به نام خدا

دانشگاه تهران
پردیس فارابی
دانشکده مهندسی
گروه مهندسی کامپیوتر

دستور کار
آزمایشگاه شبکه‌های کامپیوتری

شماره
۲

فرمان‌های پرکاربرد شبکه

Useful Network Commands

فرمان IPCONFIG

فرمان ipconfig یک راه سریع برای نمایش آدرس IP کامپیوتر شما و سایر اطلاعات مانند آدرس Gateway پیش فرض آن است. همچنین در صورتی که بخواهید آدرس IP روتر خود را نیز بدانید این فرمان مفید است.

با استفاده از این فرمان، شما لیستی از تمامی اتصالات شبکه‌ای که کامپیوتر شما از آن استفاده می‌کند را مشاهده می‌نمایید. اگر شما به یک شبکه‌ی بی‌سیم Wi-Fi متصل هستید، اطلاعات زیر بخش "Wireless LAN adapter" و اگر به شبکه‌ی باسیم متصل هستید اطلاعات زیر بخش "Ethernet adapter" را مشاهده نمایید.

```
C:\Users\persys>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection* 12:

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

Ethernet adapter Bluetooth Network Connection:

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

Wireless LAN adapter Wireless Network Connection 3:

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

Wireless LAN adapter Wireless Network Connection 2:

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

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : domain.name
   Link-local IPv6 Address . . . . . : fe80::9097:ede0:4912:28d0%12
   IPv4 Address. . . . . . . . . . . : 192.168.1.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::be34:ff:fe53:ca3e%12
                                       192.168.1.1

Ethernet adapter Local Area Connection:

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

Tunnel adapter isatap.{9BFD38AC-6532-43A0-B361-F3F5415F7B0B}:

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

Tunnel adapter isatap.{BD9DDE97-67EE-4DE0-ACF5-0546A57F3E49}:

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

- فرمان ipconfig /all : برای مشاهده‌ی کامل پیکربندی می‌توانید از این دستور استفاده نمایید.
- فرمان ipconfig /release و ipconfig /renew : فرمان ipconfig /release به همراه ipconfig /renew سیستم عامل شما را مجبور می‌کند یک IP جدید دریافت کند. این فرمان در مواردی که مشکل در اتصال به اینترنت به دلیل تداخل IPها باشد، بسیار کاربردی است.
- فرمان ipconfig /release : با وارد کردن این فرمان از شبکه جدا می‌شوید و IPای را که DHCP به شما اختصاص داده رها می‌کنید و در این زمان سیستم IP دهنده اتوماتیک یا APIPA به شما IP خواهد داد. چنانچه می‌خواهید دوباره از DHCP درخواست IP کنید کافی است ipconfig /Renew را وارد کنید. به این نکته توجه داشته باشید که ممکن است DHCP همان آدرس IP را که قبلاً به شما اختصاص داده بود، مجدداً به شما تخصیص دهد.
- فرمان ipconfig /renew : با استفاده از این فرمان از DHCP درخواست IP جدید می‌کنیم. با فرمان ipconfig /renew درخواست IPv4 و اگر از دستور ipconfig /renew6 استفاده کنید، درخواست IPv6 انجام می‌شود.
