

CS3093D: ASSIGNMENT 01

Ping

Used to send ICMP ECHO_REQUEST to network hosts

```
nikhil_b180283cs@networks_lab ping 103.170.132.19
PING 103.170.132.19 (103.170.132.19) 56(84) bytes of data.
64 bytes from 103.170.132.19: icmp_seq=1 ttl=52 time=112 ms
64 bytes from 103.170.132.19: icmp_seq=2 ttl=52 time=88.0 ms
64 bytes from 103.170.132.19: icmp_seq=3 ttl=52 time=73.1 ms
64 bytes from 103.170.132.19: icmp_seq=4 ttl=52 time=84.8 ms
^C
--- 103.170.132.19 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4006ms
rtt min/avg/max/mdev = 73.052/89.406/111.747/14.050 ms
nikhil_b180283cs@networks_lab ping 103.170.132.19 -c 5
PING 103.170.132.19 (103.170.132.19) 56(84) bytes of data.
64 bytes from 103.170.132.19: icmp_seq=1 ttl=52 time=107 ms
64 bytes from 103.170.132.19: icmp_seq=2 ttl=52 time=63.5 ms
64 bytes from 103.170.132.19: icmp_seq=3 ttl=52 time=71.6 ms
64 bytes from 103.170.132.19: icmp_seq=4 ttl=52 time=86.9 ms
64 bytes from 103.170.132.19: icmp_seq=5 ttl=52 time=74.8 ms

--- 103.170.132.19 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 63.452/80.677/106.732/15.048 ms
nikhil_b180283cs@networks_lab |
```

tracert/traceroute

Used to print the route packets trace to network host

```
nikhil_b180283cs@networks_lab traceroute 103.170.132.19
traceroute to 103.170.132.19 (103.170.132.19), 30 hops max, 60 byte packets
 1 _gateway (192.168.119.144) 839.794 ms 839.826 ms 839.908 ms
 2 * * *
 3 56.8.124.109 (56.8.124.109) 904.657 ms 56.8.124.121 (56.8.124.121) 904.767 ms 56.8.124.117 (56.8.124.117) 904.713 ms
 4 172.26.104.196 (172.26.104.196) 904.660 ms 930.919 ms 931.176 ms
 5 172.26.104.210 (172.26.104.210) 931.129 ms 172.26.104.211 (172.26.104.211) 945.439 ms 945.591 ms
 6 192.168.14.32 (192.168.14.32) 945.538 ms 103.649 ms 192.168.14.36 (192.168.14.36) 103.562 ms
 7 192.168.14.37 (192.168.14.37) 103.412 ms 43.552 ms 43.397 ms
 8 172.16.81.6 (172.16.81.6) 65.536 ms 172.16.81.2 (172.16.81.2) 65.504 ms 172.16.81.4 (172.16.81.4) 67.319 ms
 9 172.16.3.91 (172.16.3.91) 66.908 ms 67.084 ms 172.16.0.159 (172.16.0.159) 58.825 ms
10 172.16.1.204 (172.16.1.204) 86.760 ms 86.815 ms 125.520 ms
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
nikhil_b180283cs@networks_lab |
```

ip/ifconfig/ipconfig

Used to show / manipulate routing, network devices, interfaces and tunnels

```
nikhil_b180283cs@networks_lab 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: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether c0:b5:d7:26:6c:1b brd ff:ff:ff:ff:ff:ff
    inet 192.168.119.249/24 brd 192.168.119.255 scope global dynamic noprefixroute wlan0
        valid_lft 3165sec preferred_lft 3165sec
    inet6 2409:4073:4e8c:f396:57a6:2aa2:f987:2006/64 scope global dynamic noprefixroute
        valid_lft 3168sec preferred_lft 3168sec
    inet6 fe80::6be1:c99e:535a:42ea/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
nikhil_b180283cs@networks_lab ip rule
0:      from all lookup local
32766:  from all lookup main
32767:  from all lookup default
nikhil_b180283cs@networks_lab ip maddress
1:      lo
    inet 224.0.0.1
    inet6 ff02::1
    inet6 ff01::1
2:      wlan0
    link 01:00:5e:00:00:01 users 2
    link 01:00:5e:00:00:fb users 2
    link 33:33:00:00:00:01 users 2
    link 33:33:ff:5a:42:ea users 2
    link 33:33:ff:87:20:06 users 2
    inet 224.0.0.1
    inet 224.0.0.251
    inet6 ff02::1:ff87:2006
    inet6 ff02::1:ff5a:42ea
    inet6 ff02::1
    inet6 ff01::1
nikhil_b180283cs@networks_lab
```

