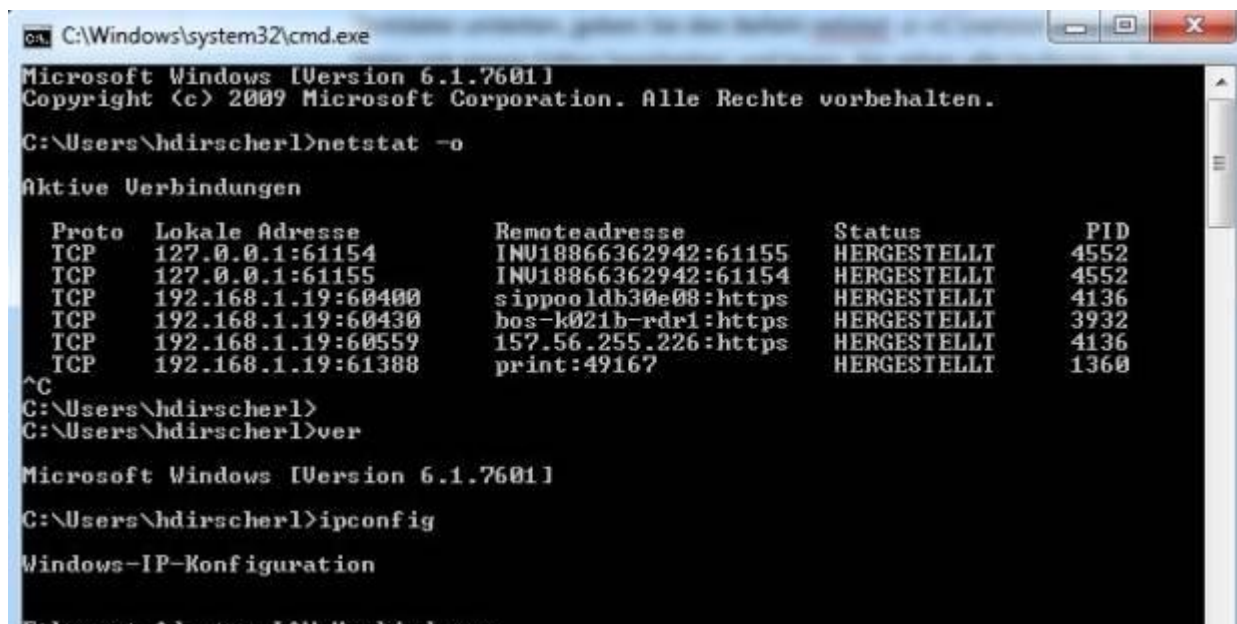


Die wichtigsten CMD-Befehle für Windows zur Netzwerkanalyse

17.05.2016 | 09:40 Uhr | Hans-Christian Dirscherl | [PC-WELT](#)



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\hdirscherl>netstat -o

Aktive Verbindungen

Proto Lokale Adresse Remoteadresse Status PID
TCP 127.0.0.1:61154 INU18866362942:61155 HERGESTELLT 4552
TCP 127.0.0.1:61155 INU18866362942:61154 HERGESTELLT 4552
TCP 192.168.1.19:60400 sipooldb30e08:https HERGESTELLT 4136
TCP 192.168.1.19:60430 bos-k021b-rdr1:https HERGESTELLT 3932
TCP 192.168.1.19:60559 157.56.255.226:https HERGESTELLT 4136
TCP 192.168.1.19:61388 print:49167 HERGESTELLT 1360
^C
C:\Users\hdirscherl>
C:\Users\hdirscherl>ver

Microsoft Windows [Version 6.1.7601]

