Link: https://www.tecchannel.de/a/die-wichtigsten-windows-befehle-fuer-netzwerk-und-internet,2021742

Netzwerkkontrolle auf der Kommandozeile

Die wichtigsten Windows-Befehle für Netzwerk und Internet

Datum: 01.04.2015
Autor(en): Hans-Christian Dirscherl

Die Kommandozeile von Windows bietet leistungsfähige Befehle, mit denen Administratoren und Webmaster schnell ihr Netzwerk oder ihre Internetverbindungen überprüfen und konfigurieren können. Wir stellen Ihnen die wichtigsten DOS-Prompt-Befehle von Windows vor.

Gerade für die Netzwerkkonfiguration und die Fehlersuche im LAN stellt die Kommandozeile einige sehr mächtige Befehle bereit, die allesamt auf eine grafische Oberfläche verzichten. Vor allem Administratoren wissen die schlichte Darstellung und die Scripting-Möglichkeiten der Kommandozeile zu schätzen. Daher bieten auch die neuesten Windows-Versionen noch das textbasierte CMD-Fenster an. Zum Teil wurden die Möglichkeiten sogar deutlich erweitert.

Die Eingabeaufforderung können Sie auf unterschiedliche Weise öffnen, unter Windows XP und Windows 7 etwa über Start, Ausführen und Eingabe von cmd. In Windows 8 und 8.1 kann cmd einfach auf dem Startbildschirm eingegeben werden. Bei den neueren Windows-Versionen startet das CMD-Fenster standardmäßig nur mit eingeschränkten Rechten. Bei vielen Befehlen ist es notwendig - oder zumindest sinnvoll -, diese als Administrator auszuführen. Das geht unter Windows 7 beispielsweise, indem Sie die Eingabe von cmd mit STRG + UMSCHALT + Eingabe bestätigen oder idem Sie unter Programme / Zubehör die Eingabeaufforderung mit der rechten Maustaste anwählen und dann als Administrator ausführen.

Wenn Sie unter Windows 8 / 8.1 cmd auf dem Startbildschirm eingeben, und die gefundene Eingabeaufforderung mit der rechten Maustaste anwählen, erscheint am unteren Bildschirmrand die Option Als Admin ausführen.

[Hinweis auf Bildergalerie: **Bildergalerie: Netzwerkbefehle für die Kommandozeile von Windows**] gal1

Hinweis: Die Screenshots stammen teilweise von älteren Windows-Versionen. Je nach dem von Ihnen eingesetzten Windows-System können Darstellung und genaue Benennung der Eingabeaufforderung leicht abweichen. Zudem stehen nicht auf allen Rechnern alle DOS-Befehle gleichermaßen zur Verfügung.

1. Generelle Tipps zum Konsolenfenster

1. Falls Sie wissen wollen, welche DOS-Version Ihr Windows zur Verfügung stellt, geben Sie einfach ver im Konsolenfenster ein.

2. Falls Sie weitergehende Informationen zu einem bestimmten DOS-Befehl benötigen, geben Sie help und den gesuchten Befehl ein. Allerdings existiert diese Hilfefunktion nur für gängige DOS-Befehle; bei weniger geläufigen Befehlen wie netsh hilft eine alternative Hilfeanfrage mit Fragezeichen, etwa netsh /? weiter.
3. Wie bei Linux können Sie auf der Kommandozeile mit der "Pfeil nach oben"- und der "Pfeil nach unten"-Taste zwischen bereits eingegebenen Befehlen navigieren und diese damit bequem erneut ausführen.
4. Wenn Sie den Rechner runterfahren wollen und gerade ein DOS-Fenster offen haben, dann können Sie durch Eingabe von shutdown samt dem passenden Parameter den PC runterfahren.
5. whoami: Zeigt Benutzername und Rechnername. Tippen Sie whoami (englisch für "Wer bin ich?") ein. Windows zeigt Ihnen daraufhin den Namen Ihres PCs und Ihren Benutzernamen an. Dieser Befehl existiert bei einigen Systemen jedoch nur, wenn Sie vorher das Windows Resource Kit installiert haben.
6. cls: Bildschirminhalt löschen. Wenn Sie bereits mehrere Befehle in einem Konsolenfenster eingetippt und dementsprechend viele Ausgaben erhalten haben, verlieren Sie womöglich den Überblick. Ordnung schafft cls (clear screen), und das Fenster ist wieder leer.
7. path: Zeigt Pfade für ausführbare Daten an. Mit path können Sie sich die Verzeichnisse anzeigen lassen, in denen Sie Dateien ablegen, die sich von der Kommandozeile aus direkt starten lassen, ohne dass Sie in das betreffende Verzeichnis wechseln müssen.

