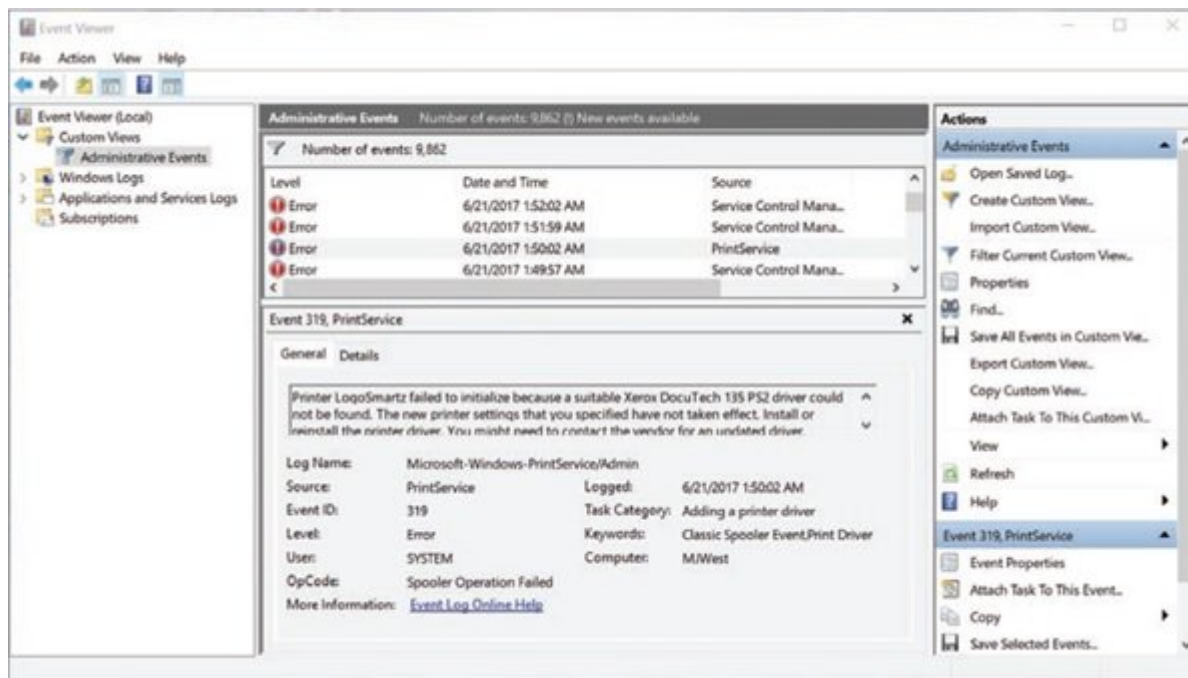




Ping و nslookup دو ابزار بسیار مهمی هستند که به شما کمک می‌کنند اطلاعات ارزشمندی درباره سامانه‌های نام دامنه، آدرس‌های تخصیص داده شده، آدرس‌دهی مجدد و... به دست آورده و جست‌وجوهای قدرتمندی روی بانک‌های اطلاعاتی DNS انجام دهید.

برای مطالعه بخش بیستم آموزش رایگان و جامع نتورک پلاس (Network+) [اینجا](#) کلیک کنید

اکنون که با اصول اولیه آدرس‌دهی شبکه آشنا شدیم، وقت آن رسیده است تا ببینیم چگونه باید مشکلات مربوط به ارتباطات شبکه را حل کنیم. Event Viewer یکی از اولین مکان‌هایی است که هر زمان کامپیوتری دچار مشکل می‌شود باید به آن مراجعه کنید. این ابزار به شما اطلاعات ارزشمندی درباره مشکلات مهم یک کامپیوتر ارائه کرده و حتی ممکن است به شما پیشنهاد کند در آینده برای اجتناب از بروز مشکلات چه تهمیداتی در نظر بگیرید. به طور مثال به تصویر زیر دقت کنید که مشکل چاپگر را نشان می‌دهد.



زمانی که Event Viewer اطلاعات کافی در اختیاران قرار نمی‌دهد، در مرحله بعد باید به سراغ فرمان‌های اشکال‌زدایی TCP/IP بروید.