C:\Users\hdirscherl>ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter LAN-Verbindung:
```

CMD: Profi-Befehle für Windows

Windows stellt leistungsfähige Befehle zur Verfügung, mit denen nicht nur Administratoren und Webmaster, sondern auch Endanwender schnell ihr Netzwerk oder ihre Internetverbindungen überprüfen und konfigurieren können. Wir stellen die wichtigsten Befehle für die Kommandozeile alias CMD von Windows XP, Vista, 7, 8.1 und 10 vor. Update: WLAN-Hotspot einrichten und Windows-Firewall konfigurieren.

Auf den **nächsten Seiten** stellen wir Ihnen die wichtigsten Windows-Befehle für Ihr Netzwerk und Ihre Internetverbindung vor, die Sie im CMD-Fenster von [Windows](#) eingeben können. Sie erfahren unter anderem, wie Sie die Mac-Adresse ermitteln, was es mit Arp auf sich hat, wie Sie die IP-Adresse Ihres Rechners herausbekommen und die Route Ihrer Datenpakete verfolgen. Wie Sie ganz einfach und schnell testen, ob Ihr Rechner überhaupt eine Verbindung ins Internet aufbauen kann und wie die Netzwerk-Konfiguration Ihres PCs konkret aussieht. Falls Sie einen Trojaner auf Ihrem PC vermuten, so stellen wir Ihnen einen Windows-Befehl vor, mit dem Sie eine solche unerwünschte Verbindung aufspüren können und alle geöffneten Internetverbindungen Ihres Rechners anzeigen.

Wir haben die CMD-/Kommandozeilen-Befehle mit Windows XP, Vista und Windows 7 getestet, weil diese Betriebssysteme im professionellen Umfeld/Unternehmenseinsatz immer noch am weitesten verbreitet sind. In der Regel sollten die CMDs aber auch mit [Windows 8.1](#) und [Windows 10](#) funktionieren. Öffnen Sie das CMD-Fenster/die Eingabeaufforderung unter Windows, indem Sie "cmd" in das Suchen-Feld der Seitenleiste von [Windows 8](#) eingeben und in der daraufhin erscheinenden Trefferliste auf "Eingabeaufforderung" klicken. Noch schneller öffnen Sie die Eingabeaufforderung mit dieser Tastenkombination: "Windows-Taste" + "R" drücken und dann "cmd" eintippen.

Hinweis zur Terminologie: Für alle Windows-Versionen ab Windows 2000 ist die korrekte Bezeichnung für das Fenster, in das Sie die CMD-Befehle eingeben, "Eingabeaufforderung" beziehungsweise "Kommandozeilen-Interpreter". Die CMD-Befehle nennt man "Kommandozeilen-Befehle" oder auch "Windows-Befehle". Die Bezeichnungen "DOS-Fenster" und "DOS-Befehle" sind dagegen streng genommen nicht mehr korrekt und gelten für die Zeit vor Windows 2000. Wir verwenden in diesem Artikel jedoch alle Bezeichnungen abwechselnd.

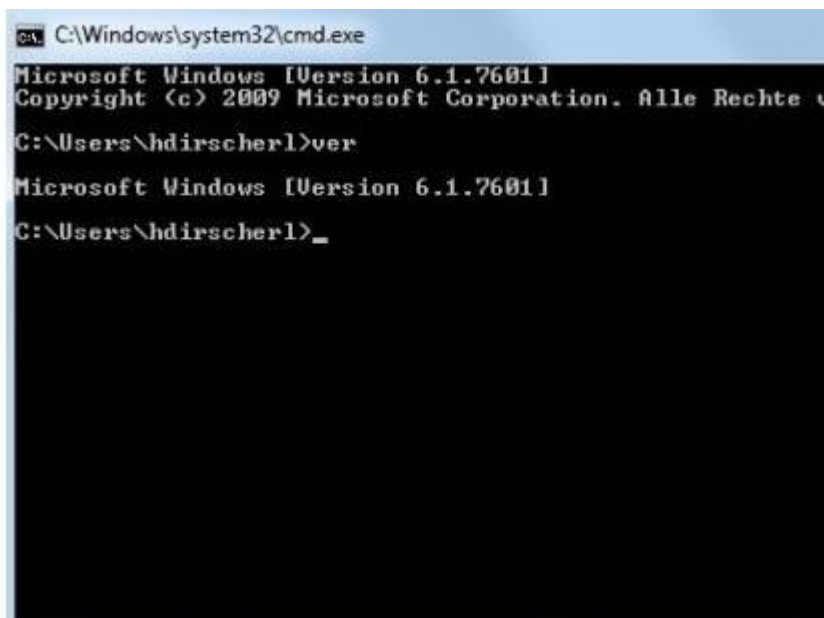
[Die besten Tools und Tipps für LAN und WLAN](#)

So geht's mit CMD: Windows-Befehle eingeben

Um die Windows-Befehle einzugeben, gehen Sie immer so vor: Öffnen Sie bei Windows XP eine Eingabeaufforderung über Start, Ausführen. Tippen Sie cmd ein und drücken Sie Return. Unter Vista geben Sie bei „Suche starten“ cmd ein. Unter Windows 7 gehen Sie über den Start-Button zu "Programme/Dateien durchsuchen" und geben dort "cmd" ein. Sie Daraufhin öffnet sich ein DOS-Fenster, in dem Sie die Kommandozeilenbefehle eingeben. Wenn Sie einen Befehl eingetippt haben, müssen Sie danach immer Return drücken, um ihn auszuführen. Ruck zuck sehen Sie dann das Ergebnis.

[Netzwerkprobleme systematisch lösen](#)

Hinweis: Die Screenshots stammen teilweise von Windows Vista Home, von Windows XP Professional und von Windows 7 Pro. Je nach dem von Ihnen eingesetztem Windows-System kann die Darstellung und die genaue Benennung der Eingabeaufforderung etwas abweichen. Zudem stehen nicht auf allen Rechnern alle DOS-Befehle gleichermaßen zur Verfügung.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.
C:\Users\hdirscher1>ver
Microsoft Windows [Version 6.1.7601]
C:\Users\hdirscher1>_
```

Windows-Version auf der Kommandozeile ermitteln

Generelle Tipps zum Konsolenfenster:

1. Falls Sie wissen wollen, welche Windowsversion Ihnen zur Verfügung stellt, geben Sie einfach **"ver"** im Konsolenfenster ein. Dabei zählt **Microsoft** aber anders, als Sie das vermutlich

- erwarten. Liefert Ihnen der ver-Befehl beispielsweise "6.1" als Ergebnis, so ist damit Windows 7 gemeint. Auf sehr alten Rechnern ermitteln Sie damit auch die DOS-Version.
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 weiter: **netsh /?**.
 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 Sie gerade ein DOS-Fenster offen haben, dann können Sie durch Eingabe von **shutdown** samt dem passenden Parameter den PC runterfahren.

```

C:\Users\strategos>login
Der Befehl "login" ist entweder falsch geschrieben oder
konnte nicht gefunden werden.

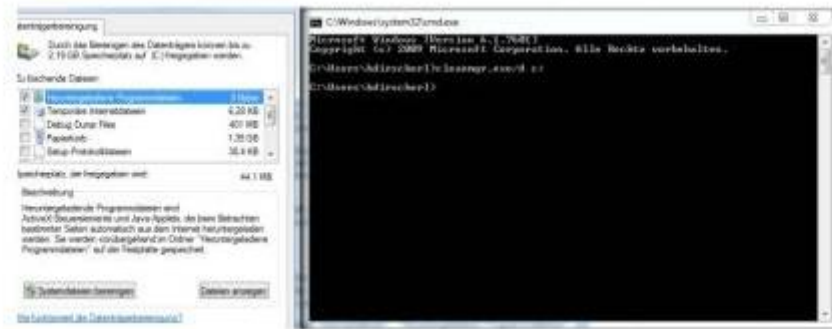
C:\Users\strategos>setpass
Der Befehl "setpass" ist entweder falsch geschrieben oder
konnte nicht gefunden werden.

C:\Users\strategos>whoami
privat-pc\strategos

C:\Users\strategos>
```

whoami

5. **whoami**: Zeigt Benutzername und Rechnername
Tippen Sie whoami (englisch für wer bin ich?) ein. Windows zeigt Ihnen darauf den Namen Ihres PCs und Ihren Benutzernamen an.
6. **cls**: Bildschirminhalt löschen
7. Wenn Sie bereits mehrere Befehle in einem Konsolenfenster eingetippt und dementsprechend viele Ausgaben erhalten haben, verlieren Sie vielleicht den Überblick. Ordnung schafft **cls** (clear screen) und das Fenster ist wieder leer.
8. **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 können ohne dass Sie in das betreffende Verzeichnis wechseln müssen. Sie können Verzeichnisse hinzufügen, indem Sie entweder Path oder das Menü des Windows-Explorers nutzen.



