

Advanced Computer Networks

Rajath U
1MS22CY059

CSE (Cyber Security)
5th Semester

Date: 03/12/2024

Experiment 7

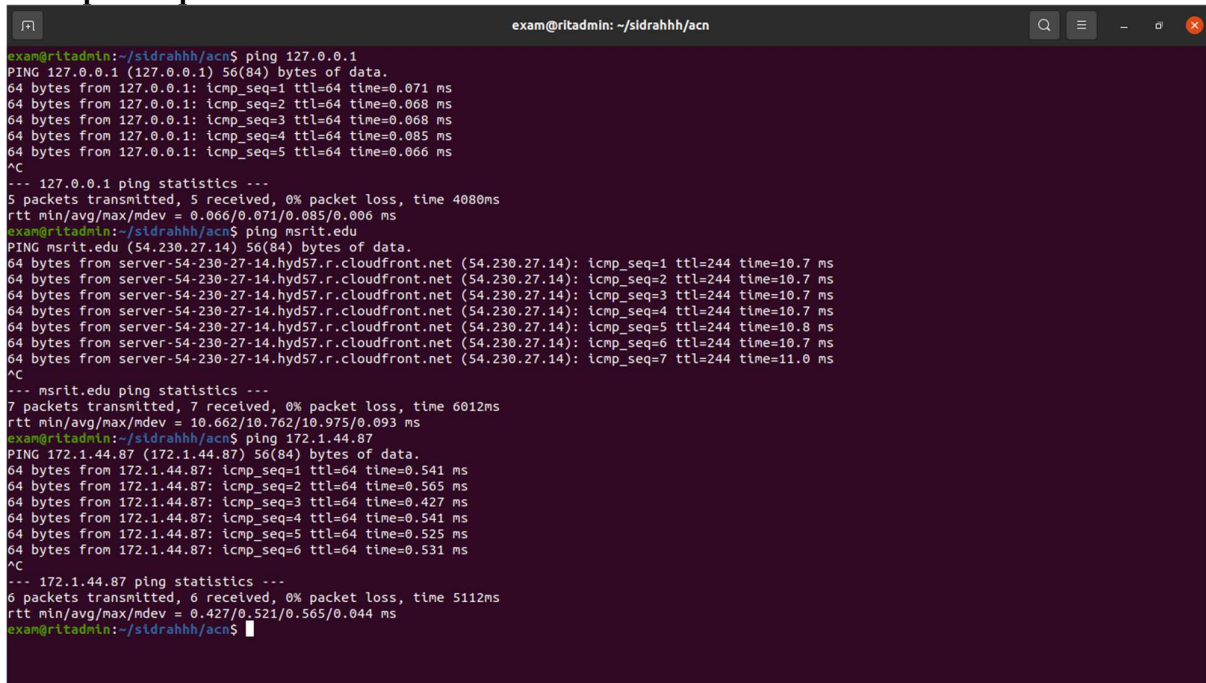
Aim: Execute the following network debugging tools with syntax and purpose:

1) ping

Syntax: ping [options] destination, where destination can be an IP address or a domain name

Purpose: The purpose of the ping command is to test the connectivity between two devices on a network. It checks whether a target host is reachable and measures the time it takes for packets to travel to the destination and back.

Example Output:



```
exam@ritadmin: ~/sidrahhh/acn$ 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=0.071 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.068 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=0.085 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.066 ms
^C
--- 127.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4080ms
rtt min/avg/max/mdev = 0.066/0.071/0.085/0.006 ms
exam@ritadmin:~/sidrahhh/acn$ ping msrit.edu
PING msrit.edu (54.230.27.14) 56(84) bytes of data.
64 bytes from server-54-230-27-14.hyds7.r.cloudfront.net (54.230.27.14): icmp_seq=1 ttl=244 time=10.7 ms
64 bytes from server-54-230-27-14.hyds7.r.cloudfront.net (54.230.27.14): icmp_seq=2 ttl=244 time=10.7 ms
64 bytes from server-54-230-27-14.hyds7.r.cloudfront.net (54.230.27.14): icmp_seq=3 ttl=244 time=10.7 ms
64 bytes from server-54-230-27-14.hyds7.r.cloudfront.net (54.230.27.14): icmp_seq=4 ttl=244 time=10.7 ms
64 bytes from server-54-230-27-14.hyds7.r.cloudfront.net (54.230.27.14): icmp_seq=5 ttl=244 time=10.8 ms
64 bytes from server-54-230-27-14.hyds7.r.cloudfront.net (54.230.27.14): icmp_seq=6 ttl=244 time=10.7 ms
64 bytes from server-54-230-27-14.hyds7.r.cloudfront.net (54.230.27.14): icmp_seq=7 ttl=244 time=11.0 ms
^C
--- msrit.edu ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6012ms
rtt min/avg/max/mdev = 10.662/10.762/10.975/0.093 ms
exam@ritadmin:~/sidrahhh/acn$ ping 172.1.44.87
PING 172.1.44.87 (172.1.44.87) 56(84) bytes of data.
64 bytes from 172.1.44.87: icmp_seq=1 ttl=64 time=0.541 ms
64 bytes from 172.1.44.87: icmp_seq=2 ttl=64 time=0.565 ms
64 bytes from 172.1.44.87: icmp_seq=3 ttl=64 time=0.427 ms
64 bytes from 172.1.44.87: icmp_seq=4 ttl=64 time=0.541 ms
64 bytes from 172.1.44.87: icmp_seq=5 ttl=64 time=0.525 ms
64 bytes from 172.1.44.87: icmp_seq=6 ttl=64 time=0.531 ms
^C
--- 172.1.44.87 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5112ms
rtt min/avg/max/mdev = 0.427/0.521/0.565/0.044 ms
exam@ritadmin:~/sidrahhh/acn$
```

