به نام خدا

گروه ۳

فرشید نوشی ۹۸۳۱۰۶۸

تاریخ

۹ فروردین ۱۴۰۱ ساعت ۱۶:۳۰-۱۹:۰۰

سوال اول

با توجه به توضیحات شکل زیر، این سوئیچ برای سایز است و با استفاده از آن میتوان سایز بافر را تغییر داد و دیتای با حجم مشخص شده ی بعد از l را میفرستد.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.613]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Farshid726> 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.

C:\Users\Farshid726>
```

با این توضیح به طور پیش فرض هنگامی که دستور ping google.com را استفاده میکنیم، عبارت bytes=32 در پیغام ها به این معنی است که حجم ارسالی یا در واقع buffer size برابر با ۳۲ بایت میباشد.

```
C:\Users\Farshid726>ping google.com

Pinging google.com [142.250.185.46] with 32 bytes of data:
Reply from 142.250.185.46: bytes=32 time=131ms TTL=105
Reply from 142.250.185.46: bytes=32 time=33ms TTL=105
Reply from 142.250.185.46: bytes=32 time=65ms TTL=105
Reply from 142.250.185.46: bytes=32 time=80ms TTL=105

Ping statistics for 142.250.185.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 131ms, Average = 77ms
```

متوجه میشویم که با استفاده از پارامتر l- میتوانیم این اندازه را تغییر بدهیم و مقدار دلخواه خودمان را به جایش قرار بدهیم.
به طور مثال با تغییر دادن buffer size به ۱۶ بایت به مانند زیر خروجی خواهیم گرفت.

```
C:\Users\Farshid726>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=153ms TTL=51
Reply from 216.58.209.142: bytes=16 time=116ms TTL=51
Reply from 216.58.209.142: bytes=16 time=115ms TTL=51
Reply from 216.58.209.142: bytes=16 time=116ms TTL=51

Ping statistics for 216.58.209.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 115ms, Maximum = 153ms, Average = 125ms
```

البته ما نمیتوانیم هر مقداری را به عنوان پارامتر l- قرار بدهیم و عدد ورودی مان باید حتما عددی بین ۰-۶۵۵۰۰ باشد.
با دادن عددی خارج از این بازه خطا دریافت خواهیم کرد.

سوال سوم

با توجه به خروجی های دستور گرفتن راهنما ?- ping در اولین option که به ما ارائه داده است این دستور آمده است.
پاسخ این سوال استفاده از option اول یعنی t- در دستور pingمان میباشد.
به طور مثال با پینگ کردن سایت گوگل به این روش خواهیم داشت:

```
C:\Users\Farshid726>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=134ms TTL=51
Reply from 216.58.209.142: bytes=32 time=147ms TTL=51
Reply from 216.58.209.142: bytes=32 time=130ms TTL=51
Reply from 216.58.209.142: bytes=32 time=116ms TTL=51
Reply from 216.58.209.142: bytes=32 time=145ms TTL=51
Reply from 216.58.209.142: bytes=32 time=119ms TTL=51
Reply from 216.58.209.142: bytes=32 time=121ms TTL=51
Reply from 216.58.209.142: bytes=32 time=117ms TTL=51
Reply from 216.58.209.142: bytes=32 time=118ms TTL=51
Reply from 216.58.209.142: bytes=32 time=146ms TTL=51
Reply from 216.58.209.142: bytes=32 time=113ms TTL=51
Reply from 216.58.209.142: bytes=32 time=116ms TTL=51
Reply from 216.58.209.142: bytes=32 time=138ms TTL=51
Reply from 216.58.209.142: bytes=32 time=114ms TTL=51
Reply from 216.58.209.142: bytes=32 time=122ms TTL=51
Reply from 216.58.209.142: bytes=32 time=116ms TTL=51
Reply from 216.58.209.142: bytes=32 time=115ms TTL=51
Reply from 216.58.209.142: bytes=32 time=130ms TTL=51
Reply from 216.58.209.142: bytes=32 time=113ms TTL=51
Reply from 216.58.209.142: bytes=32 time=130ms TTL=51
Reply from 216.58.209.142: bytes=32 time=113ms TTL=51
Reply from 216.58.209.142: bytes=32 time=127ms TTL=51
Reply from 216.58.209.142: bytes=32 time=122ms TTL=51
Reply from 216.58.209.142: bytes=32 time=118ms TTL=51
Reply from 216.58.209.142: bytes=32 time=147ms TTL=51
Reply from 216.58.209.142: bytes=32 time=130ms TTL=51
Reply from 216.58.209.142: bytes=32 time=126ms TTL=51
Reply from 216.58.209.142: bytes=32 time=174ms TTL=51
Reply from 216.58.209.142: bytes=32 time=125ms TTL=51
Reply from 216.58.209.142: bytes=32 time=160ms TTL=51
Reply from 216.58.209.142: bytes=32 time=128ms TTL=51
Reply from 216.58.209.142: bytes=32 time=205ms TTL=51
Reply from 216.58.209.142: bytes=32 time=128ms TTL=51
Reply from 216.58.209.142: bytes=32 time=119ms TTL=51
Reply from 216.58.209.142: bytes=32 time=118ms TTL=51
Reply from 216.58.209.142: bytes=32 time=115ms TTL=51
Reply from 216.58.209.142: bytes=32 time=139ms TTL=51
Reply from 216.58.209.142: bytes=32 time=113ms TTL=51
Reply from 216.58.209.142: bytes=32 time=117ms TTL=51
Reply from 216.58.209.142: bytes=32 time=120ms TTL=51
```

برای گرفتن آمار و اعداد ارقام مانند میانگین زمان رفت و برگشت و ... را پس از تعداد مشخصی گام بدهد باید از control-break استفاده بکنیم
برای توقف اجرا نیز میتوان از control+c استفاده کرد و پس از توقف به ما آمار و ارقام را نشان میدهد.

```
C:\Users\Farshid726>ping google.com -t

Pinging google.com [142.250.185.46] with 32 bytes of data:
Reply from 142.250.185.46: bytes=32 time=31ms TTL=105
Reply from 142.250.185.46: bytes=32 time=50ms TTL=105
Reply from 142.250.185.46: bytes=32 time=233ms TTL=105

Ping statistics for 142.250.185.46:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 233ms, Average = 104ms
Control-Break
Reply from 142.250.185.46: bytes=32 time=95ms TTL=105
Reply from 142.250.185.46: bytes=32 time=49ms TTL=105
Reply from 142.250.185.46: bytes=32 time=65ms TTL=105
Reply from 142.250.185.46: bytes=32 time=35ms TTL=105
Reply from 142.250.185.46: bytes=32 time=46ms TTL=105
Reply from 142.250.185.46: bytes=32 time=35ms TTL=105
Reply from 142.250.185.46: bytes=32 time=35ms TTL=105

Ping statistics for 142.250.185.46:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 233ms, Average = 67ms
Control-Break
Reply from 142.250.185.46: bytes=32 time=36ms TTL=105
Reply from 142.250.185.46: bytes=32 time=37ms TTL=105

Ping statistics for 142.250.185.46:
    Packets: Sent = 12, Received = 12, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 233ms, Average = 62ms
Control-C
```

سوال چهارم

اجرای دستور برای aut.ac.ir, facebook.com, google.com به ترتیب با خروجی های زیر مواجه شدند.