cleanmgr.exe/d c:

Sie können die in Windows integrierte Datenträgerbereinigungs-Funktion auch im Kommandozeilenfenster nutzen. Geben Sie diesen Befehl ein (unser Screenshot entstand auf einem Windows 7-PC, der Befehl funktioniert aber auch unter Windows 8.1): `cleanmgr.exe/d c:`

Gegebenenfalls müssen Sie "c:" noch durch den Laufwerksbuchstaben ersetzen, der bei ihrem System richtig ist. Die Datenträgerbereinigung von Windows benötigt nun einige Zeit, um die nicht mehr benötigten Dateien auf dem System zu ermitteln und zu berechnen, wie viel Speicherplatz durch das Löschen der Dateien freigegeben werden kann. Bei der Gelegenheit können Sie auch gleich Haken bei "Temporäre Internetdateien", "Heruntergeladene Programmdateien" und "Temporäre Dateien" setzen, um zusätzlichen Speicherplatz freizugeben, der unnötig vom System belegt wird.

tasklist: Alle laufenden Prozesse anzeigen

Bevor man ins Internet geht oder ein Netzwerk nutzt, möchte man vielleicht wissen, was überhaupt auf dem eigenen Rechner alles läuft und welche Dienste oder Anwendungen den Rechner ausbremsen könnten. Dafür gibt es den Befehl `tasklist`.

Der Befehl [tasklist](#) zeigt eine Liste der Prozesse an, die aktuell auf dem Rechner laufen. Für alle laufenden Anwendungen und Dienste. Auf dem lokalen Rechner oder auf einem Remote-Rechner. Zu jedem Prozess sehen Sie PID, Sitzungsnamen und Sitzungsnummer und vor allem die Speichernutzung. Damit identifizieren Sie Speicherfresser beziehungsweise Anwendungen, die Ihren Rechner ausbremsen.

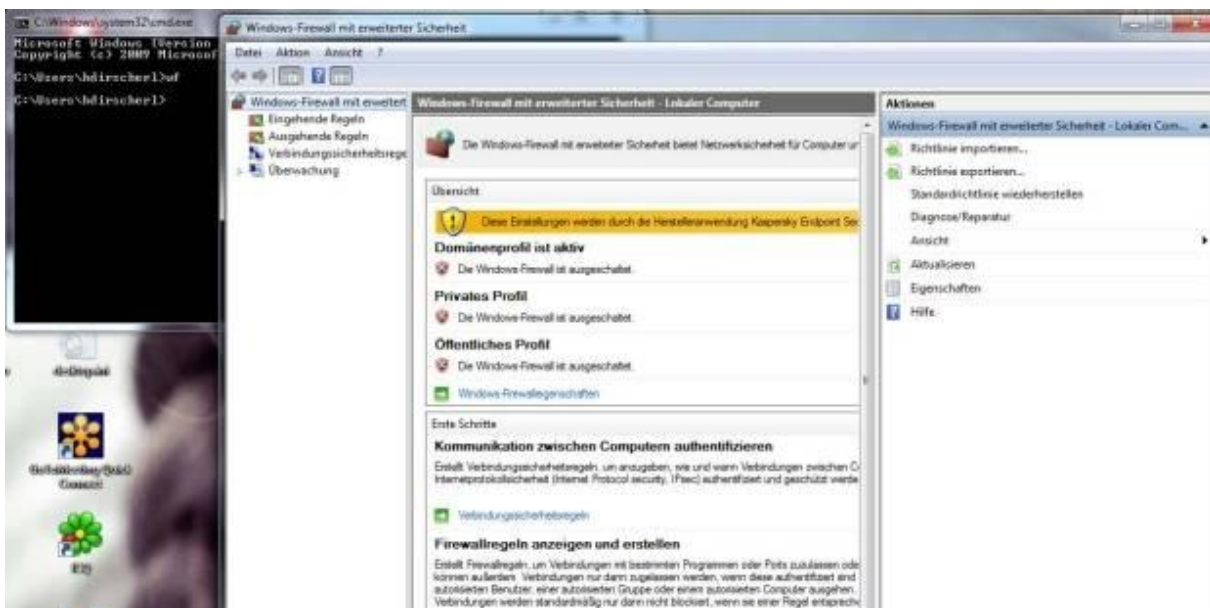
| | | | | | |
|---------------------------|------|----------|---|---------|---|
| par21.exe | 4032 | Console | 1 | 0.748 | K |
| Receiver.exe | 4928 | Console | 1 | 16.232 | K |
| JabraDirect.exe | 4940 | Console | 1 | 90.244 | K |
| CLMgr.exe | 4956 | Console | 1 | 51.584 | K |
| jusched.exe | 4996 | Console | 1 | 5.616 | K |
| SelfServicePlugin.exe | 4640 | Console | 1 | 18.492 | K |
| wfcrun32.exe | 5124 | Console | 1 | 12.336 | K |
| IpPbxOutlookAccess.exe | 5348 | Console | 1 | 8.648 | K |
| DbgSvc.exe | 6536 | Services | 0 | 12.148 | K |
| dllhost.exe | 6588 | Services | 0 | 11.784 | K |
| msdtc.exe | 6688 | Services | 0 | 8.220 | K |
| UcMapi.exe | 6844 | Console | 1 | 52.140 | K |
| OUTLOOK.EXE | 4680 | Console | 1 | 240.724 | K |
| firefox.exe | 6328 | Console | 1 | 244.404 | K |
| chrome.exe | 3276 | Console | 1 | 168.108 | K |
| chrome.exe | 6800 | Console | 1 | 4.648 | K |
| chrome.exe | 7076 | Console | 1 | 51.692 | K |
| chrome.exe | 4444 | Console | 1 | 41.004 | K |
| chrome.exe | 7324 | Console | 1 | 143.608 | K |
| plugin-container.exe | 2292 | Console | 1 | 27.068 | K |
| FlashPlayerPlugin_21_0_0_ | 8064 | Console | 1 | 10.744 | K |
| FlashPlayerPlugin_21_0_0_ | 6476 | Console | 1 | 15.060 | K |
| chrome.exe | 5360 | Console | 1 | 158.144 | K |
| MmiProSE.exe | 2652 | Services | 0 | 11.504 | K |
| chrome.exe | 5952 | Console | 1 | 34.216 | K |
| cmd.exe | 6112 | Console | 1 | 3.160 | K |
| conhost.exe | 1984 | Console | 1 | 5.776 | K |

Mit dem Befehl `tasklist` sehen Sie, welche Prozesse auf Ihrem Rechner laufen. Und welche Anwendungen zu einem Prozess gehören.

