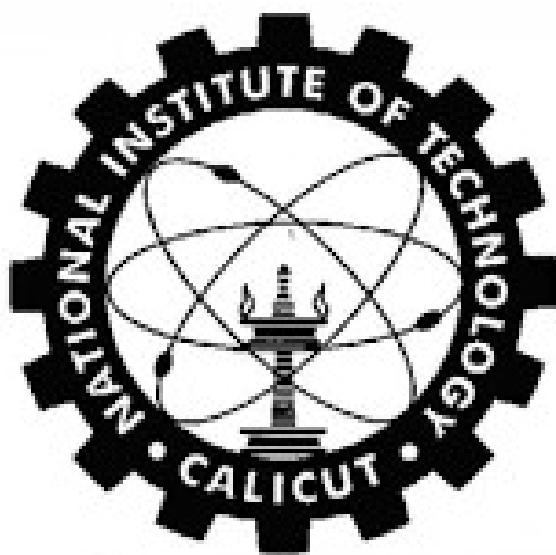


CS3009D: NETWORKS LABORATORY (EXPERIMENT 1)



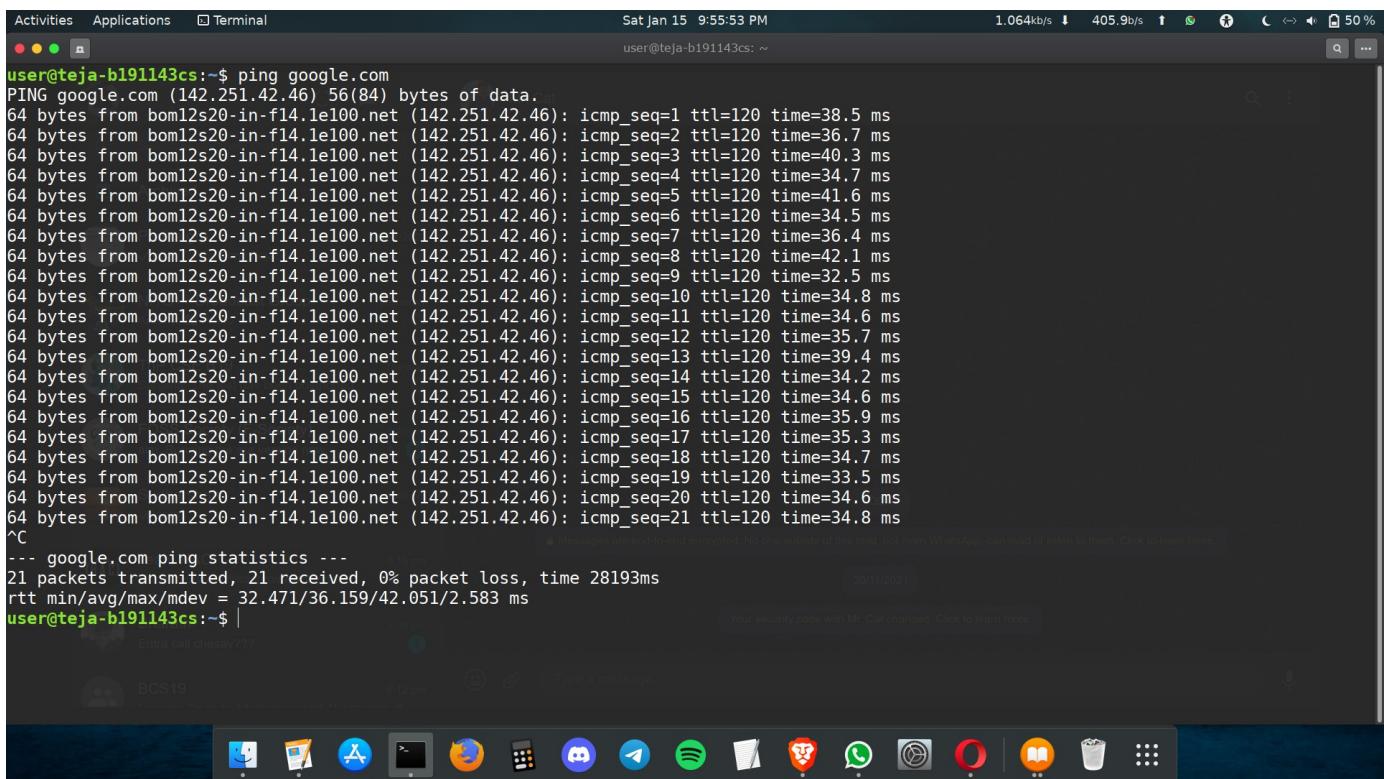
तमसो मा ज्योतिर्गमय

**Name : Panasa Teja
ROLL : B191143CS
BATCH : B**

1. ping

PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. It is used to check whether a network is available and if a host is reachable. With this command, you can check if a server is up and running. When you “ping” a remote host, your machine starts sending ICMP (Internet Control Message Protocol) echo requests and waits for a response. If the connection is established, you’ll receive an echo reply for every request. The output of the ping command contains the amount of time it takes for every packet to reach its destination and return. Also in the terminal, it keeps printing responses until it is stopped.

Ex: ping google.com
ping www.amazon.com



A screenshot of a Linux desktop environment showing a terminal window. The terminal window has a dark background and light-colored text. At the top, there's a header bar with icons for Activities, Applications, Terminal, and system status (1.064kb/s, 405.9b/s, battery level 50%, and a shutdown icon). The terminal window title is "Terminal". The command entered is "ping google.com". The output shows multiple ICMP echo requests being sent to the IP address 142.251.42.46, with details like sequence number (seq), TTL, and round-trip time (time). After several responses, a Ctrl+C interrupt is shown. Below the terminal, a messaging application window is partially visible, showing a message from "BCS19" and a list of icons for various applications like Mail, Calendar, and File Manager.

```
Activities Applications Terminal
Sat Jan 15 9:55:53 PM
user@teja-b191143cs: ~
user@teja-b191143cs:~$ ping google.com
PING google.com (142.251.42.46) 56(84) bytes of data.
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=1 ttl=120 time=38.5 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=2 ttl=120 time=36.7 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=3 ttl=120 time=40.3 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=4 ttl=120 time=34.7 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=5 ttl=120 time=41.6 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=6 ttl=120 time=34.5 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=7 ttl=120 time=36.4 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=8 ttl=120 time=42.1 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=9 ttl=120 time=32.5 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=10 ttl=120 time=34.8 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=11 ttl=120 time=34.6 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=12 ttl=120 time=35.7 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=13 ttl=120 time=39.4 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=14 ttl=120 time=34.2 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=15 ttl=120 time=34.6 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=16 ttl=120 time=35.9 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=17 ttl=120 time=35.3 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=18 ttl=120 time=34.7 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=19 ttl=120 time=33.5 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=20 ttl=120 time=34.6 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=21 ttl=120 time=34.8 ms
^C
--- google.com ping statistics ---
21 packets transmitted, 21 received, 0% packet loss, time 28193ms
rtt min/avg/max/mdev = 32.471/36.159/42.051/2.583 ms
user@teja-b191143cs:~$ |
```

Here,

ttl = TTL (Time to Live) represents the number of network hops a packet can take before a router discards it.

icmp_seq = The sequence number of each ICMP packet. Increase by one for every echo request.