  - **نکته:** اگر پس از این سوئیچ، نام کارت شبکه‌ی خاصی را وارد نکنید تغییرات بر روی همه‌ی کارت‌های شبکه اعمال می‌شود.
  - **نکته:** چنانچه می‌خواهید دوباره از DHCP درخواست IP کنید، کافی است ipconfig /renew را وارد کنید. به این نکته توجه داشته باشید که ممکن است DHCP همان IP قبلی را که سابقاً به شما اختصاص داده بود مجدداً تخصیص دهد.
  - در مثال عملی ما IP از ۱۹۲,۱۶۸,۱,۶ پس از release کردن به ۱۶۹,۲۵۴,۴۰,۲۴۰ و پس از renew به ۱۹۲,۱۶۸,۱,۱ تغییر کرده است.

- فرمان ipconfig /flushdns : همچنین پسوند کاربردی دیگر ipconfig /flushdns/ می‌باشد که باعث حذف DNS Cache می‌شود؛ به‌عبارتی به‌جای اینکه از Cache شبکه برای دسترسی به DNS server استفاده شود، مستقیماً اطلاعات را از سرور اصلی دریافت خواهد کرد (اگر شما DNS server خود را تغییر دهید، این تغییرات لزوماً بلافاصله رخ نمی‌دهند. ویندوز از یک حافظه‌ی cache برای یادآوری پاسخ‌های DNSای که دریافت کرده است استفاده می‌کند تا در زمانی که دوباره به همان آدرس در آینده دسترسی انجام می‌شود، صرفه‌جویی شود. برای اطمینان از دریافت آدرس از سرورهای DNS جدید به جای استفاده از مدخل‌های قدیمی ذخیره شده، پس از تغییر DNS server فرمان ipconfig /flushdns/ را وارد نمایید.)

فرمان PING

برای استفاده از فرمان Ping کافی است تا CMD را اجرا کنید و سپس در خط فرمان Ping را با آدرس IP مقصد یا نام سیستم مقصد وارد کنید.

دستور ping یک ابزار برای اشکال زدایی در شبکه می‌باشد. ping بررسی می‌کند تا ببیند که آیا سیستم مقابلش زنده و پاسخگو می‌باشد یا خیر. ping از پیام‌های ICMP استفاده می‌کند (پیام‌های Query Messages).

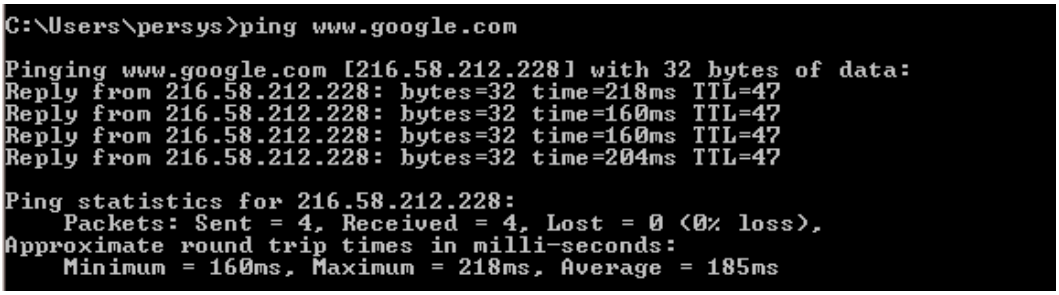
پروتکل ICMP یا Internet Control Message Protocol همدم پروتکل IP می‌باشد. در واقع ICMP یک پروتکل برای کامل کردن IP می‌باشد؛ زیرا IP چیزی برای رساندن خطاها ندارد، پس به یک پروتکل دیگر برای انجام این کار نیاز داریم. پروتکل ICMP دارای دو نوع پیام متفاوت می‌باشد: Error Reporting Message و Query Message که Query Message برای اشکال‌زدایی شبکه استفاده می‌شود. دو نوع Query Message وجود دارد:

- پیام درخواست اکو: Echo-Request Message
- پیام پاسخ اکو: Echo-Reply Message

فرآیند فرمان ping به‌صورت زیر است:

- سیستم منبع یک پیام ICMP Echo-Request به مقصد ارسال می‌کند.
- برنامه ping یک شناسه‌ی ترتیب (Sequence Identifier) را set می‌کند که توسط هر پیام Echo-Request افزایش می‌یابد. همچنین زمان TTL را هم set می‌کند.
- همچنین ping زمان ارسال را در داده‌های پیام قرار می‌دهد.
- اگر سیستم مقصد زنده و پاسخگو باشد، برای سیستم فرستنده، پیام ICMP Echo-Reply ارسال می‌کند.
- برنامه ping زمان ارسال و دریافت را یادداشت کرده و سپس زمان رفت و برگشت را محاسبه می‌کند.
- سپس Sequence Identifier را افزایش می‌دهد و یک پیام Echo-Request جدید ارسال می‌کند.

