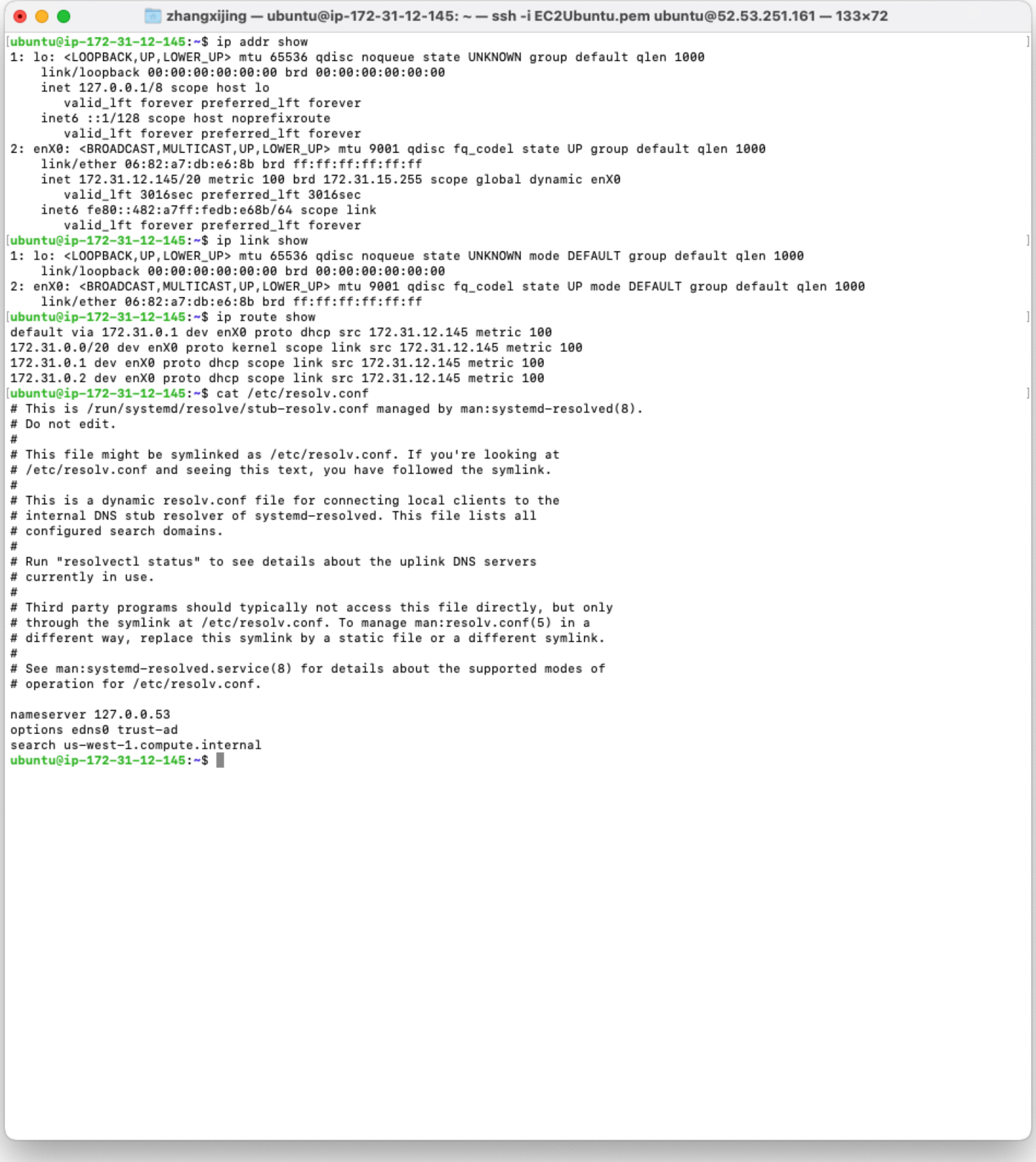
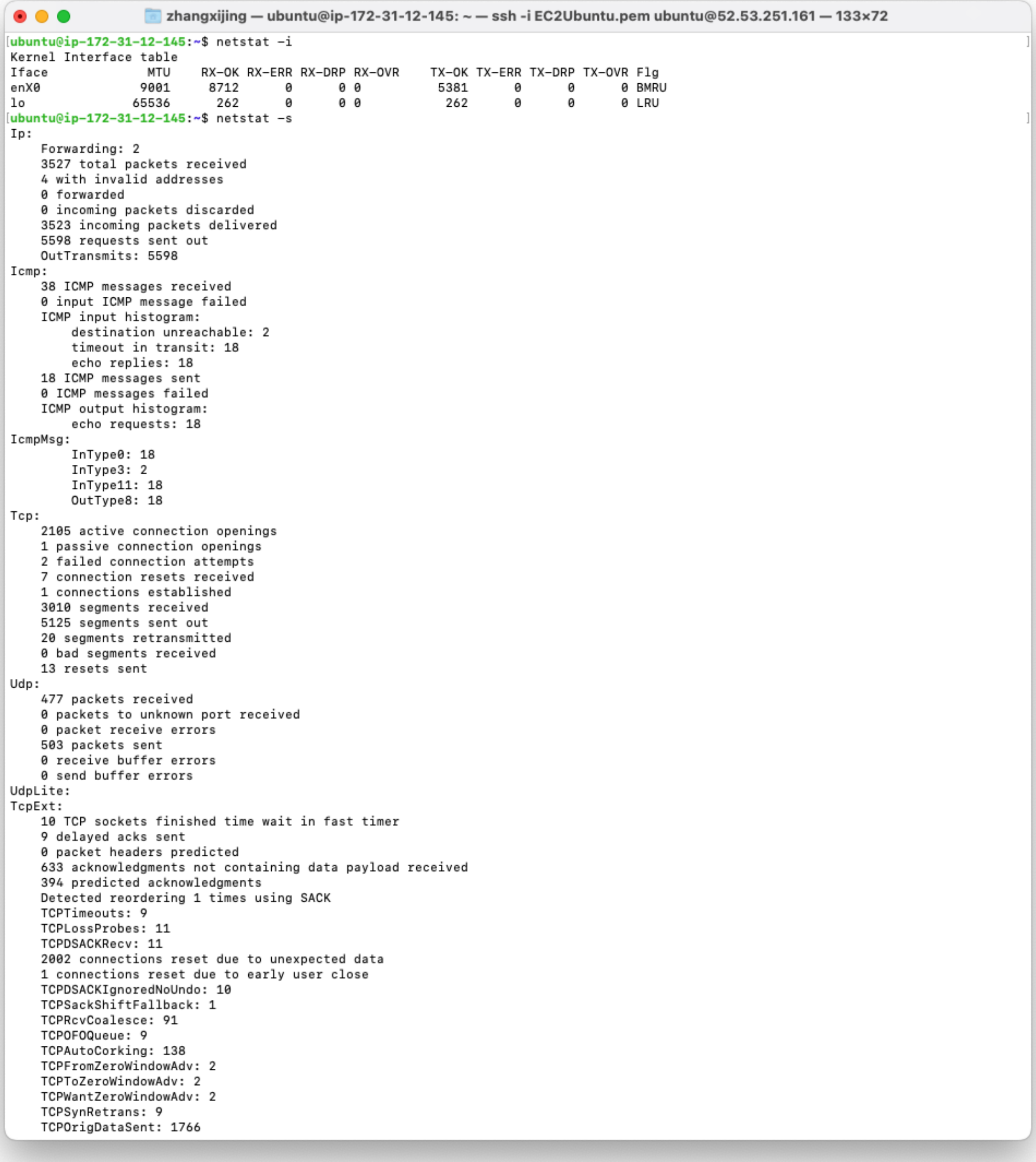
CSYE 6225: Network Structure & Cloud Computing