Interpretation:

1. Pinging an IP Address (172.1.44.102)

Command: ping -c 4 172.1.44.102

Key Points:

64 bytes: Size of the response packet, including data and headers.

icmp_seq=1: Sequence number tracking each ping.

ttl=64: Time-To-Live, indicating remaining hops; starts typically at 64.

time=0.508 ms: Round-Trip Time (RTT), showing very low latency.

Interpretation:

Fast and Reliable: RTT around 0.5 ms with no packet loss suggests the IP is on the same local network or very close, ensuring quick and stable communication.

2. Pinging a Domain Name (msrit.edu)

Command: ping msrit.edu

Key Points:

PING msrit.edu (18.172.78.74): The domain resolves to IP 18.172.78.74 via DNS.

64 bytes: Size of the response packet.

icmp_seq=1: Sequence number tracking each ping.

ttl=244: Higher TTL suggests fewer hops or a higher initial TTL setting.

time=22.1 ms: RTT significantly higher than local IP, reflecting longer distance and more network devices.

Interpretation:

Moderate Latency with Stability: Consistent RTT around 22 ms indicates a stable connection to a remote server over the internet, involving multiple hops and greater distances.

Understanding Key Components

64 bytes: Size of the received packet, including headers.

icmp_seq: Tracks the order of ping requests and responses.

ttl (Time-To-Live): Prevents infinite packet looping; higher values indicate fewer hops.

time: Measures network latency; lower is better for local networks, higher for remote connections.

Why does the time value change?

Variations in RTT (time) occur due to:

Distance: Greater physical distances increase RTT.

Network Congestion: Busy networks can slow down packet transmission.

Routing Paths: Different routes can affect speed.

Server Load: Busy servers may respond slower.

Infrastructure Quality: Better networks handle packets more efficiently, reducing RTT variability.

In the outputs:

Local IP (172.1.44.102): Low and stable RTT (~0.5 ms) indicates a nearby or same-network device.

Domain (msrit.edu): Higher and consistent RTT (~22 ms) reflects internet-based communication with more hops and longer distances.

Key Takeaways

a) Direct IP Pinging:

Faster Responses: Ideal for testing local network devices.

Immediate Communication: No DNS resolution needed, leading to quicker contact.

b) Domain Name Pinging:

Requires DNS Lookup: Translates the domain to an IP before pinging.

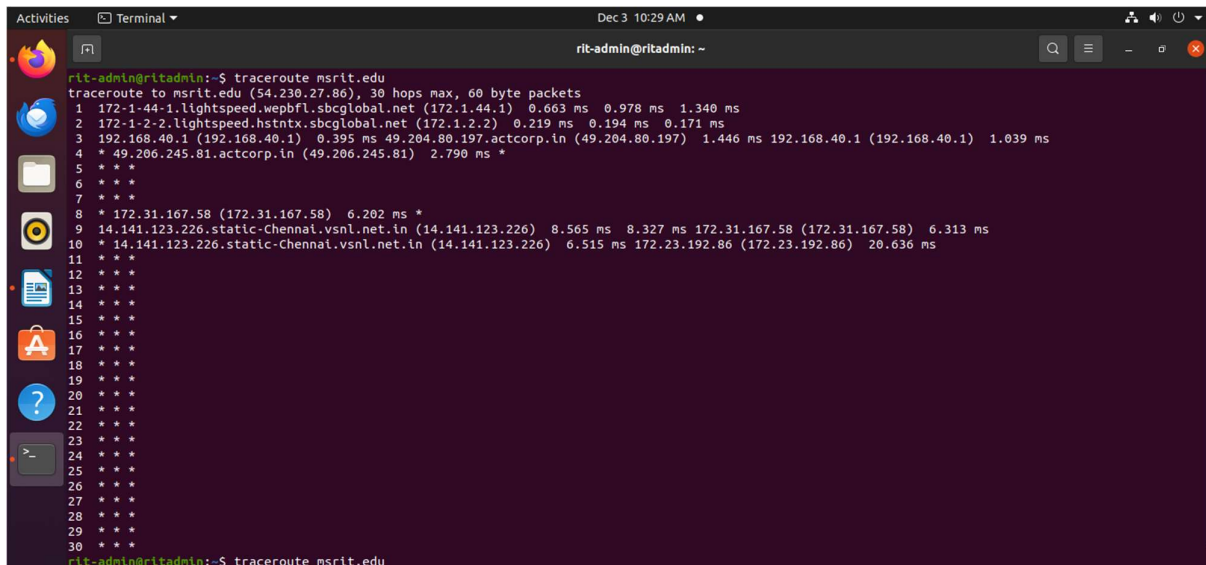
Higher Latency: Expected due to longer travel paths over the internet.