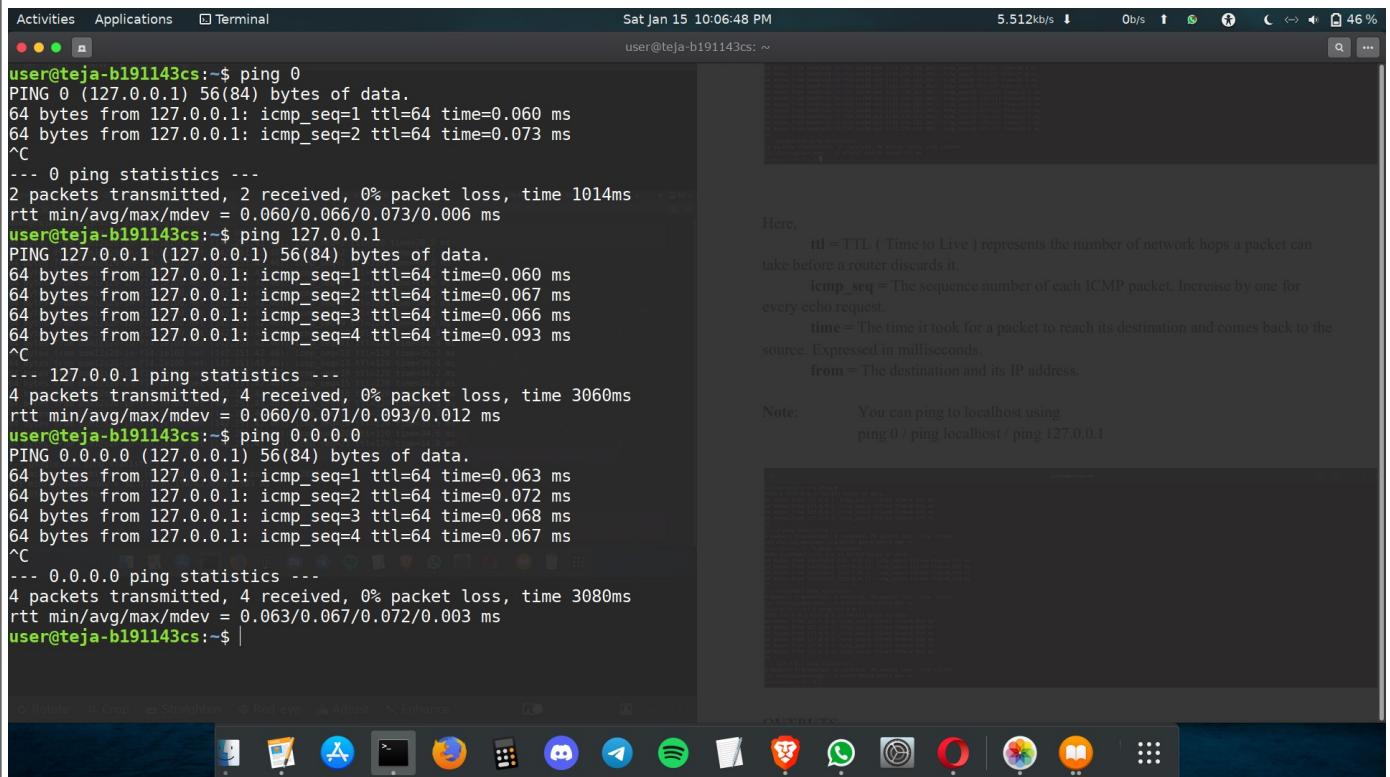
time = The time it took for a packet to reach its destination and comes back to the source. Expressed in milliseconds.

From = The destination and its IP address.

Note :

You can ping to localhost using

ping 0 / ping 127.0.0.1



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Terminal". The terminal content displays the output of several "ping" commands. The first command is "ping 0", which shows two packets transmitted to 127.0.0.1 with sequence numbers 1 and 2. The second command is "ping 127.0.0.1", which shows four packets transmitted to 127.0.0.1 with sequence numbers 1 through 4. The third command is "ping 0.0.0.0", which shows four packets transmitted to 0.0.0.0 with sequence numbers 1 through 4. The terminal window is located at the top of the desktop, and the desktop interface below includes a dock with various application icons.

```
Activities Applications Terminal
Sat Jan 15 10:06:48 PM
user@teja-b191143cs: ~
user@teja-b191143cs:~$ ping 0
PING 0 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.060 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.073 ms
^C
--- 0 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.060/0.066/0.073/0.006 ms
user@teja-b191143cs:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.060 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.067 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.066 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.093 ms
^C
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3060ms
rtt min/avg/max/mdev = 0.060/0.071/0.093/0.012 ms
user@teja-b191143cs:~$ ping 0.0.0.0
PING 0.0.0.0 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.063 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.072 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.068 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.067 ms
^C
--- 0.0.0.0 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.063/0.067/0.072/0.003 ms
user@teja-b191143cs:~|
```

OUTPUTS

Case1: If we did not get any reply from the destination then it means that there is no network connectivity between host and server/host.

Case2: If the output is “request timed out” then it means the host is down or blocking our ICMP requests.

Case3: If the output is "destination not reachable" then it means that a route to the destination cannot be found.

Here,

ttl = TTL (Time to Live) represents the number of network hops a packet can take before a router discards it.

icmp_seq = The sequence number of each ICMP packet. Increase by one for every echo request.

time = The time it took for a packet to reach its destination and comes back to the source. Expressed in milliseconds.

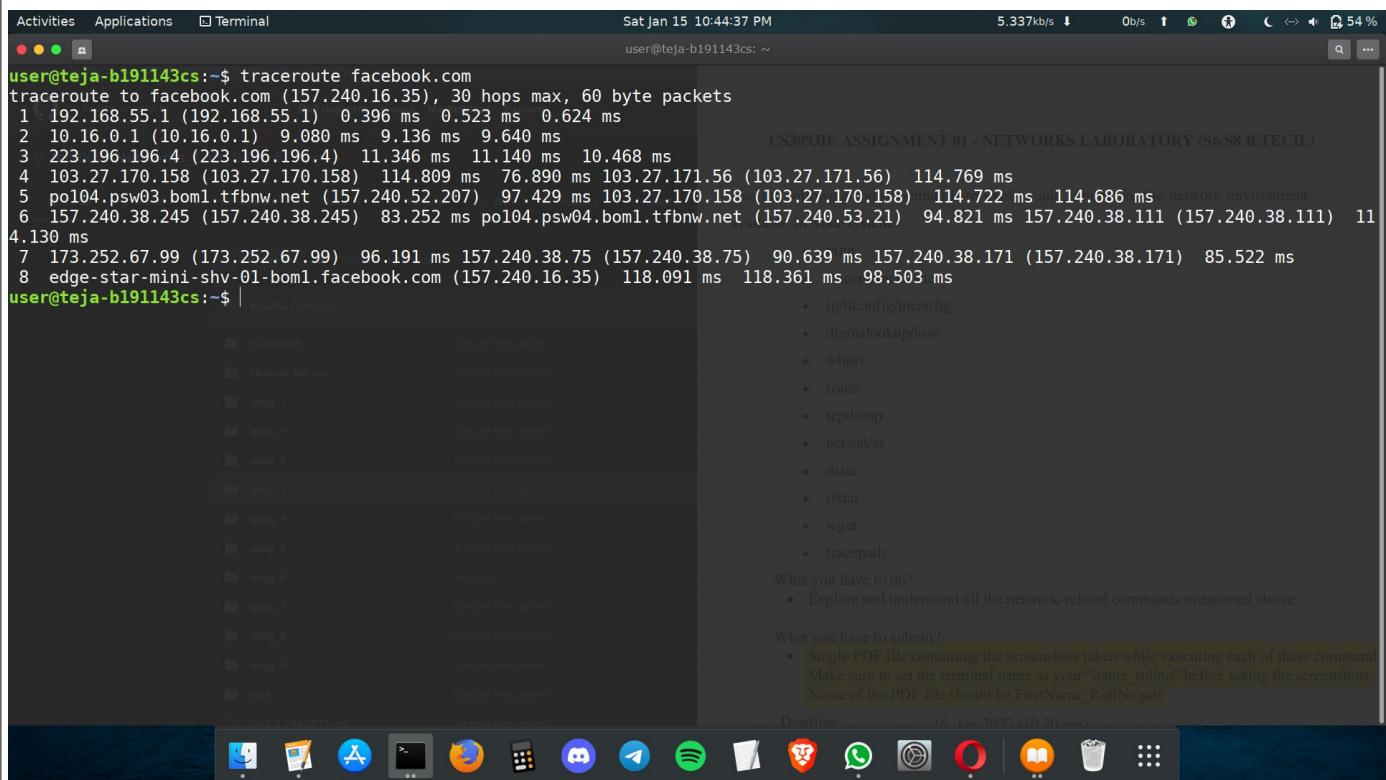
from = The destination and its IP address.