Assignment #2: Linux Networking Commands Report


zhangxijing — ubuntu@ip-172-31-12-145: ~ — ssh -i EC2Ubuntu.pem ubuntu@52.53.251.161 — 133×72

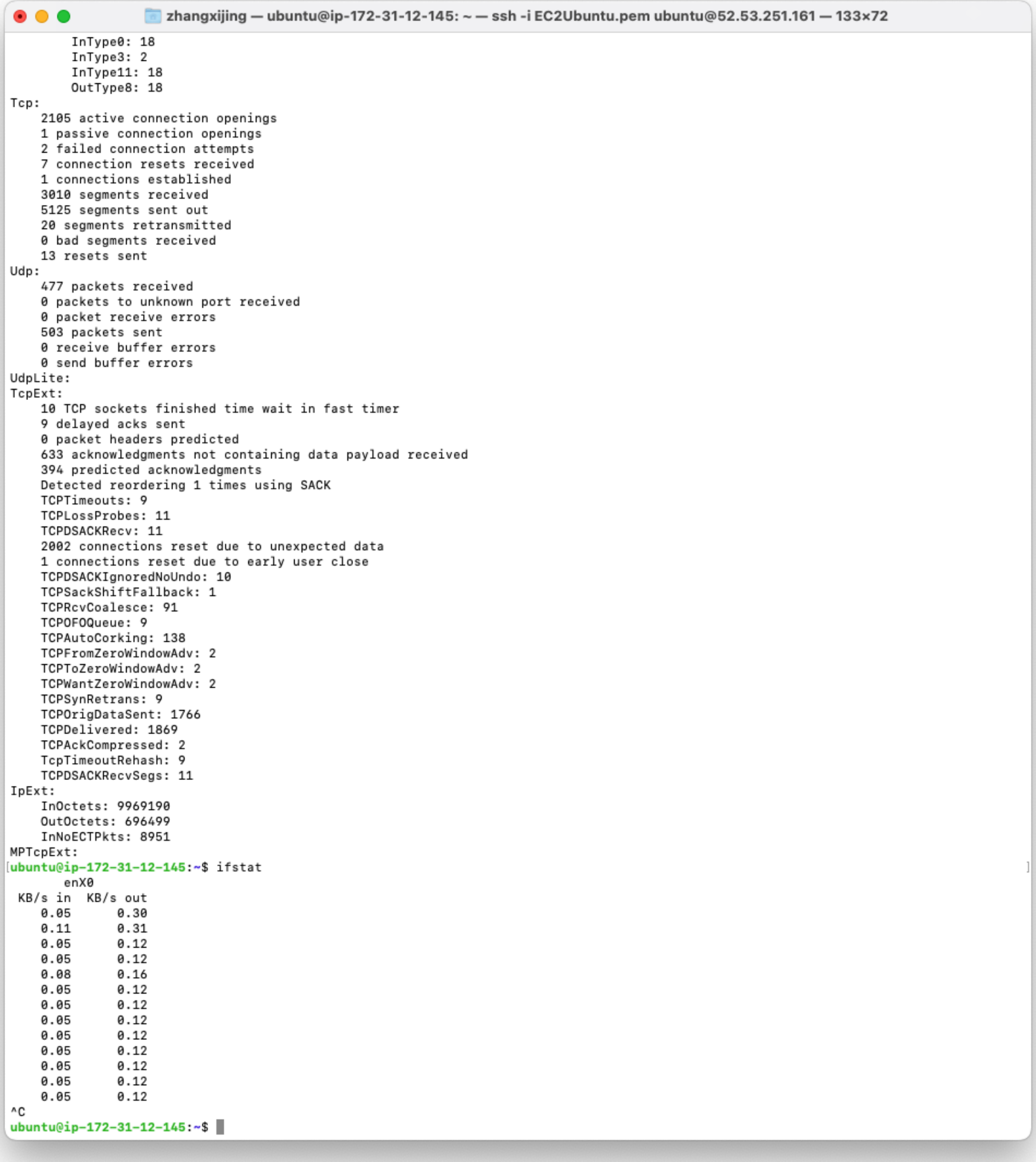
```
ubuntu@ip-172-31-12-145:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 06:82:a7:db:e6:8b brd ff:ff:ff:ff:ff:ff
    inet 172.31.12.145/20 metric 100 brd 172.31.15.255 scope global dynamic enX0
       valid_lft 3016sec preferred_lft 3016sec
    inet6 fe80::482:a7ff:fedb:e68b/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ip-172-31-12-145:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 06:82:a7:db:e6:8b brd ff:ff:ff:ff:ff:ff
ubuntu@ip-172-31-12-145:~$ ip route show
default via 172.31.0.1 dev enX0 proto dhcp src 172.31.12.145 metric 100
172.31.0.0/20 dev enX0 proto kernel scope link src 172.31.12.145 metric 100
172.31.0.1 dev enX0 proto dhcp scope link src 172.31.12.145 metric 100
172.31.0.2 dev enX0 proto dhcp scope link src 172.31.12.145 metric 100
ubuntu@ip-172-31-12-145:~$ cat /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search us-west-1.compute.internal
ubuntu@ip-172-31-12-145:~$
```