2) traceroute

Syntax: traceroute [destination]

Purpose: The traceroute command is a network diagnostic tool used to determine the path data packets take to reach a specific destination. It identifies each hop (router) along the path, measures the time it takes for data to travel between hops, and helps troubleshoot network delays, outages, or misconfigurations.

Example Output:



```
rit-admin@ritadmin:~$ traceroute msrit.edu
traceroute to msrit.edu (54.230.27.86), 30 hops max, 60 byte packets
 1 172-1-44-1.lightspeed.webpfl.sbcglobal.net (172.1.44.1) 0.663 ms 0.978 ms 1.340 ms
 2 172-1-2-2.lightspeed.hstntx.sbcglobal.net (172.1.2.2) 0.219 ms 0.194 ms 0.171 ms
 3 192.168.40.1 (192.168.40.1) 0.395 ms 49.204.80.197.actcorp.in (49.204.80.197) 1.446 ms 192.168.40.1 (192.168.40.1) 1.039 ms
 4 * 49.206.245.81.actcorp.in (49.206.245.81) 2.790 ms *
 5 * * *
 6 * * *
 7 * * *
 8 * 172.31.167.58 (172.31.167.58) 6.202 ms *
 9 14.141.123.226.static-Chennai.vsnl.net.in (14.141.123.226) 8.565 ms 8.327 ms 172.31.167.58 (172.31.167.58) 6.313 ms
10 * 14.141.123.226.static-Chennai.vsnl.net.in (14.141.123.226) 6.515 ms 172.23.192.86 (172.23.192.86) 20.636 ms
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

Interpretation:

The key parameters of the traceroute command are:

- Destination: msrit.edu (54.230.27.180)
- Maximum hops: 30 hops
- Packet size: 60 byte packets

It works by sending packets with progressively increasing time-to-live (TTL) values. Each router along the path decrements the TTL by 1. When TTL reaches 0, the router returns an ICMP "Time Exceeded" message, and the round-trip time (RTT) is recorded.

Round-Trip Time (RTT): This is the time it takes for a packet to go from the source to the destination and back. RTTs are measured in milliseconds (ms). If the RTT is consistently high or increasing significantly from one hop to another, it may indicate a bottleneck in the network.

Hop 1:

IP Address: 172.1.44.1

Round Trip Time (RTT): 0.603 ms, 0.978 ms, 1.340 ms

This is the first router on the network path, likely your local network gateway.

Hop 2:

IP Address: 172.1.2.2

RTT: 0.219 ms, 0.171 ms, 0.177 ms

This is the second router on the path, still within your local network.

Hop 3:

IP Address: 49.204.80.197

RTT: 1.446 ms

IP Address: 192.168.40.1

RTT: 1.039 ms

This hop appears to have two IP addresses reported, potentially indicating a load-balancing setup or a multi-homed router.

Hops 4-7:

All reported as * * *

This indicates that the traceroute was unable to receive a response from these hops. This could be due to network configuration, firewalls, or other issues that are preventing the ICMP packets used by traceroute from getting through.

Hop 8:

IP Address: 172.31.167.58

RTT: 0.202 ms

This hop was able to respond to the traceroute probes.

Observation:

The first few hops (1-3) show normal behavior, with low latency times around 1 ms, indicating the packet is moving efficiently through the local network.

The asterisks starting from hop 4 suggest that the traceroute is unable to reach those routers, possibly due to network configuration, firewall rules, or other issues.

The successful responses at hops 8-10 show that the packet is still making progress, but the high latency times at hop 10 (20 ms) could indicate a potential bottleneck or issue on the network path.

The inability to complete the full trace to the final destination (msrit.edu) suggests there may be some network problems or configuration preventing the traceroute from fully mapping the end-to-end path.

3) netstat/ss

Syntax: netstat [options], where options can be:

- a: Display all connections (both listening and non-listening).
- t: Show TCP connections.
- u: Show UDP connections.
- n: Show numerical addresses and port numbers instead of resolving them to hostnames.
- p: Show the PID and program name for each connection.
- r: Display the routing table.
- i: Display network interfaces statistics.
- s: Show per-protocol statistics.

Purpose: The netstat command is a network utility used to display detailed network statistics and diagnostics. It provides information about active network connections, listening ports, routing tables, network interfaces, and protocol statistics. It is widely used for troubleshooting network issues, monitoring traffic, and analyzing system security.

Example Output:

