سوال 1:

دستور Ping یا Packet Internet Group از ساده ترین و کاربردی ترین ابزارهای خطایابی قابل دسترس TCP/IP است.این کامند برای تست اتصال یک دستگاه یا سیستم به سیستم های دیگر و تایید فعال بودن سیستم مقصد استفاده می شود.همچنین برای بررسی برقراری ارتباط با یک host در شبکه نیز از این کامند استفاده می شود.زمانی که بین دو کامپیوتر مشکل برقراری اتصال وجود داشته باشد،استفاده از این کامند اولین قدم در پیدا کردن هرگونه خطا در این زمینه است.درواقع ping ساده ترین کامندی است که اگر (خدای نکرده ) یک کارشناس IT با آن آشنایی نداشته باشد،مدرکش زیر سوال میرود! حال اینکه ping به چه صورت کار می کند:ping از پروتکل ICMP یا Internet Control Message Protocol برای بررسی برقراری اتصال با یک host یا remote host استفاده می کند.درواقع این کامند با ارسال درخواست (request ) به مقصد،منتظر پاسخ (reply) می ماند و دریافت پاسخ از مقصد به معنی وجود ارتباط می باشد. د رمواردی که در برقراری اتصال به اینترنت دچار مشکل هستیم باید مراحل زیر را با استفاده از دستور ping طی کنیم .طی کردن این موارد باعث می شود متوجه شویم گره کار در کدام قسمت است.

* ابتدا برقراری اتصال سیستم خود را با شبکه از طریق ping 127.0.0.1 چک می کنیم.در صورتی که به درخواست ما (request ) پاسخ داده شود (reply ) پس مشکل از سیستم ما نمی باشد.

Ping IP Address of local host

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=64

Reply from 127.0.0.1: bytes=32 time<1ms TTL=64

Reply from 127.0.0.1: bytes=32 time<1ms TTL=64

Reply from 127.0.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 127.0.0.1:

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

Approximate round trip times in milli-seconds:

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

* سپس شبکه داخلی را تست می کنیم.برای این منظور یکی از کامپیوترهای دیگری که در شبکه محلی ما (local network) قرار دارد را ping می کنیم.

Ping IP Address of local network

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time<4ms TTL=64

Reply from 192.168.0.2: bytes=32 time<4ms TTL=64

Reply from 192.168.0.2: bytes=32 time<4ms TTL=64

Reply from 192.168.0.2: bytes=32 time<4ms TTL=64

Ping statistics for 192.168.0.2:

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

Approximate round trip times in milli-seconds:

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

* اگر در مرحله ی قبل نیز مشکلی نداشتیم default gateway را ping می کنیم .اینکار را با کامند زیر انجام می دهیم.با این کامند اتصال default gateway را با اینترنت بررسی می کنیم .در صورتی که از این کامند پاسخی (reply ) گرفتیم پس در برقراری اتصال default gateway با اینترنت مشکلی نداریم.

Ping IP Address of default gateway

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<4ms TTL=64

Reply from 192.168.0.1: bytes=32 time<4ms TTL=64

Reply from 192.168.0.1: bytes=32 time<4ms TTL=64

Reply from 192.168.0.1: bytes=32 time<4ms TTL=64

Ping statistics for 192.168.0.1:

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

Approximate round trip times in milli-seconds:

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

* در مرحله ی آخر برای بررسی برقراری ارتباط ، یک remote host (یا مثلا یک سایت مثل سایت yahoo.com ) را ping می کنیم تا برقراری ارتباط با روترهای در مسیر را چک کنیم.

Ping IP Address of remote host

Pinging itpro.ir [62.193.15.162] with 32 bytes of data:

Reply from 62.193.15.162: bytes=32 time=150ms TTL=116

Reply from 62.193.15.162: bytes=32 time=153ms TTL=116

Reply from 62.193.15.162: bytes=32 time=149ms TTL=116

Reply from 62.193.15.162: bytes=32 time=154ms TTL=116

Ping statistics for 62.193.15.162:

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

Approximate round trip times in milli-seconds:

Minimum = 406ms, Maximum = 457ms, Average = 423ms

در طی این چهار مرحله می توان قدم به قدم صحت برقراری ارتباط را در هر سطح چک کرد و بدین صورت مشکل شبکه را خطایابی کرد.دستور ping ،زیرمجموعه های ( switch ) زیادی دارد .با وارد کردن عبارت ping/? در command prompt ،کلیه ی زیرمجموعه ی این کامند را می توان مشاهده کرد. که در اینجا به چندتای آنها به طور مختصر اشاره می کنم:

شرح کلید Switch Description  
**-a** تبدیل آدرس IP به نام. اگر چه استفاده از این سوئیچ یاعث افزایش تعداد عملیات می گردد ، ولی به خواناتر شدن دستور Ping کمک فراوانی می کند.  
-f فعال نمودن فلگ مربوط به Dont Fragment به منظور جلوگیری از قطعه قطعه نمودن بسته های ارسالی به مقصد مورد نظر.معمولا مسیریاب ها جهت افزایش کارایی ، بسته ها را به قسمت های کوچکتر بسته بندی می کنند.بنابراین، این مسیریاب ها تنها بسته ها را به اندازه های مورد نظر خود تقسیم بندی می نماید. از این سوئیچ می توان جهت بررسی مشکلات مربوط به حداکثر واحد ارسالی PMTU بین دو ماشین استفاده نمود.  
-i TTL تعیین TTL Time To Live مربوط به بسته های ایجاد شده. افزایش TTL باعث ماندگاری بیشتر آن بسته در شبکه می شود. حالت پیش فرض TTL برابر 128 گام است که تا 255 گام قابل افزایش است.  
  