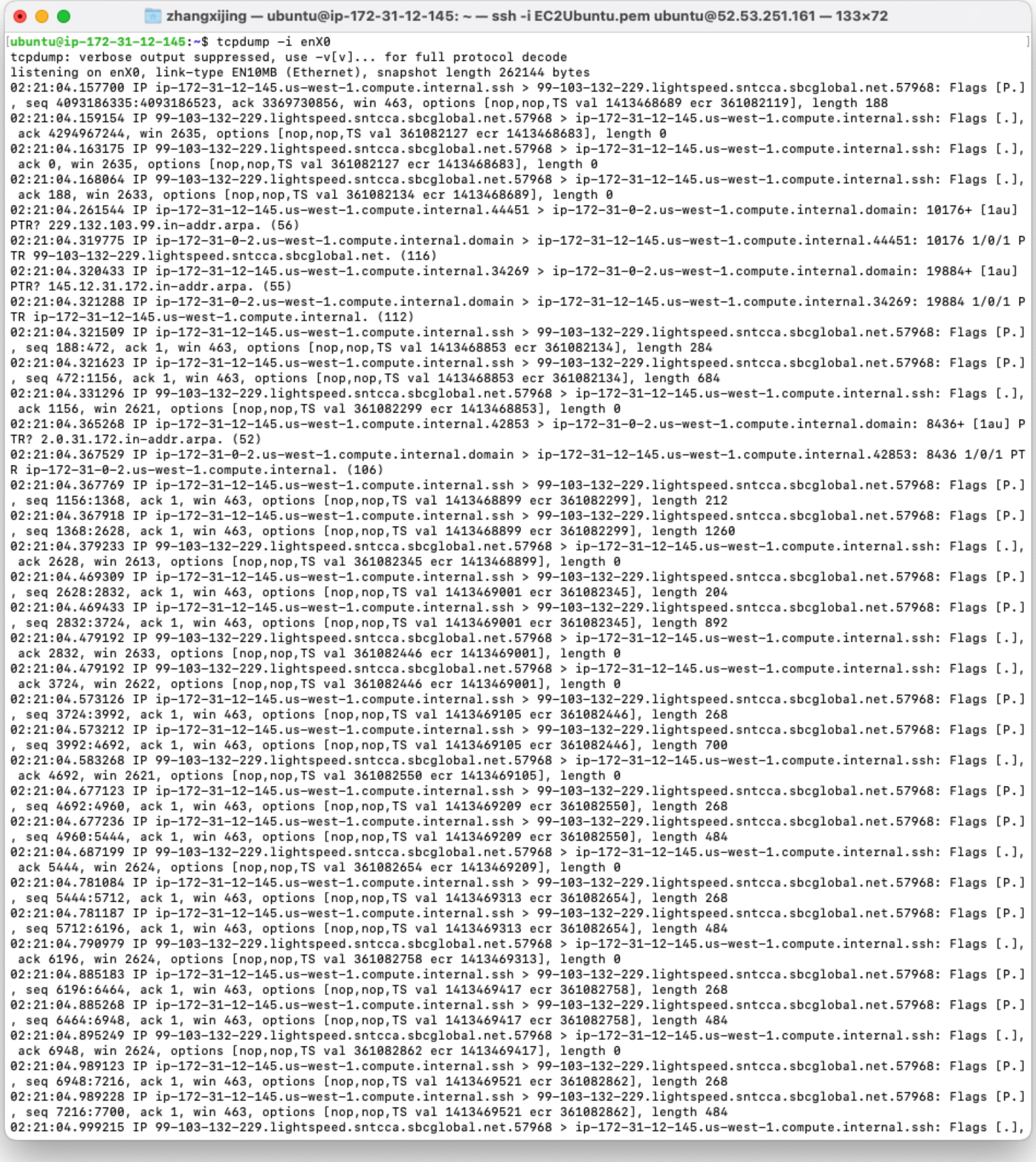


zhangxijing — ubuntu@ip-172-31-12-145: ~ — ssh -i EC2Ubuntu.pem ubuntu@52.53.251.161 — 133×72

```
ubuntu@ip-172-31-12-145:~$ netstat -i
Kernel Interface table
Iface             MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enX0             9001     8712      0      0 0          5381      0      0      0 BMRU
lo              65536      262      0      0 0           262      0      0      0 LRU
ubuntu@ip-172-31-12-145:~$ netstat -s
Ip:
    Forwarding: 2
    3527 total packets received
    4 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    3523 incoming packets delivered
    5598 requests sent out
    OutTransmits: 5598
Icmp:
    38 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 2
        timeout in transit: 18
        echo replies: 18
    18 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        echo requests: 18
IcmpMsg:
        InType0: 18
        InType3: 2
        InType11: 18
        OutType8: 18
Tcp:
    2105 active connection openings
    1 passive connection openings
    2 failed connection attempts
    7 connection resets received
    1 connections established
    3010 segments received
    5125 segments sent out
    20 segments retransmitted
    0 bad segments received
    13 resets sent
Udp:
    477 packets received
    0 packets to unknown port received
    0 packet receive errors
    503 packets sent
    0 receive buffer errors
    0 send buffer errors
UdpLite:
TcpExt:
    10 TCP sockets finished time wait in fast timer
    9 delayed acks sent
    0 packet headers predicted
    633 acknowledgments not containing data payload received
    394 predicted acknowledgments
    Detected reordering 1 times using SACK
    TCPTimeouts: 9
    TCPLossProbes: 11
    TCPDSACKRecv: 11
    2002 connections reset due to unexpected data
    1 connections reset due to early user close
    TCPDSACKIgnoredNoUndo: 10
    TCPSackShiftFallback: 1
    TCPRcvCoalesce: 91
    TCPOFOQueue: 9
    TCPAutoCorking: 138
    TCPFromZeroWindowAdv: 2
    TCPToZeroWindowAdv: 2
    TCPWantZeroWindowAdv: 2
    TCPSynRetrans: 9
    TCPOrigDataSent: 1766
```

