

«باسمه تعالی»



گزارش آزمایش دوم دستور کار
ابزارهای مدیریت شبکه های کامپیوتری



طراحی و تدوین:

مهدی رحمانی

9731701

سوال 1: به نظر شما سوییچ I- چیست و چگونه عمل میکند؟

اگر دستور -? ping را داخل cmd وارد کنیم خواهیم داشت:

```
Command Prompt
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\M R>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] [-c compartment] [-p]
          [-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
            Header).
-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).
            Per RFC 5095 the use of this routing header has been
            deprecated. Some systems may drop echo requests if
            this header is used.
-S srcaddr  Source address to use.
-c compartment Routing compartment identifier.
-p          Ping a Hyper-V Network Virtualization provider address.
-4          Force using IPv4.
-6          Force using IPv6.
```

طبق خروجی مشاهده شده میتوان گفت که I- برای سایز میباشد و به کمک آن می توان سایز بافر را تغییر داد و ارسال کرد.

برای مثال در حالت عادی وقتی google.com را ping میکنیم، عبارت Bytes = 32 ؛ حجم ارسالی یا درواقع Buffer Size پیام را مشخص میکند که به صورت دیفالت مقدار آن 32 بایت میباشد. این موضوع را میتوانید در شکل زیر ببینید:

```
C:\Users\M R>ping google.com

Pinging google.com [216.58.209.142] with 32 bytes of data:
Reply from 216.58.209.142: bytes=32 time=75ms TTL=106
Reply from 216.58.209.142: bytes=32 time=93ms TTL=106
Reply from 216.58.209.142: bytes=32 time=50ms TTL=106
Reply from 216.58.209.142: bytes=32 time=69ms TTL=106

Ping statistics for 216.58.209.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 93ms, Average = 71ms
```

حال با پارامتری ای به نام I- میتوان این سایز را تغییر داد و حداقل حجم Data بسته ارسالی را مشخص نمود.
برای مثال با دستور زیر میتوان حجم پیام ارسالی را 16 بایتی کرد:

Ping google.com -l 16

با اجرا کردن آن در cmd به صورت زیر خواهیم داشت:

```
C:\Users\M R>ping google.com -l 16

Pinging google.com [216.58.209.142] with 16 bytes of data:
Reply from 216.58.209.142: bytes=16 time=79ms TTL=106
Reply from 216.58.209.142: bytes=16 time=55ms TTL=106
Reply from 216.58.209.142: bytes=16 time=50ms TTL=106
Reply from 216.58.209.142: bytes=16 time=54ms TTL=106

Ping statistics for 216.58.209.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 79ms, Average = 59ms
```

هم چنین range قابل قبول برای سوییچ -l محدوده ی 0 تا 65500 میباشد.

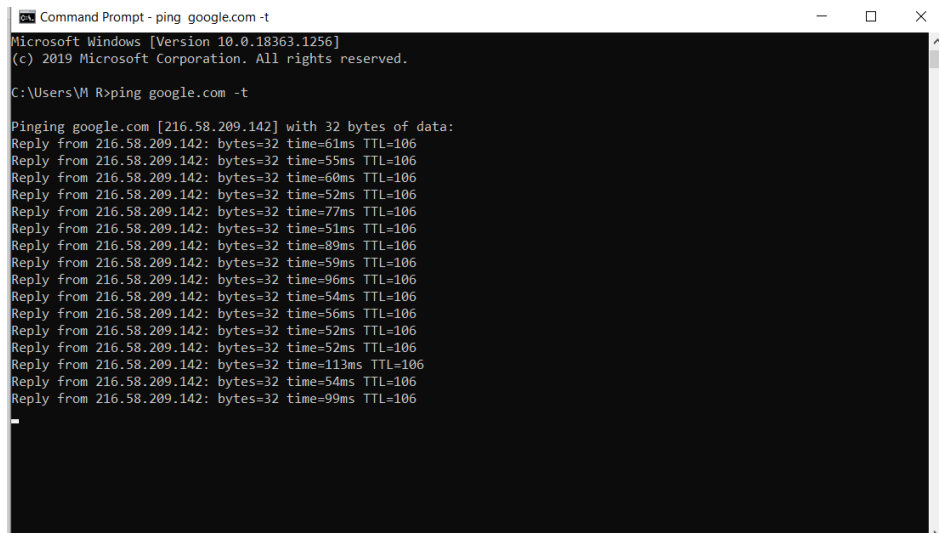
```
C:\Users\M R>ping courses.aut.ac.ir -l 100000 -t
Bad value for option -l, valid range is from 0 to 65500.
```

سوال 3: همانگونه که مشاهده کردید Ping بعد از ارسال و دریافت 4 پیام قطع میشود. دستوری پیدا کنید که ارسال و دریافت پیام را بدون توقف ادامه دهد.

