



کارگاه شبکه های محلی کامپیوتر

دانشگاه کوشیدار رشت

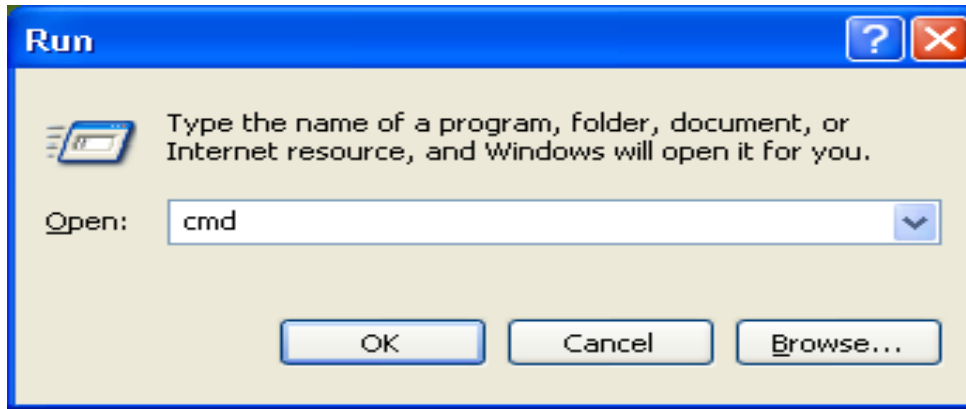
مدرس: مهندس زواره

جلسه سوم

دستورات پر کاربرد شبکه

۲۱-۱- محل اجرای دستورات

در این فصل به معرفی برخی دستورات می‌پردازیم. برای اجرای این دستورات بایستی از محیط Command Prompt استفاده نمایید. برای این کار وارد Run شده و تایپ کنید cmd.



۲۱-۲- دستور IP Config

Ipconfig یکی از دستورات مفید به منظور بررسی وضعیت پیکربندی TCP/IP در کامپیوترهای سرویس دهنده و یا سرویس گیرنده‌ای است که بر روی آنان ویندوز نصب شده است. در یونیکس و لینوکس از دستور ifconfig در این رابطه استفاده می‌شود. در سیستم‌هایی که بر روی آنان ویندوز 9x و یا Me نصب شده است، می‌توان از دستور winipcfg استفاده نمود.

برای استفاده از دستور فوق، کافی است نام آن را از طریق پنجره command prompt تایپ نمود. عملکرد ipconfig و اطلاعاتی که در اثر اجرای آن نمایش داده خواهد شد به نوع سوئیچ استفاده شده، بستگی دارد.

استفاده از ip config بدون سوئیچ، اطلاعات پیکربندی TCP/IP در ارتباط با هر یک از آداپتورهای موجود بر روی سیستم را نمایش خواهد داد:

- آدرس IP
- Subnet Mask
- Default Gateway
- اطلاعات سرویس دهنده DNS
- Domain

تایپ دستور	خروجی
C:\>ipconfig	Ethernet adapter MyLan1: Connection-specific DNS Suffix: IP Address.....: 10.10.1.1 Subnet Mask.....: 255.0.0.0 Default Gateway.....: PPP adapter My ISP : Connection-specific DNS Suffix: IP Address.....: 10.1.1.216 Subnet Mask.....: 255.255.255.255 Default Gateway.....:10.1.1.21

دستور فوق، اطلاعات مربوط به اتصالات از نوع PPP که از آنان در Dialup و VPN استفاده می‌شود را نیز نمایش خواهد داد.

استفاده از ipconfig به همراه all، علاوه بر نمایش اطلاعات اشاره شده در بخش قبل،

اطلاعات دیگری را نیز به نمایش خواهد داد :

- آدرس سخت افزاری کارت شبکه (آدرس MAC)
- اطلاعات مربوط به DHCP

C:\>ipconfig /all

Windows 2000 IP Configuration

Host Name..... :srco

Primary DNS Suffix.....:srco. Ir

Node Type..... :Broadcast

IP Routing Enabled.....: No

WINS Proxy Enabled.....: No

DNS Suffix Search List.....: srco . Ir

Ethernet adapter MyLan1:

Connection-specific DNS Suffix:

Description.....: D-Link DFE-680TX CardBus PC Card

Physical Address.....: 00-50-BA-79-DB-6A**DHCP Enabled.....: No**

IP Address.....: 10.10.1.1

Subnet Mask.....: 255.0.0.0

Default Gateway.....:

DNS Server.....:127.0.0.1

PPP adapter My ISP :

Connection-specific DNS Suffix:

Description.....: WAN(PPP/SLIP) Interface

```
Physical Address.....: 00-53-45-00-00-00-00-53-45-00-00-00
DHCP Enabled.....: No
IP Address.....: 10.1.1.216
Subnet Mask.....: 255.255.255.255
Default Gateway.....: 10.1.1.216
DNS Server.....: x1.y1.z1. w1
X2.y2.z2. w2
```

سایر سوئیچ‌های دستور ipconfig : با استفاده از دستور ipconfig و برخی سوئیچ‌های آن (renew , release)، می‌توان اطلاعات مربوط به پیکربندی TCP/IP ارائه شده توسط سرویس دهنده DHCP را که در اختیار یک سرویس گیرنده قرار داده شده است را آزاد و یا آنان را مجدداً از سرویس دهنده درخواست نمود (در مورد DHCP در فصل‌های آینده صحبت خواهیم کرد). فرآیند فوق به منظور تشخیص عملکرد صحیح سرویس دهنده DHCP در شبکه بسیار مفید و سرور است. (آیا سرویس دهنده DHCP وظایف خود را به خوبی انجام می‌دهد؟ آیا یک سرویس گیرنده قادر به برقراری ارتباط با سرویس دهنده DHCP به منظور درخواست و دریافت اطلاعات پیکربندی TCP/IP می‌باشد؟) دستور ipconfig دارای سوئیچ‌های مفید متعددی است که می‌توان با توجه به نوع خواسته خود از آنان استفاده نمود :

عملکرد	سوئیچ
<p>آدرس IP پیکربندی شده توسط DHCP را آزاد می‌نماید. در صورتی که سوئیچ فوق را به تنهایی و بدون مشخص نمودن adapter تایپ نماییم، پیکربندی IP برای تمامی آداپتورهای موجود بر روی کامپیوتر، آزاد می‌گردد. در صورتی که قصد آزادسازی اطلاعات پیکربندی مربوط به یک آداپتور خاص را داشته باشیم، می‌بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص می‌گردد. (مثلا ipconfig / releaseMyLan1)</p>	<p>/release [adapter]</p>
<p>یک آدرس IP را بر اساس اطلاعات جدیدی که از طریق DHCP دریافت می‌نماید، پیکربندی مجدد می‌نماید. در صورتی که سوئیچ فوق را به تنهایی و بدون مشخص نمودن adapter تایپ نماییم، پیکربندی IP تمامی آداپتورهای موجود بر روی کامپیوتر، مجدداً انجام خواهد شد. در صورتی که قصد ایجاد مجدد اطلاعات پیکربندی مربوط به یک آداپتور خاص را داشته باشیم، می‌بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص گردد. (مثلا ipconfig / releaseMyLan1)</p>	<p>/renew [adapter]</p>

حذف محتویات DNS Resolver Cache	/flushdns
Refresh نمودن تمامی اطلاعات تولید شده توسط DHCP برای آداپتور و ریجستر نمودن اسامی DNS	/registerdns
نمایش محتویات DNS Resolver Cache	/displaydns
نمایش تمامی DHCP Class ID مجاز برای آداپتور	/showclassid [adapter]
تغییر DHCP Class ID	/setclassid [adapter] [classidtoreset]

تشخیص نام آداپتور : نام آداپتور را می توان با کلیک (Right click) بر روی Network Neighborhood و انتخاب گزینه properties، از طریق پنجره

Network and Dial-up connections مشاهده نمود (اسامی آداپتورها، نام آیکن ها می باشند).