Mit `tasklist /?` lassen Sie sich alle Optionen dieses Befehls anzeigen. `Tasklist /v` liefert eine ausführliche Ausgabe. `Tasklist /svc` zeigt alle Dienste an, die in jedem Prozess gehostet werden. Wenn Ihnen der Name eines dort angezeigten Dienstes oder Anwendung nichts sagt, dann suchen Sie danach in einer Suchmaschine.

Ausgabe in Datei umleiten

Nicht immer ist es für die Analyse ideal, wenn die Ausgabe von Befehlen auf dem Bildschirm vorbeirauscht. Sondern für die Analyse benötigt der Profi-Anwender besser eine Datei mit allen Daten. Das lässt sich leicht bewerkstelligen: Monitor-Ausgaben von Befehlen können Sie auch in eine Datei umleiten. Ein Beispiel: `netstat -o >C:\offeneports.txt` erstellt die Text-Datei `offeneports` neu und speichert darin die geöffneten Ports und die bestehenden Internetverbindungen. Wenn Sie statt des „>“ ein „>>“ verwenden, wird die Ausgabe an den bereits bestehenden Datei-Inhalt angehängt.



Regeln für Windows-Firewall schnell aufrufen

Regeln für Windows-Firewall schnell aufrufen

Von der Kommandozeile aus starten Sie mit „wf“ das Windows-Firewall-Regelwerk. In dem dann erscheinenden Fenster können Sie die seit Vista in Windows eingebaute Firewall konfigurieren.

Auf der nächsten Seite geht es mit den besten Windows-Befehlen für Netzwerk und Internet los.

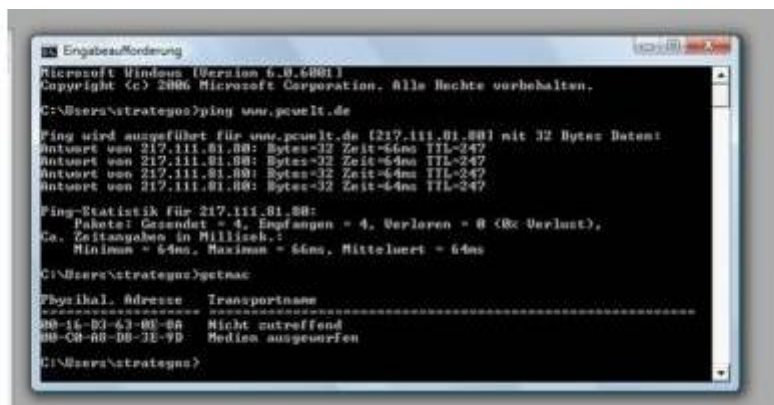
ARP und Getmac: Macadresse ermitteln und konfigurieren

Das Adress Resolution Protocol ARP übernimmt die Umsetzung der Mac-Adresse zu einer IP-Adresse. Im so genannten 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. Darauf 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. `Arp /?` zeigt alle Optionen ein. Mit `arp -s IP-ADRESSE MAC-ADRESSE` verbindet man die IP-Adresse mit der MAC-Adresse. Nach einem PC-Neustart ist dieser Eintrag allerdings verloren.

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.

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 befindetet. Die Mac-Adressen werden zentral verwaltet, jede Adresse besteht aus zwölf hexadezimalen Ziffern.



```
Microsoft Windows [Version 6.0.6002.1]
Copyright (c) 2006 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\strategus>ping www.pcwelt.de

Ping wird ausgeführt für www.pcwelt.de [217.111.01.00] mit 32 Bytes Daten:
Antwort von 217.111.01.00: Bytes=32 Zeit=64ms TTL=247
Antwort von 217.111.01.00: Bytes=32 Zeit=64ms TTL=247
Antwort von 217.111.01.00: Bytes=32 Zeit=64ms TTL=247
Antwort von 217.111.01.00: Bytes=32 Zeit=64ms TTL=247

Ping-Statistik für 217.111.01.00:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 64ms, Maximum = 64ms, Mittelwert = 64ms

C:\Users\strategus>getmac

Physikal. Adresse      Transportname
-----
00-16-8D-63-00-00     Nicht zutreffend
00-C0-00-00-3E-7D     Medien ausgeworfen

C:\Users\strategus>
```

Getmac

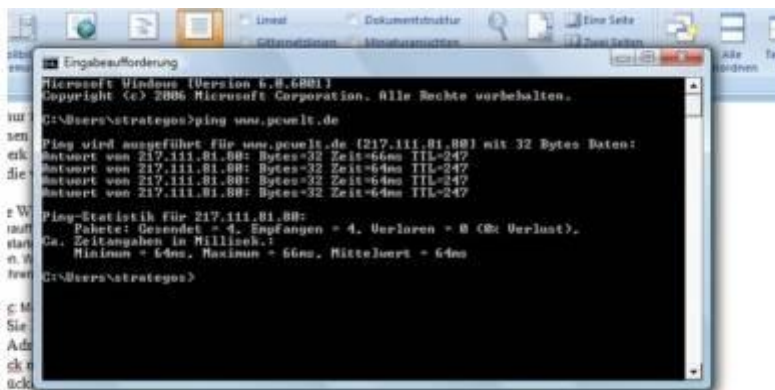
Die hinlänglich bekannten IP-Adressen, die zunächst einmal für die Adressierung der Datenpakete verantwortlich sind, werden auf die Mac-Adressen abgebildet. Bei jeder Internetkommunikation muss also die zu einer IP-Adresse gehörige Mac-Adresse gesucht werden. Dafür ist das Adress Resolution Protocol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

Wenn Sie Ihr Netzwerk oder Ihren Router konfigurieren, benötigen Sie oft die MAC-Adressen Ihrer Netzwerkadapter. Sie ermitteln seit [Windows XP](#) die Mac-Adressen ruck zuck mit dem Tool `Getmac.exe`. Geben Sie also in der Eingabeaufforderung `getmac` ein und drücken Sie Enter. 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. [Sie können winipcfg aber nach wie vor installieren.](#)

Ping: Testet die Internet-Verbindung

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.