اگر دوباره دستور `ping` را داخل `cmd` وارد کنیم و در لیست بگردیم توضیحاتی میابیم که در آن اشاره میکند که دستور `-t` این قابلیت را دارد و میتوان ارسال و دریافت پیام را بدون توقف ادامه داد.

```
-t          Ping the specified host until stopped.  
           To see statistics and continue - type Control-Break;  
           To stop - type Control-C.
```

برای مثال میتوانیم `google.com` را به این شیوه ping کنیم و خواهیم داشت:



```
Command Prompt - ping google.com -t  
Microsoft Windows [Version 10.0.18363.1256]  
(c) 2019 Microsoft Corporation. All rights reserved.  
  
C:\Users\M R>ping google.com -t  
  
Pinging google.com [216.58.209.142] with 32 bytes of data:  
Reply from 216.58.209.142: bytes=32 time=61ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=55ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=60ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=52ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=77ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=51ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=89ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=59ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=96ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=54ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=56ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=52ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=52ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=113ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=54ms TTL=106  
Reply from 216.58.209.142: bytes=32 time=99ms TTL=106  
^
```

هم چنین دو نکته ضروری است:

- اگر بخواهیم پس از تعدادی گام به ما آمار و میانگین زمان رفت و برگشت و میزان `lost` و... را بدهد و سپس به ادامه ی ارسال و دریافت پیام پردازد میتوان از `Control-Break` استفاده کرد.
- اگر بخواهیم پس از تعدادی گام ارسال و دریافت پیام را کامل متوقف کنیم میتوانیم از `Control-C` استفاده کنیم. همچنین در نهایت یک سری داده آماری از قبیل اطلاعاتی که پیش تر ذکر شد (از ابتدا تا گامی که جلو رفته است) به ما میدهد.

```
Command Prompt
C:\Users\M R>ping google.com -t

Pinging google.com [216.58.209.142] with 32 bytes of data:
Reply from 216.58.209.142: bytes=32 time=125ms TTL=106
Reply from 216.58.209.142: bytes=32 time=53ms TTL=106
Reply from 216.58.209.142: bytes=32 time=53ms TTL=106
Reply from 216.58.209.142: bytes=32 time=90ms TTL=106
Reply from 216.58.209.142: bytes=32 time=50ms TTL=106
Reply from 216.58.209.142: bytes=32 time=52ms TTL=106
Reply from 216.58.209.142: bytes=32 time=212ms TTL=106

Ping statistics for 216.58.209.142:
    Packets: Sent = 7, Received = 7, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 212ms, Average = 90ms
Control-Break
Reply from 216.58.209.142: bytes=32 time=53ms TTL=106
Reply from 216.58.209.142: bytes=32 time=54ms TTL=106
Reply from 216.58.209.142: bytes=32 time=110ms TTL=106
Reply from 216.58.209.142: bytes=32 time=56ms TTL=106
Reply from 216.58.209.142: bytes=32 time=51ms TTL=106
Reply from 216.58.209.142: bytes=32 time=256ms TTL=106

Ping statistics for 216.58.209.142:
    Packets: Sent = 13, Received = 13, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 256ms, Average = 93ms
Control-C
^C
```

سوال 4: دستور `tracert google.com` ، `tracert facebook.com` ، `tracert aut.ac.ir` را اجرا کنید.

آخرین آدرس IP که در خروجی هر سه دستور مشاهده میکنید و ارتباط آن ها با ورودی دستور `tracert` را مشخص کنید. به نظر شما چرا در خروجی `tracert facebook.com` در بعضی از گام ها به جای آدرس IP مسیر یاب ها، Request timeout قرار گرفته است؟ آخرین آدرس IP در خروجی مربوط به facebook چه ارتباطی با facebook دارد.