مفهوم DNS Cache: زمانی که یک سیستم، ترجمه (نبدیل نام Host به آدرس) را از طریق یک

سرویس دهنده DNS دریافت می نماید، برای مدت زمان کوتاهی آن را در یک Cache ذخیره می نماید. در صورتی که مجدداً از نام استفاده شود، پشته TCP/IP محتویات Cache را به منظور

یافتن رکورد درخواستی بررسی می‌نماید. بدین ترتیب امکان پاسخگویی سریعتر به درخواست ترجمه نسبت به حالتی که درخواست برای یک سرویس دهنده DNS ارسال می‌شود، فراهم می‌گردد. باتوجه به این که اندازه Cache نمی‌تواند از یک میزان منطقی و تعریف شده تجاوز نماید، هر رکورد موجود در Cache پس از مدت زمان خاص حذف می‌گردد. در صورت اعمال هر گونه تغییرات در DNS (مثلا تغییر یک رکورد DNS)، میتوان با استفاده از دستور `ipconfig /flushdns` تمامی رکوردهای موجود در Cache را حذف نمود. بدین ترتیب در صورت درخواست یک نام Host، با سرویس دهنده DNS مشورت می‌گردد و نتایج مجددا در Cache ذخیره خواهند شد. دستور `ipconfig /displaydns`، محتویات Cache را نمایش خواهد داد. از اطلاعاتی که نمایش داده می‌شود، می‌توان به منظور تشخیص این موضوع که آیا برای ترجمه نام به آدرس از Cache و یا سرویس دهنده DNS استفاده شده است، کمک گرفت.

موارد استفاده از دستور Ipconfig: از دستور فوق در مواردی که قصد تشخیص این موضوع را داریم که آیا سرویس دهنده DNS و DHCP در شبکه به درستی وظایف خود را انجام می‌دهند، استفاده می‌شود (علاوه بر مشاهده اطلاعات پیکربندی TCP/IP). مثلا با

استفاده از سوئیچ‌های release و renew، می‌توان براحتی تشخیص داد که آیا در زمینه دریافت اطلاعات پیکر بندی از یک سرویس دهنده DHCP مشکل خاصی وجود دارد. از سوئیچ‌های مرتبط با DNS می‌توان به منظور اعمال تغییرات پیکر بندی، بهنگام سازی cache محلی و یا رجیستر نمودن اطلاعات پیکر بندی جدید با یک سرویس دهنده DNS، استفاده نمود.

۲۱-۳- دستور Ping

Ping دستوری است که مشخص میکند که آیا یک کامپیوتر خاص که ما IP یا Hostname (نام کامپیوتر) آن را می‌دانیم، روشن و فعال (Active) هست یا نه، یا اینکه ما قابلیت اتصال به وی را داریم یا نه؟ و اینکه اگر فعال باشد مدت زمان رسیدن بسته‌های TCP/IP از آن کامپیوتر به کامپیوتر ما چقدر است. استفاده از این دستور به صورت زیر است:

Ping[IP-or-Hostname]

که به جای IP-or-Hostname باید آدرس IP و یا Hostname کامپیوتر مورد نظر را بگذاریم.

مثلا Ping iut.ac.ir (سایت دانشگاه صنعتی اصفهان) را در command prompt تایپ کردم
و به نتایج زیر رسیدم:

Pinging iut.ac.ir [217.219.19.121] with 32 bytes of data :

Reply from 217.219.19.121: bytes=32 time=1402ms TTL=105

Reply from 217.219.19.121: bytes=32 time=941ms TTL=105

Reply from 217.219.19.121: bytes=32 time=981ms TTL=105

Reply from 217.219.19.121: bytes=32 time=851ms TTL=105

Ping statistics for 217.219.19.121:

Packets: Sent = 4, Received=4, Lost = 0(0% loss)

Approximate round trip times in milli-seconds:

Minimum = 851 ms, Maximum = 1402ms ,Average = 1043ms

این نتایج نشان می دهد که iut.ac.ir فعال است.

در نتیجه به دست آمده، منظور از bytes، مقدار بایت‌های ارسالی و دریافتی در هر بسته است. منظور از time، مدت زمانی است که طول کشیده تا بسته موردنظر به مقصد برسد و منظور از TTL، تعداد گام‌های اعتبار بسته ارسالی است. حالا به کامپیوتری با آدرس IP شماره ۲۱۷،۲۱۹،۱۹،۱۲۱ (که همان iut.ac.ir است)، Ping می‌کنیم. نتایج همان است فقط با تغییراتی در سطر اول. (البته time که معنای مدت زمان رسیدن بسته را می‌دهد، با توجه به ترافیک شبکه، کم و زیاد خواهد شد). برای Ping کردن به این IP، دستور Ping ۲۱۷،۲۱۹،۱۹،۱۲۱ را صادر می‌کنیم.

فرض کنید که به یک IP که فعال نیست، Ping کنیم. نتیجه به صورت زیر خواهد بود :

Pinging 217. 66. 196. 1 with 32 bytes of data:

Request timed out .

Request timed out .

Request timed out .

Request timed out .

Ping statistics for 217.66.196.1 :

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

که نشان می‌دهد که آن IP در آن لحظه فعال نیست.

البته تمام مطالبی که در بالا ذکر شده، در حالی است که مستقیماً به اینترنت وصل شده‌اید و یا اگر از طریق شبکه محلی به اینترنت وصل هستید، شبکه شما به درستی پیکربندی شده باشد. اصولاً Ping یکی از بهترین دستورات برای پیدا کردن ایراد در شبکه است.

Option های مختلف دستور Ping:

Ping -t (۱)

با استفاده از پارامتر "t" می‌توان تعیین کرد تا دستور Ping تا زمان interrupted شدن توسط کاربر به Ping کردن ادامه دهد. یعنی کار ارسال بسته تا بی‌نهایت ادامه یابد، مگر اینکه کاربر آن را متوقف کند.

Ping-a (۲)

با استفاده از پارامتر “a” نیز می‌توان نام هاست IP مورد نظر را پیدا کرد. به عبارتی این پارامتر نام هاست متناظر با IP را نمایش می‌دهد.

Ping -n (۳)

با استفاده از پارامتر “n” نیز می‌توان تعداد دفعات ارسال Echo Request messages را که به طور پیش فرض چهار بار می‌باشد افزایش یا کاهش داد.