-j host-list تعیین فهرست میزبان های بسته های ICMP در اجرای دستور Ping . پس از اجرای دستور ، به هرکدام از این میزبان ها درخواست فرستاده خواهد شد. تعداد این میزبان ها حداکثر تا 9 کامپیوتر می تواند باشد. (آدرس ها باید با Space فاصله از هم جدا شوند.  
  
-k host-list هنگامی که از این سوئیچ استفاده می کنید، دستور Ping اطلاعات مسیر مربوط به لیست ایجاد شده را نیز تهیه می کند. اطلاعات بدست آمده از خروجی دستور Ping path دقیق تر می باشد. البته هنگام استفاده از این دستور در صورتی که یکی از کامپیوترهای موجود در مسیر قابل دسترس نباشد، پیغام خطایی صادر شده و بلافاصله اجرای دستور متوقف خواهد شد.  
  
-l size تعیین حجم بافر مربوط به فیلد داده موجود در یک بسته. حالت پیش فرض آن 32 بایت است و حداکثر تا حجم 65527 بایت قابل افزایش می باشد. افزایش حجم بافر باعث انجام تستی مطمئن تر شده ولی کارایی دستور را پائین می آورد.  
  
-n count تعیین تعداد درخواست های ارسال شده به یک میزبان.حالت پیش فرض 4 درخواست می باشد.  
  
-r count اجبار دستور جهت ضبط اطلاعات مسیر در سرآیند IP . این عمل باعث اضافه شدن اطلاعات به خروجی دستور Ping می شود.آرگومان Count ، تعداد گام هایی که باید اطلاعات آنها ثبت گردند را تعیین می کند. این مقدار عددی بین 1 تا 9 می باشد.  
  
-s count تعیین وضعیت سیستم جهت ضبط اطلاعات Timestamp در Internet Timestamp موجود در سرآیند IP. این مقدار عددی بین 1 تا 4 می باشد.  
  
-t اجرای دستور Ping و ادامه ارسال بسته ها بدون توقف.برای توقف دستور در این حالت دو راه وجود دارد 1- استفاده از کلیدهای Ctrl+Break که موجب توقف دستور بدون نمایش هیچ گونه وضعیتی از مسیر و گام ها می شود. 2- استفاده از کلیدهای Ctrl+C که موجب نمایش آمار مربوط به این دستور تا زمان توقف آن می شود.  
  
-v TOS تعیین نوع سرویس موجود در بسته. این سرویس باعث افزایش یا کاهش کیفیت بسته ها می شود.   
  
-w timeout تعیین زمان انتظار ، جهت رسیدن پاسخ هر درخواست. حالت پیش فرض این سوئیچ 4000 میلی ثانیه می باشد.

## دستور Ipconfig

Ipconfig یکی دیگر از دستورات کاربردی شبکه در سیستم عمل ویندوز است که برای نمایش اطلاعات مربوط به پروتکل TCP/IP استفاده می شود.این دستور همانند دیگر دستورات شبکه در command prompt اجرا می شود.با استفاده از این دستور شما می توانید تنظیمات دیگری که مربوط به IP می باشند را مشاهده کنید مثل اینکه از کدام سرور DNS استفاده می کنید.با این دستور می توانید MAC address یا همان آدرس فیزیکی مروبط به کارت شبکه ی خود را نیز مشاهده کنید.اگر پیش از یک کارت شبکه دارید،این دستور اطلاعات مربوط به هر کارت شبکه را به طور جداگانه نمایش می دهد .   
  
اگر از این کامند به تنهایی و بدون سوئیچ استفاده کنید ، اطلاعات نمایش داده به شما شامل IP Address ، subnet mask و default getway می باشد اما اگر ipconfig را با سوئیچ all/ استفاده کنید ، تمامی اطلاعات و تنظیمات موجود پروتکل TCP / IP نمایش داده می شود.در ادامه مثالی از کاربرد دستور ipconfig بدون سویچ های اضافی را مشاهده می کنید :

C:\>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . :

IPv4 Address. . . . . . . . . . . : 192.168.1.3

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::d826:ecc1:b3f5:755

IPv4 Address. . . . . . . . . . . : 192.168.179.1

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::49c3:c9db:dbd4:a87

IPv4 Address. . . . . . . . . . . : 192.168.94.1

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . :

Ipconfig /all:اجرای این دستور در command prompt خروجی مانند خروجی زیر را به کاربر نمایش می دهد.همانطور که مشاهده می کنید hostname ،IP address ،MAC address ،DNS Server و IP address مربوط به DHCP server که به سیستم شما IP address می دهد نیز نمایش داده شده است . در ادامه مثالی از کاربردی این دستور با استفاده از سویچ all/ را مشاهده می کنید :

C:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . . . . . . . . : V

Primary Dns Suffix . . . . . . . :

Node Type . . . . . . . . . . . . : Hybrid

IP Routing Enabled. . . . . . . . : No

WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Atheros AR9287 Wireless Network Adapte

Physical Address. . . . . . . . . : 78-DD-08-BD-CA-0C

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Lease Obtained. . . . . . . . . . : الخميس, أوت 16, 2012 09:23:51 ق.ظ