قسمت اول سوال:

اجرای دستور `tracert google.com` به صورت زیر میباشد:

```
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\VI R>tracert google.com

Tracing route to google.com [216.58.210.78]
over a maximum of 30 hops:
  0  *         *         *         Request timed out.
  1  *         *         *         Request timed out.
  2  *         *         *         Request timed out.
  3  95 ms     42 ms     131 ms    10.10.72.33
  4  79 ms     36 ms     41 ms     10.10.73.129
  5  79 ms     34 ms     *         10.10.73.33
  6  63 ms     35 ms     36 ms     10.10.69.65
  7  43 ms     21 ms     37 ms     10.10.69.98
  8  82 ms     19 ms     40 ms     10.0.70.245
  9  46 ms     42 ms     27 ms     10.0.178.14
 10  41 ms     17 ms     40 ms     10.0.178.1
 11  45 ms     43 ms     30 ms     10.176.68.180
 12  90 ms     35 ms     32 ms     10.176.68.131
 13  77 ms     34 ms     57 ms     10.0.14.91
 14  85 ms     36 ms     34 ms     10.0.14.90
 15  54 ms     34 ms     33 ms     10.202.4.156
 16  51 ms     28 ms     37 ms     10.21.111.10
 17  82 ms     36 ms     36 ms     10.21.0.11
 18  113 ms    66 ms     66 ms     213.202.4.172
 19  *         115 ms    83 ms     213.202.5.239
 20  149 ms    54 ms     58 ms     216.239.48.87
 21  89 ms     57 ms     56 ms     216.239.51.123
 22  105 ms    74 ms     55 ms     mct01s06-in-f14.1e100.net [216.58.210.78]

Trace complete.

C:\Users\VI R>
```

اجرای دستور `tracert facebook.com` به صورت زیر میباشد:

```
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\VI R>tracert facebook.com

Tracing route to facebook.com [10.10.34.36]
over a maximum of 30 hops:
  0  *         *         *         Request timed out.
  1  *         *         *         Request timed out.
  2  *         *         *         Request timed out.
  3  78 ms     *         *         10.10.72.37
  4  75 ms     34 ms     35 ms    10.10.73.133
  5  63 ms     41 ms     37 ms    10.10.73.37
  6  76 ms     31 ms     20 ms    10.10.69.65
  7  111 ms    21 ms     19 ms    10.10.69.98
  8  54 ms     24 ms     23 ms    10.0.70.245
  9  76 ms     25 ms     21 ms    10.0.178.14
 10  67 ms     25 ms     20 ms    10.0.178.1
 11  90 ms     22 ms     24 ms    10.176.68.180
 12  52 ms     34 ms     34 ms    10.176.68.131
 13  86 ms     34 ms     38 ms    10.0.14.91
 14  92 ms     48 ms     45 ms    10.0.14.90
 15  58 ms     31 ms     44 ms    10.202.4.156
 16  53 ms     36 ms     34 ms    10.21.111.10
 17  81 ms     33 ms     33 ms    10.21.211.10
 18  85 ms     33 ms     36 ms    10.202.4.76
 19  69 ms     30 ms     36 ms    10.201.146.3
 20  44 ms     34 ms     35 ms    185.57.202.229
 21  *         *         *         Request timed out.
 22  *         *         *         Request timed out.
 23  *         *         *         Request timed out.
 24  *         *         *         Request timed out.
 25  *         *         *         Request timed out.
 26  *         *         *         Request timed out.
 27  *         *         *         Request timed out.
 28  *         *         *         Request timed out.
 29  *         *         *         Request timed out.
 30  *         *         *         Request timed out.

Trace complete.

C:\Users\VI R>
```