Ping -l (۴)

با استفاده از پارامتر “l” نیز می‌توان حجم بسته Echo Request messages را که به طور پیش فرض ۳۲ بایت می‌باشد تغییر داد. بیشترین مقدار مجاز برای این پارامتر ۶۵،۵۲۷ می‌باشد.

Ping -i (۵)

با استفاده از پارامتر “i” نیز می‌توان مدت زمان زنده بودن بسته سرگردان را تعیین کرد. به عبارت دیگر این پارامتر TTL – Time To Live بسته Echo Request messages را تعیین می‌کند.

۶) Ping -v

با استفاده از پارامتر “v” نیز می‌توان مقدار TOS-Type Of SERVICE در هدر ای پی Echo Request messages را تعیین کرد. مقدار پیش فرض ۰ می‌باشد. محدوده مجاز این مقدار نیز ۰ تا ۲۵۵ می‌باشد.

۷) Ping -w

با استفاده از پارامتر “w” نیز می‌توان مدت زمان انتظار برای دریافت پاسخ از هاست بر حسب milliseconds را تعیین نمود.

۲۱-۴- دستور Tracert/Traceroute

همانطور که از نام این ابزار پیداست، از tracert برای پیدا کردن مسیر بین دو Host یا به عبارتی دو دستگاه دارای آدرس شبکه که همدیگر را می‌بینند استفاده می‌شود. یعنی اینکه بسته‌های ما برای رسیدن ما برای رسیدن از مبدا به مقصد از چه دستگاه‌هایی عبور می‌کند. این دستور از طریق پروتکل ICMP این عمل را انجام می‌دهد و آن بدین صورت است که

بسته Echo Request توسط کامپیوتر ما به دستگاه مقصد ارسال می‌شود و در هر مرحله‌ای از این مسیر، بسته Echo Replay ایجاد شده و به کامپیوتر مبدا (کامپیوتر ما) ارسال می‌شود. باید این نکته را خاطر نشان کنم هر یک از چهار سیستم عامل معروف امروزی دارای دستور ویژه خود در این ابزار هستند که در زیر لیست آن‌ها را آورده‌ایم :

Windows Server 2000/2003

tracert

Novell Net Ware

iptrace

Linux/UNIX/Macintosh

tracert

این دستور علاوه بر اینکه اطلاعات جامعی از هر یک از مسیریاب‌های مسیر تا رسیدن به مقصد به ما می‌دهد بلکه نام آن مسیریاب‌ها را در صورتی که در آن‌ها تنظیم شده و در دسترس قرار گرفته باشند نشان خواهد داد. همچنین زمان رفت و برگشت بسته ICMP ما از مبدا تا مسیریاب بین راه، بر مبنای میلی ثانیه نیز توسط این دستور مشخص خواهد شد. این اطلاعات به ما کمک خواهد کرد تا کشف کنیم در کجای مسیر ارتباطی بین دو نقطه از شبکه مشکل وجود دارد. در زیر یک نمونه موفق از استفاده از این دستور در ویندوز ۲۰۰۳ را مشاهده می‌کنید:

```
C:\>tracert 24.7.70.37
```

```
Tracing route to c1-p4.stt1wa1.home.net[24/7.70.37] Over a maximum  
of 30 hops :
```

```
1 30 ms 20 ms 20 ms 24.67.184.1
```

```
2 20 ms 20 ms 30 ms rd1ht-ge3-0.ok.showcable.net[24.67.224.7]
```

```
3 50 ms 30 ms 30 ms rc1wh-atm0-2-1.vc.showcable.net  
[204.209.214.193]
```

```
4 50 ms 30 ms 30 ms rc2wh-pos15-0.vc.showcable.net  
[204.209.214.90]
```

```
5 30 ms 40 ms 30 ms rc2wt-pos2-0.wa.showcable.net [66.163.76.37]
```

```
6 30 ms 40 ms 30 ms c1-pos6-3.sttlwa1.home net [24.7.70.37]
```

```
Trace complete.
```

درست مانند سایر دستورات که در این به آن پرداخته ایم دستور `tracert` هم دارای ستون‌هایی است که اطلاعات مورد نیاز ما در آن تفکیک شده اند. ستون اول شماره هاپ (گام‌های طی شده) را مشخص کرده است؛ به روایتی دیگر یعنی جایی که بسته ICMP ارسالی کامپیوتر ما با آن رسیده است. سه ستون دیگر نمایانگر زمان ارسال و برگشت بسته ارسالی به میلی ثانیه و آخرین ستون نام `Host` مقصد و آدرس `IP` دستگاه پاسخ دهنده را مشخص می‌کند. بدیهی است در صورت وجود مشکل در مسیر ارتباطی به مقصد `Trace route` های موفقیت آمیز نخواهند بود. در مثال زیر نمونه‌ای از آن را مشاهده می‌کنید:

```
C:\>tracert comptia.org
```

```
Tracing route to comptia.org [216.119.103.72]
```

```
1 27 ms 28 ms 14 ms 24.67.179.1
```

```
2 55 ms 13 ms 14 ms rd1ht-ge3-0.ok.showcable.net[24.67.224.7]
```

```
3 27 ms 27 ms 28 ms rc1wh-atm0-2-1.vc.showcable.net  
[204.209.214.19]
```

```
4 28 ms 41 ms 27 ms rc1wh-pos2-0.wa.showcable.net [66.163.76.65]
```

5 28 ms 41 ms 27 ms rc2wt-pos1-0.wa.showcable.net [66.2163.68.2]

6 41 ms 55 ms 41 ms c1-pos6-3.sttlw1.home.net [24.7.70.37]

7 54 ms 42 ms 27 ms home-gw.st6wa.ip.att.net [192.205.32.249]

8 * * * Request timed out.

9 * * * Request timed out.

10 * * * Request timed out.

در این مثال بسته ارسالی ICMP ما تنها موفق شده تا هفت مرحله پیش برود و در مرحله هشتم به مشکل برخورد کرده است که دلیل می‌تواند این باشد که دستگاهی که در مرحله هشتم قرار دارد قطع است یا اینکه دستگاه موجود در مرحله هفتم کار میکند. اما امکان مشخص کردن هاپ بعدی را ندارد. عواملی بسیاری می‌تواند وجود داشته باشد که دستگاه هفت قادر به انجام وظیفه نگردیده باشد که ممکن است مشکل در جدول Route آن باشد و یا Connection صحیحی برای آنان ایجاد نشده باشد. با توجه به موارد بالا متوجه می‌شوید که توسط این دستور شما بررسی مشکل را تنها بر روی یک یا دو دستگاه محدود کرده‌اید. این دستور همچنین می‌تواند به شما کمک کند تا شبکه‌های در مسیر با بار زیاد و متراکم را محدود سازید.

۲۱-۵- دستور Net Stat

Net Stat مخفف Network Statistics یک ابزار خط فرمان است که اتصالات شبکه را (هم به داخل و هم به خارج)، جداول هدایت کردن بسته ها و تعدادی از آمار رابطه‌های شبکه‌ای را نشان می‌دهد. همچنین این ابزار برای پیدا کردن مشکلات در شبکه و برآورد گر حجم اطلاعات ردوبدل شده در شبکه به عنوان یک اندازه گیر عملکرد استفاده می‌شود.