```
C:\Users\Farshid726>tracert google.com

Tracing route to google.com [142.250.185.46]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.0.1
  2    13 ms     5 ms     7 ms  85.15.21.65
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9    13 ms     6 ms     6 ms  10.10.53.217
 10    17 ms    19 ms     6 ms  10.21.212.10
 11    35 ms    10 ms    13 ms  10.21.21.10
 12    32 ms    42 ms    46 ms  134.0.220.186
 13    44 ms    34 ms    42 ms  213.202.5.239
 14    37 ms    30 ms    34 ms  216.239.48.87
 15    35 ms    32 ms    42 ms  142.251.48.1
 16    33 ms    34 ms    34 ms  142.250.185.46

Trace complete.
```

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.22000.613]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Farshid726>tracert facebook.com

Tracing route to facebook.com [10.10.34.35]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.0.1
  2     8 ms     6 ms     6 ms  85.15.21.65
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9    13 ms    10 ms     7 ms  10.201.177.157
 10    12 ms     5 ms     7 ms  10.21.212.10
 11    11 ms     9 ms     6 ms  10.21.212.10
 12     9 ms    10 ms     6 ms  10.202.4.76
 13    11 ms    10 ms     7 ms  10.201.146.3
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 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\Farshid726>tracert aut.ac.ir

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

  1     2 ms    <1 ms    <1 ms  192.168.0.1
  2    51 ms    10 ms     5 ms  85.15.21.65
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6    59 ms    18 ms    10 ms  85.15.4.98
  7     5 ms    11 ms     9 ms  212.16.72.66
  8    10 ms     5 ms    27 ms  185.211.88.131

Trace complete.
```

آخرین آدرس IP که در خروجی هر سه دستور tracert میبینیم در واقع همان آدرس IP سایت و سرور آن است در واقع Request timed out که به جای IP مسیریاب ها برخی جاها میبینیم دلایل مختلفی میتواند داشته باشد:

- بسیاری از روترهای اینترنتی در واقع بسته های ping, tracert را به عمد برای مسائل امنیتی خودشان کنار میگذارند اما این اتفاق تاثیری بر برنامه های استفاده کننده از این روتر ها نخواهد داشت. اسم این روش ICMP Rate Limiting میباشد و برای جلوگیری از اثر حمله های denial of service میباشد. پیام request timed out در ابتدای traceroute رایج است و میتواند نادیده گرفته شود و معمولا مال دستگاهی است که به درخواست های ردیابی(ICMP) پاسخ نمیدهد.
- میتواند به دلایل امنیتی باشد. Firewall مقصد یا سایر دستگاه های امنیتی میتوانند درخواست را بلاک بکنند.
- امکان مشکل در مسیر برگشت از سیستم مقصد نیز وجود دارد. RTT مدت زمانی را اندازه میگیرد که یک بسته برای رفت و برگشت از سیستم ما به سیستم مقصد نیاز دارد و مصرف میکند. در اصل مسیر رفت و برگشت با یکدیگر اغلب تفاوت دارند و اگر در مسیر برگشت مشکلی پیش بیاید ممکن است در خروجی فرمان مشخص نباشد.
- ممکن است در سیستم ما یا سیستم مقصد مشکل اتصال داشته باشیم و یا شبکه ی مقصد در دسترس نباشد.
- کمبود مقدار TTL که برای بررسی هر شبکه ای از هر نقطه از جهان کافی است و مقدار پیش فرض آن برابر با 64 عدد است.

سایت facebook.com چون فیلتر میباشد از یک مرحله به بعد دچار request timed out میشود. میتوانیم به جای facebook از آدرس یکی از آی پی های facebook را trace بکنیم.

```
C:\Users\Farshid726>tracert 157.240.16.35

Tracing route to 157.240.16.35 over a maximum of 30 hops

  1     1 ms     2 ms     3 ms  192.168.0.1
  2     8 ms     6 ms     7 ms  85.15.21.65
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     7 ms    10 ms     7 ms  10.10.53.225
  9     6 ms    38 ms     6 ms  10.21.212.20
 10    36 ms    15 ms    35 ms  85.132.90.153
 11     *        *        *     Request timed out.
 12    63 ms    63 ms    63 ms  157.240.66.0
 13    61 ms    59 ms    75 ms  157.240.47.152
 14    98 ms    94 ms    98 ms  129.134.40.58
 15   131 ms   113 ms   111 ms  129.134.45.103
 16   211 ms   210 ms   202 ms  173.252.66.141
 17   214 ms   210 ms   214 ms  31.13.24.41
 18   209 ms   234 ms   210 ms  157.240.35.65
 19   210 ms   206 ms   225 ms  31.13.29.205
 20   203 ms   207 ms   207 ms  157.240.38.103
 21   202 ms   203 ms   272 ms  157.240.16.35

Trace complete.
```

مشاهده میشود که در اینجا tracert به طور کامل انجام شد و آخرین IP Address مربوط به سایت facebook.com و سرور آن میباشد.
یکی از روش های فیلترینگ DNS Blocking میباشد که در آن مرحله ی تبدیل اسم سایت به آدرس IP به درستی انجام نمیشود.