2. arp und getmac: Mac-Adresse ermitteln und konfigurieren

Das Adress Resolution Protocol ARP übernimmt die Umsetzung der Mac-Adresse zu einer IP-Adresse. Im sogenannten ARP-Cache werden IP-Adressen gespeichert, die bereits in Mac-Adressen aufgelöst wurden. Wird ARP hier nicht fündig, wird eine Rundsendung (Broadcast) an alle im Netzwerk erreichbaren Rechner verschickt, um die Mac-Adresse zur angefragten IP-Adresse zu ermitteln. Das Gerät, zu dem die gesuchte IP-Adresse gehört, antwortet und schickt seine Mac-Adresse. Daraufhin trägt ARP im anfragenden Rechner die IP-Adresse in den ARP-Cache ein, alle Anfragen an diesen Rechner werden nun direkt zugestellt. Nach einem Neustart werden alle ARP-Einträge gelöscht - das erreichen Sie auch mit arp -d.

arp -a zeigt den Inhalt des ARP-Caches an. arp -s IP-Adresse Mac-Adresse erzeugt einen statischen Eintrag und verbindet manuell eine IP-Adresse mit einer MAC-Adresse. Nach einem PC-Neustart ist dieser Eintrag allerdings verloren. arp /? zeigt alle Optionen ein.

Die Verwendung des ARP-Protokolls zieht ein spezifisches Sicherheitsproblem namens ARP-Poisoning bzw. ARP-Spoofing nach sich. Hierbei weist ein Angreifer einer IP-Adresse eine falsche Mac-Adresse zu und leitet somit Anfragen um.

3. getmac: Mac-Adresse ermitteln

Jeder Netzwerkcontroller hat eine einmalige unverwechselbare und nicht veränderbare Mac-Adresse (Media Access Control), die für die Adressierung der Datenpakete im Internet unverzichtbar ist - die Mac-Adresse ist somit die physische Adresse Ihrer Netzwerkkarte, die sich in der Regel in einem festen EEPROM-Speicher auf der Netzwerkkarte beziehungsweise beim Onboard-LAN-Adapter im Bios-Chip befindet. Die Mac-Adressen werden zentral verwaltet, jede Adresse besteht aus zwölf hexadezimalen Ziffern.

Die hinlänglich bekannten IP-Adressen, die zunächst einmal für die Adressierung der Datenpakete verantwortlich sind, werden auf die Mac-Adressen abgebildet. Bei jeder Internetkommunikation muss also die zu einer IP-Adresse gehörige Mac-Adresse gesucht werden. Dafür ist das Address Resolution Procotol (ARP) zuständig.

getmac: Der Befehl ermittelt die MAC-Adresse der Netzwerkkarte.

Wenn Sie Ihr Netzwerk oder Ihren Router konfigurieren, benötigen Sie oft die MAC-Adressen Ihrer Netzwerkadapter. Sie ermitteln seit Windows XP die Mac-Adressen mit dem Kommando getmac. Unter Windows gab es früher das Tool winipcfg. Es gehört mittlerweile nicht mehr zum Funktionsumfang von Windows, weil dessen Funktionalität durch den weiter unten vorgestellten Befehl ipconfig /all zur Verfügung gestellt wird.