ابزارهای اشکال‌زدایی

ابزارهای خط‌فرمان یک راه عالی و دقیق برای شناسایی مشکلات هستند. ping و nslookup، ipconfig از ابزارهای مهم در دنیای ویندوز و dig و nslookup از ابزارهای مهم دنیای لینوکس هستند. اما این ابزارها چه کاری انجام می‌دهند؟

Ping

ابزار ping سرنام Packet Internet Groper به منظور تایید این‌که TCP/IP به درستی نصب شده، به کارت شبکه متصل شده، پیکربندی آن درست بوده و با شبکه در ارتباط است استفاده می‌شود. عملکرد این ابزار شباهت زیادی به سیگنال ارسالی نهنگ‌ها داشته که منتظر می‌مانند تا اکو آن سیگنال را دریافت کنند. یک صدای بازگشتی به نهنگ اجازه می‌دهد اطلاعات زیادی در ارتباط با جسمی که سیگنال را ارسال کرده است به دست آورد. Ping با ارسال یک سیگنال درخواست اکو (echo request) برای کامپیوتر دیگری، منتظر دریافت پاسخ می‌ماند. کامپیوتر دیگر پس از دریافت سیگنال از طریق پاسخ اکو (echo reply) به آن سیگنال پاسخ می‌دهد. پروتکلی که برای درخواست و پاسخ دادن به اکو استفاده می‌شود، ICMP سرنام Internet Control Message Protocol نام دارد. یک پروتکل سبک و روان که برای انتقال پیام‌های خطا و اطلاعاتی درباره شبکه استفاده می‌شود. زمانی که قصد دارید وضعیت ارتباط یک شبکه را ارزیابی کنید، اولین ابزاری که باید از آن استفاده کنید، ping است. فرمان ping دارای پارامترها و گزینه‌های مختلفی است که به شرح زیر هستند:

ping [-a] [-t] [-n] [-?] [IP address] [host name] [/?]

جدول زیر چند مثال کاربری از نحوه به‌کارگیری سویچ‌های این فرمان را نشان می‌دهد.

مثال‌هایی از نحوه اجرای فرمان پینگ	توضیح
ping www.google.com	پینگ کردن به نام یک میزبان برای اطمینان حاصل کردن از اینکه دسترسی به اینترنت امکان‌پذیر است. Google.com یک سایت قابل اعتماد برای چنین آزمایش‌هایی است.

ping 8.8.8.8	پینگ به یک آدرس آی پی روی اینترنت برای اطمینان حاصل کردن که دسترسی به اینترنت وجود دارد. آدرس 8.8.8.8 به سادگی حفظ شده و به سرور سامانه نام دامنه عمومی گوگل اشاره دارد.
ping -a 8.8.8.8	تست ترجمه اسامی و نمایش نام میزبان برای اطمینان حاصل کردن که سامانه نام دامنه کار می کند.
ping 92.10.11.200	در این مثال 92.10.11.200 آدرس یک میزبان روی زیرشبکه ای است که درون سازمان شما قرار دارد. این پینگ نشان می دهد که آیا شما می توانید به زیرشبکه متصل شوید یا خیر
ping 192.168.1.1	در این مثال 192.168.1.1 آدرس پیش فرض گیت وی است. این پینگ نشان می دهد که شما بدون مشکل قادر به اتصال به گیت وی پیش فرض هستید.
ping 127.0.0.1	پینگ به آدرس خودتان (loopback) است. 127.0.0.1 مشخص می کند آیا سرویس های TCP/IP ایستگاه کاری در حال اجرا هستند یا خیر
ping localhost	روش دیگری که برای پینگ کردن به آدرس خودتان می توانید استفاده کنید.
?/ping -? or ping	نمایش راهنمای متنی برای فرمان پینگ، شامل ترکیب نحوی و فهرست کاملی از پارامترها
ping -t 192.168.1.1	ادامه دادن به پینگ تا وقتی که وقفه ای به وجود آید. برای نمایش آماری از این فرمان استفاده می شود، برای متوقف کردن این فرمان باید کلیدهای Ctrl+Break یا Ctrl+C را فشار دهید.
ping -n 2 192.168.1.1	تعریف شماره ای که در یک درخواست اکو که قرار است ارسال شود استفاده می شود. به طور پیش فرض پینگ چهار درخواست اکو را ارسال می کند. در این مثال تعداد درخواست ها به 2 مورد محدود شده اند.

