



## 8 ابزار کاربردی خط فرمان ویندوز برای مدیریت و نظارت بر شبکه‌ها

تاکنون چند مرتبه از خط فرمان استفاده کرده‌اید؟ کار با یک محیط خط فرمان فاقد رابط گرافیکی پیچیده نیست و شما با تایپ دستورات به سادگی می‌توانید از آن استفاده کنید. خط فرمان یکی از پرکاربردترین ابزارهایی است که مدیران شبکه از آن استفاده می‌کنند. بیشتر مدیران شبکه ترجیح می‌دهند به جای یک رابط گرافیکی به سادگی دستورات مدنظر خود را همراه با سویچ‌های مربوطه درون این محیط وارد کنند تا سریع‌تر به کارهای خود برسند. مهم نیست یک کاربر عادی یا مدیر شبکه باشید، آشنایی با دستورات خط فرمان به شما اجازه می‌دهند با سهولت بیشتری به مدیریت شبکه‌های خانگی یا اداری بپردازید. در این مقاله با 8 فرمان کاربردی این محیط در ارتباط با شبکه‌ها آشنا خواهید شد.

### 1. Ping

پینگ یکی از ساده‌ترین و مفیدترین دستوراتی است که باید نحوه کار با آن را به خوبی یاد بگیرید. فرمان فوق اعلام می‌دارد که آیا کامپیوتر شما قادر است به آدرس آی‌پی مقصد خاص یا یک نام دامنه برسد یا خیر و اگر قادر به انجام چنین کاری است چه مدت زمان طول می‌کشد تا داده‌ها بین مبداء و مقصد در تبادل باشند. مثال زیر نحوه پینگ کردن به سایت گوگل و نتیجه پینگ را نشان می‌دهد.

```
C:\Users\Joel>ping www.google.com

Pinging www.google.com [216.58.219.228] with 32 bytes of data:
Reply from 216.58.219.228: bytes=32 time=16ms TTL=54
Reply from 216.58.219.228: bytes=32 time=20ms TTL=54
Reply from 216.58.219.228: bytes=32 time=18ms TTL=54
Reply from 216.58.219.228: bytes=32 time=16ms TTL=54

Ping statistics for 216.58.219.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 20ms, Average = 17ms
```

این فرمان با ارسال بسته‌های داده چندگانه و بررسی این مسئله که چه تعداد از این بسته‌ها باز می‌گردند کار می‌کند. اگر برخی از بسته‌ها باز نگردند، پینگ با نشان دادن واژه lost از دست رفتن بسته‌ها را اعلام می‌کند. از دست دادن بسته‌ها بیانگر عملکرد ضعیف بوده و نشان می‌دهد که فرآیند استریم به کندی صورت می‌گیرد. ابزار فوق یک راه‌کار عالی برای آزمایش عملکرد شبکه‌ها است. به‌طور پیش‌فرض پینگ چهار بسته را ارسال می‌کند و

برای هر یک بازه زمانی انتظار 4 ثانیه‌ای در نظر می‌گیرد. البته شما می‌توانید تعداد بسته‌هایی که پینگ می‌تواند آن‌ها را ارسال کند را افزایش دهید. فرمان زیر نحوه انجام این کار را نشان می‌دهد.

```
Ping www.google.com -n 10
```

شما همچنین می‌توانید مدت زمان انتظار را در واحد میلی‌ثانیه به صورت زیر افزایش دهید.

```
Ping www.google.com -w 6000
```