Note: You can ping to localhost using
ping 0 / ping localhost / ping 127.0.0.1

2. tracert/traceroute

“traceroute” command in Linux prints the route that the packet takes to reach the host or destination. It displays details about all the hops that the packet visits in between i.e it displays IP addresses and the time it took between each hop. The main use of this tool is to find where the error lies in the network if a data packet is unable to reach the destination.

Ex: traceroute facebook.com



```
Activities Applications Terminal Sat Jan 15 10:44:37 PM 5.337kb/s ↓ 0b/s ↗ 54 %
user@teja-b191143cs:~$ traceroute facebook.com
traceroute to facebook.com (157.240.16.35), 30 hops max, 60 byte packets
1 192.168.55.1 (192.168.55.1) 0.396 ms 0.523 ms 0.624 ms
2 10.16.0.1 (10.16.0.1) 9.080 ms 9.136 ms 9.640 ms
3 223.196.196.4 (223.196.196.4) 11.346 ms 11.140 ms 10.468 ms
4 103.27.170.158 (103.27.170.158) 114.809 ms 76.890 ms 103.27.171.56 (103.27.171.56) 114.769 ms
5 po104.psw03.bom1.tfbnw.net (157.240.52.207) 97.429 ms 103.27.170.158 (103.27.170.158) 114.722 ms 114.686 ms
6 157.240.38.245 (157.240.38.245) 83.252 ms po104.psw04.bom1.tfbnw.net (157.240.53.21) 94.821 ms 157.240.38.111 (157.240.38.111) 11
4.130 ms
7 173.252.67.99 (173.252.67.99) 96.191 ms 157.240.38.75 (157.240.38.75) 90.639 ms 157.240.38.171 (157.240.38.171) 85.522 ms
8 edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35) 118.091 ms 118.361 ms 98.503 ms
user@teja-b191143cs:~$ | teja863 Reduced
```

- ip/ifconfig/ipconfig
- dig/nslookup/host
- whois
- route
- tcpdump
- netstat/ss
- dstat
- ifstat
- wget
- tracepath

What you have to do?
• Explore and understand all the network-related commands mentioned above

What you have to submit?
• Single PDF file containing the screenshots taken while executing each of these command
Make sure to set the terminal name as your "name_Rollno" before taking the screenshots.
Name of the PDF file should be FirstName_RollNo.pdf

Deadline : 16 Jan 2022 (10:30 am)

3. ip/ifconfig/ipconfig

IP: IP (Internet Protocol) Address is an address of your network hardware. It helps in connecting your computer to other devices on your network and all over the world.

ipconfig stands for Internet Protocol Configuration, while ifconfig stands for Interface Configuration. It is often used for troubleshooting network connectivities. It's generally used to display the TCP/IP address of the system. Ifconfig is used at the boot time to set up the interfaces as necessary. After that, it is usually used when needed during debugging or when you need system tuning.

In ubuntu install them using : **\$sudo apt-get install net-tools**

ip r

Find the gateway address in the starting line. 192.168.55.1 is the default gateway in the given image.

```
user@teja-b191143cs:~$ ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.55.104 netmask 255.255.255.0 broadcast 192.168.55.255
          inet6 fe80::97d7:d44e:8ca3:7c7 prefixlen 64 scopeid 0x20<link>
            ether 98:07:43:23:05:c2 txqueuelen 1000 (Ethernet)
              RX packets 34938 bytes 30758992 (30.7 MB)
              RX errors 0 dropped 101 overruns 0 frame 0
              TX packets 23022 bytes 5592059 (5.5 MB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 123 bytes 10386 (10.3 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 123 bytes 10386 (10.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lxcbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        inet 10.0.3.1 netmask 255.255.255.0 broadcast 10.0.3.255
          ether 00:16:3e:00:00:00 txqueuelen 1000 (Ethernet)
            RX packets 0 bytes 0 (0.0 B) vers (Domain Name Server). It is used to query specific DNS resource records
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

4. dig/nslookup/host

nslookup is a command-line administrative tool for testing and troubleshooting DNS servers (Domain Name Server). It is used to query specific DNS resource records (RR) as well.

DNS: So basically, DNS is the phonebook of the internet. We can access information online through domain names, say linkedin.com or hackerrank.com. Web browsers interact through IP addresses. So, DNS translates domain names to IP addresses, so that the browsers can load internet resources.

Host by default is used to determine what domain a particular IP address resolves to.

Ex: nslookup facebook.com

```
Activities Applications Terminal Sun Jan 16 11:34:47 AM user@teja-b191143cs: ~
user@teja-b191143cs:~$ nslookup facebook.com
Server: 8.8.8.8
Address: 8.8.8.8#53
4. dig/nslookup/host
Non-authoritative answer: dministrative tool for testing and troubleshooting DNS
Name: facebook.com Server). It is used to query specific DNS resource records (RR) as
Address: 157.240.16.35
Name: facebook.com
Address: 2a03:2880:f12f:83:face:b00c:0:25de we can access information
on networked domain names, say linkedin.com or hackerrank.com. Web browsers
user@teja-b191143cs:~$ host facebook.com interact through IP addresses, so that
facebook.com has address 157.240.16.35
facebook.com has IPv6 address 2a03:2880:f16e:181:face:b00c:0:25de
facebook.com mail is handled by 10 smtpin.vvv.facebook.com.
user@teja-b191143cs:~$ |
```

NOTE: Type nslookup without any arguments to enter into Interactive mode so that you can set the servers to mail servers.

```
> set type=mx
> google.com
```

NOTE: Type nslookup without any arguments to enter into Interactive mode so that you can set the servers to mail servers.

```
> set type = mx
> google.com
```

```
Activities Applications Terminal Sun Jan 16 11:38:01 AM user@teja-b191143cs: ~
user@teja-b191143cs:~$ nslookup
> set type = mx
*** Invalid option: type
> set type=mx
> google.com
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
google.com mail exchanger = 20 alt1.aspmx.l.google.com.
google.com mail exchanger = 30 alt2.aspmx.l.google.com.
google.com mail exchanger = 50 alt4.aspmx.l.google.com.
google.com mail exchanger = 40 alt3.aspmx.l.google.com.
google.com mail exchanger = 10 aspmx.l.google.com.

Authoritative answers can be found from:
> amazon.com
Server: 8.8.8.8
Address: 8.8.8.8#53