```
C:\Users\persys>ping/?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t              Ping the specified host until stopped.
                    To see statistics and continue - type Control-Break;
                    To stop - type Control-C.
    -a              Resolve addresses to hostnames.
    -n count        Number of echo requests to send.
    -l size         Send buffer size.
    -f              Set Don't Fragment flag in packet (IPv4-only).
    -i TTL          Time To Live.
    -v TOS          Type Of Service (IPv4-only. This setting has been deprecated
                    and has no effect on the type of service field in the IP Head
er).
    -r count        Record route for count hops (IPv4-only).
    -s count        Timestamp for count hops (IPv4-only).
    -j host-list    Loose source route along host-list (IPv4-only).
    -k host-list    Strict source route along host-list (IPv4-only).
    -w timeout      Timeout in milliseconds to wait for each reply.
    -R              Use routing header to test reverse route also (IPv6-only).
    -S srcaddr      Source address to use.
    -4              Force using IPv4.
    -6              Force using IPv6.
```




```
> ping <destination> -l <size>
```

سایز بسته به‌طور پیش‌فرض ۳۲ بایت است. می‌توانیم با این دستور سایز بسته‌ی ارسالی را مشخص کنیم. به عنوان مثال:

```
Ping  yahoo.com  -l 512
```

```
> ping <destination> -n <number>
```

می‌توان تعداد بسته‌های ارسالی را تعیین کرد. به‌عنوان مثال:

```
ping  yahoo.com  -n 12
```

فرمان TraceRoute (tracert)

این فرمان، نوعی از فرمان `ping` است که برای نشان دادن مسیر کاملی که یک بسته طی می‌کند تا به مقصد برسد استفاده می‌شود.

```
> tracert <destination>
```

با این دستور می‌توان مسیری که بسته‌ی شما در شبکه طی می‌کند تا به مقصد مورد نظر برسد را به‌دست آورد. مثلاً اگر در پنجره خط فرمان تایپ کنیم: `tracert google.com`، مسیر سیستم شما تا سرور گوگل (اصطلاحاً نودها/گره‌ها یا روترهای میان راه) را نشان می‌دهد.

این دستور برای عیب‌یابی در شبکه بسیار کاربردی است و چنانچه بین کامپیوتر شما تا مقصد روترهایی موجود باشد، اطلاعاتی مربوط به هر یک از آن‌ها را گزارش خواهد داد.

دستور `tracert` زمان انتقال بسته‌ها از مبدأ تا هر روتر را محاسبه می‌نماید و از این طریق می‌توانیم دریابیم که در کجای مسیر ارتباطی، مشکل وجود دارد.

این دستور با دستور `ping` متفاوت است. در واقع `ping` به شما می‌گوید که آدرسی که آن را `ping` کرده‌اید فعال است یا خیر و برقراری ارتباط را بررسی می‌کند، اما `tracert` تک تک روترهایی را که بسته‌های داده در مسیر با آن برخورد خواهند داشت را به کاربر نشان می‌دهد. در واقع زمانی که بسته‌های داده به مقصد نمی‌رسند و یا زمان پاسخ دستور `ping` زمانی نامعقول و طولانی باشد از این دستور استفاده می‌کنیم.

دو دستور `tracert` و `traceroute` عملکرد مشابهی دارند با این تفاوت که دستور `tracert`در سیستم عامل ویندوز به کار می رود و `traceroute` در سیستم‌های عامل یونیکس، لینوکس و مکینتاش کاربرد دارد.

می‌توان سوئیچ‌های مختلف این دستور و عملکرد آن‌ها را همان طور که در تصویر زیر آمده است، ملاحظه نمود.