اجرای دستور `tracert aut.ac.ir` به صورت زیر میباشد:

```
C:\Users\M R>tracert aut.ac.ir

Tracing route to aut.ac.ir [185.211.88.131]
over a maximum of 30 hops:

  1  *      *      *      Request timed out.
  2  *      *      *      Request timed out.
  3  105 ms  *      75 ms  10.10.72.37
  4  85 ms  37 ms  26 ms  10.10.73.133
  5  91 ms  34 ms  29 ms  10.10.73.37
  6  38 ms  *      *      10.10.69.65
  7  66 ms  22 ms  35 ms  10.10.69.98
  8  93 ms  35 ms  34 ms  10.0.70.245
  9  97 ms  35 ms  35 ms  10.0.178.14
 10  24 ms  26 ms  32 ms  10.0.178.1
 11  53 ms  32 ms  39 ms  10.176.68.180
 12  44 ms  28 ms  34 ms  10.176.68.131
 13  52 ms  35 ms  73 ms  10.201.202.253
 14  50 ms  82 ms  31 ms  212.16.72.66
 15  72 ms  23 ms  20 ms  185.211.88.131

Trace complete.

C:\Users\M R>
```

قسمت دوم سوال:

آخرین آدرس IP که در خروجی هر سه دستور میبینیم همان آدرس IP سایت و سرور آن میباشد.

قسمت سوم سوال:

Request timed out که به جای آدرس IP مسیریاب ها قرار گرفته میتواند علت های مختلفی داشته باشد:

- بسیاری از روترهای اینترنتی بسته های ping یا traceroute را به عمد کنار می گذارند ، اما این هیچ تاثیری در برنامه های استفاده کننده از این روترها ندارد. این روش ICMP Rate Limiting نام دارد و برای جلوگیری از تأثیر روترها در اثر حملات denial-of-service استفاده می شود. پیام Request timed out در ابتدای traceroute بسیار رایج است و می توان آن را نادیده گرفت. این معمولاً دستگاهی است که به درخواست های ICMP یا ردیابی پاسخ نمی دهد.
- میتواند به خاطر دلایل امنیتی باشد . firewall مقصد یا سایر دستگاه های امنیتی میتوانند درخواست را block کنند .
- ممکن است در مسیر بازگشت از سیستم مقصد مشکلی وجود داشته باشد. round trip time مدت زمانی را اندازه میگیرد که یک بسته برای انتقال از سیستم ما به سیستم مقصد و بازگشت نیاز دارد. مسیر رفت و مسیر بازگشت اغلب باهم تفاوت دارند. اگر در مسیر بازگشت مشکلی وجود داشته باشد ، ممکن است در خروجی فرمان مشخص نباشد.
- ممکن است در سیستم ما یا سیستم مقصد مشکل اتصال وجود داشته باشد و یا شبکه مقصد در دسترس نباشد.

- کمبود مقدار TTL که به صورت پیشفرض مقدار آن 64 عدد است و برای بررسی هر شبکه ای از هر نقطه از جهان کاملاً کافی است.

قسمت چهارم سوال:

این سایت چون فیلتر میباشد از یک مرحله ای به بعد Request timed out میدهد. حال میتوانیم به جای آن یکی از آی پی های facebook (مثلاً 157.240.1.35) را trace کنیم که خواهیم داشت:

```
C:\Users\VM R>tracert 157.240.1.35

Tracing route to edge-star-mini-shv-01-lht6.facebook.com [157.240.1.35]
over a maximum of 30 hops:
  0  *      *      *      Request timed out.
  1  *      *      *      Request timed out.
  2  *      *      *      Request timed out.
  3  *      125 ms *      10.10.72.37
  4  117 ms 32 ms 37 ms 10.10.73.133
  5  40 ms 41 ms 44 ms 10.10.72.37
  6  *      *      *      Request timed out.
  7  46 ms 35 ms 46 ms 10.10.69.98
  8  39 ms 38 ms 33 ms 10.0.70.245
  9  86 ms 35 ms 38 ms 10.0.178.0
 10  79 ms 33 ms 36 ms 10.0.178.1
 11  84 ms 44 ms 20 ms 10.176.68.180
 12  69 ms 37 ms 28 ms 10.176.68.131
 13  36 ms 77 ms 37 ms 10.0.14.91
 14  41 ms 34 ms 78 ms 10.0.14.90
 15  47 ms 36 ms 30 ms 10.202.4.156
 16  51 ms 37 ms 36 ms 10.21.111.10
 17  109 ms 120 ms 134 ms 193.251.252.153
 18  99 ms 90 ms 109 ms et-0-1-3-0-fftr7.frankfurt.opentransit.net [193.251.151.189]
 19  103 ms 106 ms 110 ms ae7.cr1-fra2.ip4.gtt.net [77.67.82.93]
 20  254 ms 121 ms 138 ms ae21.cr10-lon1.ip4.gtt.net [89.149.139.5]
 21  118 ms 129 ms 123 ms ip4.gtt.net [77.67.99.254]
 22  121 ms 162 ms 128 ms po141.asw02.lhr1.tfbnw.net [129.134.45.58]
 23  124 ms 121 ms 117 ms po564.psw04.lhr6.tfbnw.net [129.134.45.47]
 24  151 ms 116 ms 118 ms 173.252.67.191
 25  127 ms 109 ms 117 ms edge-star-mini-shv-01-lht6.facebook.com [157.240.1.35]

Trace complete.
```