شکل زیر نمونه‌ای از یک پینگ موفق را نشان می‌دهد.

```
Command Prompt
C:\Users\Jill West>ping google.com

Pinging google.com [74.125.21.138] with 32 bytes of data:
Reply from 74.125.21.138: bytes=32 time=33ms TTL=40
Reply from 74.125.21.138: bytes=32 time=31ms TTL=40
Reply from 74.125.21.138: bytes=32 time=31ms TTL=40
Reply from 74.125.21.138: bytes=32 time=38ms TTL=40

Ping statistics for 74.125.21.138:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 38ms, Average = 33ms

C:\Users\Jill West>
```

شبکه IPv6 از نسخه جدیدتر پروتکل ICMP موسوم به ICMPv6 برای این منظور استفاده می‌کند. در این جا ما دو نوع پینگ برای سیستم‌عامل‌های مختلف داریم که می‌توانند از سوی آدرس‌های IPv6 استفاده شوند.

- Ping6 - روی کامپیوترهای لینوکسی که IPv6 را اجرا می‌کنند و از ping6 برای اطمینان حاصل پیدا کردن از این‌که یک میزبان IPv6 در دسترس است استفاده می‌کنند. زمانی که شما یک آدرس چندپخش (multicast) را با ping6 پینگ می‌کنید، شما پاسخی از همه میزبان‌های IPv6 روی یک زیر شبکه دریافت می‌کنید.
- Ping 6: روی کامپیوترهای ویندوزی، شما از ping با پارامتر 6- زمانی استفاده می‌کنید که در نظر دارید اطمینان حاصل کنید که ارتباط روی شبکه‌های IPv6 به درستی برقرار شده است.
- برای آن‌که فرمان‌های ping6 و ping-6 روی اینترنت کار کنند، شما مجبور هستید به اینترنت مبتنی بر پروتکل IPv6 دسترسی داشته باشید. برای این منظور شرکت ارائه‌دهنده خدمات اینترنتی باید به شکل محلی ارتباط با IPv6 را امکان‌پذیر کند. البته شما می‌توانید از طریق کارگزاری که تونلی برای IPv6 ارائه کرده به اینترنت دسترسی داشته باشید. Hurricane Electric، IPv6 Tunnel Broker، یا SixXS از جمله این کارگزارها هستند.
- برای آن‌که به سرور سامانه نام دامنه گوگل که مبتنی بر IPv6 است پینگ کنید، باید دستور زیر را اجرا کنید.

ping -6 2001:4860:4860::8888

شکل زیر نتیجه اجرای فرمان بالا روی کامپیوتری که شرکت ارائه دهنده خدمات دسترسی به اینترنت مبتنی بر IPv6 را در اختیارش قرار داده است را نشان می‌دهد. پینگ پس از یک وقفه کوتاه اجرا شده است.


```

C:\Users\MikeandJill>ping -6 2001:4860:4860::8888

Pinging 2001:4860:4860::8888 with 32 bytes of data:
Request timed out.
Reply from 2001:4860:4860::8888: time=146ms
Reply from 2001:4860:4860::8888: time=135ms
Reply from 2001:4860:4860::8888: time=159ms

Ping statistics for 2001:4860:4860::8888:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 135ms, Maximum = 159ms, Average = 146ms

C:\Users\MikeandJill>

```

ipconfig

فرمان ipconfig آدرس فعلی TCP/IP و اطلاعاتی در ارتباط با نام دامنه روی یک کامپیوتر ویندوزی را نشان می‌دهد. شما می‌توانید از ipconfig برای تغییر برخی از تنظیمات استفاده کنید. ipconfig به دو شکل زیر استفاده می‌شود:

- در پنجره خط فرمان، با وارد کردن فرمان ipconfig برای مشاهده اطلاعات آی‌پی پیکربندی شده. دقت کنید ارتباطات محلی که روی کامپیوتر شما در دسترس قرار داشته و در حال حاضر متصل هستند نشان داده می‌شود. این فرمان همچنین اطلاعاتی درباره آدرس‌های IPv4 و IPv6 فعال، ماسک زیرشبکه و گیت وی پیش‌فرض نیز ارائه می‌کند.

```

C:\Users\Jill West>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::3073:b80c:6e0f:d24e%13
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 4:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::e8dc:3628:8b89:3943%6
    IPv4 Address. . . . . : 192.168.2.154
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

Ethernet adapter Bluetooth Network Connection:

```

میزبان مجازی متصل شده است

ارتباطات شبکه محلی بی سیم عبارتند از
آدرس IPv6
آدرس IPv4
زیرشبکه
گیت وی پیش فرض

- اجرای فرمان ipconfig به شکلی مختصر که اطلاعات پیکربندی شبکه را به شکل کلی نشان می‌دهد. برای مشاهده جزئیات بیشتر می‌توانید از فرمان ipconfig/all استفاده کنید.

```

Command Prompt

Wireless LAN adapter Local Area Connection* 4:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : CA-3D-D4-41-C8-C8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC
Physical Address. . . . . : C8-3D-D4-41-C8-C8 ← آدرس مک
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e8dc:3628:8b89:3943%6(Preferred)
IPv4 Address. . . . . : 192.168.2.154(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, June 27, 2017 9:17:24 PM
Lease Expires . . . . . : Tuesday, June 27, 2017 11:17:24 PM
Default Gateway . . . . . : 192.168.2.1
DHCP Server . . . . . : 192.168.2.1 ← DHCP سرور
DHCPv6 IAID . . . . . : 80231892
DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-BF-B8-B3-C8-58-76-7B-8D-33
DNS Servers . . . . . : 8.8.8.8 ← DNS سرور
                        8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected

```

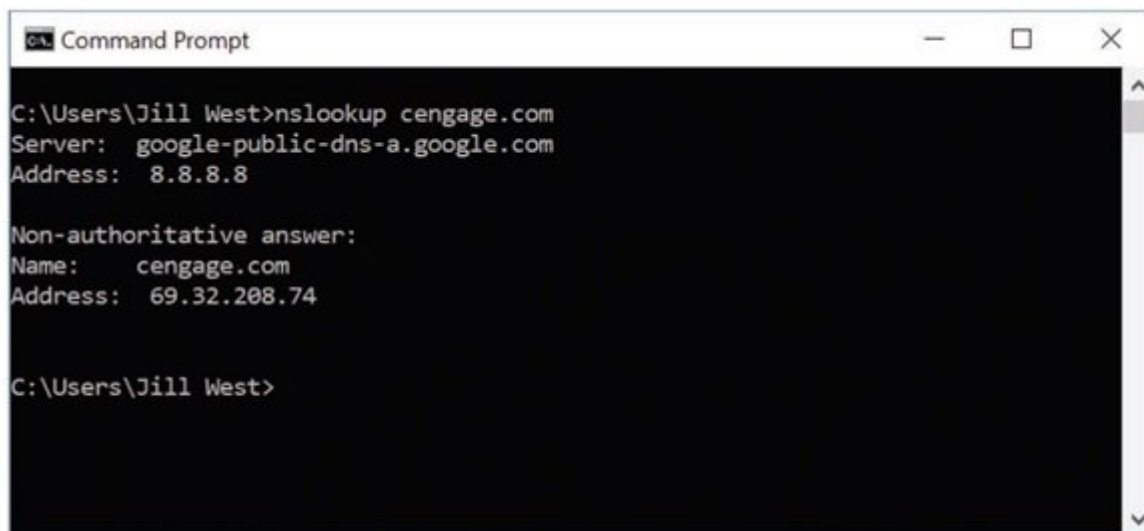
فرمان ipconfig همراه با سویچ /all / اطلاعات بیشتری در مقایسه با اجرای خود فرمان ipconfig ارائه می کند

جدول زیر پر کاربردترین سویچ های فرمان ipconfig را نشان می دهد. دقت کنید در زمان استفاده از پارامترها باید از کاراکتر اسلش / قبل از یک پارامتر استفاده کرده و میان اسلش و ipconfig یک فاصله باشد.