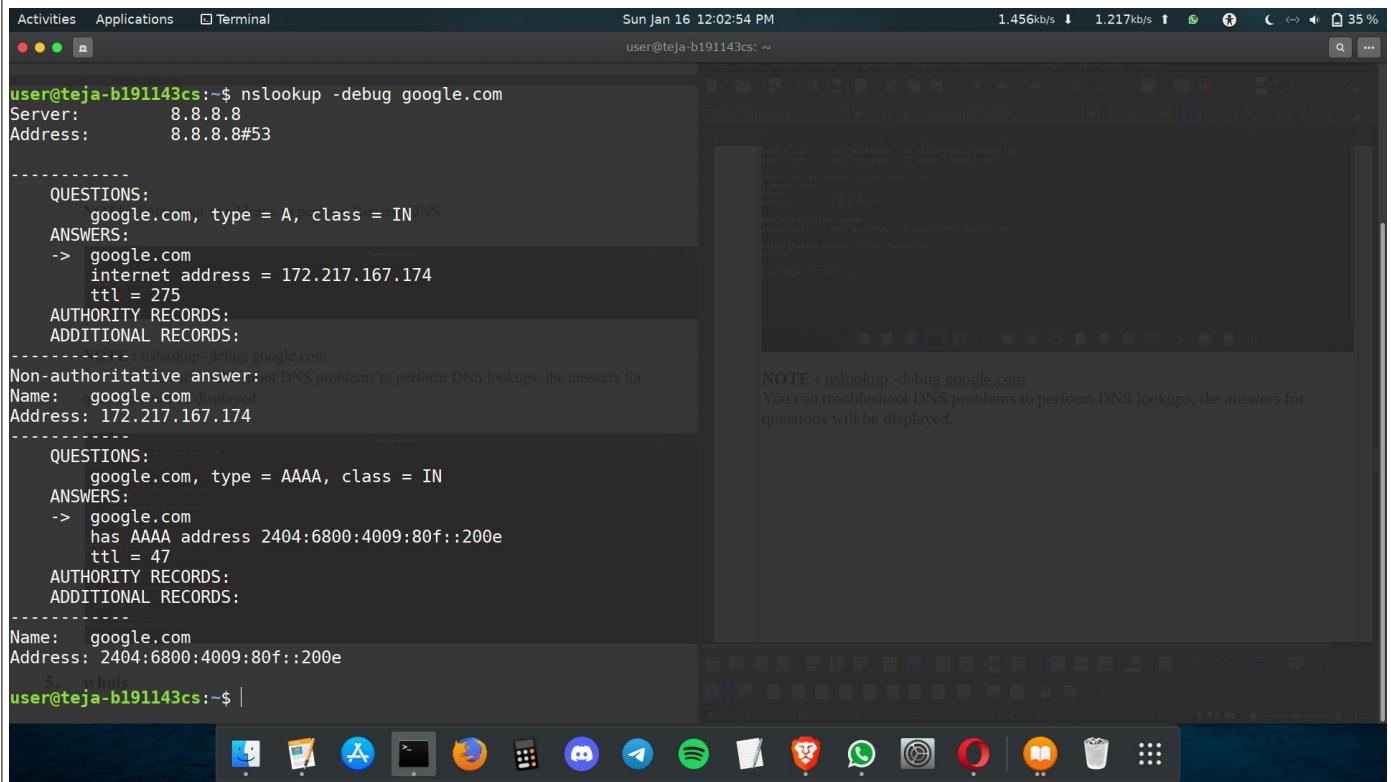
Non-authoritative answer:
amazon.com mail exchanger = 5 amazon-smtp.amazon.com.

Authoritative answers can be found from:
> exit

user@teja-b191143cs:~$ |
```

NOTE : nslookup -debug google.com

You can troubleshoot DNS problems to perform DNS lookups, the answers for questions will be displayed.



```
user@teja-b191143cs:~$ nslookup -debug google.com
Server: 8.8.8.8
Address: 8.8.8.8#53

-----
QUESTIONS:
    google.com, type = A, class = IN DNS.
ANSWERS:
-> google.com
    internet address = 172.217.167.174
    ttl = 275
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
Non-authoritative answer: Got DNS problems to perform DNS lookups, the answers for
Name: google.com
Address: 172.217.167.174
-----
QUESTIONS:
    google.com, type = AAAA, class = IN
ANSWERS:
-> google.com
    has AAAA address 2404:6800:4009:80f::200e
    ttl = 47
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
Name: google.com
Address: 2404:6800:4009:80f::200e
$ whois
user@teja-b191143cs:~$ |
```

5. whois

The whois system is a listing of records that contain details about the ownership of domains and the owners. The Internet corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership, but the list of records is held by many companies, known as registries. Anyone can query the list of records. A whois record contains contact information with the person, company or other entity that registered the DOMAIN name.

Install it using : sudo install whois

Ex: whois amazon.com

```
Activities Applications Terminal Sun Jan 16 12:05:50 PM user@teja-b191143cs: ~ 5.335kb/s ↓ 0b/s ↗ 34 %  
user@teja-b191143cs:~$ whois amazon.com  
Domain Name: AMAZON.COM  
Registry Domain ID: 281209_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.markmonitor.com  
Registrar URL: http://www.markmonitor.com  
Updated Date: 2019-05-07T20:09:37Z  
Creation Date: 1994-11-01T05:00:00Z  
Registry Expiry Date: 2024-10-31T04:00:00Z  
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.P31.DYNECT.NET  
Name Server: NS2.P31.DYNECT.NET  
Name Server: NS3.P31.DYNECT.NET  
Name Server: NS4.P31.DYNECT.NET  
Name Server: PDNS1.ULTRADNS.NET  
Name Server: PDNS6.ULTRADNS.CO.UK  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2022-01-15T08:33:31Z <<<  
within network. It is a map used by routers and gateways to track paths. The  
For more information on Whois status codes, please visit https://icann.org/epp  
Once reached, it will read through a table again for each next hop.  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration  
date of the domain name registrant's agreement with the sponsoring  
registrar. Users may consult the sponsoring registrar's Whois database to  
view the registrar's reported date of expiration for this registration.  
One of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2022-01-15T08:33:31Z <<<  
For more information on Whois status codes, please visit https://icann.org/epp  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration  
date of the domain name registrant's agreement with the sponsoring  
registrar. Users may consult the sponsoring registrar's Whois database to  
view the registrar's reported date of expiration for this registration.  
TERMS OF USE: You are not authorized to access or query our Whois  
database through the use of electronic processes that are high-volume and  
automated except as reasonably necessary to register domain names or  
modify existing registrations; the Data in VeriSign Global Registry  
Services' ("VeriSign") Whois database is provided by VeriSign for  
information purposes only, and to assist persons in obtaining information  
about or related to a domain name registration record. VeriSign does not  
guarantee its accuracy. By submitting a Whois query, you agree to abide  
by the following terms of use: You agree that you may use this Data only  
for lawful purposes and that under no circumstances will you use this Data  
to: (1) allow, enable, or otherwise support the transmission of mass  
unsolicited, commercial advertising or solicitations via e-mail, telephone,  
or facsimile; or (2) enable high volume, automated, electronic processes  
that apply to VeriSign (or its computer systems). The compilation,  
repackaging, dissemination or other use of this Data is expressly  
prohibited without the prior written consent of VeriSign. You agree not to  
use electronic processes that are automated and high-volume to access or  
query the Whois database except as reasonably necessary to register  
domain names or modify existing registrations. VeriSign reserves the right  
to restrict your access to the Whois database in its sole discretion to ensure  
operational stability. VeriSign may restrict or terminate your access to the  
5. whois  
The whois system is a listing of records that contain details about the ownership of  
domains and the owners. The Internet Corporation for Assigned Names and Numbers  
(ICANN) regulates domain name registration and ownership, but the list of records is  
held by many companies, known as registries. Anyone can query the list of records.  
A whois record contains contact information with the person, company or other entity  
that registered the DOMAIN name.  
Install it using : sudo install whois  
Ex: whois amazon.com
```