```
C:\Users\persys>tracert/?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                  Do not resolve addresses to hostnames.
    -h maximum_hops     Maximum number of hops to search for target.
    -j host-list        Loose source route along host-list (IPv4-only).
    -w timeout          Wait timeout milliseconds for each reply.
    -R                  Trace round-trip path (IPv6-only).
    -S srcaddr          Source address to use (IPv6-only).
    -4                  Force using IPv4.
    -6                  Force using IPv6.
```

- `tracert -d`

این سوئیچ در هنگام بررسی هاپ‌ها، فقط IP آنها را نشان می‌دهد و نام آن‌ها را resolve نمی‌کند. این امر باعث افزایش چشم‌گیر سرعت به پایان رسیدن عملیات trace می‌شود. کافی است یک بار بدون d- و یک بار با d– عمل trace را انجام دهید و سرعت آن‌ها را مقایسه کنید.

```
C:\Users\persys>tracert -d www.yahoo.com

Tracing route to atsv2-fp.wg1.b.yahoo.com [87.248.98.7]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  192.168.1.1
  2    27 ms    32 ms    32 ms  172.16.64.18
  3    29 ms    32 ms    31 ms  172.16.64.17
  4    31 ms    32 ms    31 ms  78.38.119.145
  5   111 ms    34 ms    28 ms  78.38.119.186
  6    67 ms    30 ms    36 ms  10.201.222.201
  7    32 ms    35 ms    34 ms  10.201.176.130
  8    38 ms     *       36 ms  10.201.42.98
  9    40 ms     *        *     10.201.177.1
 10   142 ms   142 ms   144 ms  85.132.90.241
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13   167 ms     *      167 ms  188.125.94.1
 14     *        *      165 ms  66.196.65.71
 15   188 ms     *      168 ms  66.196.65.154
 16   218 ms   174 ms   232 ms  66.196.65.23
 17   170 ms   190 ms   180 ms  77.238.186.29
 18   178 ms   198 ms   176 ms  87.248.98.7
```

در تصویر زیر، ستون اول شماره‌ی هر یک از روترهای موجود در مسیر را نشان می‌دهد؛ سه ستون بعدی زمان ارسال و برگشت هر packet را بر حسب میلی‌ثانیه نشان می‌دهد، و ستون آخر نام و IP دستگاه دریافت‌کننده‌ی packet را نشان می‌دهد.

```
C:\Users\persys>tracert www.yahoo.com

Tracing route to atsv2-fp.wg1.b.yahoo.com [87.248.98.7]
over a maximum of 30 hops:

  1     9 ms     5 ms     6 ms  192.168.1.1
  2   380 ms   504 ms   542 ms  172.16.64.18
  3   397 ms   793 ms  1064 ms  172.16.64.17
  4  1038 ms   384 ms    37 ms  78.38.119.145
  5  1035 ms  1020 ms  1067 ms  78.38.119.222
  6   185 ms    35 ms   221 ms  10.201.176.162
  7    37 ms   225 ms    42 ms  10.201.42.117
  8   884 ms  1011 ms  1073 ms  10.202.4.6
  9  1277 ms   242 ms   244 ms  xe2-3-3.marsig2.mar.seabone.net [213.144.176.156
]
 10   202 ms   265 ms   306 ms  et10-1-0.londra32.lon.seabone.net [195.22.209.63
]
 11   276 ms   203 ms   300 ms  ge-1-1-0.pat1.the.yahoo.com [195.66.224.129]
 12   257 ms   227 ms   333 ms  ae6.pat2.iry.yahoo.com [66.196.68.153]
 13  1593 ms  1730 ms  1738 ms  et-11-1-0.msr1.ir2.yahoo.com [66.196.65.23]
 14  1926 ms   941 ms   460 ms  eth-1-1-1.bas1-1-prd.ir2.yahoo.com [217.146.186.
65]
 15   187 ms   235 ms   218 ms  media-router-fp1.prod1.media.vip.ir2.yahoo.com [
87.248.98.7]

Trace complete.

C:\Users\persys>
```

- `tracert -h`

چنانچه بخواهیم فقط تا تعداد معینی از هاپ‌ها trace انجام شود، از این سوئیچ می‌توانیم استفاده کنیم. به طور پیش‌فرض تا ۳۰ هاپ نمایش داده خواهد شد.