## 2. TRACERT

Tracert سرنام دو واژه Trace Route است. شبیه به پینگ، یک بسته داده‌ای را برای اشکال‌زدایی شبکه‌ها ارسال می‌کند. به عبارت دیگر ابزار فوق برای تعیین مسیری که بسته‌های داده‌ای برای رسیدن به مقصد طی می‌کنند استفاده می‌شود. دستور tracert و پینگ متفاوت از یکدیگر هستند. پینگ به شما اعلام می‌دارد که آدرسی که به آن پینگ کرده‌اید فعال است یا خیر، اما tracert تمامی روترهایی که بسته‌های داده در مسیر با آن‌ها در تعامل هستند را به کاربر نشان می‌دهد. شکل زیر به کارگیری ابزار فوق روی دامنه گوگل را نشان می‌دهد.

```
C:\Users\Joel>tracert www.google.com

Tracing route to www.google.com [216.58.219.228]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    192.168.0.1
  1  11 ms     11 ms    13 ms    96.120.77.49
  2  11 ms     10 ms    11 ms    xe-7-3-0-32767-sur01.49thst.pa.panjde.comcast.net [6
  3  12 ms     12 ms    12 ms    be-23-ar03.newcastle.de.panjde.comcast.net [69.139.1
  4  13 ms     14 ms    13 ms    hu-0-9-0-0-ar03.ivyland.pa.panjde.comcast.net [69.13
  5  19 ms     18 ms    18 ms    be-33287-cr02.newyork.ny.ibone.comcast.net [68.86.93
  6  17 ms     17 ms    16 ms    68.86.84.218
  7  17 ms     18 ms    16 ms    as27589-2.miami.fl.ibone.comcast.net [75.149.228.186
  8  18 ms     18 ms    17 ms    216.239.62.125
  9  17 ms     16 ms    18 ms    64.233.174.117
 10  18 ms     16 ms    16 ms    lga25s41-in-f228.1e100.net [216.58.219.228]

Trace complete.
```

خروجی فرمان فوق به صورت خلاصه در هر خط وضعیت هر هاپ (hop) که شامل زمان تاخیر بین دستگاه شما و هاپ خاصی است را همراه با آدرس آی‌پی هر هاپ را (به علاوه نام دامنه در صورت موجود بودن) نشان می‌دهد.

چرا سه زمان تاخیر در هر هاپ مشاهده می‌کنیم؟ به دلیل این‌که tracert سه بسته را برای هاپ ارسال می‌کند، در برخی موارد یکی از آن‌ها ممکن است از دست رفته یا زمان طولانی مدتی را صرف کنند که باعث می‌شود زمان تاخیر واقعی نشان داده نشود.

## 3. PATHING

Pathing عملکردی شبیه به Tracert دارد، اما اطلاعات مفیدتر و جامع‌تری ارائه می‌کند. پس از آن‌که با استفاده از فرمان فوق بسته‌ها را برای مقصد خاصی ارسال کردید، ابزار فوق مسیر را تجزیه و تحلیل می‌کند و بسته‌های از دست رفته بر مبنای هر هاپ را محاسبه می‌کند. شکل زیر عملکرد ابزار فوق را نشان می‌دهد.

```

C:\Users\Joel>pathping www.google.com

Tracing route to www.google.com [216.58.219.228]
over a maximum of 30 hops:
 0  DESKTOP-44N9LCA [192.168.0.102]
 1  192.168.0.1
 2  96.120.77.49
 3  xe-7-3-0-32767-sur01.49thst.pa.panjde.comcast.net [68.86.218.117]
 4  be-23-ar03.newcastle.de.panjde.comcast.net [69.139.192.177]
 5  hu-0-9-0-0-ar03.ivyland.pa.panjde.comcast.net [69.139.193.193]
 6  be-33287-cr02.newyork.ny.ibone.comcast.net [68.86.93.173]
 7  68.86.84.218
 8  as27589-2.miami.fl.ibone.comcast.net [75.149.228.186]
 9  216.239.62.125
10  64.233.174.117
11  lga25s41-in-f228.1e100.net [216.58.219.228]

Computing statistics for 275 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
     |      Lost/Sent = Pct  Lost/Sent = Pct  |
 0   |      0/ 100 = 0%    0/ 100 = 0%     | DESKTOP-44N9LCA [192.168.0.102]
 1   | 0ms    0/ 100 = 0%    0/ 100 = 0%     | 192.168.0.1
 2   | 11ms   0/ 100 = 0%    0/ 100 = 0%     | 96.120.77.49
 3   | 12ms   0/ 100 = 0%    0/ 100 = 0%     | xe-7-3-0-32767-sur01.49thst.pa.panjde.
 4   | 13ms   0/ 100 = 0%    0/ 100 = 0%     | be-23-ar03.newcastle.de.panjde.comcast
 5   | 15ms   0/ 100 = 0%    0/ 100 = 0%     | hu-0-9-0-0-ar03.ivyland.pa.panjde.comc
 6   | 18ms   0/ 100 = 0%    0/ 100 = 0%     | be-33287-cr02.newyork.ny.ibone.comcast
 7   | 17ms   0/ 100 = 0%    0/ 100 = 0%     | 68.86.84.218
 8   | 18ms   0/ 100 = 0%    0/ 100 = 0%     | as27589-2.miami.fl.ibone.comcast.net [
 9   | ---    100/ 100 =100% 100/ 100 =100%  | 216.239.62.125
10  | ---    100/ 100 =100% 100/ 100 =100%  | 64.233.174.117
11  | 19ms   0/ 100 = 0%    0/ 100 = 0%     | lga25s41-in-f228.1e100.net [216.58.219

Trace complete.