پارامترهای ورودی

پارامترهایی که در ورودی همراه دستور وارد می‌شوند باید با - شروع شوند (در ویندوز امکان استفاده از علامت / نیز وجود دارد):

بدون پارامتر: نمایش Connection های فعال

a- : نمایش تمامی اتصالات TCP و UDP فعال در کامپیوتر .

b- : نمایش برنامه در گیر با اتصالات شبکه ای نمایش داده شده در لیست خروجی. (در ویندوز ۲۰۰۰ و ویندوزهای قبل از آن و سایر سیستم عامل های غیر ویندوزی امکان پذیر نیست)

- e-**: نمایش آمار مربوط به اترنت، از قبیل تعداد بایت‌ها و بسته‌های دریافتی و ارسالی. این پارامتر می‌تواند با `s-` نیز ترکیب شود
- f-**: نمایش FQDN برای آدرس‌های خارجی. (فقط در ویندوز Vista و سیستم عامل‌های جدیدتر)
- g-**: نمایش کارت‌های شبکه و آمار آن‌ها. (در ویندوز موجود نیست، `ipconfig` می‌تواند این کار را در ویندوز انجام دهد)
- n-**: نمایش ارتباط‌های TCP فعال، هر چند که IPها و پورت‌ها را به صورت عددی نمایش می‌دهد و تلاشی برای تشخیص نام آن‌ها نمی‌کند.
- m-**: نمایش آمار مربوط به استریم‌ها.
- o-**: نمایش اتصال‌های TCP فعال به همراه PID مربوط به آن اتصال.
- P-**: در ویندوز، پروتکل مربوط به اتصال را نمایش می‌دهد. (, UDP, ICMP, IP,
(TCP
- P-**: در لینوکس فرآیندهای مربوط به اتصال را نشان می‌دهد. (مانند کلید `b-` در ویندوز عمل می‌کند) (برای اجرای صحیح دستور باید دسترسی پایه‌ها یا `root` داشت).

-p : در سولاریس، پروتکل مربوط به اتصال را نمایش می دهد. (IP,ICMP,UDP,TP ...)
-r : جداول هدایت ipها را نشان می دهد.(معادل دستور route print در ویندوز است).
-S : نمایش آمار به تفکیک پروتکل.

-v :وقتی که با **-b** استفاده شود، توالی اجزای برنامه ها را نشان می دهد.

-h یا **--help** : نمایش راهنمایی برای دستورات موجود. (مناسب برای سیستم های یونیکس)

/? : نمایش راهنمایی برای دستورات موجود.(فقط در ویندوز)

۲۱-۶- دستور Net

دستور Net بیشتر برای کار با objectهای شبکه مورد استفاده قرار می گیرد. با این دستور بایستی کلمه ای دیگر مثل User یا Computer وارد کنید تا سیستم متوجه بشود که میخواهید با چه نوع objectی کار کنید.

- چگونگی یافتن راهنمای دستورات زیر : ابتدا دستور Net، سپس کلمه Help و سپس نوع دستور Net file، بنویسید: Net Help File

شرح دستور	نام دستور
با این دستور، وضعیت تنظیمات پسوردها(مثل طول عمر) نشان داده می شود	Net Accounts
کامپیوترها را به پایگاه داده‌ی Domain مورد نظر اضافه و یا کم می کند.	Net Computer
سررویی که توسط دستور Net pause معلق شده است را دوباره راه اندازی میکند.	Net Continue
نام تمامی فایل های بازو اشتراک گذاشته شده بر روی سرور را نمایش می دهد.	Net File
<p>لیست گروه‌های محلی تعریف شده را بیان میکند و نیز می شود فهمید در هر کدام از این گروه‌ها چه حساب‌هایی وجود دارد و نیز می شود به یک گروه خاص حسابی اضافه کرد. می خواهیم ببینیم که چه گروه‌های محلی تعریف شده است. مینویسیم:</p> <p>Net localgroup</p> <p>Aliases for \\ Computer-name</p> <p>که نتیجه می شود:</p>	Net Group

*Administrators Backup Operators Debugger User

*DHCP Administrators DHCP User Guests

*Power User Replicator Users

The command completed successfully.

دقت کنید که ویندوز معمولاً هنگام ارائه نتایج دستورات Net، می‌آید و اول اسم هر گروه یک x قرار می‌دهد تا با حساب‌ها اشتباه نشود. حالا می‌خواهیم ببینیم که مثلاً در گروه Administrators چه حساب‌هایی هست. مینویسیم:

Net local group Administrators

که نتیجه می‌شود:

Alias name administrators

Comment Administrators have Complete and unrestricted accessto

The computer/Domain

Members

Administrators

Ali

Reza

The command completed successfully.

پس سه تا حساب در حد Admin داریم. حالا میخواهیم مثلا حساب Ali را از لیست Admin ها خارج کنیم، مینویسیم :

Net local group Administrators Ali/delete

و با این کار حساب Ali از گروه حذف می شود (می توانید دوباره لیست بگیرید و ببینید که کاربر Ali دیگر در این گروه نیست). حالا می خواهیم دوباره حساب Ali را به این گروه اضافه کنیم، مینویسیم :

Net local group Administrators Ali/add

این دستور از جمله مهم ترین دستوراتی است که باید یاد بگیرید. گاهی با حسابی وارد می شویم و میخواهیم ککه این حساب را به حد Admin برسانیم و روش کار همین دستور آخری است (اینکه اجازه این کار را داریم یا نه ، بحثی است که در این مبحث نمی گنجد). وقتی حسابی وارد گروه Admin می شود، تمام مزایای این گروه را به دست می آورد.

این دستور در واقع Help دستور Net است.	Net Help
وقتی که یک دستور Net به صورتی اجرا می‌شود که خطایی پیش بیاید، ویندوز یک شماره خطای ۴ رقمی به ما می‌دهد که برای دریافت جزئیات بیشتر در مورد این خطا باید از دستور Net help msg استفاده می‌کنیم.	Net Help msg
گروه‌های محلی را نمایش، اصلاح یا اضافه می‌کند.	Net Local group
این دستور به یک پیام نام اختصاص می‌دهد و یا نام آن را پاک می‌کند.	Net Name
سرویس‌های در حال اجرا را متوقف می‌کند.	Net Pause
اطلاعات مربوط به یک صف مشخص را نمایش می‌دهد؛ اطلاعات مربوط به تمامی صف‌های مربوط به سرور نوشته شده را نمایش می‌دهد؛ اطلاعات مربوط به یک کار مشخص را نشان می‌دهد و یا کار مشخص را نشان می‌دهد و یا کار مشخص شده را کنترل می‌کند.	Net Print

Net Send

فرض کنید که میخواهیم یک Message به فرد خاصی که به سیستم وارد شده است و یک Session دارد بفرستیم (اینکه فردی Session دارد یا نه ، به کمک دستور Net Session قابل بررسی است). بدین منظور از این دستور می توانیم استفاده کنیم. مثلا اگر بخواهیم به Administrators که الان در سیستم هست ، پیام Salam mashti را بفرستیم، می نویسیم :

Net Send Administrators Salam Mashti

در این حالت کاربر Administrators ، پیام ما را می گیرد. اگر بخواهیم به همه افرادی که الان Session دارند، همین پیام را بفرستیم ، می نویسیم :

Net Send /User Salam Mashti

وپیغام را همه می گیرند. این دستور باید به صورت Local یعنی از طریق یک shell اجرا شود.