```
C:\Users\persys>tracert -h 5  www.yahoo.com

Tracing route to atsv2-fp.wg1.b.yahoo.com [87.248.98.7]
over a maximum of 5 hops:

  1     3 ms     3 ms     4 ms  192.168.1.1
  2    50 ms    35 ms    49 ms  172.16.64.18
  3    42 ms    35 ms    34 ms  172.16.64.17
  4    29 ms    28 ms    34 ms  78.38.119.145
  5    37 ms    30 ms   105 ms  78.38.119.186

Trace complete.
```

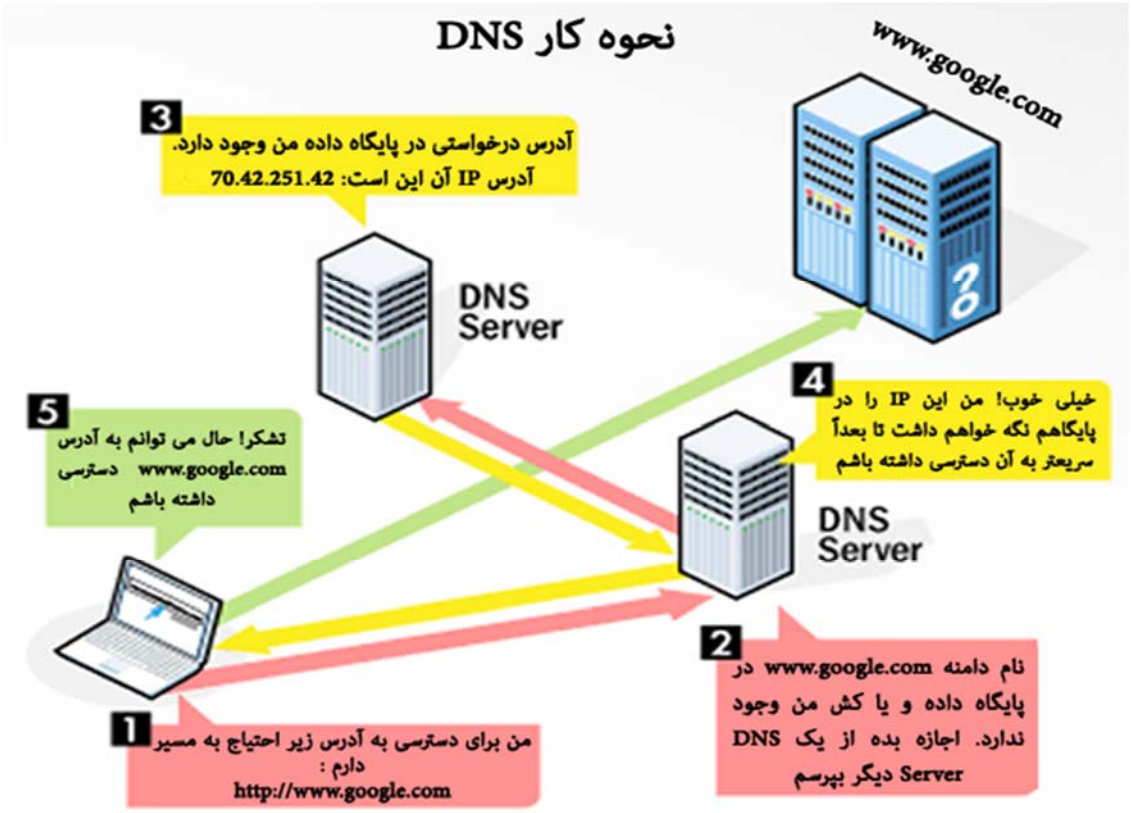
- `tracert -w`

به کمک این سوئیچ می‌توان حداکثر مدت زمانی را که باید منتظر پاسخ از هاپ بود را تعیین کرد. این مقدار بر حسب میلی‌ثانیه در نظر گرفته می‌شود. می‌توانید مدت زمان را به ۱۰ و ۱ میلی‌ثانیه تغییر دهید تا متوجه این تغییرات بشوید.