```

## IPCONFIG.4

یکی از پرکاربردترین فرمان‌های شبکه است که سیستم‌عامل ویندوز در اختیار دارد. ابزار فوق نه تنها اطلاعات مفیدی ارائه می‌کند، بلکه اجازه می‌دهد ابزار فوق را همراه با سویچ‌هایی برای انجام یک کار به خصوص استفاده کنید. شکل زیر خروجی فرمان فوق را نشان می‌دهد.

```

C:\Users\Joel>ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . . . . . :
    Link-local IPv6 Address . . . . . : fe80::c115:5e0b:95a4:5aa3%8
    IPv4 Address. . . . . : 192.168.0.102
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :

Tunnel adapter isatap.{FCEE928D-4AE1-4204-8F5F-4C64CD07A080}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . . . . . :
    IPv6 Address. . . . . : 2001:0:9d38:6ab8:2058:2d97:3f57:ff99
    Link-local IPv6 Address . . . . . : fe80::2058:2d97:3f57:ff99%3
    Default Gateway . . . . . : ::

```

خروجی پیش فرض، هر آداپتور شبکه متصل به سامانه را نشان داده و نحوه resolve کردن آدرسها توسط آداپتورها را تشریح می کند. Default Gateway و IPv4 Address که در پایین بخش Wireless LAN Adapter و Ethernet Adapter قرار دارند، اطلاعات مفید و کاربردی را نشان می دهند. شما می توانید برای پاک کردن کش سامانه نام دامنه نیز فرمان فوق را با سوییچ زیر استفاده کنید.

Ipconfig /flushdns

پاک کردن کش سامانه نام دامنه، زمانی که قادر نیستید به یک وبسایت خاص یا سروری به دلایل مختلف متصل شوید مفید است.

## GETMAC.5

هر دستگاه سازگار با استاندارد IEEE 802 یک آدرس مک منحصر به فرد دارد. آدرسهای مک توسط تولیدکنندگان به دستگاهها تخصیص داده شده و درون سخت افزار دستگاه ذخیره می شوند. برخی از مردم از آدرسهای مک برای محدود کردن دستگاههایی که می توانند به یک شبکه متصل شوند استفاده می کنند. تصویر زیر خروجی این فرمان را نشان می دهد.

```
C:\Users\Joel>getmac

Physical Address      Transport Name
-----
00-FF-CB-10-15-73    Media disconnected
28-F0-76-10-E8-E2    Media disconnected
38-C9-86-21-D0-4D    \Device\Tcpip_{FCEE928D-4AE1-4204-8F5F-4C64CD07A080}
```

بسته به کارت‌های شبکه‌ای که روی کامپیوتر خود نصب کرده‌اید، ممکن است بیش از یک مک‌آدرس را مشاهده کنید. به‌طور مثال ارتباطات اترنت و وای‌فای هر یک مک‌آدرس‌های جداگانه‌ای دارند.

### NSLOOKUP.6

Nslookup سرنام Name Server Lookup است. یکی دیگر از ابزارهای قدرتمند شبکه است که برخی از کاربران اطلاعی در مورد توانایی‌های آن ندارند. در حالت عادی ابزار فوق برای پیدا کردن آدرس آی‌پی یک دامنه خاص استفاده می‌شود. شکل زیر این موضوع را نشان می‌دهد.

```
C:\Users\Joel>nslookup www.google.com
1.0.168.192.in-addr.arpa
    primary name server = localhost
    responsible mail addr = nobody.invalid
    serial = 1
    refresh = 600 (10 mins)
    retry = 1200 (20 mins)
    expire = 604800 (7 days)
    default TTL = 10800 (3 hours)
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f8b0:4006:80d::2004
           172.217.4.68
```

توجه داشته باشید که برخی از نام‌های دامنه به یک آدرس تخصیص داده شده متصل نیستند. این حرف به این معنا است که هر بار که شما فرمان فوق را اجرا می‌کنید، ممکن است آدرس‌های آی‌پی مختلف را دریافت کنید. این موضوع در مورد وب‌سایت‌های بزرگ عادی است، زیرا آن‌ها حجم کاری خود را میان ماشین‌های مختلفی توزیع می‌کنند. اگر می‌خواهید یک آدرس آی‌پی را به یک نام دامنه تبدیل کنید، کافی است آن را در مرورگر خود تایپ کرده و ببینید چه اتفاقی رخ می‌دهد. دقت کنید که برخی از آدرس‌های آی‌پی در اینترنت در دسترس نیستند.