4. ping: testet die Internetverbindung

Neben dem bekannten TCP/IP-Protokollpaar basiert die Internetkommunikation auf einer Reihe weiterer Protokolle, unter anderem auf ICMP, dem Internet Control Message Protocol. ICMP wird für die Übertragung von kurzen Nachrichten verwendet, in erster Linie handelt es sich dabei um Status- und Fehlerinformationen. Der wichtigste Befehl des Internet Control Message Protocol ist ping.

ping: Der Befehl prüft, ob ein Rechner erreichbar ist.

ping (Paket Internet Groper) ist der Klassiker unter den Netzwerkbefehlen und erste Wahl, wenn Sie schnell testen wollen, ob Ihr Rechner oder Netzwerk ins Internet kommt beziehungsweise eine Website erreichbar ist. Geben Sie dazu ping mit der IP-Adresse oder dem Namen der gewünschten Website ein, also etwa ping www.tecchannel.de. Diese Anfrage nennt man Echo Request. Der angepingte Host antwortet, wenn er erreichbar ist, mit einem Echo, also mit einem Reply. Wenn die Verbindung einwandfrei funktioniert, sollten Sie eine Ausgabe bekommen, die anzeigt, ob von der angepingten Website Datenpakete als Antwort erhalten wurden.

Zur angepingten Website wird die IP-Adresse angegeben (diese ist maßgeblich für die Internetkommunikation, die DNS-Namen dienen ja nur als Erleichterung für die Benutzer). Ebenso angegeben wird die Zeit, die die 32 Byte großen Datenpakete benötigen - die sogenannte Antwortzeit. Die Ping-Statistik sollte keine verlorenen Datenpakete aufweisen. Sind die Antwortzeiten okay und gehen keine Pakete verloren, dann passt alles. Funktioniert ping dagegen nicht und kommt eine Zeitüberschreitung, dann stimmt etwas mit ihrer Internetverbindung nicht, oder die angepingte Website ist nicht verfügbar.

Sie können mit ping auch Ihren lokalen Host prüfen, indem Sie die Loopback-Adresse anpingen: ping localhost oder ping 127.0.0.1. Kommt daraufhin die korrekte Antwort, ist IP auf dem Host einwandfrei installiert, was eine Voraussetzung für eine funktionierende Internetverbindung ist. Das Testen des Loopback garantiert aber noch nicht, dass Sie auch ins Internet kommen, weil durch den Ping auf localhost beispielsweise keine Aussage über Ihr Gateway getroffen wird. Pingen Sie dafür die IP-Adresse Ihres Gateways an. Ist dieses erreichbar, funktioniert zumindest die Verbindung innerhalb Ihres Netzwerks bis zum Gateway.

ping sendet standardmäßig vier ICMP-Echopakete und zeigt die Zeitspanne, die bis zur Antwort vergeht. Kommt die Antwort nicht innerhalb einer Sekunde, liefert ping einen Timeout für das Paket. Wenn Sie ping mit dem Parameter -t eingeben, erfolgt ein Dauerping, den Sie mit CTRL+C abbrechen: ping www.tecchannel.de -t. Die Zeit bis zum Timeout lässt sich mit dem Parameter -w erhöhen. Zu Ping gibt es viele weitere interessante Optionen, zwei stellen wir hier vor: -a löst IP-Adressen zu Host-Namen auf, -n legt die Anzahl der ICMP-Pakete fest (default sind vier).

5. tracert: Route von Datenpaketen anzeigen

Mit dem Befehl tracert (Vorsicht: Verwechslungsgefahr mit Linux, wo der Befehl traceroute lautet) und den entsprechenden Parametern lassen sich der Weg und alle Zwischenstationen (die sogenannten Hops) eines Datenpakets zwischen zwei Hosts anzeigen. Geben Sie beispielsweise tracert www.pcwelt.de ein. Sie erfahren dann, dass das Datenpaket an pcwelt.de in unserem Beispiel im Screenshot über acht Hops geht: angefangen mit der Fritz!Box, die unser Standard-Gateway ist, über sechs Zwischenstationen - beispielsweise bei unserem Provider, diversen Routern und Gateways - bis zum Zielserver von pcwelt.de. Sie erfahren zudem, wie viel Zeit das Datenpaket von einer Station zur nächsten benötigt. Für tracert gibt es unter der Free- und Shareware Visualisierungs-Tools, die eine Art Weltkarte liefern, auf der die Route Ihres Paketes eingezeichnet ist.