```
exam@ritadmin: ~/sidrahhh/acn$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 172-1-44-102.ligh:57946 172.64.155.209:https    ESTABLISHED
tcp        0      0 172-1-44-102.ligh:52060 172.64.155.209:https    ESTABLISHED
tcp        0      0 172-1-44-102.ligh:56522 93.243.107.34.bc.:https ESTABLISHED
udp        0      0 172-1-44-102.lig:bootpc 172-1-2-10.light:bootps ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State       I-Node   Path
unix    2      [ ]      DGRAM      CONNECTED   42170    /run/user/1001/systemd/notify
unix    4      [ ]      DGRAM      CONNECTED   26687    /run/systemd/notify
unix    2      [ ]      DGRAM      CONNECTED   26701    /run/systemd/journal/syslog
unix   17      [ ]      DGRAM      CONNECTED   26711    /run/systemd/journal/dev-log
unix    8      [ ]      DGRAM      CONNECTED   26715    /run/systemd/journal/socket
unix    3      [ ]      STREAM     CONNECTED   30490    /run/dbus/system_bus_socket
unix    3      [ ]      STREAM     CONNECTED   41504
unix    3      [ ]      STREAM     CONNECTED   61728    /run/user/1001/pulse/native
unix    3      [ ]      STREAM     CONNECTED   35837    /run/systemd/journal/stdout
unix    2      [ ]      DGRAM
unix    3      [ ]      STREAM     CONNECTED   45583
unix    3      [ ]      STREAM     CONNECTED   45550
unix    3      [ ]      STREAM     CONNECTED   42174
unix    3      [ ]      STREAM     CONNECTED   51638    /run/user/1001/bus
unix    3      [ ]      STREAM     CONNECTED   40670
unix    3      [ ]      STREAM     CONNECTED   68059
unix    3      [ ]      STREAM     CONNECTED   21499    /run/dbus/system_bus_socket
unix    3      [ ]      STREAM     CONNECTED   52641
unix    3      [ ]      STREAM     CONNECTED   48720
unix    3      [ ]      STREAM     CONNECTED   49253    /run/systemd/journal/stdout
unix    3      [ ]      STREAM     CONNECTED   35974
unix    3      [ ]      STREAM     CONNECTED   32539
unix    3      [ ]      STREAM     CONNECTED   18175    /run/systemd/journal/stdout
unix    3      [ ]      STREAM     CONNECTED   62362    /run/user/1001/bus
unix    3      [ ]      STREAM     CONNECTED   47831
unix    3      [ ]      STREAM     CONNECTED   44348
unix    3      [ ]      STREAM     CONNECTED   55116
unix    3      [ ]      STREAM     CONNECTED   27512
unix    3      [ ]      SEQPACKET  CONNECTED   66805
unix    3      [ ]      STREAM     CONNECTED   66691
```

Interpretation:

The netstat command provides information about active network connections, routing tables, interface statistics, and Unix domain sockets.

1. Active Internet Connections:

- Proto: The protocol used for the connection (TCP or UDP).
- Recv-Q: The count of bytes not copied by the user program connected to this socket. It's typically 0 unless there's congestion.
- Send-Q: The count of bytes not acknowledged by the remote host. It also tends to be 0 unless the connection is under heavy use.
- Local Address: The IP address and port number of your machine. For example, 172-1-44-102.ligh:36662 means your machine has a local IP of 172-1-44-102.ligh and is using port 36662.
- Foreign Address: The remote IP address and port number of the connected peer. For example, 172.64.155.209:https means the remote host is 172.64.155.209 on port https (port 443).
- State: The current state of the connection (e.g., ESTABLISHED, LISTEN, CLOSE_WAIT). ESTABLISHED means the connection is open and data can be transmitted.

2. Active UNIX domain Sockets

- Proto: The protocol used for communication, here it's unix (Unix domain sockets).
- RefCnt: The reference count, which indicates how many active users (processes) are using this socket.
- Flags: Any flags associated with the socket (e.g., [] means no special flags are set).
- Type: The type of socket (DGRAM for Datagram or STREAM for stream-based communication).
- State: The state of the socket (e.g., CONNECTED, LISTEN).
- I-Node: The inode number associated with the socket (internal file system identifier).
- Path: The file system path of the Unix domain socket, typically found in /run.

The main parameters are:

a) Protocol (Proto):

- TCP: Transmission Control Protocol (connection-oriented, reliable).
- UDP: User Datagram Protocol (connectionless, unreliable).
- unix: Unix domain sockets (used for inter-process communication on the same machine).

b) Recv-Q / Send-Q:

These columns track the state of data waiting to be read (Recv-Q) or acknowledged (Send-Q). A value of 0 typically means the connection is stable and no data is stuck in the queues.

c) Local Address:

This shows the local IP address and port number used by the local machine for a connection. The port number is shown in numeric form (e.g., 36662), or sometimes by the service name (e.g., https).

d) Foreign Address:

- This shows the IP address and port of the remote peer in the connection. For example, 172.64.155.209:https means the connection is going to IP 172.64.155.209 on port 443.

e) State:

- LISTEN: The socket is waiting for incoming connections.
- ESTABLISHED: The connection is active and data can be transmitted.
- CLOSE_WAIT: The connection is in the process of being closed, waiting for the local side to finish closing.
- TIME_WAIT: The connection has been closed, and the system is waiting to ensure that the connection is fully terminated.

f) Unix Domain Sockets:

- These are for communication between processes on the same machine.
- DGRAM: A datagram socket, used for connectionless communication.
- STREAM: A stream socket, used for connection-based communication (similar to TCP).
- State: The state of the Unix socket (e.g., CONNECTED, LISTEN).

4) mtr

Syntax: mtr [destination]

Purpose: The mtr (My Traceroute) command is a powerful network diagnostic tool that combines the functionality of the ping and traceroute commands. It provides real-time analysis of the route packets take to reach a specific destination and includes statistics about packet loss and latency at each hop in the route.

Example Output:

```
ritadmin (172.1.44.87)
Keys: Help  Display mode  Restart statistics  Order of fields  quit

My traceroute  [v0.93]
2024-12-03T09:27:51+0530

Host
1. 172-1-44-1.lightspeed.webpfl.sbcglobal.net
2. 172-1-2-2.lightspeed.hstntx.sbcglobal.net
3. 49.204.80.197.actcorp.in
4. (waiting for reply)
5. (waiting for reply)
6. (waiting for reply)
7. broadband.actcorp.in
8. 99.83.69.114
9. 150.222.219.32
10. 150.222.219.47
11. (waiting for reply)
12. (waiting for reply)
13. (waiting for reply)
14. (waiting for reply)
15. (waiting for reply)
16. 15.230.251.4
17. server-18-161-246-50.maa50.r.cloudfront.net

Packets
Loss% Snt Last Avg Best Wrst StDev
0.0% 20 0.9 4.6 0.8 73.6 16.2
0.0% 20 0.3 0.3 0.3 0.3 0.0
0.0% 20 1.5 1.9 1.5 2.9 0.4
0.0% 20 6.2 6.2 6.1 7.0 0.2
0.0% 20 10.0 7.8 6.2 23.8 3.9
0.0% 20 9.3 8.3 6.4 17.3 2.8
0.0% 20 8.6 8.0 6.3 16.5 2.4
0.0% 19 7.4 6.6 6.5 7.4 0.2
0.0% 19 6.4 6.3 6.3 6.5 0.1

Ping Statistics (Last, Avg, Best, Wrst, StDev)
0.0% 20 0.9 4.6 0.8 73.6 16.2
0.0% 20 0.3 0.3 0.3 0.3 0.0
0.0% 20 1.5 1.9 1.5 2.9 0.4
0.0% 20 6.2 6.2 6.1 7.0 0.2
0.0% 20 10.0 7.8 6.2 23.8 3.9
0.0% 20 9.3 8.3 6.4 17.3 2.8
0.0% 20 8.6 8.0 6.3 16.5 2.4
0.0% 19 7.4 6.6 6.5 7.4 0.2
0.0% 19 6.4 6.3 6.3 6.5 0.1
```

Interpretation:

1. with domain name msrit.edu

Overview

The output shows the path taken by packets from the source (ritadmin) to a destination server (server-18-161-246-50.maa50.r.cloudfront.net). It lists each hop (intermediate router) in the path, measuring latency and packet loss for each one.

Key Sections

- Host Column: Displays the names or IP addresses of intermediate routers or hosts along the path.
 - For example:
 - 172-1-44-1.lightspeed.webpfl.sbcglobal.net: The first hop (likely the local gateway/router).
 - 49.204.80.197.actcorp.in: An intermediate hop on the route.
 - server-18-161-246-50.maa50.r.cloudfront.net: The final destination.
 - (waiting for reply): Indicates that no response was received from certain hops (e.g., hops 11–15).
- Loss%: Shows the percentage of packet loss at each hop.
 - In this case, there is 0% packet loss for the hops that responded, meaning no packets were dropped for these routers.
- Snt: The number of packets sent to each hop (usually 20 by default).
- Ping Statistics (Last, Avg, Best, Wrst, StDev):
 - Last: Latency (in milliseconds) for the most recent packet sent to the hop.
 - Avg: Average latency across all packets sent to that hop.
 - Best: Lowest latency observed for that hop.
 - Wrst: Highest latency observed for that hop.
 - StDev: Standard deviation of latency, showing variability in response times.
 - For example:
 - Hop 1 (172-1-44-1.lightspeed...):
 - Last = 0.9 ms, Avg = 4.6 ms, Best = 0.8 ms, Wrst = 73.6 ms, StDev = 16.2 ms.
 - Indicates a very stable connection at this hop with occasional spikes (worst-case latency at 73.6 ms).

Interpretation

- The path to the destination is relatively stable with no packet loss, but certain hops (e.g., hop 6) show slightly higher average latencies.
- Some intermediate hops are not responding (waiting for reply), which might be due to firewalls or configurations blocking ICMP responses. This does not necessarily indicate an issue.

2. with localhost ip

Overview

This is a simplified MTR output showing only the first hop (172-1-44-87.lightspeed.webpfl.sbcglobal.net), likely a local router or gateway.

Key Sections

- Host Column: Only one host is listed, which is the first hop in the path.
 - 172-1-44-87.lightspeed.webpfl.sbcglobal.net: Likely the local network router.
- Packet Statistics:
 - Loss% = 0.0%: No packet loss observed at this hop.
 - Snt = 8: Only 8 packets were sent in this test (compared to 20 in the previous run).
- Ping Statistics:
 - Last = 0.1 ms, Avg = 0.1 ms, Best = 0.1 ms, Wrst = 0.1 ms, StDev = 0.0 ms.
 - Indicates a highly stable and extremely fast response time to the local router.

Interpretation

- The connection to the local router is working perfectly with negligible latency, suggesting no issues at the initial stage of the network.

5) ifconfig

Syntax: ifconfig

Purpose: The ifconfig (interface configuration) command is used to configure and manage network interfaces in Unix-based operating systems like Linux. It is a part of the net-tools package and allows administrators to view and modify network interface settings.

Example Output:

```
exam@ritadmin: ~/sidrahhh/acn$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:b2:3b:e8:e7 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    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

eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.1.44.102 netmask 255.255.254.0 broadcast 172.1.45.255
    inet6 fe80::410a:1ce2:ebac:242a prefixlen 64 scopeid 0x20<link>
    ether d8:bb:c1:e6:01:db txqueuelen 1000 (Ethernet)
    RX packets 36970 bytes 27444457 (27.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14078 bytes 1772398 (1.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 16 memory 0xb1200000-b1220000

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 1116 bytes 113463 (113.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1116 bytes 113463 (113.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```


Interpretation:

The `ifconfig` command is used to configure and display information about network interfaces on a Unix-like operating system. It shows the network interfaces, their IP addresses, MAC addresses, transmission statistics, and various other parameters.

1. docker0 interface:

docker0: Name of the interface (created by Docker for container networking).

- flags=4099<UP,BROADCAST,MULTICAST>:
- UP: Indicates that the interface is up (active).
- BROADCAST: The interface supports broadcast communication (sending to all devices on a network).
- MULTICAST: The interface supports multicast communication (sending data to a specific group of devices).
- mtu 1500: Maximum Transmission Unit (MTU). This is the maximum size of a packet that can be transmitted on the network. 1500 is standard for Ethernet.
- inet 172.17.0.1: The IPv4 address of the interface.
- netmask 255.255.0.0: Subnet mask for the network. This determines which part of the IP address refers to the network and which part refers to the host. The 255.255.0.0 mask means the first 16 bits are the network portion.
- broadcast 172.17.255.255: The broadcast address for the network. This is used to send messages to all devices in the network (in this case, devices with the 172.17.* IP range).
- ether 02:42:b2:3b:e8:e7: The MAC (Media Access Control) address of the interface. It's a unique identifier for the network interface at the data link layer.
- txqueuelen 0: Transmission queue length, which is the number of packets to be queued for transmission. 0 suggests no queue, or it's using a default value.
- RX packets 0 bytes 0 (0.0 B): The number of received packets (RX), the total number of bytes received, and the total amount of data received.
- RX errors 0 dropped 0 overruns 0 frame 0: Statistics for received packets:
 - errors: Errors during reception.
 - dropped: Packets dropped due to system overload or buffer issues.
 - overruns: Packets received when the buffer was full.
 - frame: Frame errors.
- TX packets 0 bytes 0 (0.0 B): The number of transmitted packets (TX), the total number of bytes sent, and the total amount of data sent.
- TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0: Statistics for transmitted packets:
 - errors: Errors during transmission.
 - dropped: Packets dropped while sending.
 - overruns: Packets dropped due to buffer overrun.
 - carrier: Carrier errors (usually related to physical connection issues).
 - collisions: Network collisions, which happen when two devices transmit at the same time on the same network.

2. en01 interface:

eno1: Name of the Ethernet interface.

- flags=4163<UP,BROADCAST,RUNNING,MULTICAST>:
- RUNNING: The interface is up and operational.
- mtu 1500: The MTU value is the same as above (1500 bytes).
- inet 172.1.44.102: The IPv4 address of the interface.
- netmask 255.255.254.0: The subnet mask.
- broadcast 172.1.45.255: The broadcast address.
- inet6 fe80::410a:1ce2:ebac:242a: The IPv6 address of the interface.
- prefixlen 64: The prefix length for the IPv6 address (determines the network portion of the address).
- ether d8:bb:c1:e6:01:db: The MAC address of the Ethernet interface.
- txqueuelen 1000: Transmission queue length, set to 1000 for this interface.
- RX packets 36970 bytes 27444457 (27.4 MB): Total received packets and the amount of data received (27.4 MB).
- TX packets 14078 bytes 1772398 (1.7 MB): Total transmitted packets and data sent (1.7 MB).
- device interrupt 16 memory 0xb1200000-b1220000: Information about the device's interrupt number and memory range used for network processing.