Net Session

به کمک این دستور مشخص می شود که چه کسانی الان در سیستم یک Session دارند. به عبارت دیگر ، برای مشاهده اینکه چه کسانی به

صورت Remote به سیستم وارد شده‌اند. این دستور را تایپ کنید:

Net Session

ها را خاتمه Session تا لیست این افراد نمایان شود. اگر بخواهیم همه بدهیم، می‌نویسیم:

Net Session / delete

این دستور، رابطه این کامپیوتر با سایر کامپیوترهای شبکه قطع می‌کند (نه ارتباط فیزیکی، بلکه اتصالاتی که مثلا با برنامه Remote Desktop ایجاد شده‌اند). اگر فقط بخواهیم یک Session را با یک کامپیوتر خاص تمام کنیم، می‌نویسیم:

Net Session \\xxx.xxx.xxx.xxx/delete

این در حالتی است که با آن کامپیوتر Session داشته باشیم. دقت کنید که به جای دستور Net Session می‌توانید از دستور Net Session یا Net Sess استفاده کنید.

Net Share

این دستور به ما کمک می‌کند که Shareها را به صورت محلی مدیریت کنیم (دستور بالایی به صورت Remote استفاده می‌شود). می‌خواهیم ببینیم که الان چه Shareهایی وجود دارد. می‌نویسیم:

Net Share

و جواب میگیریم :

Share name Resource Remark

سرویس های شبکه را آغاز یا لیست می کند.

Net Start

آمار مربوط به پایگاه های کاری یا سرورها را نشان می دهد.

Net Statistics

سرویس ها را متوقف می کند.

Net Stop

ما از این دستور برای فهمیدن زمان روی یک سرور استفاده می کنیم.
اگر به صورت محلی استفاده می کنید، بنویسید:

Net Time

Net Time

ولی اگر به صورت Remote، میخواهید زمان یک کامپیوتر را پیدا کنید، بنویسید:

Net time \\xxx.xxx.xxx.xxx

که xxx.xxx.xxx.xxx همان آدرس IP است که برای آن Session داریم.

این دستور دو کاربرد مهم دارد. اولین کاربرد، Connect یل Disconnect شدن به یک کامپیوتر با پورت ۱۳۹ باز (یعنی Firewall آن پورت را نبسته باشد) و NetBIOS فعال است. مثلا اگر بخواهیم با حساب Administrator و با پسورد ۱۲۳ به کامپیوتری با آدرس Ip xxx.xxx.xxx.xxx متصل شده و به پوشه Share شده‌ای به اسم IPC\$ دسترسی یابیم، (این Share معملا هست، به همین دلیل از این Share استفاده کردیم)، مینویسیم:

```
Net use \\xxx.xxx.xxx.xxx\IPC$ "123"  
/User:"Administrator"
```

این کاربرد اول بود که این را قبل از دستور Net view انجام می‌دهیم. می‌توانستیم یک null Session تشکیل دهیم، به این صورت که قسمت مربوط به Username و Password را خالی بگذاریم. به این صورت:

```
Net use \\xxx.xxx.xxx.xxx\IPC$ "" /User: ""
```

حالا Session تشکیل شده است. کاربرد بعدی اینه که بعد از اینکه دستور بالا را اجرا کردیم و بعد دستور Net view را اجرا کردیم و لیست کامل Share ها

را بدست آوردیم، بیاییم و یکی از این Share ها را استفاده کنیم. مثلا اگر اسم Share که لیست شده، SharedDocs باشد، و بخواهیم یک درایو جدید (Map Drive) را به آن نسبت بدهیم که بتوانیم با آن کار کنیم، می نویسیم :

```
Net use * \\xxx.xxx.xxx.xxx\SharedDocs
```

معنی کاراکتر * این است که اگر مثلا آخرین درایو در کامپیوتر من (با احتساب سی-دی درایو) مثلا G باشد، درایوی که برای اتصال به پوشه Share شده استفاده می شود، درایو بعدی یعنی H می باشد. می توانستیم اینطوری هم بنویسیم:

```
Net use H: \\xxx.xxx.xxx.xxx\SharedDocs
```

خوب حالا می توانیم مثل یک درایو محلی با آن پوشه Share شده کار کنیم. وقتی کارمان با Share تموم شد، باید Disconnect کنیم ، با این دستور:

```
Net use /delete H:
```


Net User

این دستور به ما کمک می کند که به صورت محلی بدانیم که چه حساب‌هایی در سیستم تعریف شده است و نیز اینکه اطلاعاتی در مورد هر یک بدست آورده و نیز حساب جدید تعریف کنیم. اول می خواهیم بدانیم چه حساب‌هایی تعریف شده، می نویسیم:

Net User

که نتیجه می شود:

User accounts for \\computer-name

Administrator ali Reza

ASPNET Guest

The command completed successfully.

خوب حالا مثلا می خواهیم راجع به حساب Reza اطلاعاتی بگیریم،
مینویسیم:

Net User Reza

و جواب می گیریم.

User name Guest

User name Reza

Full Name

Comment

User's comment

Country code 000 (System Default)

Account expires Never

Password last set 24/11/2010 06:33:06.a

Password expires Never

Password changeable 24\11\2010 06:33:06.a

Password required No

User may change password Yes

Workstations allowed All

Logon script

User profile

Home directory

Last logon 26\12\2010 07:54:48

Logon hours allowed All

Local Group Memberships*Administrators *Debugger

Users*Help Library Updaters *Home Users

Global Group memberships *None

The command completed successfully.

می بینید که در سطر ۲ تا مانده به آخر

(سطر Local group Memberships) دقیقا بیان شده است که این حساب

به چه گروه‌هایی تعلق دارد. دقت کنید که به جای دستور Net User، از

دستور Net Users هم می‌توانید استفاده کنید. حالا می‌خواهیم یک حساب جدید اضافه کنیم. اسم حساب می‌خواهیم Ali بوده و رمز آن ۱۲۳ باشد، می‌نویسیم:

```
Net User Ali 123 /Add
```

حالا می‌خواهیم همین حساب را پاک کنیم:

```
Net User Ali/delete
```

دقت کنید که در دستور پاک کردن دیگر لزومی به وارد کردن رمز عبور نیست.

Net view

فرض کنید که یک Netbios Session تشکیل داده‌ایم (یعنی به یک کامپیوتر راه دور متصل شده ایم؛ مثلا توسط تایپ آدرس IP آن در Run) (گاهی Null Session هم جواب می‌دهد) و حالا می‌خواهیم ببینیم که چه منابعی برایمان Share شده است، می‌نویسیم:

```
Net view \\xxx.xxx.xxx.xxx
```

و مثلا جواب می‌گیریم :

Shared resources at \\xxx.xxx.xxx.xxx

Share name Type Used as Comment

Shared Docs Disk

The command completed successfully.