### NETSTAT .7

Netstat یکی دیگر از ابزارهای کاربردی شبکه است که برای آمارگیری، تشخیص خطا و تحلیل‌ها از آن استفاده می‌شود. یک ابزار قدرتمند و پیچیده که البته اگر از کاربردهای پیشرفته آن صرف‌نظر کنید به یک ابزار ساده و کارآمد تبدیل می‌شود. شکل زیر خروجی این فرمان را نشان می‌دهد.

```
C:\Users\Joel>netstat
```

```
Active Connections
```

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1564	DESKTOP-44N9LCA:1565	ESTABLISHED
TCP	127.0.0.1:1565	DESKTOP-44N9LCA:1564	ESTABLISHED
TCP	127.0.0.1:1566	DESKTOP-44N9LCA:1567	ESTABLISHED
TCP	127.0.0.1:1567	DESKTOP-44N9LCA:1566	ESTABLISHED
TCP	127.0.0.1:1589	DESKTOP-44N9LCA:1590	ESTABLISHED
TCP	127.0.0.1:1590	DESKTOP-44N9LCA:1589	ESTABLISHED
TCP	127.0.0.1:1594	DESKTOP-44N9LCA:1595	ESTABLISHED
TCP	127.0.0.1:1595	DESKTOP-44N9LCA:1594	ESTABLISHED
TCP	127.0.0.1:1645	DESKTOP-44N9LCA:1646	ESTABLISHED
TCP	127.0.0.1:1646	DESKTOP-44N9LCA:1645	ESTABLISHED
TCP	192.168.0.102:1552	bn3sch020010540:https	ESTABLISHED
TCP	192.168.0.102:1560	client:https	CLOSE_WAIT
TCP	192.168.0.102:1568	api:https	CLOSE_WAIT
TCP	192.168.0.102:1597	104.16.59.37:https	ESTABLISHED
TCP	192.168.0.102:1601	qo-in-f109:imaps	ESTABLISHED
TCP	192.168.0.102:1603	s154:imaps	ESTABLISHED
TCP	192.168.0.102:1606	qo-in-f109:imaps	ESTABLISHED
TCP	192.168.0.102:1630	qo-in-f109:imaps	ESTABLISHED
TCP	192.168.0.102:1633	qo-in-f109:imaps	ESTABLISHED
TCP	192.168.0.102:1635	qo-in-f109:imaps	ESTABLISHED
TCP	192.168.0.102:1636	qo-in-f109:imaps	ESTABLISHED
TCP	192.168.0.102:1637	qo-in-f109:imaps	ESTABLISHED
TCP	192.168.0.102:1648	ec2-52-32-153-92:https	ESTABLISHED
TCP	192.168.0.102:1709	pat-ash2:5222	ESTABLISHED
TCP	192.168.0.102:1740	ec2-52-73-156-0:https	ESTABLISHED

به طور پیش فرض، این فرمان همه اتصالات فعال روی سیستم را (اتصالات به شبکه محلی و اینترنت) را نشان می دهد. یک اتصال فعال به معنای آن نیست که در حال انتقال داده ها است، بلکه می تواند پورتی باشد که باز بوده و آماده دریافت یک ارتباط است. این ابزار اطلاعات جامعی در ارتباط با پورت ها در اختیاران قرار می دهد.