```
C:\Users\persys>tracert -d -w 1000  www.yahoo.com

Tracing route to atsv2-fp.wg1.b.yahoo.com [87.248.98.7]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  192.168.1.1
  2    95 ms    66 ms    45 ms  172.16.64.18
  3    66 ms    67 ms    90 ms  172.16.64.17
  4    87 ms    90 ms    95 ms  78.38.119.145
  5    83 ms    89 ms    92 ms  217.218.189.134
  6   108 ms   134 ms   137 ms  10.201.42.34
  7    56 ms     *       127 ms  10.201.42.98
  8   326 ms   278 ms   229 ms  62.208.212.145
  9   242 ms     *         *     195.2.2.89
 10   275 ms   307 ms   273 ms  80.81.192.115
 11   322 ms     *       300 ms  66.196.65.218
 12   382 ms   395 ms   344 ms  66.196.65.217
 13     *      248 ms   212 ms  66.196.65.21
 14   243 ms     *       301 ms  217.146.185.176
 15   293 ms   210 ms   275 ms  87.248.98.7

Trace complete.
```

DNS یا Domain Name System چیست؟

کلیه آدرس‌ها در شبکه بر مبنای IP Address است، یعنی برای وارد شدن به هر سایتی باید آدرس آن سایت یا به عبارتی IP مربوط به آن سایت را بدانیم. در اینجاست که اهمیت سرویس DNS مشخص می‌شود. در واقع DNS ، IPها را به اسم سایت‌ها و بالعکس، اسامی سایت‌ها را به IPهای آن‌ها تبدیل می‌کند. یعنی شما زمانی که در نوار آدرس مرورگر خود آدرس سایتی را تایپ می‌کنید، DNS فوراً IP مربوط به این سایت را پیدا می‌کند و از طریق IP آن، وارد سایت می‌شوید.



فرمان nslookup

فرمان nsLookup مخفف Name Server Lookup ابزاری است به منظور رفع اشکال (Troubleshooting) و رفع مشکلات DNS که با کمک آن امکان به‌دست آوردن اطلاعات مربوط به دامنه ها از طریق Name Serverها فراهم می‌باشد. این اطلاعات همان اطلاعات مربوط به ZoneFile هر دامنه می‌باشد.