dig/nslookup/host

Used to lookup DNS entries for a given domain

```
nikhil_b180283cs@networks_lab dig nitc.ac.in

; <<>> DiG 9.16.24 <<>> nitc.ac.in
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 15713
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;nitc.ac.in.                IN      A

;; ANSWER SECTION:
nitc.ac.in.                21600   IN      A      103.160.223.4

;; Query time: 183 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Jan 16 13:24:09 IST 2022
;; MSG SIZE rcvd: 55

nikhil_b180283cs@networks_lab |
```

Whois

Used to query the whois directory service. Shows who owns a particular ip or host

```
nikhil_b180283cs@networks_lab whois 103.160.223.4
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '103.160.223.0 - 103.160.223.255'

% Abuse contact for '103.160.223.0 - 103.160.223.255' is 'cnc@nitc.ac.in'

inetnum:        103.160.223.0 - 103.160.223.255
netname:        NITC
descr:          Director National Institute Of Technology Calicut
admin-c:        DN395-AP
tech-c:         DC2821-AP
country:        IN
mnt-by:         MAINT-IN-IRINN
mnt-irt:        IRT-NITC-IN
mnt-routes:     MAINT-IN-NITC
status:         ASSIGNED PORTABLE
last-modified:  2020-12-24T12:46:13Z
source:         APNIC

irt:            IRT-NITC-IN
address:        Director National Institute Of Technology Calicut, NIT Campus P.O , Kozhikode, India,Kozhikode,Kerala-673601
e-mail:         director@nitc.ac.in
abuse-mailbox:  cnc@nitc.ac.in
admin-c:        DC2821-AP
tech-c:         DC2821-AP
auth:           # Filtered
mnt-by:         MAINT-IN-NITC
last-modified:  2020-12-24T12:39:05Z
source:         APNIC
```

Route

Used to show / manipulate the IP routing table

```
nikhil_b180283cs@networks_lab route
Kernel IP routing table
Destination      Gateway           Genmask           Flags Metric Ref    Use Iface
default          _gateway         0.0.0.0           UG    600    0      0 wlan0
192.168.119.0    0.0.0.0         255.255.255.0    U     600    0      0 wlan0
nikhil_b180283cs@networks_lab |
```

Tcpdump

Used to dump traffic on a network

```
nikhil_b180283cs@networks_lab sudo tcpdump -c 5 -i wlan0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:29:23.016554 IP whatsapp-cdn-shv-01-tir2.fbcdn.net.https > DeathStar.41680: Flags [P.], seq 1511176129:1511176201, ack 332612906, win 278, options [nop,nop,TS val 2130346674 ecr 506181150], length 72
13:29:23.016582 IP DeathStar.41680 > whatsapp-cdn-shv-01-tir2.fbcdn.net.https: Flags [.], ack 72, win 501, options [nop,nop,TS val 506182017 ecr 2130346674], length 0
13:29:23.076273 IP6 DeathStar.40813 > maa05s09-in-x0a.1e100.net.https: UDP, length 1230
13:29:23.095174 IP DeathStar.56234 > dns.google.domain: 44971+ PTR? 60.228.240.157.in-addr.arpa. (45)
13:29:23.173655 IP6 maa05s09-in-x0a.1e100.net.https > DeathStar.40813: UDP, length 1230
5 packets captured
38 packets received by filter
8 packets dropped by kernel
nikhil_b180283cs@networks_lab |
```