tracert: Die Eingabe zeigt alle Zwischenstationen (die so genannten Hops) eines Datenpakets zwischen zwei Hosts an.

tracert kann sowohl mit einer IP-Adresse als auch mit einem Host-Namen genutzt werden. Bei Host-Namen gibt tracert die IP-Adresse an.

Der Ausdruck Time to Live (TTL) bezeichnet die Lebensdauer eines Datenpaketes im Netz. Maximal kann ein Paket über 255 Router gehen, wobei Time to Live bei jedem Router-Übergang (Hop) um eins reduziert wird. Erreicht TTL null und konnte es bis dahin nicht zugestellt werden, wird das Paket verworfen.

6. pathping: Kombination aus tracert und ping

pathping ist die Weiterentwicklung der Befehle tracert und ping. Der obere Teil der Ausgabe entspricht weitgehend dem Ergebnis von tracert. Darunter folgt eine ausführliche Analyse mit Informationen zur Weiterleitung der Datenpakete über die einzelnen Hops.

pathping: Das Kommando ist die kombinierte Weiterentwicklung der Befehle tracert und ping.

Alle Zwischenstationen respektive Router erhalten individuelle Pings. Anhand der Antworten berechnet pathping eine Statistik. Paketverluste und Antwortzeiten werden zu jedem einzelnen Router angezeigt; somit lassen sich Ursachen für Fehler innerhalb einer Route schnell identifizieren.

7. ipconfig: Netzwerkkonfiguration des Rechners anzeigen

Geben Sie ipconfig ein, um auf einen Blick alle Konfigurationseinstellungen Ihrer Netzwerkschnittstellen (LAN und WLAN) angezeigt zu bekommen. Sie sehen beispielsweise die derzeit noch nicht so wichtige IP6-Adresse Ihres PCs, dessen IP4-Adresse, die Subnetzmaske und die IP-Adresse des Standard-Gateways, über das Sie ins Internet gehen (oft die Adresse des DSL-Routers). Auch zum DNS-Server, der für Ihren Rechner zuständig ist, finden Sie mit ipconfig Informationen.

ipconfig: Der Befehl liefert auf einen Blick alle Konfigurations-Einstellungen Ihrer Netzwerkschnittstellen.

Wenn Sie wirklich alle Informationen haben wollen, geben Sie ipconfig mit dem entsprechenden Parameter ein: ipconfig /all. Falls Ihr Rechner mehrere Netzwerkcontroller besitzt, liefert ipconfig zu jedem Controller alle Informationen. Mit ipconfig /release geben Sie Ihre aktuelle IP-Adresse frei. Mit ipconfig /renew fordern Sie anschließend vom DHCP-Server eine neue IP-Adresse an. So können Sie potenzielle Probleme mit einer vom DHCP-Server falsch zugeteilten IP-Adresse beheben.

ipconfig bietet auch Optionen zum Löschen des DNS-Cache. In diesem Cache werden die Ergebnisse von DNS-Anfragen abgelegt, damit dafür keine neuen Anfragen an DNS-Server nötig sind und unnötiger Traffic vermieden wird. Mit ipconfig /displaydns zeigen Sie alle im DNS-Cache vorhandenen Einträge an. Mit ipconfig /flushdns leeren Sie den DNS-Cache.

Hinweis: Sie können den DNS-Speicher nur unter Windows mit diesen Befehlen löschen. Der Linux-Kernel cacht keine DNS-Anfragen, deshalb gibt es keinen zu Windows vergleichbaren Befehl.