می بینید که share Docs، پوشه‌ای است که Share شده است. حالا با دستور Net use می‌توانیم از Share استفاده کنیم.

۲۱-۷- دستور nslookup

Nslookup.exe ابزاری است که به مدیران شبکه امکان تست و رفع اشکال سرویس DNS را می‌دهد. Nslookup یک برنامه از نوع خط فرمان (command-line) است که مخفف

Name Server Lookup می‌باشد. به وسیله NSLookup می‌توان از Name Serverهای مختلف اطلاعات مربوط به دامنه‌های مورد نظر را در صورت امکان بدست آورد.

اطلاعاتی که درباره دامنه از طریق NSLookup مشاهده می‌کنیم ، در واقع همان اطلاعاتی است که در Zone File مربوط به دامنه وجود دارد.

آشنایی کامل با امکانات این دستور برای یک مدیر شبکه که با سرویس DNS سرور کار دارد خیلی مهم و حیاتی است.

Nslookup را می‌توان به دو شکل Interactive و غیر Interactive استفاده کرد.

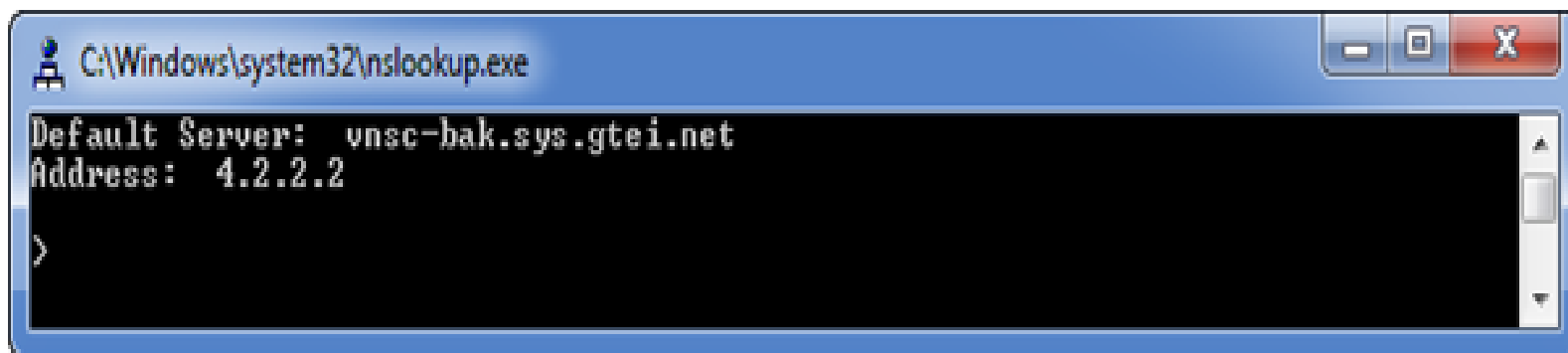
حالت غیر Interactive تنها زمانی کاربرد دارد که فقط قصد اجرای یک دستور را دارید و علاقه دارید پس از اتمام آن دوباره به محیط command برگردید.

شکل دستور nslookup در محیط غیر Interactive به صورت زیر است:

```
Nslookup [-option] [hostname] [server]
```

برای استفاده از nslookup به صورت Interactive کافی است دستور nslookup را وارد کنید.

پس از ورود به محیط دستور nslookup محیطی مانند شکل زیر نمایش داده می‌شود :



```
C:\Windows\system32\nslookup.exe
Default Server: vns-c-bak.sys.gte-i.net
Address: 4.2.2.2
>
```

دستور nslookup پس از اجرا شدن، با توجه با تنظیمات TCP/IP کامپیوتر شما، پیش فرض کامپیوتر را به عنوان سرور انتخاب می کند و سعی می کند با استفاده از ارسال درخواست Reverse نام سرور را نمایش می دهد و در غیر اینصورت Unknown نمایش داده می شود، اینکه nslookup موفق با تبدیل IP به نام شود یا نه تاثیری بر دستوراتی که در ادامه وارد می کنید ندارد و تنها برای اطلاع شما است.

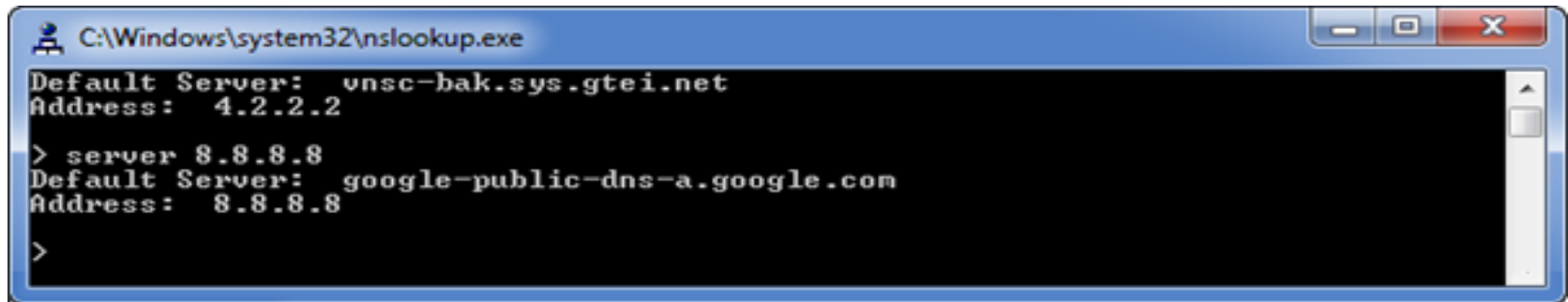
در قسمت Address هم آدرس IP سرور را نمایش می دهد در خط بعد با نمایش علامت < منتظر دریافت دستور می شود. حال شما می توانید دستورات دلخواه خود را وارد نمایید.

برای مشاهده لیست دستورات و توضیحات آن‌ها می‌توانید از علامت ؟ یا دستور Help استفاده کنید.