Lease Expires . . . . . . . . . . : الجمعة, أوت 17, 2012 09:24:02 ق.ظ

Default Gateway . . . . . . . . . : 192.168.1.1

DHCP Server . . . . . . . . . . . : 192.168.1.1

DNS Servers . . . . . . . . . . . : 192.168.1.1

192.168.1.1

NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VM

1

Physical Address. . . . . . . . . : 00-50-56-C0-00-01

DHCP Enabled. . . . . . . . . . . : No

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::d826:ecc1:b3f5:755a%18(Preferred

IPv4 Address. . . . . . . . . . . : 192.168.179.1(Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . :

DHCPv6 IAID . . . . . . . . . . . : 637554774

DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-14-4A-46-57-54-42-49-E9-3E

DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1

fec0:0:0:ffff::2%1

fec0:0:0:ffff::3%1

NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VM 8

Physical Address. . . . . . . . . : 00-50-56-C0-00-08

DHCP Enabled. . . . . . . . . . . : No

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::49c3:c9db:dbd4:a879%19(Preferred

IPv4 Address. . . . . . . . . . . : 192.168.94.1(Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . :

DHCPv6 IAID . . . . . . . . . . . : 654331990

DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-14-4A-46-57-54-42-49-E9-3E

DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1

fec0:0:0:ffff::2%1

fec0:0:0:ffff::3%1

NetBIOS over Tcpip. . . . . . . . : Enabled

 سوئیچ ها :

/all       : به منظور نمایش تمامی پیکربندی های IP موجود در کامپیوتر استفاده می شود.

/showclassid   : به منظور نمایش ClassID های DHCP که برای وفق دهی مجاز  هستند به کار می رود.

C:\>ipconfig

USAGE:

    ipconfig [/? | /all | /renew [adapter] | /release [adapter] |

              /flushdns | /displaydns | /registerdns |

              /showclassid adapter |

              /setclassid adapter [classid] ]

where

    adapter         Connection name

                   (wildcard characters \* and ? allowed, see examples)

    Options:

       /?           Display this help message

       /all         Display full configuration information.

       /release     Release the IP address for the specified adapter.

       /renew       Renew the IP address for the specified adapter.

       /flushdns    Purges the DNS Resolver cache.

       /registerdns Refreshes all DHCP leases and re-registers DNS names

       /displaydns  Display the contents of the DNS Resolver Cache.

       /showclassid Displays all the dhcp class IDs allowed for adapter.

       /setclassid  Modifies the dhcp class id.

The default is to display only the IP address, subnet mask and

default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address

leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid, if no ClassId is specified, then the ClassId is removed.

Examples:

    > ipconfig                   ... Show information.

    > ipconfig /all              ... Show detailed information

    > ipconfig /renew            ... renew all adapters

    > ipconfig /renew EL\*        ... renew any connection that has its

                                     name starting with EL

    > ipconfig /release \*Con\*    ... release all matching connections,

                                     eg. "Local Area Connection  "Local Area Connection 2"

سوال 2:

Whois چیست ؟

هنگامی که اینترنت هنوز جوان بود و دامنه یک امتیاز و اطلاعات در هیچ دایرکتوری ثبت نمی شد مفهوم مالکیت دامنه برای اولین بار معرفی شد وقتی شما برای اولین بار برای خرید دامنه اقدام می کنید اطلاعاتی درباره فرد یا سازمان که صاحب امتیاز دامنه برای آن می شود را پر می کنید این اطلاعات به عنوان اطلاعات WHOIS شناخته می شوند.

**تاریخچه WHOIS**

زمانی که فقط یک سرویس دهنده اینترنت بنام ARPANET بود ,یک سازمان بنام DARPA تنها مسئول ثبت دامنه وجود دارد و تمامی دامنه ها به راحتی قابل دسترسی به اطلاعات پایگاه داده WHOIS بود . واقعیت این است که تنها یک سازمان مدیریت هر دو دامنه ها را ثبت  و جزئیات مربوط به WHOIS را منتشر می کنند.به آرامی و با تکامل شبکه جهانی وب [ثبت دامنه](http://www.tehranhost.com/domain.php" \o "ثبت دامنه) و مدیریت WHOIS به دور از DARPA منتقل شده و اکنون می توانید دامنه خود را توسط چند  شرکت معتبر اطالاعات خود را ثبت نمایید تعدادی از دامنه ها در همان زمان که تعداد آنها نیز زیاد بود و همچنین این اطلاعات تمامی مشخصات فرد و سازمان  را در اختیار عموم قرار میداد که از همه مهمتر ایمیل اشخاص بود که هکرها با استفاده از این موقعیت حملات فیشینگ را به راحتی انجام میدادند و همچنین هرزنامه های زیادی در آن زمان رایج بود و بدلیل نمایش و مشکلات در اطلاعات WHOIS پروتکل WHOIS تجدید نظر شد و جستجو کلمات و ایمیلها ممنوع شد و امروزه نمایش ایمیل توسط سرویس دهنده ها بصورت تصویر می باشد که این عمر تا حد زیادی از خرابکاری ها توسط هکرها و هرزنامه ها را میگیرد

**دسترسی به اطلاعات WHOIS یک دامنه**

دسترسی به اطلاعات WHOIS یک دامنه به کاربر اجازه می دهد که از طریق کامپیوتر به دو صورت اطلاعات را مشاهده کنید

1. بصورت خط فرمان و محیط گرافیکی

2. نمایش اطلاعات WHOIS بصورت آنلاین

**نمایش اطلاعات WHOIS بصورت خط فرمان و محیط گرافیکی**

با استفاده از خط فرمان و محیط گرافیکی در سیستم عامل یونیکس و یا مبتنی بر یونیکس یکی از قدرتمد ترین راهها می باشد . با استفاده از ترمینال در لینوکس می توانید اطلاعات یک دامنه را با استفاده از خط فرمان و بدون قالب بندی بدست آورید این راه در هر توزیع لینوکس قابل اجرا است و کار با آن بسیار محبوب است.