```
> nslookup
```

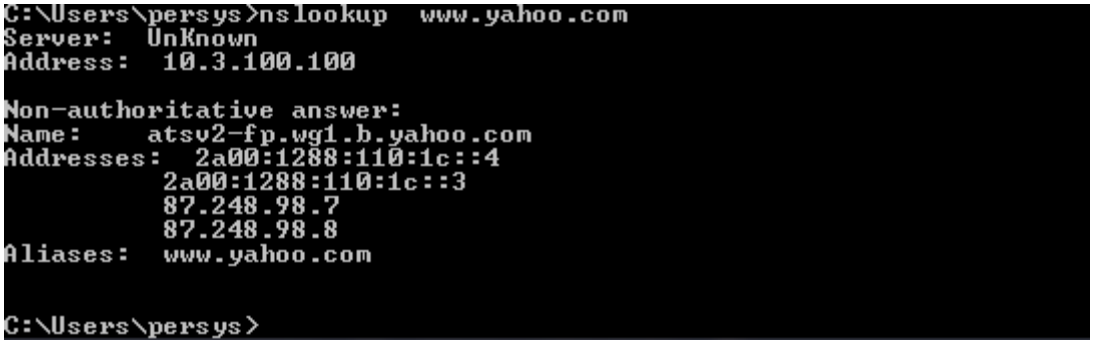
این دستور به منظور عیب‌یابی، تمام رکوردهای سرور DNS را بررسی می‌کند و چنانچه رکوردی وجود نداشته باشد یا اشتباه باشد، می‌توان مشکل را بررسی نمود.

دستور nslookup پس از اجرا شدن با توجه با تنظیمات TCP/IP کامپیوتر شما، DNS پیش‌فرض کامپیوتر را به عنوان سرور انتخاب می‌کند و سعی می‌کند با استفاده از ارسال درخواست reverse نام سرور را نیز پیدا کند و به شما نمایش دهد. اگر موفق به تبدیل IP به نام شود در قسمت Default Server نام سرور را نمایش می‌دهد؛ در غیراین‌صورت Unknown نمایش داده می‌شود. اینکه nslookup موفق به تبدیل IP به نام شود یا نه تأثیری بر دستوراتی که در ادامه وارد می‌کنید ندارد و تنها برای اطلاع شما است.

یکی از مهم‌ترین ویژگی‌های ابزار nslookup این است که دارای دو حالت Interactive و NonInteractive می‌باشد.

حال به cmd بروید، ابتدا تایپ کنید `nslookup www.yahoo.com` . این‌گونه اجرای دستور را NonInteractive یا حالت غیرتعاملی می‌نامند و فقط یک دستور اجرا می‌شود و تمام.

در حالت noninteractive، تنها یک دستور nslookup تایپ نمی‌شود، بلکه گزینه‌های دیگری نیز در ادامه‌ی آن تایپ می‌شود. مثلاً اگر برای حل مشکل خود به دنبال یک IP به‌خصوص می‌باشید، می‌توانید پس از تایپ nslookup، نام سایتی که به‌دنبال IP آن هستید را تایپ کنید؛ یا بالعکس یعنی اگر IP را دارید و به دنبال نام سایت هستید نیز می‌توانید از این حالت استفاده کنید.



برای رفتن به حالت InterActive فقط کافی است تایپ کنید nslookup سپس وارد رابط مربوطه می شوید . در این حالت با نوشتن واژه help به جای ?/ به اطلاعات جزیی در این زمینه دسترسی پیدا می کنید . برای خروج از این حالت نیز واژه exit را تایپ کنید.

در حالت interactive شما خیلی ساده تنها دستور nslookup را در خط فرمان تایپ می‌کنید. این حالت زمانی استفاده می‌شود که شما در پایگاه داده‌ی DNS خود می‌خواهید بیشتر از یک مورد را بررسی کنید. بهتر است بدین صورت بیان کنیم: زمانی که دستور nslookup را در command prompt تایپ می‌کنیم، ابتدا نام وIP مربوط به DNS Serverی که سیستم شما از آن استفاده می‌کند نشان داده می‌شود، سپس در سطر بعدی، نشانگر چشمک‌زن، منتظر وارد کردن دستور بعدی nslookup می‌ماند و تا زمانی که کلید exit یا ctrl + c را نزنیم این انتظار ادامه پیدا خواهد کرد. فرض کنید برای از انتظار در آوردن این خط فاصله‌ی چشمک‌زن، yahoo.com را تایپ کنیم، دراین صورت کلیه‌ی IP های مربوط به این سایت، و همچنین مجدداً IPمربوط به DNS Serverی که از آن استفاده می‌کنیم را مشاهده خواهیم کرد.

```
C:\Users\persys>nslookup
Default Server:  UnKnown
Address:  10.3.100.100

> yahoo.com
Server:  UnKnown
Address:  10.3.100.100

Non-authoritative answer:
Name:    yahoo.com
Addresses:  2001:4998:58:1836::11
          2001:4998:c:1023::5
          2001:4998:58:1836::10
          2001:4998:c:1023::4
          2001:4998:44:41d::3
          2001:4998:44:41d::4
          72.30.35.9
          98.137.246.8
          98.138.219.231
          72.30.35.10
          98.138.219.232
          98.137.246.7