برای خروج از nslookup نیز می‌توانید از کلیدهای Ctrl+C یا دستور Exit استفاده کنید. اگر قصد تست کردن سرور دیگری غیر سرور مشخص شده در قسمت Address دارید می‌توانید از دستور زیر استفاده کنید. بدین ترتیب دستوراتی که در ادامه خواهد می‌کنیم، به این سرور ارجاع داده می‌شود:

Server<server ip/name>

مثال: برای اینکه سوالاتی که در آینده از nslookup می‌پرسیم به DNS سروری با آدرس ۸,۸,۸,۸ ارجاع شود باید به این صورت عمل کنید :



```
C:\Windows\system32\nslookup.exe
Default Server: vnsc-bak.sys.gtei.net
Address: 4.2.2.2
> server 8.8.8.8
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8
>
```


برای اینکه نوع رکوردی که می‌خواهید از DNS سرور پرسیده شود را تغییر دهید، باید به کمک دستور Set Type یا Set Querytype این کار را انجام دهید و مقدار Type را به یکی از موارد زیر تغییر دهید :

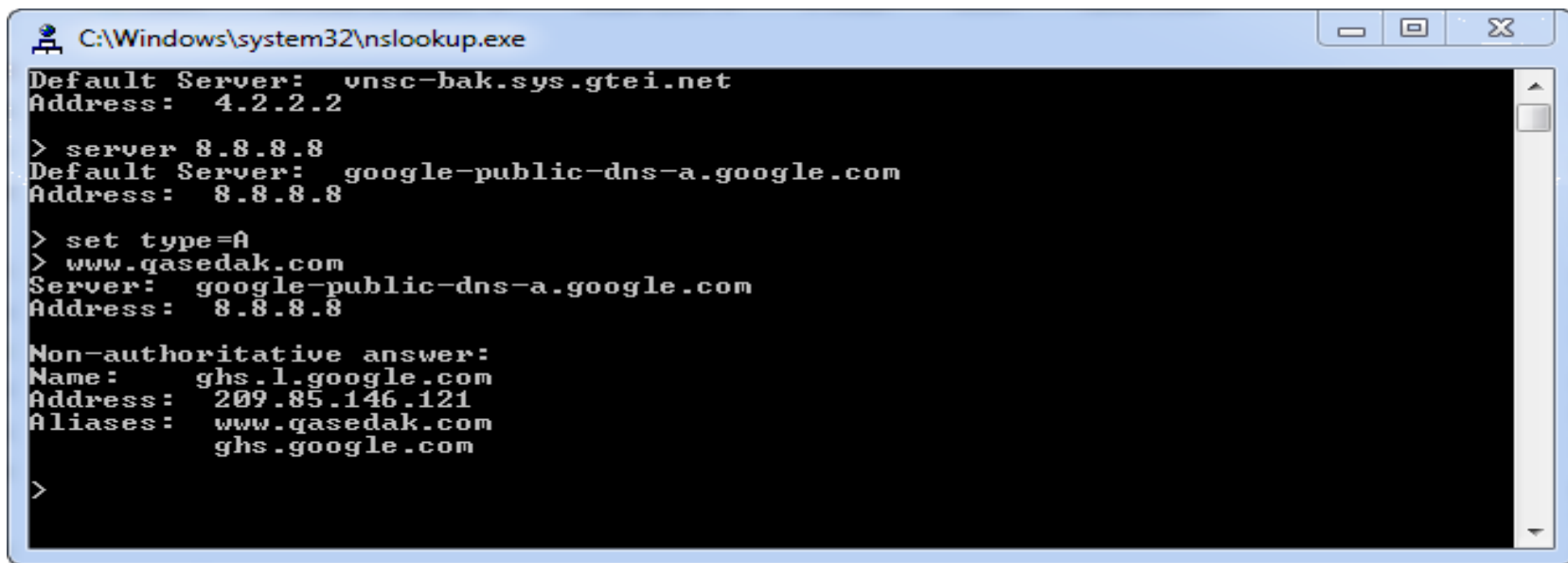
A, CNAME, MX, NS, PTR, SOA, SRV A, AAAA, AA+AAA, ANY

مفهوم این کلمات در فصل DNS Server آمده است.

در صورتی که متغیر Type را مشخص نکنید، از حالت پیش فرض یعنی AA+AAA استفاده می‌شود.

پس از مشخص نمودن نوع سوال می‌توانید درخواست خود را تایپ و کلید Enter را بزنید. بدین ترتیب پرس و جوهای شما به پرس و جوهای خاصی محدود می‌شود. مثلا فقط IP کامپیوترها یا فقط Mail Server ها .

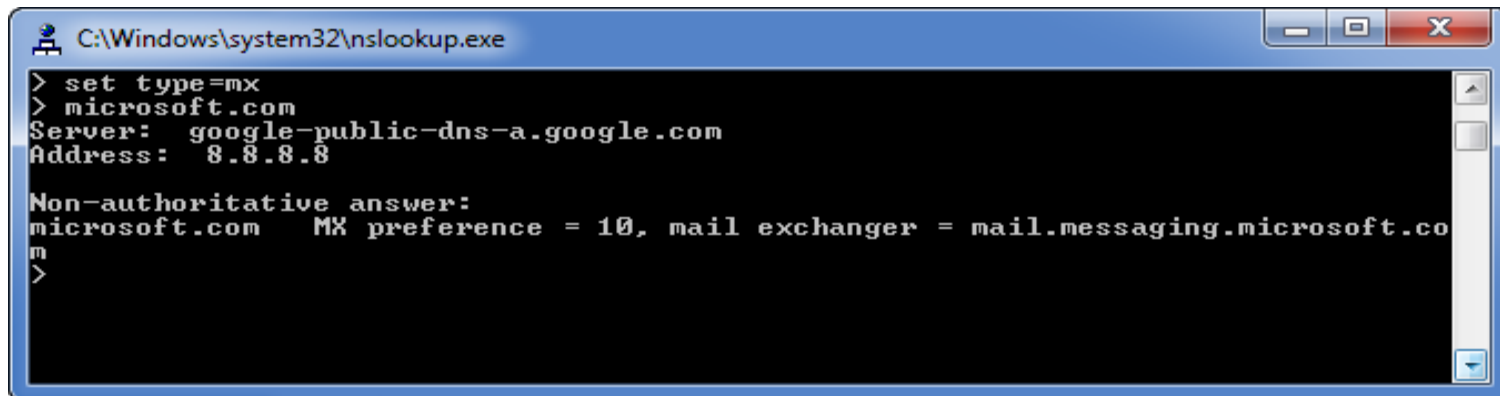
مثال (۱): برای تبدیل نام www.qasedak.com به IP



```
C:\Windows\system32\nslookup.exe
Default Server: vnsc-bak.sys.gtei.net
Address: 4.2.2.2
> server 8.8.8.8
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8
> set type=A
> www.qasedak.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: ghs.l.google.com
Address: 209.85.146.121
Aliases: www.qasedak.com
ghs.google.com
>
```