دو دستور زیر برای سیستم های لینوکس و یونیکس قابل اجراست و بجای example نام دامنه خود را وارد کنید.

whois example.com #

 whois example.com $

برای نمایش اطلاعات در محیط ویندوز باید از نرم افزاهایی مختص به نمایش اطلاعات WHOIS استفاده کنید.

**نمایش اطلاعات WHOIS بصورت آنلاین**

برای کسانی که دسترسی به سیستم عامل های لینوکس ندارد بهترین روش نمایش اطلاعات WHOIS بصورت آنلاین است و می توانید ساختار اطلاعات را بصورت HTML و همچنین اطلاعات DNS , WHOIS را مشاهده کنید و چنین ابزارهایی در سایت های مختلفی از اینترنت به صورت رایگان وجود دارد.

لینک برخی از وب سایتهایی که این خدمات را بصورت رایگان ارائه می دهند در زیر آمده است

برای مشاهده اطلاعات WHOIS دامنه های ir از لینک زیر استفاده کنید

http://whois.nic.ir

و برای مشاهده اطلاعات WHOIS دامنه های com , info , net , cc , info , biz , tv ,… از لینکهای زیر استفاده کنید

http://whois.domaintools.com

http://www.whoisfinder.com

http://www-whois.domainpeople.com

http://www.internic.net/whois.html

http://who.is

**حفاطت در اطلاعات WHOIS**

حفاطت در اطلاعات WHOIS امروزه یک امر حیاتی است و صاحبان دامنه این امکان را دارند تا اطلاعات خود را از چشم عموم مخفی نگه دارند و به این ترتیب در برابر هرزنامه یا حملات فیشینگ محافطت می شوند مخفی نگه داشتن اطلاعات در دامنه های زیر قابل دسترس است

com, .net, .org, .info, .biz, .me, .tv, .asia, .cc.

و می توان اطلاعات WHOIS و ID را بطور مستقیم محافطت کرد و یا اطلاعات خود را تغییر دهید برای تغییر و محافطت باید با ثبت کننده دامنه خود تماس یا از پنل دامنه خود این کار را انجام دهید.

مثال عینی:

بررسی اطلاعات در [whois](http://whois.avasite.ir/) :

یکی از سایت های پرطرفدار جهت بررسی هویز – [whois](http://whois.avasite.ir/) دامنه سایت Domain Tools است . شما در این سایت می توانید با وارد کردن آدرس سایت یا آِ پی آن براحتی اطلاعات مالک سایت را بدست بیاورید.

[برای ورود به Domain Tools کلیک کنید](http://www.domaintools.com/)

بعد از وارد شدن به سایت دامین تولز در بالای سایت قسمت WHOIS LOOKUP آدرس سایت مورد نظر خود را وارد کنید و سپس اینتر کنید و منتظر باشید.

بعد از بررسی در صفحه جدید اطلاعات مالک ظاهر خواهد شد.

به عنوان مثال ما آدرس سایت آوا – AvaSite.ir را بررسی کرده ایم و مشخصات زیر نمایان شد :

domain:                avasite.ir  
ascii:                avasite.ir  
remarks:        (Domain Holder) Reza Alizadeh  
remarks:        (Domain Holder Address) karaj, Tehran, Tehran, IR  
holder-c:        ra1450-irnic  
admin-c:        mi355-irnic  
tech-c:                mi355-irnic  
nserver:        ns1.avawebhost.com  
nserver:        ns2.avawebhost.com  
last-updated:        ۲۰۱۳-۱۰-۲۶  
expire-date:        ۲۰۱۴-۰۹-۱۱  
source:                IRNIC # Filtered

nic-hdl:        ra1450-irnic  
person:                Reza Alizadeh  
e-mail:          rahilcompuer@yahoo.com  
address:        karaj, Tehran, Tehran, IR  
phone:                +۹۸۲۱۶۵۱۱۱۶۱  
source:                IRNIC # Filtered

همانطور که می بینید در مشخصه های بالا نام, شماره تماس, شناسه نیک, ایمیل و آدرس آمده است .

همچنین می توانید از [whois](http://whois.avasite.ir/) دامنه برای بررسی آزاد و یا مسدود بودن دامنه مورد نظر نیز استفاده کنید.

