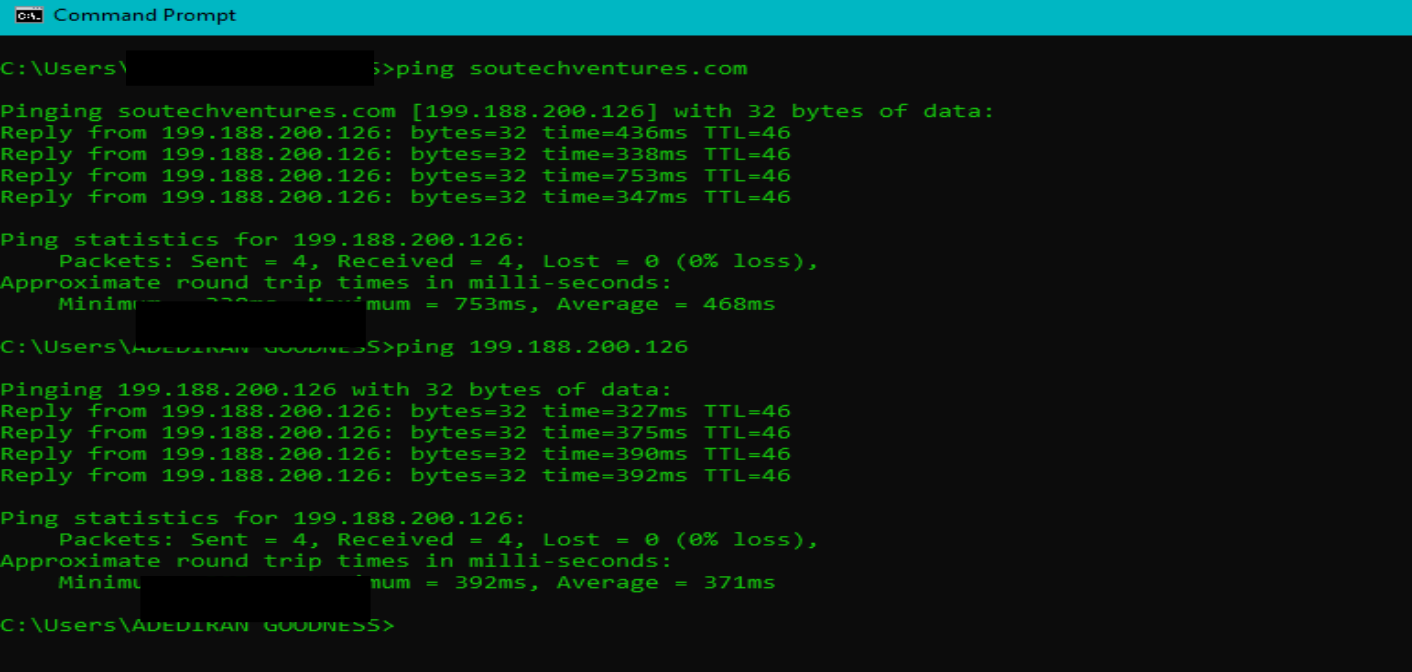


Gathering information using Windows Command Line Utilities

Case Study: Consider a network where you have access to a Windows PC connected to the Internet. Using Windows-based tools, let's gather some information about the target. You can assume any target domain or IP address, in our case, we are using **example.com** as a target.

Open Windows Command Line (cmd) from Windows PC. Enter the command “ **Ping example.com** ” to ping.



```
Command Prompt
C:\Users\>ping soutechventures.com

Pinging soutechventures.com [199.188.200.126] with 32 bytes of data:
Reply from 199.188.200.126: bytes=32 time=436ms TTL=46
Reply from 199.188.200.126: bytes=32 time=338ms TTL=46
Reply from 199.188.200.126: bytes=32 time=753ms TTL=46
Reply from 199.188.200.126: bytes=32 time=347ms TTL=46

Ping statistics for 199.188.200.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 338ms, Maximum = 753ms, Average = 468ms

C:\Users\ADEDIRAN GOODNESS>ping 199.188.200.126

Pinging 199.188.200.126 with 32 bytes of data:
Reply from 199.188.200.126: bytes=32 time=327ms TTL=46
Reply from 199.188.200.126: bytes=32 time=375ms TTL=46
Reply from 199.188.200.126: bytes=32 time=390ms TTL=46
Reply from 199.188.200.126: bytes=32 time=392ms TTL=46

Ping statistics for 199.188.200.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 327ms, Maximum = 392ms, Average = 371ms

C:\Users\ADEDIRAN GOODNESS>
```

From the output, you can observe and extract the following information:

1. Example.com is live
2. IP address of example.com.
3. Round Trip Time
4. TTL value
5. Packet loss statistics

Now, Enter the command “**Ping example.com -f -l 1500**” to check the value of fragmentation

```
Command Prompt
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 327ms, Maximum = 392ms, Average = 371ms

C:\Users\ >ping soutechventures.com -f -l 1500
Bad option -l.

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\ >ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
```

```
Command Prompt
C:\Users\ >Tracert soutechventures.com

Tracing route to soutechventures.com [199.188.200.126]
over a maximum of 30 hops:

  0  2 ms   1 ms   1 ms  homerouter.cpe [192.168.8.1]
  1  *      *      *      Request timed out.
  2  215 ms 271 ms 101 ms 10.6.1.1
  3  395 ms 141 ms 302 ms 10.6.1.37
  4  508 ms 214 ms 197 ms 129.56.0.67
  5  512 ms 816 ms 405 ms te0-1-0-5-2.ccr22.lon01.atlas.cogentco.com [149.14.251.81]
  6  337 ms 312 ms 386 ms be2870.ccr41.lon13.atlas.cogentco.com [154.54.58.173]
  7  628 ms 160 ms 246 ms be2791.ccr21.lon02.atlas.cogentco.com [154.54.56.78]
  8  361 ms 170 ms 211 ms ae-33.r02.londen03.uk.bb.gin.ntt.net [129.250.66.145]
  9  160 ms 159 ms 165 ms ae-11.r21.londen12.uk.bb.gin.ntt.net [129.250.4.85]
 10  386 ms 600 ms 303 ms ae-3.r24.asbnva02.us.bb.gin.ntt.net [129.250.2.111]
 11  972 ms 640 ms *      ae-2.r24.snjsca04.us.bb.gin.ntt.net [129.250.6.237]
 12 1012 ms 450 ms 301 ms ae-0.a02.snjsca04.us.bb.gin.ntt.net [129.250.2.3]
 13  468 ms 875 ms 336 ms 192.80.16.179
 14  378 ms 662 ms 308 ms 107.154.13.242.ip.incapdns.net [107.154.13.242]
 15  396 ms 404 ms 306 ms 172.21.0.62
 16  *      *      1083 ms 199.193.7.174
 17  948 ms 1037 ms 605 ms 199.193.7.46
 18  *      *      *      Request timed out.
 19  572 ms 417 ms 340 ms host62.registrar-servers.com [199.188.200.126]

Trace complete.
```

Over maximum of 30 hops: means that there are over 30 Servers between your Source (My PC) to the Destination(Server) where the website(Soutechventures.com) was hosted.