3. Loopback interface (lo):

- lo: The loopback interface, used for internal communication within the host.
- flags=73<UP,LOOPBACK,RUNNING>: Indicates the interface is up, running, and specifically for loopback purposes.
- mtu 65536: The MTU is much higher than the typical Ethernet interface because the loopback interface can handle larger packets.
- inet 127.0.0.1: The IPv4 address of the loopback interface, commonly known as localhost.
- netmask 255.0.0.0: The netmask for the loopback network (this is standard for loopback addresses).
- inet6 ::1: The IPv6 address for the loopback interface, typically ::1 (the equivalent of 127.0.0.1 in IPv6).
- loop txqueuelen 1000: Indicates this is a loopback interface, and it has a queue length of 1000.
- RX packets 1116 bytes 113463 (113.4 KB): The loopback interface has received 1116 packets, totaling 113.4 KB.
- TX packets 1116 bytes 113463 (113.4 KB): The loopback interface has transmitted 1116 packets, also totaling 113.4 KB.

6) tcpdump

Syntax: tcpdump

Example Output:

Interpretation:

1. Timestamp:

- Example: 09:47:59.159409
 - Indicates the precise time the packet was captured.
2. Source and Destination:
- Format: <Source IP/Hostname>.<Source Port> > <Destination IP/Hostname>.<Destination Port>
 - Example:
 - 172-1-44-87.lightspeed.wepbfl.sbcglobal.net.34636 > maa03s39-in-f3.1e100.net.http
 - Source: 172-1-44-87.lightspeed.wepbfl.sbcglobal.net on port 34636
 - Destination: maa03s39-in-f3.1e100.net on port http (port 80).
3. Flags:
- Example: Flags [F.]
 - Flags in the TCP header:
 - F: FIN (Finish), indicates the sender is closing the connection.
 - .: ACK (Acknowledgment), confirms receipt of data.
 - Other possible flags:
 - S: SYN, used to initiate a connection.

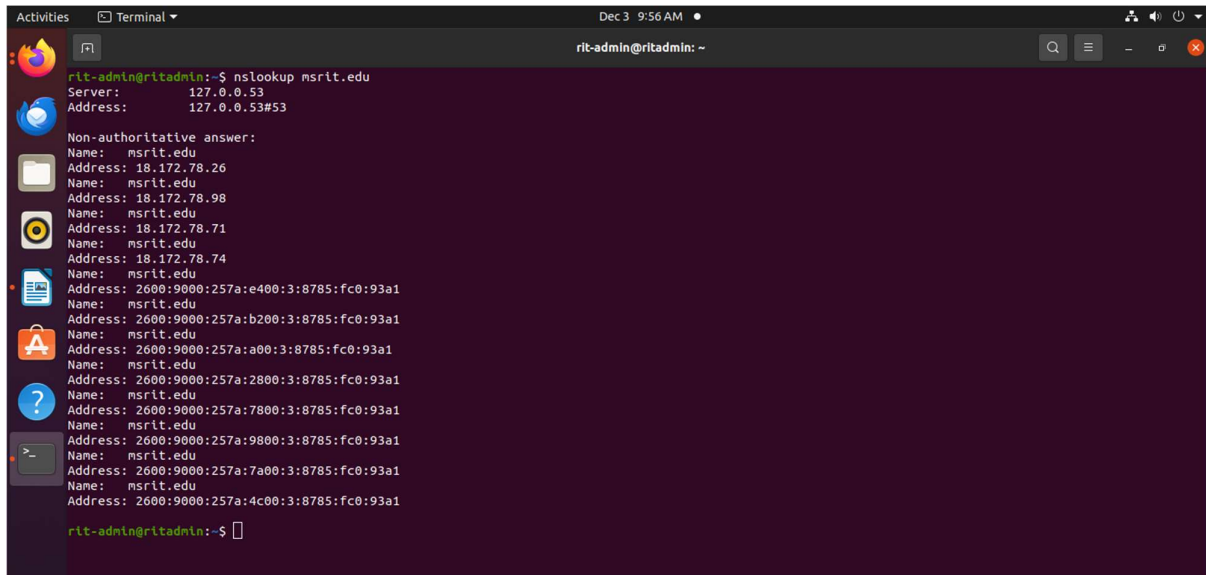
- P: PSH, indicates data should be pushed immediately to the receiving application.
 - R: RST, resets the connection.
4. Sequence and Acknowledgment Numbers:
 - Example: seq 3913240276, ack 2678214762
 - seq: Sequence number of the data in the packet.
 - ack: Acknowledgment number, confirming the receipt of data.
 5. Window Size (win):
 - Example: win 501
 - The size of the TCP receive window, indicating how much data the sender can accept before requiring an acknowledgment.
 6. Options:
 - Example: [nop,nop,TS val 355573457 ecr 3393137770]
 - nop: No operation, used as a spacer.
 - TS val: Timestamp value for the packet.
 - ecr: Echo reply timestamp, reflecting the timestamp value received.
 7. Length:
 - Example: length 0
 - Indicates the size of the payload in the packet. In this case, length 0 means the packet has no application-layer data (common in TCP control packets like ACK or FIN).