سوال 3:

**دامنه چیست؟**

به آدرس های سایت دامنه می گویند. مانند www.google.com که دامنه آن google.com است. شاید اجزای هر URL را بدانید ولی دامنه یکی از مهم ترین قسمت های سایت و URL است. برای مثال دامنه زیر را ببینید:

https://www.bsi.ir

پسوند IR ، پسوند این دامنه است ولی دقت کنید:

https://www.bsi.ir/default.aspx

aspx پسوند فایل default و IR پسوند دامنه ماست. خب حالا فرق .com و .net و .ir و … در چیست؟ هر یک از پسوند های دامنه معنای خاصی دارد. مثلا پسوند .ac.com یا ac.ir را برای دانشگاه ها و موسسات آموزش می گذارند. هر دامنه بسته به نوع خود در سازمان مربوطه و هر سازمان اجازه اجاره آن را از سازمان خاصی می گیرد. برای مثال برای ثبت دامنه phpassistant.ir ، ما باید به سازمان نیک مراجعه کنیم تا آن را برای ما ثبت کنند. دامنه هایی با پسوند عمومی مثل net یا com در سازمانی به نام Domain Name Register Center ثبت می شود. اگر شما بخواهید دامنه ای ثبت کنید مشخصات شما را می خواهند. خواستن مشخصات به این دلیل است که مشخصات شما در پایگاه Whois ثبت شود و از دزدیده شدن دامنه شما جلوگیری شود. Whois چیست؟ کجاست؟ Whois یک پایگاه وابسته به سازمان ثبت دامنه است که با جستجوی هر دامنه DNS ، نام مشخصات مالک و نام ثبت کننده نمایش داده می شود که آن را در سایت های اجاره دامنه حتما دیده اید.

**DNS دامنه چیست؟**

مانند آجرهای یک خانه است. آدرس DNS ها ممکن است به صورت زیر باشد:

ns1.server.com  
ns2.server.com

DNS برای این که هاست شما به دامنه شما مربوط شود ، تنظیم می شود. سرور های ns1 ممکن است قطع باشند به همین دلیل باید ns2 کار کند. اگر به هر دلیلی Data Center هاست شما از بین برود ، DNS های شما نیز از بین می روند تا دامنه بدون هاست شما دزدیده نشود.

**هاست یا Host یعنی چه؟**

با توضیحات بالا فهمیدید که هاست و دامنه به یک دیگر وابسته اند. هاست (Host) در زبان انگلیسی به معنی میزبان است. یعنی میزبانی سایت شما برعهده  شرکتی است که شما انتخاب کردید. Host یک کامپیوتر تحت شبکه است که توسط cpanel سایت شما کنترل می شود. محتوای این کامپیوتر یک سیستم عامل است که شما انتخاب کردید لینوکس یا ویندوز. و در درایو های دیگر محتوایی که شما از طریق cpanel برای سایت خود ریخته اید وجود دارد. پس Host هم یک کامپیوتر است که با وسایل جانبی پیشرفته و مودم های مخصوص ، به cpanel متصل شده و در شبکه اینترنت پخش می شود. برای این هاست ها باید حتما DNS دامنه تنظیم شود. ممکن است بگویید من و دوستم از یک هاست خریده ایم ولی DNS هایمان فرقی ندارد. چرا؟ DNS پرتکول خاصی ندارد و تنظیمات DNS نیز توسط مرورگر ها قابل مشاهده نیست. DNS فقط شامل یک نشانی نیست بلکه به طور اتوماتیک یوزرنیم و پسورد هاست مربوطه نیز در هاست ها به آدرس DNS فرستاده می شود تا بتوان کنترل DNS را در دست گرفت.

**هاست VPS چیست؟** هاست VPS فقط در یک کامپیوتر اجرا می شود و توسط سخت افزار های مخصوص مجازی سازی می شود. یک سوپر کامپیوتر وظیفه چندین کامپیوتر را دارد و به هر سایت مقداری رم و فضا اختصاص می دهد. این هاست ها معمولا گران هستند ولی سرعت آن ها بیش از بقیه هاست است. هاست VPS معمولا برای سازمان های هاستینگ خیلی قوی و پرمشتری گذاشته می شود.

**Data Center چیست؟** وقتی سایت هایی مثل فیس بوک تا این حد بازدید دارند خب بدیهیست که اگر بخواهند تمام اطلاعات میلیون ها کاربر را بر روی یک کامپیوتر هاست مجازی یا هاست معمولی ذخیره کنند کامپیوتر بلافاصله کرش کرده و تمام اطلاعات کاربران در عرض یک چشم به هم زدن از بین می رود. پس باید جهت کمتر شدن هزینه و افزایش مقدار فضا آن ها را به قسمت های مختلفی که شبیه کابل های برق هستند و در آن اطلاعات ۰ و ۱ رد و بدل می شود. هر هاست معمولی مجازی یا هر نوع هاست باید یک یا چند Data Center داشته باشد.

**چگونه دامنه ir ثبت کنیم**

قدم اول : ایجاد حساب کاربری در سایت nic.ir   
  
جهت ثبت دامین ir. و ایران. به نام خودتان ، لازم است که حتما یک اکانت در سایت nic.ir کارگزار رسمی ثبت دامنه ir. و ایران داشته باشید.  
  
ساخت هندل(اکانت) در nic.ir رایگان می باشد. برای این کار کافی است روی لینک زیر کلیک نمایید و اطلاعات خواسته شده را دقیقا در فرم مزبور وارد نمایید:  
  
<https://www.nic.ir/Create_New_Handle>  
  
یا در صفحه اصلی سایت nic.ir ، در بالای صفحه روی "ساخت شناسه کاربری" کلیک نمائید.  
  