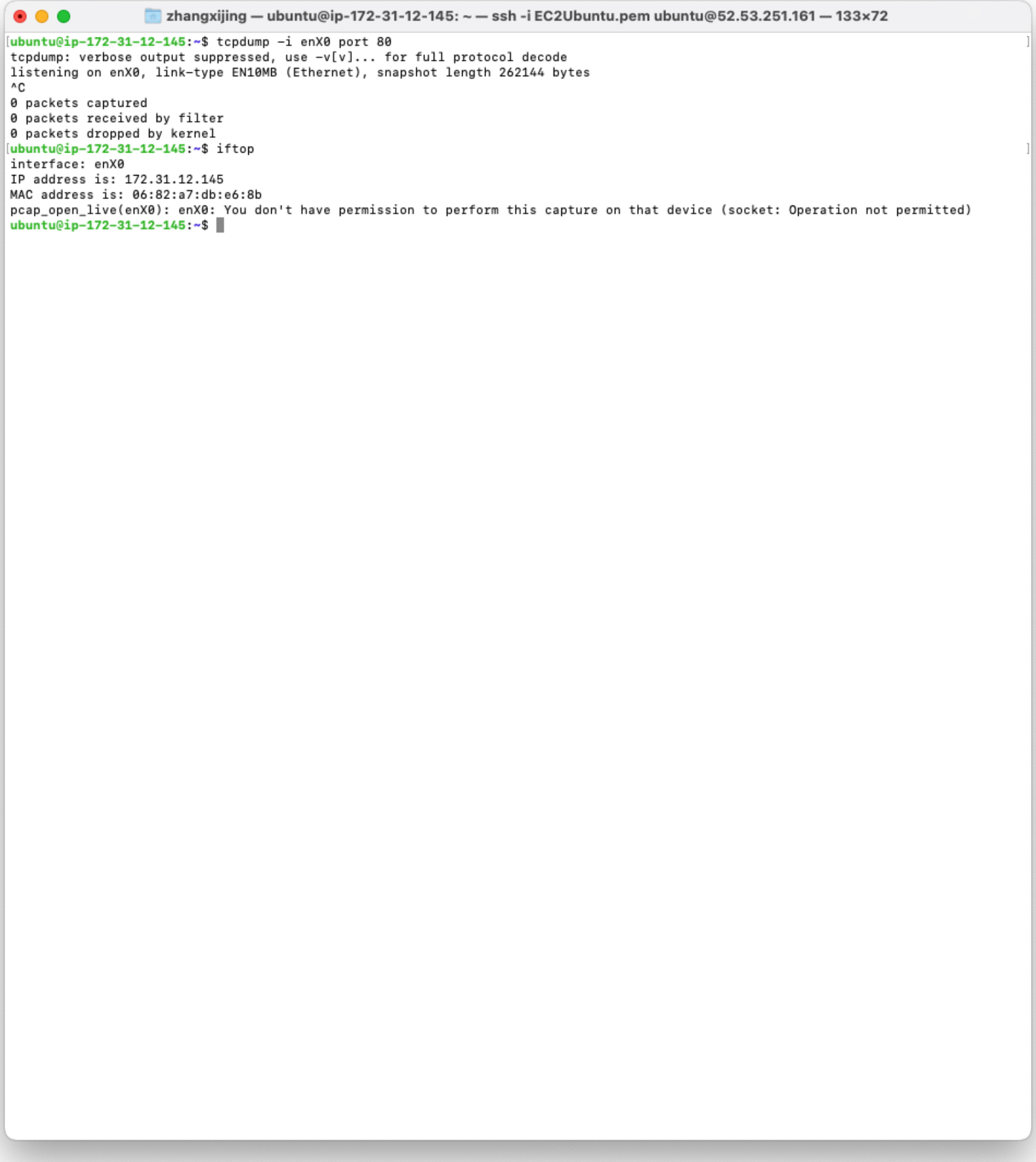

zhangxijing — ubuntu@ip-172-31-12-145: ~ — ssh -i EC2Ubuntu.pem ubuntu@52.53.251.161 — 133×72

```
        InType0: 18
        InType3: 2
        InType11: 18
        OutType8: 18
Tcp:
    2105 active connection openings
    1 passive connection openings
    2 failed connection attempts
    7 connection resets received
    1 connections established
    3010 segments received
    5125 segments sent out
    20 segments retransmitted
    0 bad segments received
    13 resets sent
Udp:
    477 packets received
    0 packets to unknown port received
    0 packet receive errors
    503 packets sent
    0 receive buffer errors
    0 send buffer errors
UdpLite:
TcpExt:
    10 TCP sockets finished time wait in fast timer
    9 delayed acks sent
    0 packet headers predicted
    633 acknowledgments not containing data payload received
    394 predicted acknowledgments
    Detected reordering 1 times using SACK
    TCPTimeouts: 9
    TCPLossProbes: 11
    TCPDSACKRecv: 11
    2002 connections reset due to unexpected data
    1 connections reset due to early user close
    TCPDSACKIgnoredNoUndo: 10
    TCPSackShiftFallback: 1
    TCPRcvCoalesce: 91
    TCPOFOQueue: 9
    TCPAutoCorking: 138
    TCPFromZeroWindowAdv: 2
    TCPToZeroWindowAdv: 2
    TCPWantZeroWindowAdv: 2
    TCPSynRetrans: 9
    TCPOrigDataSent: 1766
    TCPDelivered: 1869
    TCPAckCompressed: 2
    TcpTimeoutRehash: 9
    TCPDSACKRecvSegs: 11
IpExt:
    InOctets: 9969190
    OutOctets: 696499
    InNoECTPkts: 8951
MPTcpExt:
ubuntu@ip-172-31-12-145:~$ ifstat
       enX0
 KB/s in  KB/s out
    0.05      0.30
    0.11      0.31
    0.05      0.12
    0.05      0.12
    0.08      0.16
    0.05      0.12
    0.05      0.12
    0.05      0.12
    0.05      0.12
    0.05      0.12
    0.05      0.12
    0.05      0.12
    0.05      0.12
^C
ubuntu@ip-172-31-12-145:~$ 
```