فرمان ipconfig	توضیحات
ipconfig /? or ipconfig /?	یک راهنمای متنی برای فرمان ipconfig نشان می دهد که شامل ترکیب نحوی و فهرستی از همه پارامترها است.
ipconfig /all	اطلاعات پیکربندی جاری TCP/IP برای هر آداپتور شبکه را نشان می دهد
ipconfig /release	زمانی که آدرس دهی پویای آی پی استفاده شد، آدرس آی پی جاری را پاک می کند. با پاک کردن آدرس آی پی ارتباط کامپیوتر با شبکه تا زمانی که آدرس آی پی جدید اختصاص پیدا می کند قطع می شود.
ipconfig /release6	یک آدرس آی پی IPv6 را حذف می کند
ipconfig /renew	یک آدرس آی پی جدید را از سرور DHCP دریافت کرده و اجاره (Lease) می دهد. برای حل مشکلاتی همچون تکراری بودن آدرس های آی پی، پیکربندی اشتباه DHCP یا پیکربندی اشتباه DNS، ریست کردن ارتباط TCP/IP با وارد کردن یکی از دو فرمان زیر انجام می شود. ipconfig /release ipconfig /renew
ipconfig /renew6	یک آدرس آی پی جدید IPv6 را از سرور DHCPv6 دریافت کرده و اجاره می دهد.
ipconfig /displaydns	اطلاعاتی درباره نام دامنه ای که ویندوز به تازگی اطلاعات مربوط به آن را در DNS کش کرده است ارائه می کند.
ipconfig /flushdns	کش را پاک می کند. اجرای این فرمان ممکن است زمانی که یک مرورگر نمی تواند یک میزبان روی اینترنت را پیدا کرده یا زمانی که سرور DNS به اشتباه پیکربندی شده و اطلاعات اشتباهی را ارسال می کند مشکل را حل کند.

Nslookup

فرمان nslookup سرنام name space lookup به شما اجازه می‌دهد بانک اطلاعاتی DNS را از طریق هر یک از کامپیوترهای شبکه جست‌وجو کرده و نام میزبان یک دستگاه را با مشخص کردن آدرس آی‌پی آن پیدا کنید. این ابزار برای اطمینان حاصل کردن از این‌که یک میزبان به درستی پیکربندی شده مفید است. به‌طور مثال، اگر می‌خواهید بدانید که آیا میزبان cengage.com در حال کار است، کافی است فرمان nslookup cengage.com را اجرا کنید. شکل زیر نتیجه اجرای یک فرمان nslookup ساده را نشان می‌دهد.



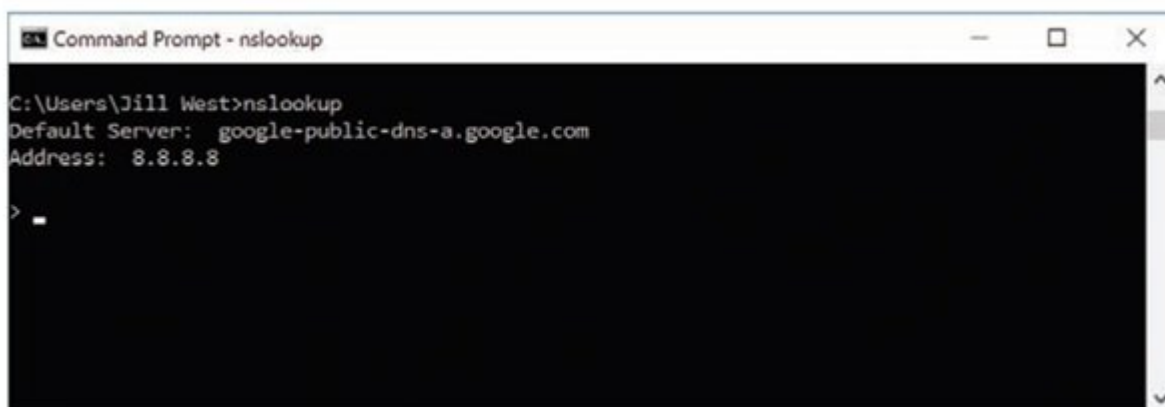
```
Command Prompt
C:\Users\Jill West>nslookup cengage.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:     cengage.com
Address:  69.32.208.74

C:\Users\Jill West>
```