توجه داشته باشید که اکانت خود را به هرنامی که ایجاد نمایید مالک کلیه دامین های ثبت شده در آن همان شخص خواهد بود، لذا لازم است که اطلاعات خود را کاملا دقیق وارد نمایید چون تغییر مالکیت دامین ها دارای شرایط ویژه و قوانین خاصی می باشد که آنها را می توانید در سایت nic.ir و در لینک زیر بخوانید:  
  
  
<https://www.nic.ir/Rules_and_Contracts>  
  
  
ایجاد یک اکانت در وب سایت nic.ir شامل چهار مرحله زیر می باشد :  
  
1-انتخاب نوع شناسه :  
  
برای ایجاد اکانت شما باید یکی از پنج نوع شناسه زیر را انتخاب نمائید و روی دکمه "تکمیل فرم و دریافت شناسه" کلیک نمائید  
  
شخص حقیقی   
شرکت ، موسسه یا نهاد غیر دولتی   
وزارتخانه ، سازمان یا شرکت دولتی   
مرکز آموزشی و پژوهشی   
شناسه ی محدود   
  
  
ما در اینجا مراحل ساخت اکانت برای شخص حقیقی را شرح می دهیم  
  
2-وارد کردن مشخصات شناسه :  
  
در این قسمت باید مشخصات خود را مانند مثال های آورده شده در هر کادر درج نمائید  
  
ابتدا نام و نام خانوادگی و نام سازمان را به فارسی و لاتین وارد نمائید  
  
  
سپس شماره کد ملی و یا اطلاعات گذرنامه خود را وارد نمائید (وارد کردن فقط یکی از مشخصات ذیل کافی می باشد)  
  
  
در قسمت بعد باید اطلاعات مربوط به نشانی پستی خود را درج نمائید. دقت نمائید که اطلاعات همانند نمونه وارد شود  
  
  
در قسمت بعد باید نشانی پست الکترونیکی و پرسش و پاسخ محرمانه را وارد نمائید. دقت نمائید که پرسش و پاسخ آن هنگامی که رمز عبور را فراموش می کنید لازم است.  
  
  
در انتها وضعیت رابط های مجاز را تعیین نمائید و روی بازنگری کلیک نمائید.

3-بازنگری و امضا :  
  
پس از کلیک روی بازنگری در مرحله قبل و عدم بروز مشکل در اطلاعات وارد شده وارد این مرحله می شوید ، در این مرحله اطلاعات درج شده توسط شما جهت تائید نمایش داده می شود و پس از اطمینان از صحت اطلاعات شخصی تان در پایین این صفحه نام کامل خود را با حروف لاتین و همچنین کد امنیتی درج شده را وارد نمائید و دکمه "موافقم دریافت شناسه " کلیک نمائید.  
  
  
4-ساختن شناسه :  
  
پس از طی مراحل فوق در مرحله آخر پیغامی همانند تصویر زیر برایتان نمایش می یابد و شناسه شما به همراه پسورد یه ایمیلی که در فرم ها وارد کرده اید ارسال می گردد.  
  
  
دقت نمائید که ایمیل ارسال شده ممکن است در شاخه Spam ایمیل شما قرار گرفته باشد.  
  
در قدم بعد شما باید به حساب ایمیل خود رفته و در ایمیلی که از سایت nic.ir دریافت نموده اید روی لینک " به سیستم وارد شوید " کلیک نمائید سپس صفحه log in سایت nic.ir برای شما باز می شود و باید بوسیله نام کاربری و پسوردی که در اختیارتان گذاشته شده log in نمائید.  
  
  
پس از ورود از شما خواسته می شود که نسبت به تغییر پسورد خود اقدام نمائید. برای اینکار باید پاسخ پرسش محرمانه خود و همچنین پسورد جدید مورد نظر خود را وارد نمائید ، پس از وارد کردن مجدد پسورد جهت تایید ، روی دکمه "نشاندن گذرواژه کلیک نمائید.  
  
پس از اینکار مجددا باید با پسورد جدید در سایت nic.ir لاگین نمائید.

سوال 4:

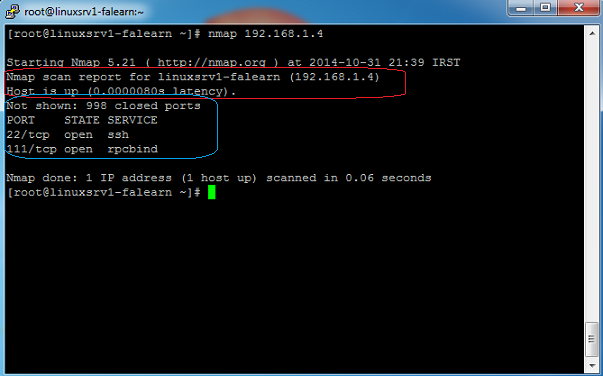
[nmap](http://falearn.ir/?cat=433) ابزاری open source تحت سیستم عامل های شبه یونیکسی مانند لینوکس برای اسکنر امنیتی شبکه برای کشف سرور ها و کلاینت های (ماشین های) درون شبکه به کار می رود. nmap به منظور کشف ماشین های شبکه توسط پاسخ های ping، ، پیدا کردن اطلاعات سیستم عامل راه دور و درون شبکه به کار گرفته می شود. به طور مثال می توان به منظور سیاست های امنیتی، برای پیدا کردن پورت های باز و بسته، ماشین محلی یا راه دور را اسکن کرد.

هدف از این مطلب اسکن شبکه و پیدا کردن ماشین ها توسط تعیین کردن محدوده ای از آدرس های IP است. ساده ترین شکل به صورت زیر است.

