

به نام خدا



ابزار های مدیریت شبکه های کامپیوتری

فصل یک، آزمایش دو



محمد جواد زندیه ۹۸۳۱۰۳۲

۱ مهر ۱۴۰۱

دانشگاه صنعتی امیرکبیر، دانشکده مهندسی کامپیوتر، آزمایشگاه شبکه های کامپیوتری

سوال ۱: به نظر شما سوییچ ۱- چیست و چگونه کار می کند؟

برای بررسی ارتباط با سیستم های دیگر از دستور ping استفاده می کنیم. با استفاده از سوییچ ۱- میتوان تعداد بایت داده مورد نظر که قصد داریم با سیستم دیگر رد و بدل کنیم را مشخص کرد و ارزیابی ارتباط را با مقادیر مختلف داده انجام داد(مقدار پیش فرض داده ای که رد و بدل میشود ۳۲ بایت است)

در واقع سایز بافر را میتوان با آن به اندازه های دلخواه معین کرد.

```
C:\Users\Javad\Desktop\cmdr
λ ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=566ms TTL=103
Reply from 8.8.8.8: bytes=32 time=497ms TTL=103
Reply from 8.8.8.8: bytes=32 time=397ms TTL=103
Reply from 8.8.8.8: bytes=32 time=631ms TTL=103

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 397ms, Maximum = 631ms, Average = 522ms
```

شکل (۱) ping با میزان پیش فرض داده

```
C:\Users\Javad\Desktop\cmdr
λ ping 8.8.8.8 -l 64

Pinging 8.8.8.8 with 64 bytes of data:
Reply from 8.8.8.8: bytes=64 time=397ms TTL=103
Reply from 8.8.8.8: bytes=64 time=307ms TTL=103
Reply from 8.8.8.8: bytes=64 time=467ms TTL=103
Reply from 8.8.8.8: bytes=64 time=401ms TTL=103

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 307ms, Maximum = 467ms, Average = 393ms
```

شکل (۲) ping با ۶۴ بایت داده

سوال ۲: با استفاده از CMD دستورات زیر را اجرا کنید:

Ping aut.ac.ir

Ping google.com

چه تفاوتی بین میانگین زمان رفت و برگشت بین این دو آدرس وجود دارد؟ به نظر شما این اختلاف از کجا ناشی می شود؟ دستور ping dolat.ir را نیز اجرا کنید و میانگین زمان رفت و برگشت را مقایسه کنید.

در حال حاضر به دلیل نبودن در داخل دانشگاه میانگین زمان رفت و برگشت برای هر دو آدرس تقریباً مشابه است، اما اگر در داخل دانشگاه این آزمایش را انجام میدادیم مشاهده میشد که میانگین زمان رفت و برگشت برای aut.ac.ir کمتر از google.com است، زیرا به سرور نزدیک تر میبودیم و زمان رفت و برگشت کمتر میشد.

تفاوت دیگر در زمان TTL یا Time To Live است که بین این دو سرور متفاوت است.

```
C:\Users\Javad\Desktop\cmdr
λ ping aut.ac.ir

Pinging aut.ac.ir [185.211.88.131] with 32 bytes of data:
Reply from 185.211.88.131: bytes=32 time=293ms TTL=54
Reply from 185.211.88.131: bytes=32 time=433ms TTL=54
Reply from 185.211.88.131: bytes=32 time=381ms TTL=54
Reply from 185.211.88.131: bytes=32 time=278ms TTL=54

Ping statistics for 185.211.88.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 278ms, Maximum = 433ms, Average = 346ms

C:\Users\Javad\Desktop\cmdr
λ ping google.com

Pinging google.com [172.217.20.78] with 32 bytes of data:
Reply from 172.217.20.78: bytes=32 time=538ms TTL=107
Reply from 172.217.20.78: bytes=32 time=460ms TTL=107
Reply from 172.217.20.78: bytes=32 time=339ms TTL=107
Reply from 172.217.20.78: bytes=32 time=299ms TTL=107

Ping statistics for 172.217.20.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 299ms, Maximum = 538ms, Average = 409ms
```

شکل (۳) مقایسه ping بین aut.ac.ir و google.com

به دلیل مسائل امنیتی و جلوگیری از حملات، ping مربوط به dolat.ir بسته شده است و request timed out رخ میدهد و ۱۰۰ درصد packet loss رخ میدهد.

```
C:\Users\Javad\Desktop\cmdr
λ ping dolat.ir

Pinging dolat.ir [194.225.148.177] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 194.225.148.177:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

شکل (۴) ping به dolat.ir

سوال ۳: همانطور که مشاهده کردید ping بعد از ارسال و دریافت ۴ پیغام قطع می شود. دستوری پیدا کنید که ارسال و دریافت پیغام را بدون توقف ادامه دهد.

با استفاده از سوییچ -t مربوط به دستور ping میتوان این کار را انجام داد. برای متوقف کردن ارسال و دریافت میتوان از دستور ctrl + c استفاده کرد و با انجام این کار در انتها کمینه و بیشینه و میانگین زمان رفت و برگشت و درصد loss را هم نمایش میدهد.