Tipp: Falls Sie Windows und parallel Linux nutzen, müssen Sie auf die jeweils richtige Schreibweise des Befehls achten. Unter Linux heißt er ifconfig und nicht ipconfig. Zudem gibt es iwconfig für die WLAN-Schnittstelle unter Linux.

8. netstat: zeigt alle geöffneten Netzwerkverbindungen an

M i t netstat zeigen Sie alle geöffneten TCP- und UDP-Verbindungen an. UDP ist ein Alternativprotokoll zu TCP, das weniger Traffic verursacht, dafür aber nicht über die Kontrollfunktion von TCP verfügt. Zu jeder Verbindung liefert Ihnen netstat das verwendete Internetprotokoll, die IP-Adresse Ihres Rechners samt den dafür benutzten Port - den sogenannten Socket -, die Ziel-/Remote-Adresse und den aktuellen Status, beispielsweise hergestellt (also verbunden). Wenn Sie sich wirklich alle Netzwerkverbindungen anzeigen lassen wollen, geben Sie netstat -ao ein. In diesem Fall werden dann auch UDP-Verbindungen ("a" steht für all) und alle Prozess-IDs ("o" zeigt die PIDs an), die zu einer Netzwerkverbindung gehören, angezeigt.

netstat: Die Eingabe zeigt alle geöffneten Netzwerkverbindungen an.

Mit diesem sehr nützlichen Befehl können Sie Verbindungen zum Internet aufspüren, die überhaupt nicht bestehen sollten, beispielsweise wenn ein Trojaner oder eine Spyware ins Web funkt.

9. nbtstat

nbtstat liefert die Verbindungsinformationen für NetBIOS over TCP/IP (NBT); es entspricht von der Funktionalität her also ipconfig.

nbtstat: Das Kommando liefert die Verbindungsinformationen für NetBIOS over TCP/IP.

Remote-Rechner können via IP-Adresse oder über ihren Host-Namen angesprochen werden. Der Befehl hat etliche Parameter; wie gehabt, gibt die Hilfefunktionen Auskunft.

10. net und netsh: nützliche Netzwerkbefehle

Die Befehlsfamilie um net stellt eine Reihe von Funktionen zur Verfügung, die nicht alle unbedingt mit dem Netzwerk in Verbindung stehen. Die net-Befehle haben zudem nichts mit dem Microsoft-.net-Framework zu tun. Einige Beispiele: net accounts listet die Benutzerkontenrichtlinien auf. net localgroup zeigt die vorhandenen lokalen Benutzergruppen an. Mit net localgroup /add Tester fügen Sie eine neue Benutzergruppe namens Tester hinzu. net localgroup /add Tester neuertester fügt den User neuertester hinzu. Mit net user neuer_nutzer neues_passwort /add legen Sie den Benutzer neuer_nutzer mit dem Passwort neues_passwort an.

net user: Der Befehl verwaltet die Benutzerkonten.

net share zeigt alle Freigaben des lokalen Rechners an. Mit net share Name_des_freigegebenen_Laufwerks lassen Sie sich Details zur angegebenen Freigabe anzeigen. Mit net session sehen Sie, wer mit dem Server verbunden ist - dieser Befehl macht natürlich nur auf einem Serversystem und nicht auf dem Client Sinn. net /? zeigt alle verfügbaren net-Befehle an. net help BEFEHL liefert die passende Hilfeinformation.

11. netsh

netsh stellt eine Shell für Netzwerkbefehle dar. Ein Beispiel: Sie können das derzeit kaum benötigte IPV6 deinstallieren und mit den Befehlen netsh interface ipv6 uninstall und netsh interface ip reset c:\reset.txt die IP-Konfiguration komplett zurücksetzen (Install-Zustand).

12. route und nslookup: Routing-Tabellen und DNS-Umwandlung

Routing bezeichnet das Weiterleiten von Datenpaketen von einem Netzwerk (LAN, Internet) in ein anderes. Der Router besitzt hierfür sogenannte Routing-Tabellen.

route print: Die Eingabe zeigt die Routing-Tabelle an.