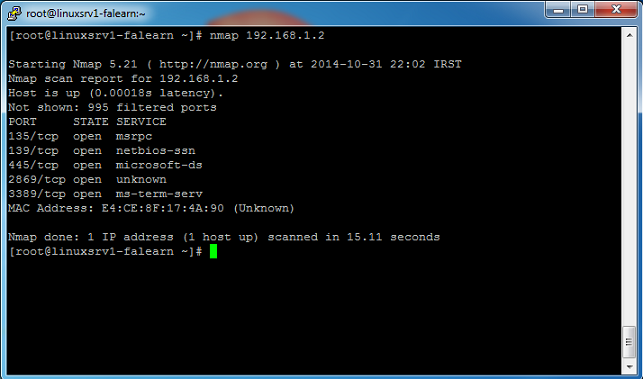
nmap IP\_ADDRESS

به طور مثال دستور زیر شبکه را برای آدرس 192.16.1.4 پویش می کند. (در اینجا 192.168.1.4 آدرس ماشین محلی است)

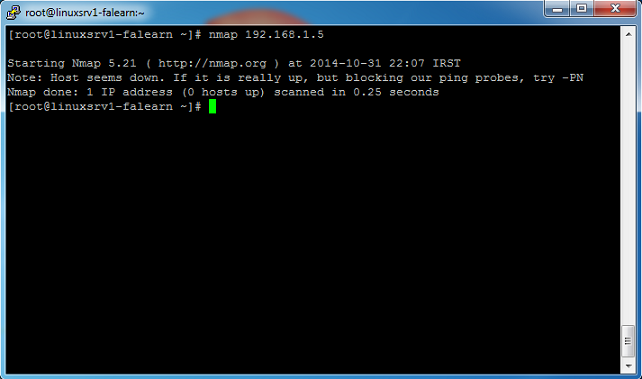
nmap 192.168.1.4

[](http://falearn.ir/wp-content/uploads/2014/10/nmap_ip_scan.png)

شکل بالا نشان می دهد که ماشین 192.168.1.4 (در اینجا ماشین محلی) up بوده و 998 پورت بر روی آن بسته و دو پورت 22 و 111 باز است. شکل زیر در شبکه آدرس 192.168.1.2 را پویش می کند.

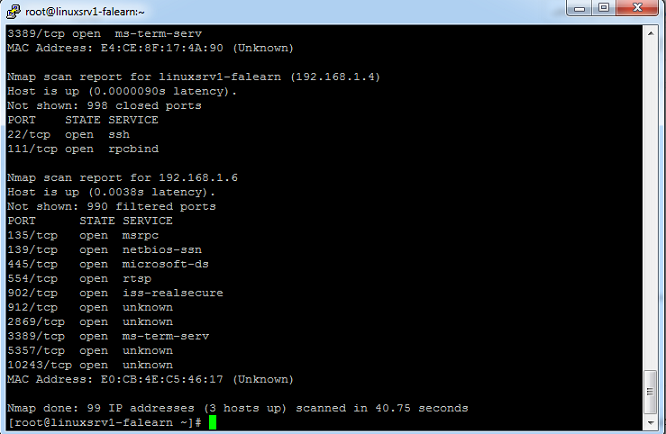
[](http://falearn.ir/wp-content/uploads/2014/10/nmap_ip_scan0.png)

در صورتی که آدرسی را در شبکه پویش کنید و سیستم خاموش باشد و یا اینکه از شبکه (سوییچ) قطع شده باشد و یا ping توسط فایروال بلاک شده باشد، آنگاه خطای زیر را نشان داده خواهد شد.

[](http://falearn.ir/wp-content/uploads/2014/10/nmap_ip_scan1.png)

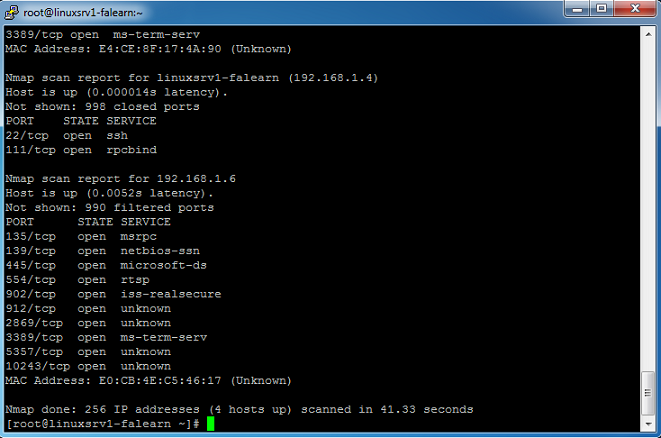
می توان محدوده ای از آدرس ها را در شبکه پویش کرد. به طور مثال محدوه آدرس های 192.168.1.2 تا 192.168.100 را توسط دستور زیر پویش می کنیم.

nmap 192.168.1.2-100

[](http://falearn.ir/wp-content/uploads/2014/10/nmap_ip_scan2.png)

 اما اگر بخواهید کل یک شبکه را پویش کنید، به طور مثال شبکه به آدرس 192.168.1.0 و Net Mask به آدرس 255.255.255.0 که معادل 24/ است، از دستور زیر استفاده کنید.

nmap 192.168.1.0/24

[](http://falearn.ir/wp-content/uploads/2014/10/nmap_ip_scan3.png)

اما اگر می خواهید تنها اسکن بر اساس پاسخ های ping و به منظور پویش شبکه برای آگاهی از up بودن یک یا محدوده ای از سیستم ها (آدرس ها) را انجام دهید، از سوییچ sp- (یعنی Scan Ping) استفاده کنید.