```
C:\Users\Javad\Desktop\cmdr
λ ping -t 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=60ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103
Reply from 8.8.8.8: bytes=32 time=56ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103
Reply from 8.8.8.8: bytes=32 time=56ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103
Reply from 8.8.8.8: bytes=32 time=55ms TTL=103
Reply from 8.8.8.8: bytes=32 time=58ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103
Reply from 8.8.8.8: bytes=32 time=65ms TTL=103
Reply from 8.8.8.8: bytes=32 time=59ms TTL=103
Reply from 8.8.8.8: bytes=32 time=59ms TTL=103
Reply from 8.8.8.8: bytes=32 time=63ms TTL=103
Reply from 8.8.8.8: bytes=32 time=56ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103
Reply from 8.8.8.8: bytes=32 time=58ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103
Reply from 8.8.8.8: bytes=32 time=60ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103
Reply from 8.8.8.8: bytes=32 time=56ms TTL=103
Reply from 8.8.8.8: bytes=32 time=57ms TTL=103

Ping statistics for 8.8.8.8:
    Packets: Sent = 25, Received = 25, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 55ms, Maximum = 65ms, Average = 57ms
Control-C
^C
```

شکل (۵) استفاده از دستور ping -t

سوال ۴: دستور tracert google.com, tracert facebook.com و tracert aut.ac.ir را اجرا کنید. آخرین آدرس IP که در خروجی هر سه دستور مشاهده می کنید و ارتباط آنها 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، request timed out قرار گرفته است؟ آخرین آدرس IP در خروجی مربوط به facebook چه ارتباطی با facebook دارد.

آخرین آدرس IP در خروجی هر دستور برابر با آدرس IP همان host ای است که مسیر پیغام تا آن را پیگیری کرده ایم.

در برخی از گام های tracert facebook.com به این علت request timed out مشاهده می کنیم که آن مسیر یاب ها ping خود را به علت مسائل امنیتی بسته اند و یا شاید در شبکه مشکلی پیش آمده است.

توجه: بدون استفاده از فیلتر شکن برای facebook دائما request timed out میخوریم، پس برای این امر از فیلتر شکن استفاده شده است.

```
C:\Users\Javad\Desktop\cmdr
λ tracert google.com

Tracing route to google.com [142.250.187.110]
over a maximum of 30 hops:

  1  2 ms  1 ms  2 ms  192.168.61.20
  2  *    *    *    Request timed out.
  3  97 ms 28 ms 41 ms 10.176.211.65
  4 134 ms 37 ms 66 ms 10.196.212.16
  5  *    *    *    Request timed out.
  6  44 ms 43 ms 41 ms 10.196.212.65
  7  *    *    *    Request timed out.
  8 108 ms 45 ms 39 ms 10.136.131.142
  9  85 ms 70 ms 45 ms 10.136.135.130
 10  98 ms 45 ms 56 ms 10.21.249.50
 11 118 ms 57 ms 55 ms 85.132.90.129
 12  *    *    *    Request timed out.
 13 207 ms 140 ms 132 ms 72.14.212.229
 14 193 ms 138 ms 124 ms 108.170.251.208
 15 213 ms 129 ms 135 ms 108.170.226.3
 16 133 ms 133 ms 143 ms 142.250.210.151
 17 222 ms 207 ms 163 ms 108.170.250.161
 18 166 ms 146 ms 132 ms 142.251.52.81
 19 135 ms 142 ms 199 ms sof02s44-in-f14.1e100.net [142.250.187.110]

Trace complete.
```

شکل (۶) tracert google.com

```
C:\Users\Javad\Desktop\cmdr
λ tracert aut.ac.ir

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

  1  1 ms  1 ms  6 ms  192.168.61.20
  2  *    *    *    Request timed out.
  3  35 ms 37 ms 34 ms 10.176.211.65
  4  44 ms 35 ms 29 ms 10.196.212.6
  5  *    *    *    Request timed out.
  6  36 ms 49 ms 43 ms 10.196.212.65
  7  *    *    *    Request timed out.
  8  46 ms 39 ms 42 ms 10.136.131.142
  9 121 ms 46 ms 37 ms 10.196.119.1
 10  59 ms 41 ms 41 ms 10.201.203.65
 11  66 ms 61 ms 56 ms 212.16.72.66
 12  55 ms 38 ms 56 ms 185.211.88.131