>
```

```
Default Server:  UnKnown
Address:  10.3.100.100

> help
Commands:   (identifiers are shown in uppercase, [] means optional)
NAME            - print info about the host/domain NAME using default server
NAME1 NAME2     - as above, but use NAME2 as server
help or ?       - print info on common commands
set OPTION      - set an option
    all                 - print options, current server and host
    [no]debug           - print debugging information
    [no]d2              - print exhaustive debugging information
    [no]defname         - append domain name to each query
    [no]recurse         - ask for recursive answer to query
    [no]search          - use domain search list
    [no]vc              - always use a virtual circuit
    domain=NAME         - set default domain name to NAME
    srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME           - set root server to NAME
    retry=X             - set number of retries to X
    timeout=X           - set initial time-out interval to X seconds
    type=X              - set query type (ex. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR
SOA,SRV)
    querytype=X         - same as type
    class=X             - set query class (ex. IN (Internet), ANY)
    [no]msxfr           - use MS fast zone transfer
    ixfrver=X           - current version to use in IXFR transfer request
server NAME     - set default server to NAME, using current default server
lserver NAME    - set default server to NAME, using initial server
root            - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
    -a          -  list canonical names and aliases
    -d          -  list all records
    -t TYPE     -  list records of the given RFC record type (ex. A,CNAME,MX,NS,
PTR etc.)
view FILE           - sort an 'ls' output file and view it with pg
exit            - exit the program

> ^C
C:\Users\persys>
```

فرمان netstat

Netstat مخفف Network Statistics می‌باشد و با ترکیب پسوندهای مختلف، انواع آمارهای مختلف شبکه را در اختیار ما می‌گذارد.

Netstat آمارهای مختلفی از کامپیوترهایی که ارتباطات فعال TCP/IP با کامپیوتر ما دارند را نشان می‌دهد. این ابزار زمانی مفید است که در پروتکل‌هایی مانند HTTP و FTP با مشکل مواجه شویم.

کاربرد این دستور زمانی می‌باشد که دستگاهی (Device) را به کامپیوتر متصل کرده‌ایم و به درستی عمل نمی‌کند. همچنین، برای یافتن بدافزارها (malwares) روی سیستم کاربرد دارد. به طور مثال چنانچه شک دارید که سیستم شما با بدافزارهایی مانند تروجان‌ها آلوده شده و سعی در برقراری ارتباط مخربی داشته باشد می‌توانید از دستور netstat درمحیط خط فرمان بهره بگیرید. همچنین این دستور علاوه بر عیب‌یابی در شبکه در برآورد حجم اطلاعات رد و بدل شده در شبکه استفاده می‌شود.

- دستور `netstat –an` : یکی از انواع پرکاربرد این دستور می‌باشد که لیستی از پورت‌های باز و IP آن‌ها و وضعیت هر یک از آنها بر روی سیستم را به ما می‌دهد.
- دستور `netstat` بدون پارامتر: نمایش اتصالات فعال
- دستور `netstat -a`: نمایش تمامی اتصالات TCP و UDP فعال در کامپیوتر
- دستور `netstat -b`: نمایش برنامه‌ی درگیر با اتصالات شبکه‌ای نمایش‌داده شده در لیست خروجی
- دستور `netstat -e`: نمایش آمار مربوط به اترنت، از قبیل تعداد بایت‌ها و بسته‌های دریافتی و ارسالی
- دستور `netstat -f`: نمایش FQDN برای آدرس‌های خارجی (فقط در ویندوز ۷ به بعد)
- دستور `netstat -n`: نمایش ارتباط‌های TCP فعال، هرچند که IPها و پورت‌ها را به‌صورت عددی نمایش می‌دهد و تلاشی برای تشخیص نام آنها نمی‌کند.
- دستور `netstat -m`: نمایش آمار مربوط به جریان‌ها (streams)
- دستور `netstat -o`: نمایش اتصالات TCO فعال به‌همراه شناسه‌ی فرآیند PID مربوط به آن اتصال
- دستور `netstat -p`: نمایش پروتکل مربوط به اتصال در ویندوز
- دستور `netstat -r`: نمایش جدول هدایت IPها
- دستور `netstat -s`: نمایش آمار به تفکیک پروتکل
- دستور `netstat /?`: نمایش راهنما برای سوئیچ‌های موجود (فقط در ویندوز)