```
Activities Applications Terminal Sun Jan 16 12:05:55 PM user@teja-b191143cs: ~ 369.3b/s ↓ 738.5b/s ↑ 34 %  
user@teja-b191143cs:~$ whois amazon.com  
Domain Name: AMAZON.COM  
Registry Domain ID: 281209_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.markmonitor.com  
Registrar URL: http://www.markmonitor.com  
Updated Date: 2019-05-07T20:09:37Z  
Creation Date: 1994-11-01T05:00:00Z  
Registry Expiry Date: 2024-10-31T04:00:00Z  
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.P31.DYNECT.NET  
Name Server: NS2.P31.DYNECT.NET  
Name Server: NS3.P31.DYNECT.NET  
Name Server: NS4.P31.DYNECT.NET  
Name Server: PDNS1.ULTRADNS.NET  
Name Server: PDNS6.ULTRADNS.CO.UK  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2022-01-15T08:33:31Z <<<  
within network. It is a map used by routers and gateways to track paths. The  
For more information on Whois status codes, please visit https://icann.org/epp  
Once reached, it will read through a table again for each next hop.  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration  
date of the domain name registrant's agreement with the sponsoring  
registrar. Users may consult the sponsoring registrar's Whois database to  
view the registrar's reported date of expiration for this registration.  
One of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2022-01-15T08:33:31Z <<<  
For more information on Whois status codes, please visit https://icann.org/epp  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration  
date of the domain name registrant's agreement with the sponsoring  
registrar. Users may consult the sponsoring registrar's Whois database to  
view the registrar's reported date of expiration for this registration.  
TERMS OF USE: You are not authorized to access or query our Whois  
database through the use of electronic processes that are high-volume and  
automated except as reasonably necessary to register domain names or  
modify existing registrations; the Data in VeriSign Global Registry  
Services' ("VeriSign") Whois database is provided by VeriSign for  
information purposes only, and to assist persons in obtaining information  
about or related to a domain name registration record. VeriSign does not  
guarantee its accuracy. By submitting a Whois query, you agree to abide  
by the following terms of use: You agree that you may use this Data only  
for lawful purposes and that under no circumstances will you use this Data  
to: (1) allow, enable, or otherwise support the transmission of mass  
unsolicited, commercial advertising or solicitations via e-mail, telephone,  
or facsimile; or (2) enable high volume, automated, electronic processes  
that apply to VeriSign (or its computer systems). The compilation,  
repackaging, dissemination or other use of this Data is expressly  
prohibited without the prior written consent of VeriSign. You agree not to  
use electronic processes that are automated and high-volume to access or  
query the Whois database except as reasonably necessary to register  
domain names or modify existing registrations. VeriSign reserves the right  
to restrict your access to the Whois database in its sole discretion to ensure  
operational stability. VeriSign may restrict or terminate your access to the  
5. whois  
The whois system is a listing of records that contain details about the ownership of  
domains and the owners. The Internet Corporation for Assigned Names and Numbers  
(ICANN) regulates domain name registration and ownership, but the list of records is  
held by many companies, known as registries. Anyone can query the list of records.  
A whois record contains contact information with the person, company or other entity  
that registered the DOMAIN name.  
Install it using : sudo install whois  
Ex: whois amazon.com
```

```
Activities Applications Terminal Sun Jan 16 12:06:34 PM 737.7b/s ↓ 0b/s ↗ 33 %  
user@teja-b191143cs: ~  
  
The Registry database contains ONLY .COM, .NET, .EDU domains and  
Registrars.  
Domain Name: amazon.com  
Registry Domain ID: 281209_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.markmonitor.com, please visit https://icann.org/epp  
Registrar URL: http://www.markmonitor.com  
Updated Date: 2019-08-26T19:19:56+0000  
Creation Date: 1994-11-01T05:00:00+0000  
Registrar Registration Expiration Date: 2024-10-30T07:00:00+0000  
Registrar: MarkMonitor, Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com  
Registrar Abuse Contact Phone: +1.2083895770  
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)  
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)  
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)  
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)  
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)  
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)  
Registry Registrar ID:  
Registrant Name: Hostmaster, Amazon Legal Dept.  
Registrant Organization: Amazon Technologies, Inc.  
Registrant Street: P.O. Box 8102  
Registrant City: Reno  
Registrant State/Province: NV  
Registrant Postal Code: 89507  
Registrant Country: US  
Registrant Phone: +1.2062664064  
Registrant Phone Ext:  
Registrant Fax: +1.2062667010  
Registrant Fax Ext:  
Registrant Email: hostmaster@amazon.com
```

```
Activities Applications Terminal Sun Jan 16 12:06:41 PM 369.0b/s ↓ 332.1b/s ↑ 33 %  
user@teja-b191143cs: ~  
  
Web-based WHOIS:  
https://domains.markmonitor.com/whois  
  
If you have a legitimate interest in viewing the non-public WHOIS details, send  
your request and the reasons for your request to whoisrequest@markmonitor.com  
and specify the domain name in the subject line. We will review that request and  
may ask for supporting documentation and explanation.  
  
The data in MarkMonitor's WHOIS database is provided for information purposes,  
and to assist persons in obtaining information about or related to a domain  
name's registration record. While MarkMonitor believes the data to be accurate,  
the data is provided "as is" with no guarantee or warranties regarding its  
accuracy.  
TERMS OF USE: You are not authorized to access or query our Whois  
database through the use of electronic processes that are high-volume and  
lawful purposes and that, under no circumstances will you use this data to:  
(1) allow, enable, or otherwise support the transmission by email, telephone,  
or facsimile of mass, unsolicited, commercial advertising, or spam; or  
(2) enable high volume, automated, or electronic processes that send queries,  
data, or email to MarkMonitor (or its systems) or the domain name contacts (or  
its systems).  
MarkMonitor reserves the right to modify these terms at any time.  
By submitting this query, you agree to abide by this policy.  
Protecting companies and consumers in a digital world.  
Visit MarkMonitor at https://www.markmonitor.com  
Contact us at +1.8007459229  
In Europe, at +44.02032062220
```

6. route

ROUTING TABLE : A routing table is a file containing information on how the information or packets should be transferred: the network path to all nodes or devices within a network. It is a map used by routers and gateways to track paths. The hop-by-hop routing is widely used, the packet contains the routing table to reach the next hop, once reached, it will read the routing table again to reach the next hop. Using the route command you can communicate with subnets and different networks, you can also block the traffic between networks or devices by modifying the routing table.

Ex: route

: To display routing table entries.

Ex: route -n

: To display routing tables in full numerical entities.

Ex: sudo route add default gw 169.154.0.0 : To add default gateway.

Ex: sudo route add -host 192.168.1.151 reject : To reject a host/network.

Ex: route -Cn

: To list routing cache information of

Device

Ex: ip route

: To get details of IP routing table

Ex: ip route show table local

: To get details of local table with

destination of localhost.

Ex: ip -4/-6 route

: To get details of IPv4/IPv6 details.

The screenshot shows a terminal window with the following content:

```
user@teja-b191143cs:~$ route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
default         192.168.55.1   0.0.0.0       UG    100    0    0 enp2s0
10.0.3.0        0.0.0.0       255.255.255.0 U      0      0    0 lxcbr0
link-local      0.0.0.0       255.255.0.0   U      1000   0    0 enp2s0
192.168.55.0    0.0.0.0       255.255.255.0 U      100    0    0 enp2s0
user@teja-b191143cs:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         192.168.55.1   0.0.0.0       UG    100    0    0 enp2s0
10.0.3.0        0.0.0.0       255.255.255.0 U      0      0    0 lxcbr0
169.254.0.0     0.0.0.0       255.255.0.0   U      1000   0    0 enp2s0
192.168.55.0    0.0.0.0       255.255.255.0 U      100    0    0 enp2s0
user@teja-b191143cs:~$ sudo route add default gw 192.168.55.2
sudo: unable to resolve host teja-b191143cs: Name or service not known
[sudo] password for user:
user@teja-b191143cs:~$ ip route
default via 192.168.55.2 dev enp2s0
default via 192.168.55.1 dev enp2s0 proto dhcp metric 20100
10.0.3.0/24 dev lxcbr0 proto kernel scope link src 10.0.3.1 linkdown
169.254.0.0/16 dev enp2s0 scope link metric 1000
192.168.55.0/24 dev enp2s0 proto kernel scope link src 192.168.55.104 metric 100
user@teja-b191143cs:~$ ip route show table local
broadcast 10.0.3.0 dev lxcbr0 proto kernel scope link src 10.0.3.1 linkdown
local 10.0.3.1 dev lxcbr0 proto kernel scope host src 10.0.3.1
broadcast 10.0.3.255 dev lxcbr0 proto kernel scope link src 10.0.3.1 linkdown
broadcast 127.0.0.0 dev lo proto kernel scope link src 127.0.0.1
local 127.0.0.1 dev lo proto kernel scope host src 127.0.0.1
broadcast 127.255.255.255 dev lo proto kernel scope link src 127.0.0.1
broadcast 192.168.55.0 dev enp2s0 proto kernel scope link src 192.168.55.104
local 192.168.55.104 dev enp2s0 proto kernel scope host src 192.168.55.104
```

7. tcpdump

“tcpdump” tool allows you to capture and analyze network traffic such as TCP/IP packets going through the system. Normally used to troubleshoot network issues, also used as a security tool. It scans from all OSI layers (1-7) and saves the captured information as **.pcap** file which can be viewed on WIRESHARK or through the command tool itself.

Ex: sudo tcpdump

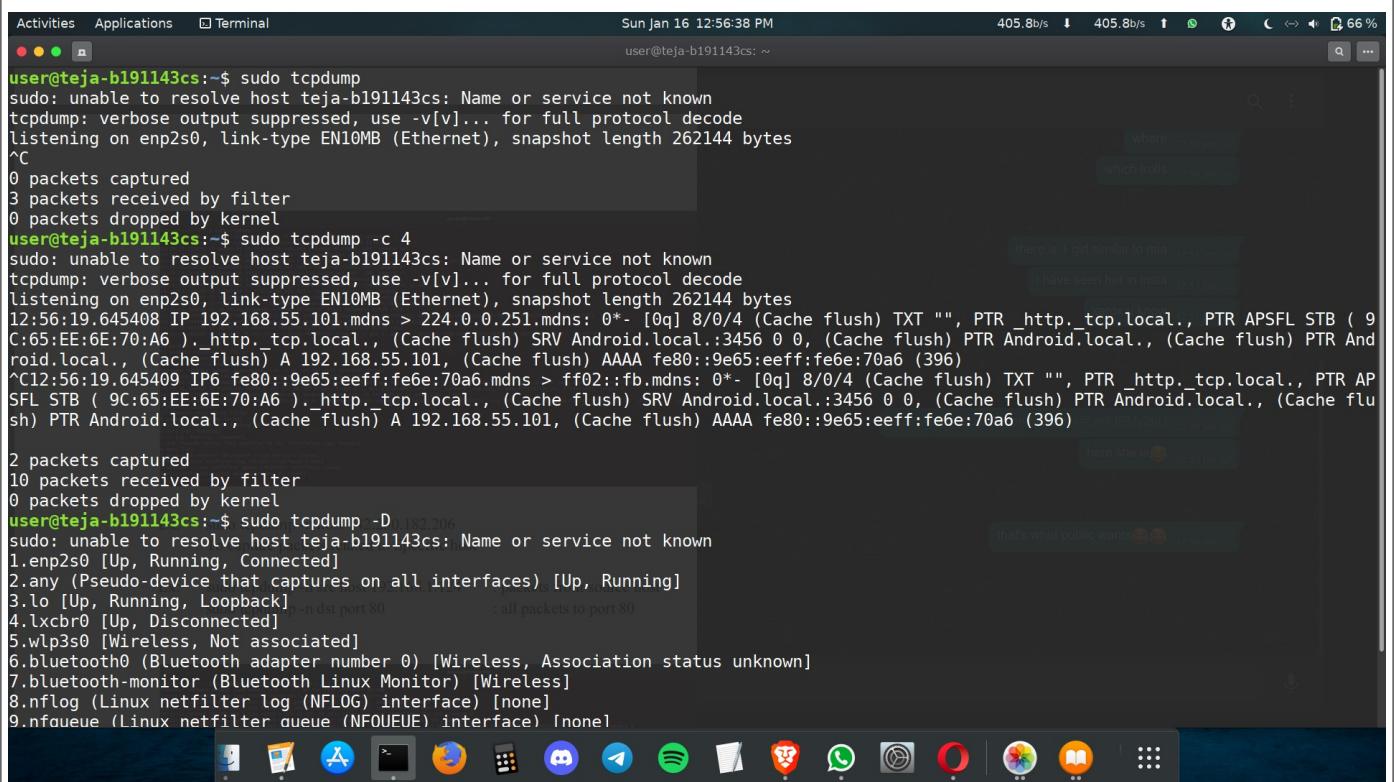
It will capture packets from the current interface of the network through which the system is connected to the internet.

Ex: sudo tcpdump -c 4

It will capture only 4 packets from the interface.

Ex: sudo tcpdump -D

It will print all the list of available networks that this tool can capture packets from.



The screenshot shows a terminal window with the following command history:

```
user@teja-b191143cs:~$ sudo tcpdump
sudo: unable to resolve host teja-b191143cs: Name or service not known
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
3 packets received by filter
0 packets dropped by kernel
user@teja-b191143cs:~$ sudo tcpdump -c 4
sudo: unable to resolve host teja-b191143cs: Name or service not known
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:56:19.645408 IP 192.168.55.101.mdns > 224.0.0.251.mdns: 0*- [0q] 8/0/4 (Cache flush) TXT "", PTR _http._tcp.local., PTR APSFL STB ( 9
C:65:EE:6E:70:A6 )._http._tcp.local., (Cache flush) SRV Android.local.:3456 0 0, (Cache flush) PTR Android.local., (Cache flush) PTR And
roid.local., (Cache flush) A 192.168.55.101, (Cache flush) AAAA fe80::9e65:eff:fe6e:70a6 (396)
^C12:56:19.645409 IP6 fe80::9e65:eff:fe6e:70a6.mdns > ff02::fb.mdns: 0*- [0q] 8/0/4 (Cache flush) TXT "", PTR _http._tcp.local., PTR AP
SFL STB ( 9C:65:EE:6E:70:A6 )._http._tcp.local., (Cache flush) SRV Android.local.:3456 0 0, (Cache flush) PTR Android.local., (Cache flu
sh) PTR Android.local., (Cache flush) A 192.168.55.101, (Cache flush) AAAA fe80::9e65:eff:fe6e:70a6 (396)

2 packets captured
10 packets received by filter
0 packets dropped by kernel
user@teja-b191143cs:~$ sudo tcpdump -D
sudo: unable to resolve host teja-b191143cs: Name or service not known
1.enp2s0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.lxcr0 [Up, Disconnected]
5.wlp3s0 [Wireless, Not associated]
6.bluetooth0 (Bluetooth adapter number 0) [Wireless, Association status unknown]
7.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
8.nflog (Linux netfilter log (NFLOG) interface) [none]
9.nfqueue (Linux netfilter queue (NFOQUEUE) interface) [none]
```

Ex: sudo tcpdump -n host 142.250.182.206

To capture packets related to Specific host

Ex: sudo tcpdump -n src host 192.168.55.104 : packets from source host

sudo tcpdump -n dst port 80 : all packets to port 80

8. netstat/ss

netstat is a command tool which displays network connections for TCP/UDP and stats for Interfaces, Network protocols, routing tables, etc. ss replaces netstat. ss command tool which dumps socket stats and displays information similarly but it is faster than netstat.

With ss, we get detailed information about how Linux is communicating with othermachines, networks, details about network stats, network protocols, linux socket connections. So, using this information, it's easy to troubleshoot network issues.

- Ex: ss : Displays all connections
- Ex: ss -a : Displays non listening connections
- Ex: ss -l : Displays current listening connections
- Ex: ss -t : Displays TCP connections
- Ex: ss -u : Displays UDP connections
- Ex: ss -x : Displays UNIX connections
- Ex: ss -s : Displays summary stats
- Ex: ss -t -r state established : Displays sockets by state
- Ex: ss -a dst 192.168.1.1 : Displays connections to specific address

A listening connection means the socket is waiting for connection. A non listening socket implies the connection is already made.