Trace complete.
```

شکل (۷) tracert aut.ac.ir

```

C:\Users\Javad\Desktop\cmdr
λ tracert -h 50 facebook.com

Tracing route to facebook.com [31.13.80.36]
over a maximum of 50 hops:

  1  240 ms  253 ms  236 ms  10.125.178.1
  2  289 ms  239 ms  245 ms  198.8.85.253
  3  292 ms  249 ms  230 ms  199.229.249.2
  4  *        *        *        Request timed out.
  5  241 ms  235 ms  267 ms  be2089.ccr21.ymq01.atlas.cogentco.com [154.54.45.113]
  6  325 ms  242 ms  249 ms  be3259.ccr31.yyz02.atlas.cogentco.com [154.54.41.205]
  7  249 ms  255 ms  251 ms  38.88.241.26
  8  249 ms  238 ms  249 ms  po103.psw04.yyz1.tfbnw.net [204.15.23.245]
  9  245 ms  238 ms  265 ms  157.240.38.231
 10  243 ms  238 ms  258 ms  edge-star-mini-shv-01-yyz1.facebook.com [31.13.80.36]

Trace complete.

```

شکل (۸) tracert facebook.com

سوال ۵: با استفاده از ipconfig و ping plotter و آدرس فیزیکی دروازه شبکه و یکی از دوستان خود را پیدا کنید.

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Ralink RT3290 802.11bgn Wi-Fi Adapter
Physical Address. . . . . : 00-71-CC-2F-8B-55
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::7048:32ef:b10f:f518%4(Preferred)
IPv4 Address. . . . . : 192.168.61.76(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, March 21, 2022 12:34:13 PM
Lease Expires . . . . . : Monday, March 21, 2022 1:34:12 PM
Default Gateway . . . . . : 192.168.61.20
DHCP Server . . . . . : 192.168.61.20
DHCPv6 IAID . . . . . : 67137996
DHCPv6 Client DUID. . . . . : 00-01-00-01-26-BF-5D-52-C4-34-6B-04-53-A3
DNS Servers . . . . . : 192.168.61.20
NetBIOS over Tcpip. . . . . : Enabled

```

شکل (۹) بدست آوردن آدرس دروازه شبکه توسط ipconfig

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Ralink RT3290 802.11bgn Wi-Fi Adapter
Physical Address. . . . . : 00-71-CC-2F-8B-55
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::7048:32ef:b10f:f518%4(Preferred)
IPv4 Address. . . . . : 192.168.61.76(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, March 21, 2022 12:34:13 PM
Lease Expires . . . . . : Monday, March 21, 2022 1:34:12 PM
Default Gateway . . . . . : 192.168.61.20
DHCP Server . . . . . : 192.168.61.20
DHCPv6 IAID . . . . . : 67137996
DHCPv6 Client DUID. . . . . : 00-01-00-01-26-BF-5D-52-C4-34-6B-04-53-A3
DNS Servers . . . . . : 192.168.61.20
NetBIOS over Tcpip. . . . . : Enabled

```

شکل (۱۰) بدست آوردن آدرس فیزیکی شبکه توسط ipconfig

توسط دستور ipconfig متوجه شدیم که آدرس IP مربوط به default gateway برابر با ۱۹۲.۱۶۸.۶۱.۲۰ است، پس از روی آن و با کمک ping plotter هم میتوان MAC Address مربوط به default gateway را بدست آورد.

The screenshot shows the PingPlotter Pro application window. The 'Local Network Discovery' tab is active. Under 'Discovery Methods', four options are checked: Subnet Scan, UPnP / SSDP, mDNS / Bonjour / Zeroconf, and Address Resolution Protocol. The 'Machine' dropdown is set to 'Local Machine'. Below these settings is a table displaying the results of the network discovery.

IP	MAC Address	MAC Vendor	Hostname	Ping	Protocols	Description
192.168.61.20	02:42:95:be:32:0e			10	ICMP ARP	
192.168.61.76			DESKTOP-9SJ4G2F	0.25	ICMP	
192.168.110.254	00:50:56:fd:b8:45	VMware VMWare, Inc.			ARP	
192.168.88.254	00:50:56:fb:d6:c5	VMware VMWare, Inc.			ARP	

شکل (۱۱) بدست آوردن MAC Address مربوط به default gateway

MAC Address مربوط به default gateway برابر است با 02:42:95:be:32:0e