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\strategos>ping www.pcwelt.de

Ping wird ausgeführt für www.pcwelt.de [217.111.81.88] mit 32 Bytes Daten:
Antwort von 217.111.81.88: Bytes=32 Zeit=64ms TTL=247
Antwort von 217.111.81.88: Bytes=32 Zeit=64ms TTL=247
Antwort von 217.111.81.88: Bytes=32 Zeit=64ms TTL=247
Antwort von 217.111.81.88: Bytes=32 Zeit=64ms TTL=247

Ping-Statistik für 217.111.81.88:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Gd., Zeitangaben in Millisek.:
    Minimum = 64ms, Maximum = 66ms, Mittlungszeit = 64ms

C:\Users\strategos>
```

Ping

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 IP-Adresse" oder "ping ww.name-der-gewünschten-website.de" ein. Also beispielsweise ping www.pcwelt.de. Diese Anfrage nennt man Echo Request. Der angepingte Host antwortet, wenn er erreichbar ist, mit einem Echo 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), sowie die Zeit, die die 32 Bytes großen Datenpakete benötigen – die so genannte 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 können, 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 ein Time out für das Paket. Wenn Sie ping mit dem Parameter -t eingeben, erfolgt ein Dauerping, den Sie mit CTRL+C abbrechen: ping www.pcwelt.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 Hostnamen auf. -n legt die Anzahl der ICMP-Pakete fest (default sind 4).

tracert und pathping: 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 so genannten Hops) eines Datenpakets zwischen zwei Hosts anzeigen. Geben Sie beispielsweise "`tracert www.pcwelt.de`" ein. Sie erfahren dann, dass das Datenpaket an `pcwelt.de` über – in unserem konkreten Beispiel siehe Screenshot – acht Hops geht. Angefangen mit der Fritzbox (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.

```
C:\Users\strategos>net
Die Syntax dieses Befehls lautet:

NET
 [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPPRG | LOCALGROUP | PAUSE | PRINT | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\strategos>net view
Systemfehler 6118 aufgetreten.
Die Liste der Server in dieser Arbeitsgruppe ist zurzeit nicht verfügbar.

C:\Users\strategos>net Computer
Die Syntax dieses Befehls lautet:

NET COMPUTER
 \\Computername [/ADD | /DEL]

C:\Users\strategos>net time
^C
C:\Users\strategos>tracert www.pcwelt.de
Routenverfolgung zu www.pcwelt.de [217.111.81.88] über maximal 30 Abschnitte:

  1  <1 ms    1 ms    <1 ms    Fritz.Fon [192.168.178.1]
  2  40 ms    41 ms    40 ms    217.0.118.30
  3  41 ms    42 ms    41 ms    87.106.240.18
  4  49 ms    49 ms    49 ms    217.239.40.226
  5  49 ms    50 ms    49 ms    194.25.289.38
  6  64 ms    63 ms    64 ms    212.74.72.43
  7  64 ms    64 ms    65 ms    62.96.179.118
  8  67 ms    65 ms    64 ms    217.111.81.88

Ablaufverfolgung beendet.
C:\Users\strategos>
```

tracert

Tracert kann sowohl mit einer IP-Adresse als auch mit einem Hostnamen genutzt werden. Zu Hostnamen gibt Tracert die IP-Adresse an.

Der Ausdruck Time to Live TTL bezeichnet übrigens die Lebensdauer eines Datenpaketes im Netz. Maximal kann ein Paket über 255 Router gehen, wobei Time to Live bei jedem Routerübergang (Hop) um eins reduziert wird. Erreicht TTL 0 und konnte es bis dahin nicht zugestellt werden, wird das Paket verworfen.

```

C:\>pathping
Microsoft Windows [Version 5.1.2600]
(c) Copyright 1995-2001 Microsoft Corp.

C:\>pathping

Syntax: pathping [-w Hostliste] [-b max. Abschnitte] [-j Adresse] [-u]
               [-p Erprobung] [-r Erprobungsanzahl] [-s Zeitlimit] [-P] [-R]
               [-I] [-A] [-V] Erloesung

Optionen:
-w Hostliste      "Leere Stringe Route" gemäß Hostliste.
-b max. Abschnitte  Max. Anzahl an Abschnitten bei Zielsuche.
-i Adresse        Toleranz für unvollst. Zieladresse.
-j Adresse        Adresse(n) nicht in Routenplan auf lösen.
-p Erprobung      Suchzeit in Millisekunden zwischen Pfaden.
-r Erprobungsanzahl  Anzahl der Abfragen pro Abschnitt.
-s Zeitlimit      Zeitlimit in Millisekunden für eine Route.
-P               Überprüft MSSP-Feldinhalt (1/0).
-R               Überprüft, ob jeder Abschnitt MSSP unterstützt.
-I               Überprüft Überbindung zu jedem Abschnitt mit
                 Layer-2-Protokollen.
-A               Erfordert Datenmenge von 1Pb.
-V               Erfordert Verwendung von IPb.