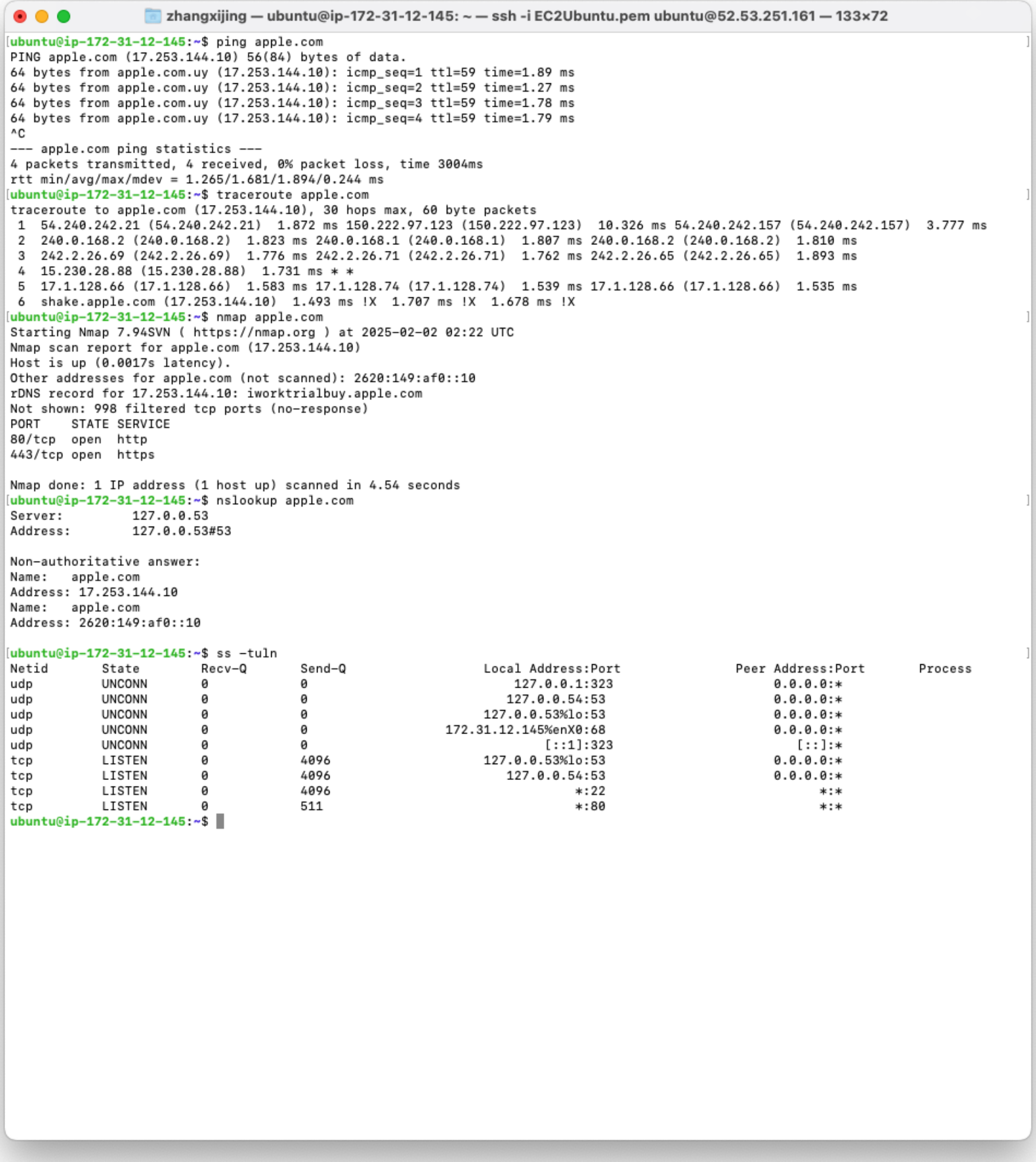


zhangxijing — ubuntu@ip-172-31-12-145: ~ — ssh -i EC2Ubuntu.pem ubuntu@52.53.251.161 — 133×72

```
ubuntu@ip-172-31-12-145:~$ tcpdump -i enX0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enX0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
02:21:04.157700 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 4093186335:4093186523, ack 3369730856, win 463, options [nop,nop,TS val 1413468689 ecr 361082119], length 188
02:21:04.159154 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
 ack 4294967244, win 2635, options [nop,nop,TS val 361082127 ecr 1413468683], length 0
02:21:04.163175 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
 ack 0, win 2635, options [nop,nop,TS val 361082127 ecr 1413468683], length 0
02:21:04.168064 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
 ack 188, win 2633, options [nop,nop,TS val 361082134 ecr 1413468689], length 0
02:21:04.261544 IP ip-172-31-12-145.us-west-1.compute.internal.44451 > ip-172-31-0-2.us-west-1.compute.internal.domain: 10176+ [1au]
PTR? 229.132.103.99.in-addr.arpa. (56)
02:21:04.319775 IP ip-172-31-0-2.us-west-1.compute.internal.domain > ip-172-31-12-145.us-west-1.compute.internal.44451: 10176 1/0/1 P
TR 99-103-132-229.lightspeed.sntcca.sbcglobal.net. (116)
02:21:04.320433 IP ip-172-31-12-145.us-west-1.compute.internal.34269 > ip-172-31-0-2.us-west-1.compute.internal.domain: 19884+ [1au]
PTR? 145.12.31.172.in-addr.arpa. (55)
02:21:04.321288 IP ip-172-31-0-2.us-west-1.compute.internal.domain > ip-172-31-12-145.us-west-1.compute.internal.34269: 19884 1/0/1 P
TR ip-172-31-12-145.us-west-1.compute.internal. (112)
02:21:04.321509 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 188:472, ack 1, win 463, options [nop,nop,TS val 1413468853 ecr 361082134], length 284
02:21:04.321623 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 472:1156, ack 1, win 463, options [nop,nop,TS val 1413468853 ecr 361082134], length 684
02:21:04.331296 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
 ack 1156, win 2621, options [nop,nop,TS val 361082299 ecr 1413468853], length 0
02:21:04.365268 IP ip-172-31-12-145.us-west-1.compute.internal.42853 > ip-172-31-0-2.us-west-1.compute.internal.domain: 8436+ [1au] P
TR? 2.0.31.172.in-addr.arpa. (52)
02:21:04.367529 IP ip-172-31-0-2.us-west-1.compute.internal.domain > ip-172-31-12-145.us-west-1.compute.internal.42853: 8436 1/0/1 PT
R ip-172-31-0-2.us-west-1.compute.internal. (106)
02:21:04.367769 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 1156:1368, ack 1, win 463, options [nop,nop,TS val 1413468899 ecr 361082299], length 212
02:21:04.367918 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 1368:2628, ack 1, win 463, options [nop,nop,TS val 1413468899 ecr 361082299], length 1260
02:21:04.379233 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
 ack 2628, win 2613, options [nop,nop,TS val 361082345 ecr 1413468899], length 0
02:21:04.469309 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 2628:2832, ack 1, win 463, options [nop,nop,TS val 1413469001 ecr 361082345], length 204
02:21:04.469433 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 2832:3724, ack 1, win 463, options [nop,nop,TS val 1413469001 ecr 361082345], length 892