```

Activities Applications Terminal Sun Jan 16 1:14:16 PM user@teja-b191143cs: ~ 13.37kb/s ↓ 460.9b/s ↑ 82 %
user@teja-b191143cs:~$ ss -t
State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
ESTAB 0 0 192.168.55.104:41208 157.240.237.60:https
ESTAB 0 0 192.168.55.104:53104 18.67.153.78:https
ESTAB 0 0 192.168.55.104:43266 140.82.112.26:https
CLOSE-WAIT 78 0 192.168.55.104:40658 107.21.16.69:https
ESTAB 0 0 192.168.55.104:56190 172.217.160.165:https
ESTAB 0 0 192.168.55.104:48558 157.240.16.52:https
ESTAB 0 0 192.168.55.104:54930 13.224.193.84:https
ESTAB 0 0 192.168.55.104:40410 172.217.194.188:5228
ESTAB 0 0 192.168.55.104:59548 52.25.64.13:https
user@teja-b191143cs:~$ ss -u
Recv-Q Send-Q Local Address:Port Peer Address:Port Process
0 0 192.168.55.104:36075 142.250.192.138:https
0 0 192.168.55.104:36171 142.251.10.189:https
0 0 192.168.55.104:enp2s0:bootpc 192.168.55.1:bootps
0 0 192.168.55.104:59720 216.58.196.74:https
user@teja-b191143cs:~$ ss -a dst 192.168.55.104
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
user@teja-b191143cs:~$ ss -s
Total: 1383
TCP: 30 (estab 7, closed 11, orphaned 0, timewait 0)

Transport Total IP IPv6
RAW 1 0 1
UDP 16 14 2
TCP 19 16 3
INET 36 30 6
FRAG 0 0 0

```

user@teja-b191143cs:~\$ ss -p
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

```

Activities Applications Terminal Sun Jan 16 1:14:27 PM user@teja-b191143cs: ~ 0b/s ↓ 0b/s ↑ 82 %
user@teja-b191143cs:~$ ss -p
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
udp ESTAB 0 0 sers:(("opera",pid=7242,fd=81)) 192.168.55.104:36075 142.250.192.138:https
udp ESTAB 0 0 sers:(("opera",pid=7242,fd=71)) 192.168.55.104:36171 142.251.10.189:https
udp ESTAB 0 0 sers:(("opera",pid=7242,fd=24)) 192.168.55.104:44375 172.217.27.206:https
udp ESTAB 0 0 sers:(("opera",pid=7242,fd=36)) 192.168.55.104:enp2s0:bootpc 192.168.55.1:bootps
udp ESTAB 0 0 sers:(("opera",pid=7242,fd=36)) 192.168.55.104:37021 142.251.42.10:https
udp ESTAB 0 0 sers:(("opera",pid=7242,fd=36)) 192.168.55.104:54075 8.8.8.8:domain
tcp CLOSING 1 1 192.168.55.104:enp2s0:58968 35.232.111.17:http
tcp ESTAB 0 0 sers:(("whatsie",pid=3572,fd=80)) 192.168.55.104:41208 157.240.237.60:https
tcp SYN-SENT 0 1 sers:(("opera_autoupdat",pid=19833,fd=11)) 192.168.55.104:47742 37.228.108.132:https
tcp ESTAB 0 0 sers:(("brave",pid=4330,fd=33)) 192.168.55.104:53104 18.67.153.78:https
tcp ESTAB 0 0 sers:(("opera",pid=7242,fd=44)) 192.168.55.104:43266 140.82.112.26:https
tcp ESTAB 0 0 sers:(("opera",pid=7242,fd=40)) 192.168.55.104:56190 172.217.160.165:https
tcp ESTAB 0 0 sers:(("brave",pid=4330,fd=28)) 192.168.55.104:54930 13.224.193.84:https
tcp ESTAB 0 0 sers:(("opera",pid=7242,fd=28)) 192.168.55.104:40410 172.217.194.188:5228
tcp ESTAB 0 0 sers:(("brave",pid=4330,fd=31)) 192.168.55.104:59548 52.25.64.13:https
user@teja-b191143cs:~$ |

```

9. dstat

dstat is a tool that is used to retrieve information or statistics from components of the system such as network connections, IO devices, or CPU, etc. It is generally used by system administrators to retrieve a handful of information about the above-mentioned components of the system. It itself performs like vmstat, netstat, etc. By using this tool

one can even see the throughput for block devices that make up a single filesystem or storage system.

Install it by : sudo apt install dstat

Ex: dstat --vmstat

To display information displayed by vmstat. It displays process and memory stats.

Ex: dstat

The output indicates :

CPU Stats: CPU usage by user, system processes and number of idle processes, and Number of waiting processes, hardware and software interrupts.

Disk Stats: Total number of read and write operations on the disk.

Network Stats: Total amount of Bytes received and sent on network interfaces.

Paging Stats: Number of times information is copied into and moved out of memory.

System Stats: Number of interrupts and context switches.

```
Activities Applications Terminal Sun Jan 16 1:21:37 PM user@teja-b191143cs: ~
user@teja-b191143cs:~$ 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
10 3 87 0 0| 551k 462k| 0 0| 177B 18k| 1522 3229
 6 2 92 0 0| 0 296k| 0 0| 0 0| 1109 2831
 7 2 92 0 0| 0 464k| 0 0| 0 0| 1124 2794
total-cpu-usage-- -dsk/total- -net/total- ---paging-->
usr sys idl wai stl|read writ|recv send|in out|>
10 3 87 0 0| 24 0| 0 0| 0 0| >
 8 3 90 0 0| 280 0| 0 0| 0 0| >
12 3 85 0 0| 0 0| 0 0| 0 0| >
 6 2 91 0 0| 200 0| 0 0| 0 0| >
 5 3 92 0 0| 0 0| 530B 66B| 0 0| >
 7 2 91 0 0| 376k 6145B 5030B| 0 0| 0 0| >
 5 2 93 0 0| 0 1047B 75B| 0 0| 0 0| >
 6 1 93 0 0| 272k 66B 268B| 0 0| 0 0| >
 6 1 93 0 0| 0 963B 0| 0 0| 0 0| >
 6 2 92 0 0| 0 168k 590B 334B| 0 0| 0 0| >
 8 1 91 0 0| 0 16k 66B 66B| 0 0| 0 0| >
 6 1 93 0 0| 0 0 75B| 0 0| 0 0| >
 7 2 92 0 0| 0 1192B 375B| 0 0| 0 0| >
 5 1 94 0 0| 0 4378B 3213B| 0 0| 0 0| >
 5 2 92 1 0| 0 1008k 694B 1144B| 0 0| 0 0| >
 6 1 92 0 0| 0 360k 237B 341B| 0 0| 0 0| >
 9 2 89 0 0| 0 160k 0 0| 0 0| 0 0| >
 7 2 91 0 0| 0 0 0| 0 0| 0 0| >
10 5 85 0 0| 0 56k 0 0| 0 0| 0 0| >
15 6 79 0 0| 72k 8768B 218B 96B| 0 4248B| >[IA
15 4 81 0 0| 0 168k 0 0| 0 0| 0 0| >C
14 4 82 0 0| 0 0 0| 0 0| 0 0| >C
user@teja-b191143cs:~$ |
```

CPU Stats: CPU usage by user, system processes and number of idle processes, and Number of waiting processes, hardware and software interrupts.

Disk Stats: Total number of read and write operations on the disk.

Network Stats: Total amount of Bytes received and sent on network interfaces.

Paging Stats: Number of times information is copied into and moved out of memory.

System Stats: Number of interrupts and context switches.

10. ifstat

As dstat, iostat, vmstat displays stats regarding the components of System. ifstat displays

network interface statistics. This tool keeps records of the previous data files and displays

differences between last and current calls.

Install it using : **\$sudo apt install ifstat**

Ex: ifstat