Mit route und den passenden Optionen beziehungsweise Befehlen ändern Sie die Routing-Tabelle Ihres Rechners. Sie können beispielsweise ein neues Gateway einstellen route change oder die vorhandene Route ausdrucken route print. Das Ergebnis entspricht auch dem Ergebnis des Befehls netstat -r. Mit add samt einer Reihe von Optionen fügen Sie eine neue Route hinzu, mit route /s zeigen Sie alle Optionen an.

Diese Routing-Tabellen werden normalerweise dynamisch erstellt, entweder durch das OSPF- oder durch das RIP-Protokoll. Router verfügen übrigens über zusätzliche Befehle zum Routen-Management, beispielsweise show ip route.

13. nslookup

Mithilfe des DNS-Protokolls (Domain Name System) werden für den Menschen leichter zu merkende Host-Namen mit einer IP-Adresse verbunden. Mit nslookup können Sie manuell eine Anfrage an einen Name-Server schicken, um einen Host-Namen aufzulösen. Außerdem können Sie mit nslookup Ihren Name-Server ermitteln und Probleme bei der Namensauflösung ermitteln.

nslookup liefert alle Informationen zum DNS-Server Ihres Rechners. Wenn Sie bei gestartetem nslookup einen Host-Namen eingeben, dann löst nslookup ihn in eine IP-Adresse auf.

14. ftp: Datei-Upload und -Download via File Transfer Protocol

ftp: Die Eingabe greift auf die Kommandos des File Transfer Protocols zu.

Für gewöhnlich erledigen Sie FTP-Transfers mit einem grafischen FTP-Client wie Filezilla oder einem Dateimanager mit integrierter ftp-Funktion wie Total Commander. Doch für den Fall der Fälle steht die ftp-Befehlsfamilie auch auf der Kommandozeile zur Verfügung. Durch Eingabe von ftp, das für File Transfer Protocol steht, beginnen Sie eine ftp-Sitzung, mit quit beenden Sie diese wieder. Lesen Sie sich die Hilfeinformationen durch, bevor Sie eine ftp-Sitzung starten.

Übrigens: Ebenso wie der Klassiker ftp steht auch der Befehltelnet auf der Kommandozeile zur Verfügung. Mit ihm können Sie sich mit einem Telnet-Server verbinden. Beachten Sie bei beiden Befehlen aber, dass die Datenübertragung nicht verschlüsselt ist und somit Passwörter und Zugangsdaten im Klartext übertragen werden. (ala/mje)

Diesen Beitrag haben wir von unserer Schwesterpublikation **PC Welt**[1] übernommen.

Links im Artikel:

[1] **http://www.pcwelt.de/**

Bildergalerien im Artikel:

gal1 **Bildergalerie: Netzwerkbefehle für die Kommandozeile von Windows**

Kommandozeilenbefehle für das Netzwerk
Mit diesen Kommandos verwalten Sie Ihr Netz spielend leicht.
Foto: everythingpossible - Fotolia.com

whoami
whoami zeigt Benutzername und Rechnername.

getmac
getmac ermittelt die MAC-Adresse der Netzwerkkarte.

ping
ping prüft, ob ein Rechner erreichbar ist.

tracert
tracert zeigt alle Zwischenstationen (die so genannten Hops) eines Datenpakets zwischen zwei Hosts an.

pathping
pathping ist die kombinierte Weiterentwicklung der Befehle tracert und ping.

ipconfig
ipconfig liefert auf einen Blick alle Konfigurations-Einstellungen Ihrer Netzwerkschnittstellen.

netstat
netstat zeigt alle geöffneten Netzwerkverbindungen an.

nbtstat
nbtstat liefert die Verbindungsinformationen für NetBIOS over TCP/IP.

net user
net user verwaltet die Benutzerkonten.

route print

route print zeigt die Routing-Tabelle an.

ftp

ftp nutzt das File Transfer Protocol von der Kommandozeile aus.