مثال (۲): برای اطلاع از Mail Server های موجود در دامنه Microsoft.com



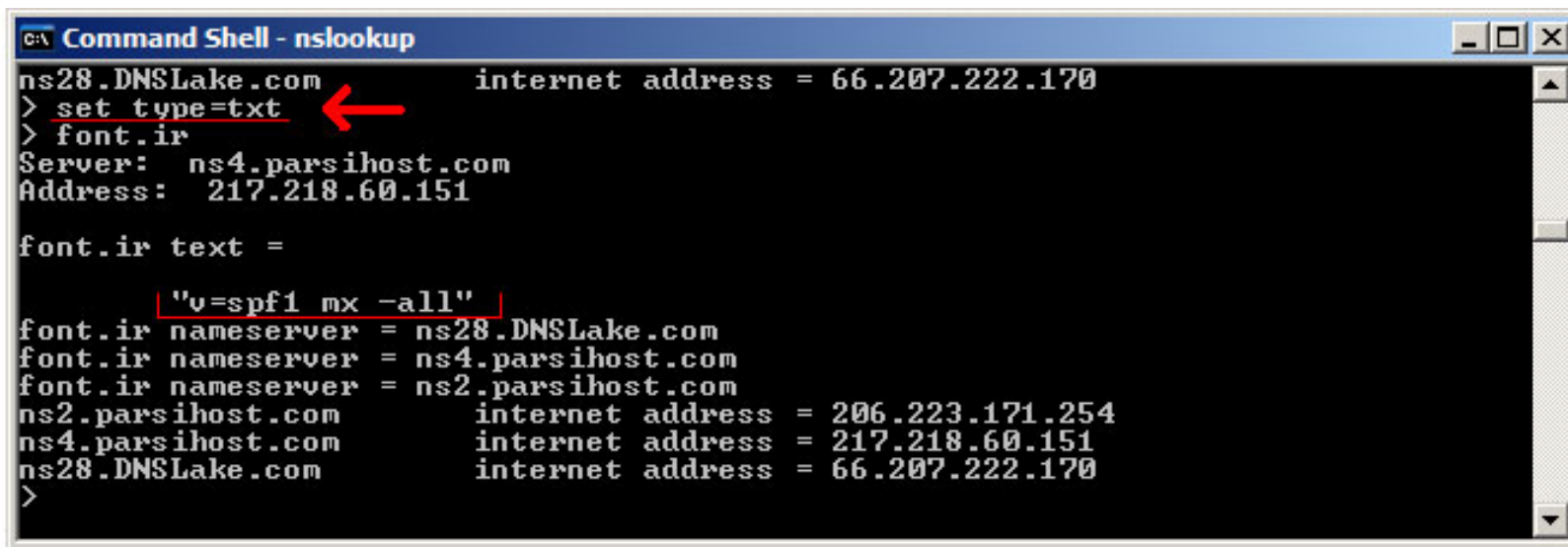
```
C:\Windows\system32\nslookup.exe
> set type=mx
> microsoft.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
microsoft.com MX preference = 10, mail exchanger = mail.messaging.microsoft.co
m
>
```

نکته مهم: اگر nslookup در جواب، عبارت Non-authoritative answer را نمایش داد، به این معنی است که سروری که از آن سوال شده، جواب را از Cache خوانده و به سراغ سرور مسئول دامنه نرفته و اگر این عبارت وجود نداشت یعنی اینکه سوال مستقیماً از سرور مسئول دامنه پرسیده شده است. معمولاً اگر در این حالت یکبار دیگر سوال را تکرار کنید عبارت Non-authoritative نمایش داده می‌شود.

مثال (۳): پرس و جو رکوردهای TXT

دستور `set type=txt` را تایپ می‌کنیم و درباره دامنه `font.ir` پرس و جو می‌کنیم.



```
C:\ Command Shell - nslookup
ns28.DNSLake.com      internet address = 66.207.222.170
> set type=txt
> font.ir
Server: ns4.parsihost.com
Address: 217.218.60.151

font.ir text =

"v=spf1 mx -all"
font.ir nameserver = ns28.DNSLake.com
font.ir nameserver = ns4.parsihost.com
font.ir nameserver = ns2.parsihost.com
ns2.parsihost.com     internet address = 206.223.171.254
ns4.parsihost.com     internet address = 217.218.60.151
ns28.DNSLake.com     internet address = 66.207.222.170
>
```

همانطور که در شکل می بینید، دستور فوق اطلاعات مربوط به رکورد TXT دامنه را نمایش می دهد.

دیگر امکانات دستور nslookup

(۱) تست Zone Transfer

برای اینکه عمل Zone Transfer را توسط nslookup شبیه سازی کنید می توانید از دستور Is استفاده کنید. مثال : Is -d <zone name>

(2) Time out

در صورت کندی اینترنت یا DNS سرور می توانید زمان Timeout را بالا ببرید. مقدار پیش فرض ۲ ثانیه است. مثال : Set timeout=<timeout second>

برای مشاهده تنظیمات فعلی nslookup، از دستور set all استفاده کنید.

۲۱-۸- دستور Whoami

دستور Whoami (?Who am I) نام دامنه، نام رایانه، نام کاربر و نام گروه‌هایی که کاربر عضو آن می‌باشد را نشان می‌دهد:

```
Whoami [{/user | /groups | /priv} /all]
```

پارامترها:

User: برای نمایش نام کاربر به همراه نام دامنه

Groups: نام گروه‌هایی که کاربر عضو آن می‌باشد را نشان می‌دهد.

Priv: مجوز‌هایی که با کاربر داده شده است را نشان می‌دهد. مانند قابلیت تغییر ساعت ویندوز، نصب و حذف برنامه‌ها، تغییرات در تنظیمات شبکه و...

All: تمامی موارد فوق.

۲۱-۹- دستور Getmac

این دستور برای نمایش آدرس فیزیکی کارت شبکه به همراه لیستی از پروتکل‌های شبکه‌ای که به کارت شبکه مربوط می‌شود، استفاده می‌شود. آدرس فیزیکی ۱۲ رقم طول دارد که کاراکترها بر مبنای هگزا دسیمال (مبنای ۱۶) می‌باشد که توسط خط تیره از هم جدا می‌شوند. مثلاً به آدرس رو به رو دقت کنید: 00-15-18-00-04-F9. آدرس فیزیکی تجهیزات شبکه بوده و تکراری نیست. همچنین این آدرس‌ها قابلیت تغییر ندارند. مثال:

```
C:\> GetMac
```

```
Physical Address
```

```
Transport Name
```

```
=====
```

```
=====
```

```
08-00-27-0-90-59
```

```
\Device\Tcpip_{F6ED027D-A0B6-49B9-84C5-2736E61146CA}
```

پارامترها:

/s: برای مشخص کردن نام رایانه یا آدرس IP

/u: برای مشخص کردن نام کاربر به همراه نام دامنه

/p: برای مشخص کردن کلمه عبور. معمولاً این پارامتر به همراه پارامتر **/u** استفاده میشود و مورد آن زمانی است که بخواهیم آدرس فیزیکی یک رایانه راه دور را ببینیم. به همین دلیل باید نام کاربری و کلمه عبور رایانه راه دور را داشته باشیم.

۲۱-۱۰- دستور SFC

دستور SFC یا System File Checker نسخه و صحت کلیه پرونده‌های سیستمی ویندوز را از روی سی دی ویندوز بررسی می‌کند و اگر مغایرتی بین این پرونده‌ها پیدا کند، آن را مجدداً از روی سی دی کپی کرده و آن را اصلاح می‌کند. قالب دستور به صورت زیر است:

SFC [/scannow] [/acanboot]

پارامترها :

/scannow: این دستور تمامی پرونده‌هایی که توسط ویندوز محافظت می‌شود را بلافاصله اسکن و بررسی می‌نماید.

/scanboot: این دستور تمامی پرونده‌هایی که توسط ویندوز محافظت می‌شود را هر بار که رایانه راه‌اندازی می‌شود را اسکن و بررسی می‌نماید.

۲۱-۱۱ - دستور SystemInfo

این دستور گزارش کاملی از کلیه تجهیزات سخت‌افزاری و سیستم عامل نشان می‌دهد.