C:\>pathping www.pccw.de

Routeenerfolgung zu www.pccw.de [192.111.81.88]
Über maximal 30 Abschnitte:
  0  CERNF02M111.idgmc.idg [192.168.1.94]
  1  192.168.1.254
  2  idg-fu-1-berlin.idgmc.idg [192.168.9.200]
  3  www.pccw.de [192.111.81.88]

Berechnung der Statistiken dauert ca. 7s Sekunden...
Abz. Zeit  Src.,Dst.  s  Dstl.,Ges.  s  Adresse
  0
  1  1ms  0/ 100 - 0:  0/ 100 - 0:  192.168.1.254
  2  10ms 0/ 100 - 0:  0/ 100 - 0:  idg-fu-1-berlin.idgmc.idg [192.16
  9.200]
  3  10ms 0/ 100 - 0:  0/ 100 - 0:  www.pccw.de [192.111.81.88]

Routeenerfolgung beendet.
C:\>

```

Pathping

Pathping ist die Weiterentwicklung der Befehle tracert und ping. Der obere Teil der Ausgabe entspricht weitgehend dem Ergebnis von tracert. Darunter folgte eine ausführliche Analyse mit Informationen zur Weiterleitung der Datenpakete über die einzelnen Hops. Alle Zwischenstationen respektive Router erhalten Pings, anhand deren 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.

Ipconfig: Netzwerk-Konfiguration des Rechners anzeigen (displaydns/flushdns)

Geben Sie ipconfig ein um auf einen Blick alle Konfigurations-Einstellungen 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 (das dürfte bei den meisten Heimanwendern die Adresse des DSL-Routers sein). Auch zum für Ihren Rechner zuständigen DNS-Server finden Sie mit ipconfig Informationen.

```
C:\Users\hd\rechner>ipconfig
Windows-IP-Konfiguration

Ethernet-Adapter LAN-Verbindung:
    Verbindungsgeschwindigkeit: 300-Mbit/s
    Verbindungskabel: 1000-Mbit/s
    IP4-Adresse . . . . . : 192.168.1.22
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.1.254

Tunnel-Adapter {antap.1dgmz.1dgt}
    Medienstatus . . . . . : Medien getrennt
    Verbindungsgeschwindigkeit: 1000-Mbit/s

C:\Users\hd\rechner>ipconfig /all
Windows-IP-Konfiguration

Hostname . . . . . : HD13866362948
    Primäres DNS-Suffix . . . . . : 1dgmz.1dgt
    Protokolltyp . . . . . : IPv4
    IP-Bootstrapping aktiviert . . . . . : Nein
    DNS-Proxy aktiviert . . . . . : Nein
    DNS-Suffixsuchliste . . . . . : 1dgmz.1dgt

Ethernet-Adapter LAN-Verbindung:
    Verbindungsgeschwindigkeit: 1000-Mbit/s
    Beschreibung . . . . . : Intel(R) Ethernet Connection I217-V
    Verbindungskabel: 1000-Mbit/s
    DHCP aktiviert . . . . . : Ja
    AutoStart ignorieren aktiviert . . . . . : Ja
    Verbindungskabel: 1000-Mbit/s
    IP4-Adresse . . . . . : 192.168.1.22 (Beantwortet)
    Subnetzmaske . . . . . : 255.255.255.0
    Lease erhalten . . . . . : Mittwoch, 21. Oktober 2015 00:22:28
    Lease läuft ab . . . . . : Mittwoch, 21. Oktober 2015 10:22:27
    DHCP-Server . . . . . : 192.168.1.1
    DHCP-Client-ID . . . . . : 2-45-25-14
    DHCP-Client-UUID . . . . . : 00-0E-00-01-10-0F-07-20-00-10-10-0E-19-E1-66
    DNS-Server . . . . . : 192.168.1.1
    192.168.1.10
    Primärer WINS-Server . . . . . : 192.168.1.10
    Sekundärer WINS-Server . . . . . : 192.168.1.15
    Metriken über TCP/IP . . . . . : Aktiviert

Tunnel-Adapter {antap.1dgmz.1dgt}
    Medienstatus . . . . . : Medien getrennt
    Verbindungsgeschwindigkeit: 1000-Mbit/s
    Beschreibung . . . . . : Microsoft-Internet-Adapter #2
    Verbindungskabel: 1000-Mbit/s
    IP4-Adresse . . . . . : 192.168.1.1
    DHCP aktiviert . . . . . : Ja
    AutoStart ignorieren aktiviert . . . . . : Ja
```

Die Ausgabe von ipconfig (oben) und ipconfig /all (unten).

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 vielleicht Probleme mit einer vom DHCP-Server falsch zugewiesenen IP-Adresse beheben.

ipconfig /displaydns

Ipconfig bietet auch Optionen zum Löschen des DNS-Cache (DNS: Domain Name Service). In diesem Cache werden die Ergebnisse von DNS-Anfragen abgelegt, also konkret Webseitenname und die dazu gehörige IP-Adresse. Die Folge: Wenn Sie im Browser eine Webseite aufrufen, die Sie bereits angesurft haben, dann muss dafür keine neuen Anfrage an den DNS-Server gesendet werden. Damit vermeiden Sie etwas Traffic und vor allem wird die Webseite schneller geladen.

```
Eintragstyp . . . . . : 1
Gültigkeitsdauer . . . . : 11
Datenlänge . . . . . : 4
Abschnitt . . . . . : Antwort
<Host->A-Eintrag . . . : 173.194.113.105

Eintragsname . . . . . : docs.google.com
Eintragstyp . . . . . : 1
Gültigkeitsdauer . . . . : 11
Datenlänge . . . . . : 4
Abschnitt . . . . . : Antwort
<Host->A-Eintrag . . . : 173.194.113.102

Eintragsname . . . . . : docs.google.com
Eintragstyp . . . . . : 1
Gültigkeitsdauer . . . . : 11
Datenlänge . . . . . : 4
Abschnitt . . . . . : Antwort
<Host->A-Eintrag . . . : 173.194.113.110