همانطور که مشاهده میشود در اینجا Trace کامل انجام شد و مانند بقیه آخرین آدرس IP همان IP مربوط به سایت facebook.com و سرور آن میباشد.

یکی از روش های فیلترینگ DNS Blocking میباشد که در آن تبدیل اسم سایت به آدرس IP به درستی انجام نمیشود .

سوال 5: با استفاده از **ipconfig** و **ping plotter** آدرس فیزیکی دروازه شبکه و یکی از دوستان خود را پیدا کنید.

ابتدا به کمک **ipconfig** باید آدرس IP برای **Default Gateway** را بیابیم. پس ابتدا در **cmd** دستور زیر را مینویسیم:

Ipconfig /all

اطلاعاتی را نمایش خواهد داد که با جست و جو میتوان مورد ذکر شده را یافت:

```
Command Prompt
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 02-03-8C-4F-4E-87
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
Physical Address. . . . . : F8-03-8C-4F-4E-87
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2074:9514:ad7e:2987%20(Preferred)
IPv4 Address. . . . . : 192.168.43.175(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, March 8, 2021 2:57:01 PM
Lease Expires . . . . . : Monday, March 8, 2021 9:29:26 PM
Default Gateway . . . . . : 192.168.43.1
DHCP Server . . . . . : 192.168.43.1
DHCPv6 IAID . . . . . : 116392844
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-C5-00-D7-2C-4D-54-39-7A-32
DNS Servers . . . . . : 192.168.43.1
NetBIOS over Tcpip. . . . . : Enabled

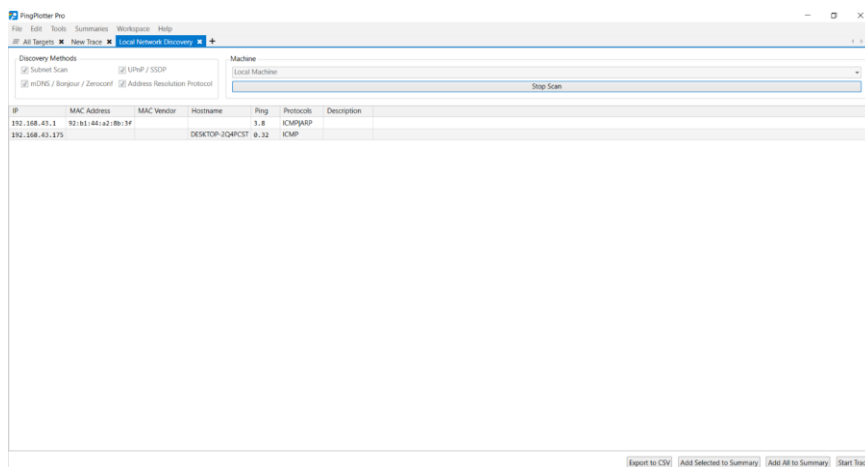
Ethernet adapter Bluetooth Network Connection:

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

باتوجه به بالا میتوان گفت که آدرس **Gateway** برابر است با: **192.168.43.1**

حال در نرم افزار **ping plotter** به قسمت **tools** رفته و سپس **local network discovery** را انتخاب میکنیم. با زدن **start scan** کار اسکن را شروع میکنم.

حال در نهایت در نتایج داده شده در ستون **IP** به دنبال آدرس **Default Gateway** (که مرحله قبل پیدا کردیم) میگردیم و در ستون مقابل آن میتوان آدرس فیزیکی یا همان **MAC Address** را میتوان یافت.



بنابراین همانطور که از تصویر پیدا هست MAC Address مربوط دروازه شبکه میشود:

92:b1:44:a2:8b:3f