ein **ping nicht erfolgreich** ist, ist es oft hilfreich, heraus zu bekommen, bis zu welchem Rechner eines Netzwerkes man noch kommt, bevor das entsprechende gesendete Paket verworfen wird.

Dies lässt sich mit Hilfe des Befehls traceroute ermitteln:

- Traceroute gibt jeweils den nächsten erreichten Hop (System) in tabellarischer Form aus, so dass man den Weg, den das Paket genommen hat, verfolgen kann.
- Das letzte System, das man in der Ausgabe des traceroute sieht, wird höchstwahrscheinlich das System sein, das das Problem verursacht (z.B. falsche Routing Einträge etc.).
- Grafische Darstellung: http://www.visualroute.com/

Funktionsweise:

- Um den Pfad, den die Pakete zu einem bestimmten Host nehmen, sichtbar zu machen, wird das TTL-Feld (Time To Live) des IP-Headers gezielt verändert.

- Das TTL-Feld enthält einen Wert zwischen 1 und 255, der angibt, wie lange das Paket noch geroutet werden soll. Jeder Router ("Hop") verringert den Wert im Paket um eins, und wenn der Wert 0 erreicht wird, wird das Paket verworfen. Somit kann ein Paket maximal 255 Hops mitmachen, was in der Praxis aber mehr als genug ist.

- Das Traceroute-Programm sendet nun Paketfolgen mit aufsteigender TTL - also zuerst eins mit einer TTL von 1, dann 2, 3, 4 usw. Der Sinn liegt nun darin, daß jeder Host, der ein Paket verwirft weil die TTL abgelaufen ist, eine ICMP-Nachricht vom Typ ICMP_TIME_EXCEEDED an den Sender zurück schickt. Das Traceroute-Programm bekommt also von jedem Host auf dem Weg zum Ziel eine ICMP-Nachricht geschickt, und hat somit dessen Adresse.

netstat:

Mit Hilfe dieses Befehls werden Informationen über die aktuellen Netzwerkverbindungen angezeigt:

- aktive Ports bzw. den Zustand der Ports.
- mit wem die entsprechenden Ports gerade verbunden sind
- wieviele Pakete schon gesendet bzw. empfangen wurden.
- den Inhalt der Routing-Tabelle.
- Freeware TCPView (von Sysinternals) listet alle TCP- und UDP-Ports auf, zeigt deren Zustand und greift bei Bedarf auf die einzelnen Verbindungen zu.

ifconfig (Linux) bzw. **winipcfg/all** (Windows)**:**

Mit Hilfe dieser Befehle werden Informationen zu den Netzwerkkarten ausgegeben:

- MAC Adresse,
- IP-Adresse,
- Subnetmask und
- Standardgateways.
- Broadcast Adresse
- gesendete und empfangene Pakete etc. aus.

route (Linux) bzw. **route print** (Windows):

Informationen zur momentanen Routing Tabelle anzeigen lassen (vgl. **netstat –r**).

- **route add:** Hinzufügen neuer Routen z.B.
  route add -net 192.168.200.0 netmask 255.255.255.0 dev eth1
- **route del:** Löschen gesetzter Routen

nslookup wird verwendet,

- um IP-Adressen oder Domänen eines bestimmen Computers mittels DNS herauszufinden.

Die **NICs (Network Information Center)** vergeben die DNS-Namen:

- DENIC
- RIPE (Réseaux IP Européens),
- ARIN (American Registry for Internet Numbers),
- APNIC (Asia-Pacific Network Information Center)

Das ICANN bzw. die IANA ist die oberste Behörde zur Vergabe von IP-Adressen.

Online-Tools:

- http://ping.eu: (Online Ping, Traceroute, DNS lookup, Reverse lookup, WHOIS, Port check, Proxy checker, Mail relaying, Bandwidth meter)
- http://www.wieistmeineip.de/ DSL-Speedtest, Ping
- http://de.wikibooks.org/wiki/Netzwerktechnik Wikibook Netzwerktechnik
- http://www.bsi-fuer-buerger.de/ Bundesamt für die Sicherheit in der Informationstechnik