Eintragsname . . . . . : docs.google.com
Eintragstyp . . . . . : 1
Gültigkeitsdauer . . . . : 11
Datenlänge . . . . . : 4
```

`ipconfig /displaydns`

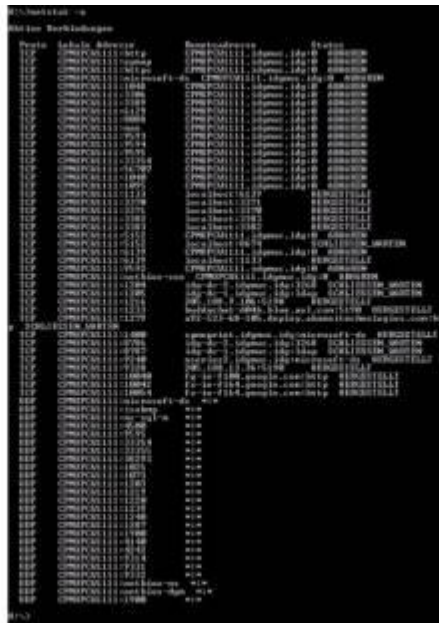
Mit `ipconfig /displaydns` zeigen Sie alle im DNS-Cache vorhandenen Einträge an, siehe den obigen Screenshot, der nur einen kleinen Ausschnitt des DNS-Cache unseres Windows-PCs darstellt. Weil die Liste mit den DNS-Einträgen recht lang ist, empfiehlt es sich den Befehl mit folgender Syntax einzugeben: `ipconfig /displaydns | more`. Das Pipe-Symbol `|` erreichen Sie durch die Kombination aus „<>-Taste“ und „ALTGR“. Danach können Sie bequem durch die Anzeige per Druck auf die Entertaste blättern.

Zu jedem Eintrag finden Sie nicht nur den Domainnamen und die IP-Adresse, sondern auch die Gültigkeitsdauer des jeweiligen Eintrags in Sekunden. Unter den Einträgen im DNS-Cache finden Sie auch die Webseiten, die Ihnen in irgendeiner Form Werbung präsentieren, ohne dass Sie diese Webseiten besucht haben. Das läuft stattdessen über die Werbenetzwerke.

ipconfig /flushdns

Mit `ipconfig /flushdns` leeren Sie den DNS-Cache. Tippen Sie danach `ipconfig /displaydns` erneut ein. Nun sollte der Cache leer sein. Doch schon bald finden Sie wieder Einträge. Zum Beispiel wenn Ihr Mailclient Mails abrufen. Oder wenn Sie eine Webseite wieder im Browser angesurft haben. Rufen Sie denn erneut den DNS-Cache auf und Sie sehen die entsprechenden neuen Einträge, gegebenenfalls mit den ganzen Werbenetzwerken, die dahinter stehen.

Netstat: Zeigt alle geöffneten Netzwerkverbindungen an



netstat

Mit netstat zeigen Sie alle geöffneten TCP- und UDP-Verbindungen an (UDP ist ein Alternativ-Protokoll 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 so genannten Socket, die Ziel-/Remoteadresse und den aktuellen Status, beispielsweise hergestellt (also verbunden). Wenn Sie wirklich alle Netzwerk-Verbindungen anzeigen lassen, geben Sie "netstat -ao" ein. In diesem Fall werden dann auch UDP-Verbindungen (das a steht für all) und alle Prozess-IDs (o zeigt die PIDs an), die zu einer Netzwerkverbindung gehören, angezeigt.

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. Zur eingehenden Analyse empfiehlt es sich den eingangs empfohlenen Tipp anzuwenden und die Ausgabe von netstat in eine Datei umzuleiten.

```
H:\>netstat -c
LAN-Verbindung:
Knoten-IP-Adresse: [192.168.1.14] Bereichskennung: []

NetBIOS-Remotecache-Namentabelle
-----
Name                Typ                Hostadresse        Dauer [Sek.]
-----
MSERIES2            <20> EINDEUTIG        192.168.11.2      422

H:\>hostname
CPMUPCW1111

H:\>netstat -a CPMUPCW1111
LAN-Verbindung:
Knoten-IP-Adresse: [192.168.1.14] Bereichskennung: []

NetBIOS-Namentabelle des Remotecomputers
-----
Name                Typ                Status
-----
CPMUPCW1111        <00> EINDEUTIG        Registriert
IDGNUM              <00> GRUPPE          Registriert
CPMUPCW1111        <20> EINDEUTIG        Registriert
IDGNUM              <1E> GRUPPE          Registriert

MAC Adresse = 00-30-05-9D-BF-9A
```

nbstat

nbtstat liefert die Verbindungsinformationen für NetBIOS over TCP/IP (NBT), es entspricht von der Funktionalität her also ipconfig. Remoterechner können via IP-Adresse oder über ihren Hostnamen angesprochen werden. Der Befehl hat etliche Parameter, wie gehabt gibt die Hilfefunktionen Auskunft.

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.

```
H:\>net user
Benutzerkonten für \\CPMUPCW1111
-----
Administrator          ASPNET          Gast
hc                      paragon_db_scheduler
Der Befehl wurde erfolgreich ausgeführt.
H:\>_
```

net user

Net share zeigt alle Freigaben des lokalen Rechners an. Mit net share Name_des_freigegebenen_Laufwerks lassen Sie sich Details zu der 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.

Netsh

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

Netsh für WLAN

Mit „Netsh wlan show drivers“ lassen Sie sich alle Informationen zum verbauten WLAN-Modul und den dafür installierten Treibern anzeigen. Von oben nach unten liefert dieser Befehl Modellname, Anbieter des Moduls, Treiber-Version, -Datum und die verschiedenen Treiber-Dateien. In der Zeile „Unterstützte Funktypen“ steht, ob das WLAN-Modul auch 5 GHz unterstützt. Steht dort nur 802.11b, 802.11g und 802.11n, dann funkt das WLAN-Modul nur über 2,4 GHz. Steht dort aber 802.11a oder 802.11ac, dann können Sie sich mit ihm auch über 5 GHz mit einem passenden Router verbinden.

Danach folgen Angaben zum Verschlüsselungsverfahren der WLAN-Adapter. „WPA2-Personal CCMP“ ist Pflicht - dann können Sie WPA2 nutzen. WPA2-Enterprise ist nur für Unternehmen interessant, bei denen ein spezieller Server den Zugang zum WLAN verwaltet. CCMP steht hier für Counter Mode Cipher Block Chaining Message Authentication Code Protocol: Ein Verschlüsselungsprotokoll, das den Verschlüsselungsalgorithmus AES nutzt. Oft auch als WPA2-AES. Bei der Fritzbox von AVM als WPA2 (CCMP) bezeichnet.

Starten Sie Ihren eigenen WLAN-Hotspot

Windows bietet seit Windows 7 die Funktion Virtual Wifi, mit der Sie Ihren PC in einen WLAN-Hotspot verwandeln. Vorausgesetzt in Ihrem PC ist eine WLAN-Karte verbaut.

Verbinden Sie Ihren PC also mit einem LAN-Anschluss und geben Sie dann im Startmenü „cmd“ ein und starten Sie den Befehl per Rechtsklick mit der Maus über „Als Administrator ausführen“. Geben Sie in die Eingabeaufforderung dann diese beiden Zeilen ein:

```
Netsh wlan set hostednetwork mode=allow ssid=meinwlan key=meinwlan
```

```
netsh wlan start hostednetwork
```

Die Angaben für ssid (Netzname) und key (Kennwort) können Sie frei wählen.

Gehen Sie danach über die Systemsteuerung auf „Netzwerk- und Freigabecenter -> Adaptereinstellungen ändern“. Dort konfigurieren Sie die Verbindung des Kabelnetzwerkadapters neu. Klicken Sie mit der rechten Maustaste auf den primären Netzadapter (meist Ethernet) und wählen Sie „Eigenschaften“. Auf der Registerkarte „Freigabe“ aktivieren Sie „Gemeinsame Nutzung der Internetverbindung“. Wählen Sie unter „Freigabe“ per Drop-down-Feld den vorher eingerichteten virtuellen Adapter aus.

Tipp: Bei einigen Systemen liefert netsh start hostednetwork eine Fehlermeldung. Das Problem lässt sich meist über den Gerätemanager lösen. Suchen Sie dort nach dem „Microsoft Virtual Wifi Miniport Adapter“ und aktivieren Sie diesen.

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 so genannte Routing-Tabellen.

```
C:\>route print
=====
Schnittstellenliste
0x1 ..... MS TCP Loopback interface
0x2 ...00 30 05 9d bf 9a ..... Intel(R) PRO/1000 CT Network Connection - Paketp
laner-Miniport
=====
Aktive Routen:
  Netzwerkziel    Netzwerkmaske    Gateway    Schnittstelle    Anzahl
  0.0.0.0         0.0.0.0         192.168.1.254    192.168.1.14    20
  127.0.0.0      255.0.0.0       127.0.0.1       127.0.0.1       1
  192.168.1.0    255.255.255.0   192.168.1.14    192.168.1.14    20
  192.168.1.14  255.255.255.255 127.0.0.1       127.0.0.1       20
  192.168.1.255 255.255.255.255 192.168.1.14    192.168.1.14    20
  224.0.0.0     240.0.0.0       192.168.1.14    192.168.1.14    20
  255.255.255.255 255.255.255.255 192.168.1.14    192.168.1.14    1
Standardgateway: 192.168.1.254
=====
Ständige Routen:
Keine
```

route print

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`.

Mit Hilfe des DNS-Protokolls (Domain Name System) werden für den Menschen leichter zu merkende Hostnamen mit einer IP-Adresse verbunden. Mit `nslookup` können Sie manuell eine Anfrage an einen Nameserver schicken, um einen Hostnamen 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. Geben Sie bei gestartetem `nslookup` einen Hostnamen ein, zum Beispiel `www.pcwelt.de`. `Nslookup` löst ihn in eine IP-Adresse auf.

Hostname, FTP, Telnet FTP: Datei-Upload und -Download via File Transfer Protocol

Hostname

Ermittelt Sie den Hostnamen Ihres PCs.



```
ca\ Eingabeaufforderung
H:\>ftp
ftp> help
Befehle können abgekürzt werden. Befehle sind:

?          delete          literal          prompt          send
?          debug           ls              put             status
append    dir             mdelete        pwd            trace
ascii    disconnect    mdir           quit           type
bell      get            nget          quote          user
binary   glob           mkdir         recv          verbose
bye      hash          mls           remotehelp
cd       help          mput         rename
close   lcd           open         rmdir
ftp> quit

H:\>_
```

Hostname, FTP, Telnet FTP: Datei-Upload und -Download via File Transfer Protocol

Für gewöhnlich erledigen Sie FTP-Transfers mit einem geeigneten FTP-Client wie [Filezilla](#) oder einem Datei-Manager mit integrierter FTP-Funktion wie [Total Commander](#). FTP-Uploads machen Sie beispielsweise wenn Sie Ihren Webauftritt aktualisieren; FTP-Downloads kommen vor, wenn Sie sich die neueste Firefox-Version direkt vom FTP-Server von Mozilla.org runterziehen wollen noch bevor diese offiziell bekannt ist. 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 Befehl **Telnet** zur Verfügung. Mit ihm können Sie sich von einem Telnet-Client aus 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.

[Tipp: Windows bietet noch mehr geheime Kommandozeilen-Befehle.](#)

Hier finden Sie weitere Windows-Tipps

Fanden Sie die Tipps nützlich? Dann könnte Ihnen auch unser Sonderheft **Windows Tipps und Tricks** mit 300 Tricks für maximale Power gefallen. Sie können das digitale Sonderheft in unserer Magazin-App kaufen und lesen. Die digitale Version entspricht komplett der gedruckten Version, inklusive einer Online-Heft-DVD. [Die Magazin-App bekommen Sie hier.](#) Tippen Sie nach der Installation in der App auf „Heft-Kiosk“ und suchen Sie sich das Sonderheft aus.

Übrigens: Wenn Sie die App zum ersten Mal installieren, bekommen Sie ein Heft gratis. [Hier finden Sie weitere Infos zur App.](#)



Lesen Sie dieses Windows-Sonderheft der PC-WELT in der neuen Magazin-App für Android, iOS und Windows.