

Network Lab Assignment 01

Naveen S D
B190707CS

ping

- ping sends ICMP(Internet Control Message Protocol) ECHO_REQUEST to network host
- Measures round trip time
- ping -c n host
 - Sends n requests to the host server
- ping -O host
 - This command will display a message if no response was received

```
Naveen_B190707CS ping -c 3 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=57 time=28.5 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=57 time=27.7 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=57 time=28.0 ms

--- 1.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 27.704/28.056/28.516/0.339 ms
```

```
Naveen_B190707CS ping -Oc 3 eduserver.nitc.ac.in
PING eduserver.nitc.ac.in (103.241.136.151) 56(84) bytes of data.
no answer yet for icmp_seq=1
no answer yet for icmp_seq=2

--- eduserver.nitc.ac.in ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2019ms
```

traceroute

- Traces the movement of a packet from our system to the host
- It utilizes the IP Protocols TTL (Time To Live) and waits for ICMP TIME_EXCEEDED response from each gateway along the path to the host.

```

Naveen_B190707CS traceroute eduserver.nitc.ac.in
traceroute to eduserver.nitc.ac.in (103.241.136.151), 30 hops max, 60 byte packets
 1 _gateway (192.168.1.1)  0.426 ms  0.486 ms  0.555 ms
 2 10.212.154.1 (10.212.154.1)  5.648 ms  9.222 ms  12.565 ms
 3 218.248.113.230 (218.248.113.230)  16.807 ms 218.248.126.214 (218.248.126.214)  20.425 ms 218.248.123.218 (218.248.123.218)  23.549 ms
 4 117.216.207.220 (117.216.207.220)  30.976 ms  33.165 ms  33.144 ms
 5 117.216.207.221 (117.216.207.221)  33.517 ms  33.977 ms  33.952 ms
 6 115.110.161.85.static.vsnl.net.in (115.110.161.85)  45.210 ms  44.829 ms  45.904 ms
 7 172.31.180.58 (172.31.180.58)  55.674 ms  26.627 ms  27.847 ms
 8 14.143.173.150.static-hyderabad.vsnl.net.in (14.143.173.150)  28.024 ms  27.723 ms  27.778 ms
 9 103.233.124.7 (103.233.124.7)  27.910 ms  27.936 ms  28.328 ms
10 103.233.124.27 (103.233.124.27)  28.295 ms 103.233.124.19 (103.233.124.19)  29.599 ms  31.313 ms
11 103.233.124.237 (103.233.124.237)  29.515 ms 103.233.124.241 (103.233.124.241)  27.694 ms 103.233.124.239 (103.233.124.239)  27.915 ms
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

```

- There are different flags to change the number of queries, wait time, etc

ip

- This command is used to manipulate routing devices
- ip address shows the address of all the attached devices.

```
Naveen_B190707CS ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 90:78:41:ca:2b:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.104/24 brd 192.168.1.255 scope global dynamic noprefixroute wlp2s0
        valid_lft 3707sec preferred_lft 3707sec
    inet6 fe80::4692:f165:99b2:41c9/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp59s0u1u4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 94:05:bb:1b:2b:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.13/24 brd 192.168.1.255 scope global dynamic noprefixroute enp59s0u1u4
        valid_lft 79060sec preferred_lft 79060sec
    inet6 fe80::16a5:a658:be5e:f69d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
Naveen_B190707CS
```

dig

- DNS lookup utility
- +short flag will just give the ip address for the asked domain name.

```
Naveen_B190707CS dig eduserver.nitc.ac.in

; <<>> DiG 9.16.23 <<>> eduserver.nitc.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3232
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;eduserver.nitc.ac.in.          IN      A

;; ANSWER SECTION:
eduserver.nitc.ac.in.  19086   IN      A      103.241.136.151

;; Query time: 6 msec
;; SERVER: 218.248.112.97#53(218.248.112.97)
;; WHEN: Sun Jan 16 08:57:54 IST 2022
;; MSG SIZE rcvd: 65

Naveen_B190707CS dig +short eduserver.nitc.ac.in
103.241.136.151
Naveen_B190707CS 
```

whois

- this command will give all the details related to the given domain or ip address.

```
Naveen_B190707CS whois youtube.com
Domain Name: YOUTUBE.COM
Registry Domain ID: 142504053_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-01-14T09:38:42Z
Creation Date: 2005-02-15T05:13:12Z
Registry Expiry Date: 2023-02-15T05:13:12Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-01-15T11:48:08Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

route

- Command to show / manipulate the IP routing table

```
Naveen_B190707CS route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
default          _gateway        0.0.0.0          UG    100    0      0 enp59s0u1u4
default          _gateway        0.0.0.0          UG    600    0      0 wlp2s0
192.168.1.0      0.0.0.0         255.255.255.0    U     100    0      0 enp59s0u1u4
192.168.1.0      0.0.0.0         255.255.255.0    U     600    0      0 wlp2s0
Naveen_B190707CS route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
0.0.0.0          192.168.1.1     0.0.0.0          UG    100    0      0 enp59s0u1u4
0.0.0.0          192.168.1.1     0.0.0.0          UG    600    0      0 wlp2s0
192.168.1.0      0.0.0.0         255.255.255.0    U     100    0      0 enp59s0u1u4
192.168.1.0      0.0.0.0         255.255.255.0    U     600    0      0 wlp2s0
Naveen_B190707CS
```

tcpdump

- Shows the network traffic in a network