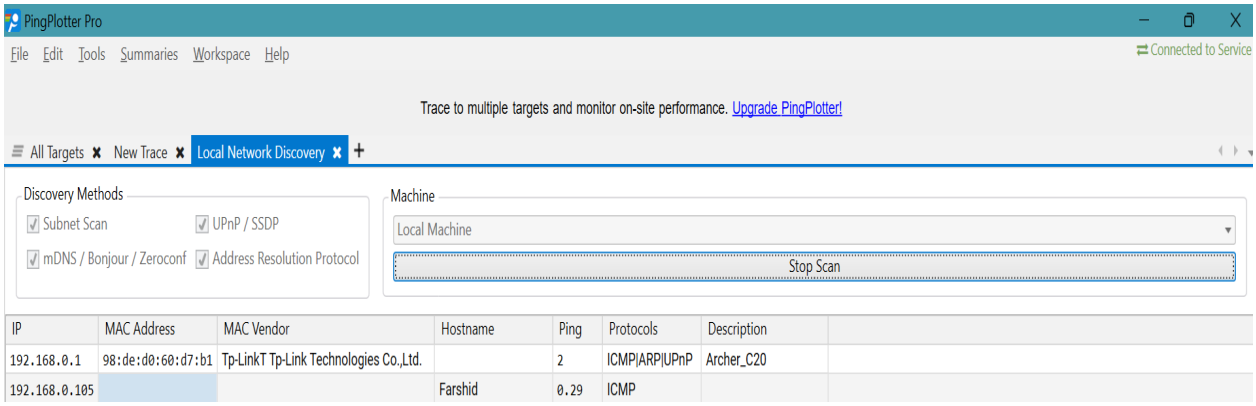
سوال پنجم

برای این قسمت ابتدا باید آدرس IP مربوط به Default gateway را پیدا بکنیم که برای اینکار میتوانیم از دستور ipconfig /all استفاده بکنیم. این دستور اطلاعات زیادی را برای ما به نمایش میگذارد که در داخل آنان میتوان مقدار default gateway را یافت که در تصویر زیر نیز آمده است.

```
Administrator: Command Prompt
Wireless LAN adapter Local Area Connection* 5:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #10
   Physical Address. . . . . . . . . : F4-D1-08-8D-FD-70
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 6:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #11
   Physical Address. . . . . . . . . : F6-D1-08-8D-FD-6F
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F4-D1-08-8D-FD-6F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6d82:d86c:7e36:49dc%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.105(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, April 23, 2022 5:00:23 PM
   Lease Expires . . . . . . . . . . : Saturday, April 23, 2022 9:12:34 PM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 452251912
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-16-B4-A4-F4-D1-08-8D-FD-6F
   DNS Servers . . . . . . . . . . . : 192.168.0.1
                                       0.0.0.0
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : F4-D1-08-8D-FD-73
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

با توجه به تصویر بالا میتوان گفت که آدرس gateway برابر است با 192.168.0.1

در نرم افزار ping plotter به قسمت tools میرویم و local network discovery را انتخاب میکنیم و start scan را میزنیم تا کار اسکن شروع بشود در نتایجی که در صفحه می آیند در ستون IP به دنبال default gateway خودمان میگردیم که در قسمت قبلی پیدایش کردیم و در ستون کناری آن آدرس فیزیکی یا همان MAC Address موجود است.



که با توجه به تصویر مقدار MAC Address برابر است با:

98:de:d0:60:d7:b1