02:21:04.479192 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
 ack 2832, win 2633, options [nop,nop,TS val 361082446 ecr 1413469001], length 0
02:21:04.479192 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
 ack 3724, win 2622, options [nop,nop,TS val 361082446 ecr 1413469001], length 0
02:21:04.573126 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 3724:3992, ack 1, win 463, options [nop,nop,TS val 1413469105 ecr 361082446], length 268
02:21:04.573212 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 3992:4692, ack 1, win 463, options [nop,nop,TS val 1413469105 ecr 361082446], length 700
02:21:04.583268 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
 ack 4692, win 2621, options [nop,nop,TS val 361082550 ecr 1413469105], length 0
02:21:04.677123 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 4692:4960, ack 1, win 463, options [nop,nop,TS val 1413469209 ecr 361082550], length 268
02:21:04.677236 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 4960:5444, ack 1, win 463, options [nop,nop,TS val 1413469209 ecr 361082550], length 484
02:21:04.687199 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
 ack 5444, win 2624, options [nop,nop,TS val 361082654 ecr 1413469209], length 0
02:21:04.781084 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 5444:5712, ack 1, win 463, options [nop,nop,TS val 1413469313 ecr 361082654], length 268
02:21:04.781187 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 5712:6196, ack 1, win 463, options [nop,nop,TS val 1413469313 ecr 361082654], length 484
02:21:04.790979 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
 ack 6196, win 2624, options [nop,nop,TS val 361082758 ecr 1413469313], length 0
02:21:04.885183 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 6196:6464, ack 1, win 463, options [nop,nop,TS val 1413469417 ecr 361082758], length 268
02:21:04.885268 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 6464:6948, ack 1, win 463, options [nop,nop,TS val 1413469417 ecr 361082758], length 484
02:21:04.895249 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
 ack 6948, win 2624, options [nop,nop,TS val 361082862 ecr 1413469417], length 0
02:21:04.989123 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 6948:7216, ack 1, win 463, options [nop,nop,TS val 1413469521 ecr 361082862], length 268
02:21:04.989228 IP ip-172-31-12-145.us-west-1.compute.internal.ssh > 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968: Flags [P.]
, seq 7216:7700, ack 1, win 463, options [nop,nop,TS val 1413469521 ecr 361082862], length 484
02:21:04.999215 IP 99-103-132-229.lightspeed.sntcca.sbcglobal.net.57968 > ip-172-31-12-145.us-west-1.compute.internal.ssh: Flags [.],
```


zhangxijing — ubuntu@ip-172-31-12-145: ~ — ssh -i EC2Ubuntu.pem ubuntu@52.53.251.161 — 133×72

```
ubuntu@ip-172-31-12-145:~$ tcpdump -i enX0 port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enX0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
ubuntu@ip-172-31-12-145:~$ iftop
interface: enX0
IP address is: 172.31.12.145
MAC address is: 06:82:a7:db:e6:8b
pcap_open_live(enX0): enX0: You don't have permission to perform this capture on that device (socket: Operation not permitted)
ubuntu@ip-172-31-12-145:~$ 
```