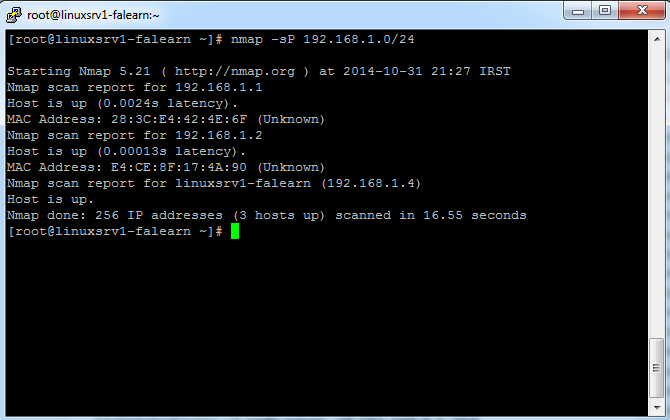
nmap -sP 192.168.1.2

[nmap_ip_scan4](http://falearn.ir/wp-content/uploads/2014/10/nmap_ip_scan4.png)

همانطور که از شکل بالا پیدا است، با استفاده از سوییچ sP- بر خلاف دستور های پیشین دیگر پویش برای نمایش پورت ها دیگر انجام نمی شود. همچنین می توانید این سوییچ را برای محدوده از آدرس ها و یا کل شبکه انجام دهید.

nmap -sP 192.168.1.2-100

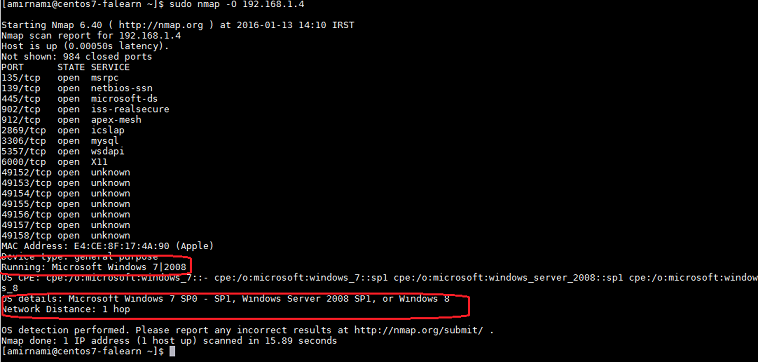
nmap -sP 192.168.1.0/24

[](http://falearn.ir/wp-content/uploads/2014/10/nmap_ip_scan5.png)

یکی دیگر از کاربردهای [nmap](http://falearn.ir/?cat=433) تشخیص نوع سیستم عاملی است که بر روی ماشین های راه دور نصب شده اند. درون یک شبکه انواع گوناگونی از سیستم عامل ها همچون سیستم عامل های خانواده ویندوز و سیستم عامل لینوکس وجود دارد. دستور nmap دارای سوئیچ های متفاوتی است که امکان پویش یا Scan کل شبکه را می دهد تا بتوانیم نوع سیستم عامل ها را پیدا کنیم.

OS fingerprinting فرایند و مفهومی است که نوع یک سیستم عامل را بر روی یک ماشین تشخیص می دهد. از سوئیچ O- برای تشخیص و چاپ نوع سیستم عامل در خروجی استفاده می شود.

nmap -O 192.168.1.4

[](http://falearn.ir/wp-content/uploads/2016/01/nmap_os_detiction1.png)

nmap -O –osscan-limit  192.168.1.4

nmap -O -v  192.168.1.4

همانطور که از شکل بالا مشخص است سیستمی عاملی که برای رو ماشین راه دور 192.168.1.4 نصب شده است یکی از سیستم عامل های ویندوز 7، 2008 یا ویندوز 8 است. همچنین در خروجی یک خط با OS CPE مشخص شده است. CPE که محفف Common Platform Enumeration است یک روش استاندارد برای نام گذاری نرم افزارها (برنامه های کاربردی)، سخت افزارها و سیستم عامل ها است.در خروجی nmap از CPE برای تشخیص سیستم عامل استفاده می شود.

یک CPE یک URL متشکل از هفت فیلد زیر است.

<cpe:/<part>:<vendor>:<product>:<version>:<update>:<edition>:<language

برخی از این هفت فیلد ممکن است که مقدار دهی نشده باشند. اصلی ترین بخش این هفت فیلد، فیلد part است که دارای یکی از سه مقدار زیر می باشد.

a برای application

h برای hardware

o برای operating system

به طور مثال از خروجی شکل بالا

cpe:/**o**:**microsoft**:**windows\_7**::sp1

و به عنوان مثال های دیگر

cpe:/o:freebsd:freebsd:3.5.1

cpe:/a:mysql:mysql:5.1.48

vendor نام شرکت و کمپانی تولید کننده محصول سخت افزاری و نرم افزاری است.

product نام محصول سخت افزاری یا نرم افزاری است که تشخیص داده شده است.

version نسخه را نشان می دهد.

update لیستی از بروز رسانی هایی که تشخیص داده شده است. به طور مثال sp1

edition ویرایش تشخیص داده شده را نشان می دهد.

language زبان تشخیص داده شده را نشان می دهد. به طور مثال English