netstat/ss

another utility to investigate sockets

```
nikhil_b180283cs@networks_lab ss -l
```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
n1	UNCONN	0	0	rt1:signal-desktop/1505	*	
n1	UNCONN	0	0	rt1:NetworkManager/556	*	
n1	UNCONN	0	0	rt1:signal-desktop/2224	*	
n1	UNCONN	0	0	rt1:kernel	*	
n1	UNCONN	0	0	rt1:brave/1504	*	
n1	UNCONN	0	0	rt1:brave/1693	*	
n1	UNCONN	0	0	rt1:iwd/557	*	
n1	UNCONN	0	0	rt1:signal-desktop/2224	*	
n1	UNCONN	0	0	rt1:signal-desktop/1505	*	
n1	UNCONN	0	0	rt1:brave/1693	*	
n1	UNCONN	0	0	rt1:brave/1504	*	
n1	UNCONN	0	0	rt1:iwd/557	*	
n1	UNCONN	0	0	rt1:NetworkManager/556	*	
n1	UNCONN	4352	0	tcpdiag:ss/2530728	*	
n1	UNCONN	768	0	tcpdiag:kernel	*	
n1	UNCONN	0	0	xfrm:kernel	*	
n1	UNCONN	0	0	selinux:kernel	*	
n1	UNCONN	0	0	audit:systemd/1	*	
n1	UNCONN	0	0	audit:-1934067345	*	
n1	UNCONN	0	0	audit:kernel	*	
n1	UNCONN	0	0	audit:NetworkManager/556	*	
n1	UNCONN	0	0	audit:systemd/1	*	
n1	UNCONN	0	0	fiblookup:kernel	*	

Dstat

versatile tool for generating system resource statistics

```
nikhil_b180283cs@networks_lab 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
48 19 33 0 0 | 24k 70k | 0 0 | 0 0 | 737 2022
9 4 87 0 0 | 0 0 | 1643B 0 | 0 0 | 1712 5155
7 5 88 0 0 | 0 0 | 1160B 0 | 0 0 | 1697 5206
7 5 88 0 0 | 0 0 | 963B 0 | 0 0 | 1743 4945
7 4 88 0 0 | 0 0 | 515B 0 | 0 0 | 1666 5110
8 4 87 1 0 | 0 168k | 1697B 0 | 0 0 | 1703 5141
8 4 88 0 0 | 0 0 | 3756B 1220B | 0 0 | 1669 5043
11 5 84 0 0 | 0 0 | 969B 322B | 0 0 | 2190 6639
13 6 81 0 0 | 0 0 | 0 0 | 0 0 | 2446 7086
12 5 82 1 0 | 0 136k | 0 0 | 0 0 | 2283 6898
13 6 81 0 0 | 0 0 | 490B 684B | 0 0 | 2239 6782
13 6 81 0 0 | 0 136k | 0 0 | 0 0 | 2239 6782
8 4 87 0 0 | 0 0 | 2345B 0 | 0 0 | 1712 5207
7 5 88 0 0 | 0 0 | 3276B 1220B | 0 0 | 1761 5382
7 5 88 0 0 | 0 0 | 1167B 0 | 0 0 | 1595 4734
13 5 82 1 0 | 0 96k | 1167B 0 | 0 0 | 1891 6027
20 3 76 0 0 | 0 184k | 1530B 0 | 0 0 | 8246 11
10 4 86 0 0 | 0 224k | 1501B 0 | 0 0 | 2527 6933
```

Ifstat

handy utility to read network interface statistics

```
nikhil_b180283cs@networks_lab 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
wlan0           550 0           368 0           228957 0        161440 0
                0 2             0 0             0 0             0 0
peer2           355 0           366 0           172504 0        138600 0
                0 0             0 0             0 0             0 0
```

Wget

The non-interactive network downloader

```
nikhil_b180283cs@networks_lab wget www.google.com
--2022-01-16 18:43:11-- http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.195.132, 2404:6800:4007:82a::2004
Connecting to www.google.com (www.google.com)[142.250.195.132]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html           [  =>          ] 16.00K  ---KB/s   in 0.01s

2022-01-16 18:43:11 (1.55 MB/s) - 'index.html' saved [16385]

nikhil_b180283cs@networks_lab
```

Tracepath

traces path to a network host discovering MTU along this path. Similar to traceroute

```
nikhil_b180283cs@networks_lab traceroute 192.168.40.3
traceroute to 192.168.40.3 (192.168.40.3), 30 hops max, 60 byte packets
 1  10.13.13.1 (10.13.13.1)  3.996 ms  17.546 ms  18.428 ms
 2  dspace-Precision-T3610 (172.18.0.1)  19.067 ms  19.237 ms  19.202 ms
 3  _gateway (192.168.230.1)  19.965 ms  19.910 ms  19.459 ms
 4  192.168.40.3 (192.168.40.3)  20.414 ms  20.484 ms  20.494 ms
nikhil_b180283cs@networks_lab
```