zhangxijing — ubuntu@ip-172-31-12-145: ~ — ssh -i EC2Ubuntu.pem ubuntu@52.53.251.161 — 133×72

```
ubuntu@ip-172-31-12-145:~$ ping apple.com
PING apple.com (17.253.144.10) 56(84) bytes of data.
64 bytes from apple.com.uy (17.253.144.10): icmp_seq=1 ttl=59 time=1.89 ms
64 bytes from apple.com.uy (17.253.144.10): icmp_seq=2 ttl=59 time=1.27 ms
64 bytes from apple.com.uy (17.253.144.10): icmp_seq=3 ttl=59 time=1.78 ms
64 bytes from apple.com.uy (17.253.144.10): icmp_seq=4 ttl=59 time=1.79 ms
^C
--- apple.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.265/1.681/1.894/0.244 ms
ubuntu@ip-172-31-12-145:~$ traceroute apple.com
traceroute to apple.com (17.253.144.10), 30 hops max, 60 byte packets
 1  54.240.242.21 (54.240.242.21)  1.872 ms 150.222.97.123 (150.222.97.123)  10.326 ms 54.240.242.157 (54.240.242.157)  3.777 ms
 2  240.0.168.2 (240.0.168.2)  1.823 ms 240.0.168.1 (240.0.168.1)  1.807 ms 240.0.168.2 (240.0.168.2)  1.810 ms
 3  242.2.26.69 (242.2.26.69)  1.776 ms 242.2.26.71 (242.2.26.71)  1.762 ms 242.2.26.65 (242.2.26.65)  1.893 ms
 4  15.230.28.88 (15.230.28.88)  1.731 ms * *
 5  17.1.128.66 (17.1.128.66)  1.583 ms 17.1.128.74 (17.1.128.74)  1.539 ms 17.1.128.66 (17.1.128.66)  1.535 ms
 6  shake.apple.com (17.253.144.10)  1.493 ms !X  1.707 ms !X  1.678 ms !X
ubuntu@ip-172-31-12-145:~$ nmap apple.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 02:22 UTC
Nmap scan report for apple.com (17.253.144.10)
Host is up (0.0017s latency).
Other addresses for apple.com (not scanned): 2620:149:af0::10
rDNS record for 17.253.144.10: iworktrialbuy.apple.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.54 seconds
ubuntu@ip-172-31-12-145:~$ nslookup apple.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   apple.com
Address: 17.253.144.10
Name:   apple.com
Address: 2620:149:af0::10

ubuntu@ip-172-31-12-145:~$ ss -tuln
Netid       State        Recv-Q       Send-Q                   Local Address:Port                Peer Address:Port       Process
udp         UNCONN       0            0                             127.0.0.1:323                      0.0.0.0:*
udp         UNCONN       0            0                            127.0.0.54:53                       0.0.0.0:*
udp         UNCONN       0            0                         127.0.0.53%lo:53                       0.0.0.0:*
udp         UNCONN       0            0                    172.31.12.145%enX0:68                       0.0.0.0:*
udp         UNCONN       0            0                                 [::1]:323                         [::]:*
tcp         LISTEN       0            4096                      127.0.0.53%lo:53                       0.0.0.0:*
tcp         LISTEN       0            4096                         127.0.0.54:53                       0.0.0.0:*
tcp         LISTEN       0            4096                                  *:22                             *:*
tcp         LISTEN       0            511                                   *:80                             *:*
ubuntu@ip-172-31-12-145:~$ █
```

1 Basic Network Information

Commands Used:

- ip addr show
  ip link show
  ip route show
  cat /etc/resolv.conf

Explanation: These commands display network interfaces, their statuses, routing tables, and DNS configuration.

2 Network Statistics

Commands Used:

-
  ```
  netstat -i
  netstat -s
  ifstat
  ```

Explanation: These commands show network statistics, errors, and interface activity.

3 Packet Analysis

Commands Used:

-
  ```
  sudo tcpdump -i enX0
  sudo tcpdump -i enX0 port 80
  iftop
  ```

Explanation: Captures live network traffic and displays bandwidth usage.

4 Network Troubleshooting

Commands Used:

-
  ```
  ping google.com
  traceroute google.com
  nmap google.com
  nslookup google.com
  ss -tuln
  ```

Explanation: These commands check connectivity, trace routes, scan ports, and resolve DNS.

5 Advanced Packet Analysis

Commands Used:

-
  ```
  sudo tcpdump -i enX0 -w capture.pcap
  tcpdump -r capture.pcap
  ```

Explanation: Captures and analyzes packets from a saved `.pcap` file.

Challenges Faced:

1. Permission issues with `tcpdump` - Resolved using `sudo`.

2. Missing tools (`netstat`, `traceroute`, `nmap`) - Installed via `apt`.