nslookup سرور DNS و اطلاعات مربوط به نام میزبان وب را نشان می‌دهد

دقت کنید که این فرمان آدرس آی‌پی میزبان مقصد، نام و آدرس سرور DNS اصلی شبکه محلی را ارائه می‌کند. برای پیدا کردن نام میزبان یک دستگاه که آدرس آی‌پی آن را می‌دانید، شما باید یک فرآیند واکنشی معکوس اطلاعات از DNS را همچون 69.32.208.74 nslookup انجام دهید. در این حالت، پاسخ نام و آدرس میزبان و سرور اصلی DNS است. ابزار nslookup به دو شکل تعاملی و غیرتعاملی استفاده می‌شود. در حالت غیر تعاملی پاسخی برای یک دستور nslookup ارائه می‌شود. این حالت برای مواقعی خوب است که شما در نظر دارید فقط یک سرور را بررسی کرده یا به دنبال آن هستید تا اطلاعاتی درباره یکی از تجهیزات متصل به شبکه به شکل لحظه‌ای به دست آورید. برای آزمایش چند سرور DNS در یک لحظه، شما باید از وضعیت تعاملی ابزار nslookup که گزینه‌های بیشتری در اختیارتان قرار می‌دهد استفاده کنید. برای اجرای این ابزار در حالت تعاملی باید این فرمان را بدون پرانتز اجرا کنید. زمانی که این nslookup در خط فرمان اجرا شده و کلید اینتر فشار داده شد کاراکتر خط فرمان به حالت > تبدیل می‌شود. اکنون می‌توانید از فرمان‌های اضافی‌تر برای پیدا کردن اطلاعات بیشتری درباره بانک اطلاعاتی DNS استفاده کنید.



```
Command Prompt - nslookup
C:\Users\Jill West>nslookup
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8
>
```

به‌طور مثال، روی کامپیوتری که یونکس را اجرا می‌کند، برای مشاهده فهرستی از همه آدرس‌های آی‌پی و نام‌های

میزبانی که مربوط به سرور DNS خاص هستند از فرمان ls می‌توانید استفاده کنید. شما می‌توانید سرور DNS را از درون حالت تعاملی و از طریق زیرفرمان سرور و تعیین آدرس آی‌پی ویژه‌ای برای سرور DNS جدید تغییر دهید. به‌طور مثال، اختصاص یک سرور DNS جدید همچون سرور OpenDNS با فرمان `server 208.67.222.222` انجام می‌شود.

```
Command Prompt - nslookup
C:\Users\Jill West>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

> server 208.67.222.222
Default Server: resolver1.opendns.com
Address: 208.67.222.222

>
```

برای خروج از حالت تعاملی و بازگشت به خط فرمان عادی دستور `exit` را اجرا کنید. nslookup گزینه‌های متعددی دارد که برای مشاهده سوییچ‌های آن کافی است عبارت `nslookup/?` را تایپ کنید.

در شماره آینده **نتورک پلاس** این مبحث را ادامه خواهیم داد.

لطفا نظرات خود در مورد این آموزش و ادامه آن را در بخش دیدگاه در انتهای صفحه اعلام نمایید و نظارت سایر کاربران را نیز ببینید.

تمام قسمت‌های دوره نتورک پلاس (Network+)

معرفی آموزشگاه‌های معتبر دوره نتورک پلاس در سراسر کشور

استان تهران (تهران): آموزشگاه عصر شبکه

برگزار کننده دوره‌ها بصورت حضوری و مجازی هم‌زمان

تلفن: 02188735845 کانال: @Asrehashabakeh

استان گیلان (رشت): آموزشگاه هیوا شبکه

تلفن: 01333241269 کانال: @HivaShabakeh

تاریخ انتشار:

01 اسفند 1397

نشانی منبع:

<https://www.shabakeh-mag.com/networking-technology/14666/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-network-%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%D8%A8%D8%A7-%D9%81%D8%B1%D9%85%D8%A7%D9%86%E2%80%8C%D9%87%D8%A7%DB%8C-ping-%D9%88-nslookup>