## NETSH.8

Netsh سرنام Network Shell است. فرمانی که به شما اجازه مشاهده و پیکربندی هر کارت شبکه ای که روی سیستم خود دارید را داده و در مقایسه با فرمان قبلی اطلاعات بیشتری ارائه می کند. اجرای این دستور در محیط خط فرمان باعث می شود تا کنترل این محیط در اختیار فرمان فوق قرار گیرد. درون پوسته این فرمان زمینه های مختلفی قرار دارند که شامل فرمان های مرتبط با مسیریابی، فرمان های مرتبط با DHCP، شناسایی و... هستند. برای مشاهده تمامی پوسته های شبکه این فرمان از دستور زیر استفاده کنید.

```

C:\Users\Joel>netsh /?

Usage: netsh [-a AliasFile] [-c Context] [-r RemoteMachine] [-u [DomainName\]UserNam
          [Command | -f ScriptFile]

The following commands are available:

Commands in this context:
?           - Displays a list of commands.
add         - Adds a configuration entry to a list of entries.
advfirewall - Changes to the `netsh advfirewall' context.
branchcache - Changes to the `netsh branchcache' context.
bridge     - Changes to the `netsh bridge' context.
delete     - Deletes a configuration entry from a list of entries.
dhcpcclient - Changes to the `netsh dhcpcclient' context.
dnsclient  - Changes to the `netsh dnsclient' context.
dump       - Displays a configuration script.
exec       - Runs a script file.
firewall   - Changes to the `netsh firewall' context.
help       - Displays a list of commands.
http       - Changes to the `netsh http' context.
interface  - Changes to the `netsh interface' context.
ipsec      - Changes to the `netsh ipsec' context.
lan        - Changes to the `netsh lan' context.
mbn        - Changes to the `netsh mbn' context.

```

برای مشاهده تمامی فرمان‌های درون یک زمینه از دستور زیر استفاده کنید:

```

C:\Users\Joel>netsh wlan /?

The following commands are available:

Commands in this context:
?           - Displays a list of commands.
add         - Adds a configuration entry to a table.
connect     - Connects to a wireless network.
delete     - Deletes a configuration entry from a table.
disconnect  - Disconnects from a wireless network.
dump       - Displays a configuration script.
export      - Saves WLAN profiles to XML files.
help       - Displays a list of commands.
refresh     - Refresh hosted network settings.
reportissues - Generate WLAN smart trace report.
set        - Sets configuration information.
show       - Displays information.
start      - Start hosted network.
stop       - Stop hosted network.

To view help for a command, type the command, followed by a space, and then
type ?.

```

برای مشاهده زیرفرمان‌های درون فرمان‌ها نیز از ترکیب نحوی زیر استفاده کنید:

```
C:\Users\Joel>netsh wlan show /?

The following commands are available:

Commands in this context:
show all - Shows complete wireless device and networks information.
show allowexplicitcreds - Shows the allow shared user credentials settings.
show autoconfig - Shows whether the auto configuration logic is enabled or
disabled.
show blockednetworks - Shows the blocked network display settings.
show createalluserprofile - Shows whether everyone is allowed to create all
user profiles.
show drivers - Shows properties of the wireless LAN drivers on the system.
show filters - Shows the allowed and blocked network list.
show hostednetwork - Show hosted network properties and status.
show interfaces - Shows a list of the wireless LAN interfaces on
the system.
show networks - Shows a list of networks visible on the system.
show onlyUseGPPProfilesforAllowedNetworks - Shows the only use GP profiles on GP conf
show profiles - Shows a list of profiles configured on the system.
show randomization - Shows whether MAC randomization is enabled or
disabled.
show settings - Shows the global settings of wireless LAN.
show tracing - Shows whether wireless LAN tracing is enabled or disabled.
show wirelesscapabilities - Shows the wireless capabilities of the system
show wlanreport - Generate a report showing recent wireless session information.
```

به طور مثال، شما می‌توانید از فرمان زیر برای مشاهده همه درایورهای شبکه بی‌سیم که روی سیستم دارید همراه با ویژگی‌های آن‌ها استفاده کنید.

Netsh wlan show drivers

دستور بالا، یک فرمان پیشرفته است که توضیح آن خود به یک مقاله مفصل نیاز دارد. هر زمان به دنبال دریافت اطلاعات فنی ویژه‌ای در ارتباط با پیکربندی شبکه خود هستید، بهتر است از فرمان فوق استفاده کنید.

**تاریخ انتشار:**  
15 مرداد 1398

**نشانی منبع:**

<https://www.shabakeh-mag.com/tricks/network-tricks/15813/8-%D9%81%D8%B1%D9%85%D8%A7%D9%86-%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%AF%DB%8C-%D9%85%D9%87%D9%85-%D8%AE%D8%B7-%D9%81%D8%B1%D9%85%D8%A7%D9%86-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%85%D8%AF%DB%8C%D8%B1%DB%8C%D8%AA-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%DA%A9%D8%A7%D9%85%D9%BE%DB%8C%D9%88%D8%AA%D8%B1%DB%8C-%D8%AF%D8%B1-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2>