```
user@teja-b191143cs:~$ ifstat
  enp2s0          lxcbr0
KB/s in KB/s out KB/s in KB/s out
  2.34      0.16    0.00      0.00
  0.87      0.00    0.00      0.00
  0.00      0.06    0.00      0.00
  0.93      0.00    0.00      0.00
  0.00      0.00    0.00      0.00
  0.00      0.00    0.00      0.00
  0.13      0.15    0.00      0.00
^C
user@teja-b191143cs:~$ ifstat
  enp2s0          lxcbr0
KB/s in KB/s out KB/s in KB/s out
  0.00      0.00    0.00      0.00
  0.16      0.07    0.00      0.00
  0.00      0.00    0.00      0.00
  0.58      0.33    0.00      0.00
  0.06      0.00    0.00      0.00
  1.18  get  0.00    0.00      0.00
^C
user@teja-b191143cs:~$ | e network downloader which is used to download files from the
server even when the user has not logged on to the system and it can work in
the background without hindering the current process. With Wget, you can download
files using HTTP, HTTPS, and FTP protocols. Wget provides a number of options
allowing you to download multiple files, resume downloads, limit the bandwidth,
recursive downloads, download in the background, mirror a website, and much more.
```



11. wget

Wget is the non-interactive network downloader which is used to download files from the server even when the user has not logged on to the system and it can work in the background without hindering the current process. With Wget, you can download files using HTTP, HTTPS, and FTP protocols. Wget provides a number of options allowing you to download multiple files, resume downloads, limit the bandwidth, recursive downloads, download in the background, mirror a website, and much more.

Install it using : **\$sudo apt install wget**

Ex: wget [options] [url]

Ex: wget google.com

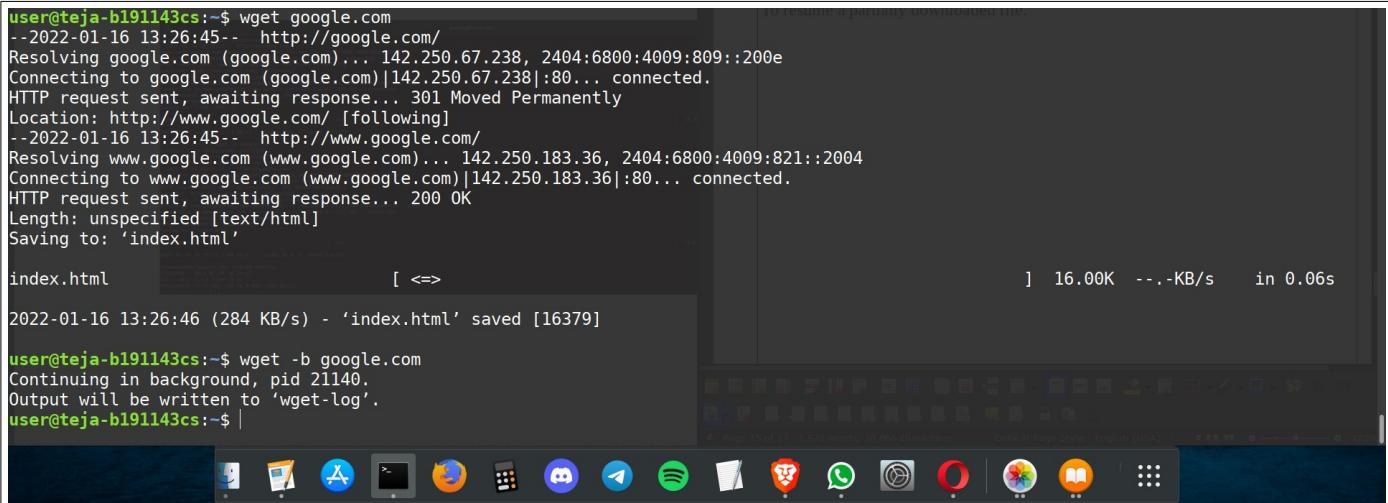
Ex: wget -b google.com

To download the file in background

Ex: wget google.com -o/path/filename.txt

To overwrite the log file of wget command.Ex: wget -c google.com

To resume a partially downloaded file.



```
user@teja-b191143cs:~$ wget google.com
--2022-01-16 13:26:45-- http://google.com/
Resolving google.com (google.com)... 142.250.67.238, 2404:6800:4009:809::200e
Connecting to google.com (google.com)|142.250.67.238|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2022-01-16 13:26:45-- http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.183.36, 2404:6800:4009:821::2004
Connecting to www.google.com (www.google.com)|142.250.183.36|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

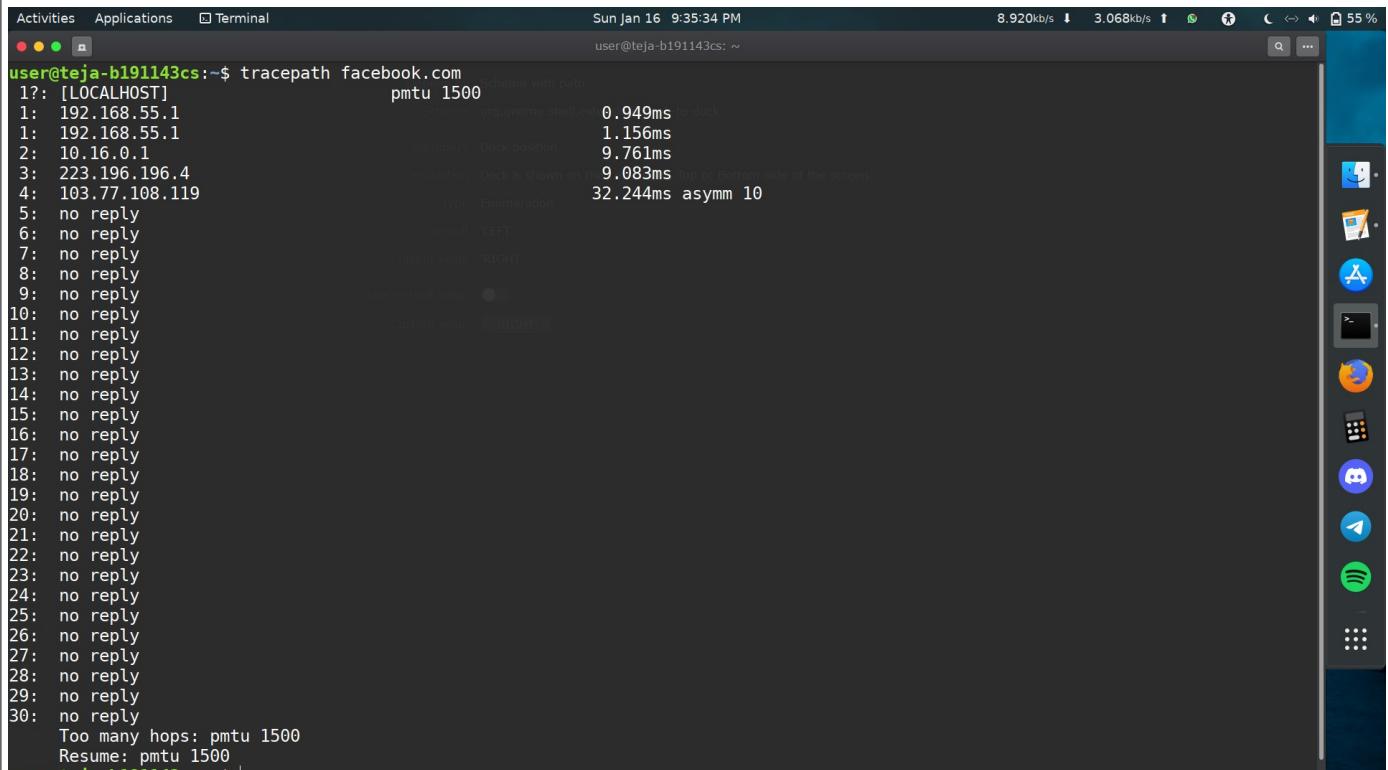
index.html                                              [ <=> ]   16.00K  --.-KB/s  in 0.06s

2022-01-16 13:26:46 (284 KB/s) - 'index.html' saved [16379]

user@teja-b191143cs:~$ wget -b google.com
Continuing in background, pid 21140.
Output will be written to 'wget-log'.
user@teja-b191143cs:~$
```

12. tracepath

Tracepath command in Linux is used to traces path to destination discovering MTU along this path. It uses UDP port or some random port. It is similar to traceroute, but it does not require superuser privileges and has no fancy options.



```
Activities Applications Terminal Sun Jan 16 9:35:34 PM 8.920kb/s 3.068kb/s user@teja-b191143cs:~
```

```
user@teja-b191143cs:~$ tracepath facebook.com
1?: [LOCALHOST] pmtu 1500
1: 192.168.55.1
1: 192.168.55.1
2: 10.16.0.1
3: 223.196.196.4
4: 103.77.108.119
5: no reply
6: no reply
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 1500
Resume: pmtu 1500
user@teja-b191143cs:~$ |
```