```
Naveen_B190707CS sudo tcpdump -i enp59s0u1u4
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp59s0u1u4, link-type EN10MB (Ethernet), snapshot length 262144 bytes
09:17:43.427414 IP yoda.39768 > multiplay.bsnl.in.domain: 52100+ A? play.google.com. (33)
09:17:43.427456 IP yoda.39768 > multiplay.bsnl.in.domain: 52108+ AAAA? play.google.com. (33)
09:17:43.433174 IP multiplay.bsnl.in.domain > yoda.39768: 52100 1/0/0 A 172.217.163.206 (49)
09:17:43.433234 IP multiplay.bsnl.in.domain > yoda.39768: 52108 1/0/0 AAAA 2404:6800:4007:810::200e (61)
09:17:43.497218 IP yoda.48601 > multiplay.bsnl.in.domain: 6026+ PTR? 97.112.248.218.in-addr.arpa. (45)
09:17:43.504261 IP multiplay.bsnl.in.domain > yoda.48601: 6026 1/2/0 PTR multiplay.bsnl.in. (114)
09:17:43.603814 IP yoda.59533 > multiplay.bsnl.in.domain: 17648+ A? play.google.com. (33)
09:17:43.603831 IP yoda.59533 > multiplay.bsnl.in.domain: 41708+ AAAA? play.google.com. (33)
09:17:43.612627 IP multiplay.bsnl.in.domain > yoda.59533: 17648 1/0/0 A 172.217.163.206 (49)
09:17:43.616176 IP multiplay.bsnl.in.domain > yoda.59533: 41708 1/0/0 AAAA 2404:6800:4007:810::200e (61)
^XC09:17:44.080775 ARP, Request who-has yoda tell 192.168.1.5, length 46

11 packets captured
93 packets received by filter
19 packets dropped by kernel
Naveen_B190707CS
```

ss

- a command used to investigate the sockets

```
Naveen_B190707CS ss
```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
u_dgr	ESTAB	0	0	/run/systemd/notify 559	* 0	
u_dgr	ESTAB	0	0	/run/systemd/journal/dev-log 564	* 0	
u_dgr	ESTAB	0	0	/run/systemd/journal/socket 586	* 0	
u_seq	ESTAB	0	0	00000d 72729	* 72728	
u_seq	ESTAB	0	0	00000e 65043	* 65044	
u_seq	ESTAB	0	0	00000f 65045	* 65046	
u_seq	ESTAB	0	0	00000a 72728	* 72729	
u_seq	ESTAB	0	0	00000b 69017	* 69018	
u_seq	ESTAB	0	0	00000c 69018	* 69017	
u_str	ESTAB	0	0	* 35004	* 35005	
u_str	ESTAB	0	768	/run/user/1000/bus 31611	* 27440	
u_str	ESTAB	0	0	/run/systemd/journal/stdout 28000	* 27173	
u_str	ESTAB	0	0	* 20235	* 13805	
u_str	ESTAB	0	0	* 17246	* 19098	
u_str	ESTAB	0	0	* 66000	* 66000	

dstat

- See system resource statistics

```
Naveen_B190707CS dstat
```

You did not select any stats, using -cdngy by default.

--total-cpu-usage--				-dsk/total-		-net/total-		---paging--		---system--		
usr	sys	idl	wai	stl	read	writ	recv	send	in	out	int	csw
3	1	96			806	507					1033	2315
3	1	97				272	244	256			1168	1784
1		99				88	254	150			422	1078
1		98									413	929
1		99					166	150			362	822

ifstat

- Shows network interface statistics

```
Naveen_B190707CS ifstat
#kernel
Interface      RX Pkts/Rate    TX Pkts/Rate    RX Data/Rate    TX Data/Rate
                RX Errs/Drop    TX Errs/Drop    RX Over/Rate    TX Coll/Rate
lo              0 0             0 0             0 0             0 0
                0 0             0 0             0 0             0 0
wlp2s0          36 0            16 0            1900 0           1080 0
                0 0             0 0             0 0             0 0
enp59s0u1u4     374 0           335 0           48460 0          60462 0
                0 33            0 0             0 0             0 0
Naveen_B190707CS
```

wget

- To download pages from the web

```
Naveen_B190707CS wget https://raw.githubusercontent.com/naveensd101/cpTemplates/main/__soln.cpp
--2022-01-16 10:07:00-- https://raw.githubusercontent.com/naveensd101/cpTemplates/main/__soln.cpp
SSL_INIT
Loaded CA certificate '/etc/ssl/certs/ca-certificates.crt'
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 541 [text/plain]
Saving to: '__soln.cpp'

__soln.cpp                               100%[=====]
2022-01-16 10:07:00 (68.9 MB/s) - '__soln.cpp' saved [541/541]
```


tracert

- This command is similar to [tracert](#)
- This will discover the path along with that it will discover the MTU (Maximum Transmission Unit).

```
Naveen_B190707CS tracert youtube.com
1?: [LOCALHOST] pmtu 1460
1: _gateway 0.518ms
1: _gateway 0.373ms
2: 10.212.154.1 9.854ms
3: ??? 5.761ms asymm 4
4: no reply
5: no reply
6: 72.14.218.250 19.981ms asymm 10
7: no reply
8: no reply
9: no reply
10: no reply
11: no reply
12: no reply
13: no reply
14: no reply
15: no reply
16: no reply
17: no reply
18: no reply
19: no reply
20: no reply
21: no reply
22: no reply
23: no reply
24: no reply
25: no reply
26: no reply
27: no reply
28: no reply
29: no reply
30: no reply
    Too many hops: pmtu 1460
    Resume: pmtu 1460
Naveen_B190707CS
```