7) nslookup

Syntax: nslookup [hostname] [server], where hostname is the domain name or IP address you want to query and server (optional) is a DNS server to perform the query.

Purpose: nslookup is a command-line tool used to query the Domain Name System (DNS) to obtain domain name or IP address mappings and other DNS records. It is primarily used for diagnosing and troubleshooting DNS-related issues.

Example Output:



```
rit-admin@ritadmin:~$ nslookup msrit.edu
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   msrit.edu
Address: 18.172.78.26
Name:   msrit.edu
Address: 18.172.78.98
Name:   msrit.edu
Address: 18.172.78.71
Name:   msrit.edu
Address: 18.172.78.74
Name:   msrit.edu
Address: 2600:9000:257a:e400:3:8785:fc0:93a1
Name:   msrit.edu
Address: 2600:9000:257a:b200:3:8785:fc0:93a1
Name:   msrit.edu
Address: 2600:9000:257a:a00:3:8785:fc0:93a1
Name:   msrit.edu
Address: 2600:9000:257a:2800:3:8785:fc0:93a1
Name:   msrit.edu
Address: 2600:9000:257a:7800:3:8785:fc0:93a1
Name:   msrit.edu
Address: 2600:9000:257a:9800:3:8785:fc0:93a1
Name:   msrit.edu
Address: 2600:9000:257a:7a00:3:8785:fc0:93a1
Name:   msrit.edu
Address: 2600:9000:257a:4c00:3:8785:fc0:93a1

rit-admin@ritadmin:~$
```

Interpretation:

The nslookup output for msrit.edu provides detailed information about the DNS resolution of the domain.

1. DNS Server Used

- Server: 127.0.0.53
 - The query is being resolved by a local DNS resolver running on the system (127.0.0.53, a loopback address).
 - This is typically managed by a service like systemd-resolved on Linux.
- Address: 127.0.0.53#53
 - The query is sent to the DNS service on port 53, the standard DNS port.

2. Non-Authoritative Answer

- Non-Authoritative Answer:
 - This means the DNS server that responded is not the authoritative source for msrit.edu, but it retrieved the information from another DNS server in the hierarchy.

3. IPv4 Addresses (A Records)

- Addresses:
 - 18.172.78.26
 - 18.172.78.98
 - 18.172.78.71
 - 18.172.78.74
- These are the IPv4 addresses associated with msrit.edu. The domain has multiple IP addresses likely for load balancing or fault tolerance, where requests can be distributed among several servers.

4. IPv6 Addresses (AAAA Records)

- Addresses:
 - 2600:9000:257a:e400:3:8785:fc0:93a1
 - 2600:9000:257a:b200:3:8785:fc0:93a1

- 2600:9000:257a:a00:3:8785:fc0:93a1
- 2600:9000:257a:2800:3:8785:fc0:93a1
- 2600:9000:257a:7800:3:8785:fc0:93a1
- 2600:9000:257a:9800:3:8785:fc0:93a1
- 2600:9000:257a:7a00:3:8785:fc0:93a1
- 2600:9000:257a:4c00:3:8785:fc0:93a1
- These are the IPv6 addresses for msrit.edu, showing the domain is IPv6-enabled and has multiple addresses for redundancy and load distribution in IPv6 networks.

Key Observations

1. Multiple IP Addresses:
 - The domain resolves to multiple IPv4 and IPv6 addresses, which is common for domains using load balancing or hosted on distributed infrastructure like Content Delivery Networks (CDNs).
2. Dual Stack Support:
 - The presence of both IPv4 (A records) and IPv6 (AAAA records) indicates the domain supports dual-stack networking, allowing it to serve clients using either protocol.
3. Efficient DNS Configuration:
 - This configuration ensures high availability and scalability, as traffic can be distributed among the multiple IP addresses.

8) nmap

Syntax: nmap [target]

Purpose: nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It can be used by network administrators to discover hosts and services on a computer network, perform port scanning to determine open ports and running services, identify operating systems and software versions running on devices, detect vulnerabilities by finding misconfigurations or weaknesses and audit network security by simulating attacks to evaluate defenses.

Example Output:

```

rlt-admin@ritadmn:~$ nmap msrit.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2024-12-03 10:15 IST
Nmap scan report for msrit.edu (54.230.27.14)
Host is up (0.011s latency).
Other addresses for msrit.edu (not scanned): 54.230.27.42 54.230.27.114 54.230.27.86 2600:9000:257a:9600:3:8785:fc0:93a1 2600:9000:257a:7600:3:8785:fc0:93a1 2600:9000:257a:d800:3:8785:fc0:93a1 2600:9000:257a:4600:3:8785:fc0:93a1 2600:9000:257a:f200:3:8785:fc0:93a1 2600:9000:257a:de00:3:8785:fc0:93a1
2600:9000:257a:c800:3:8785:fc0:93a1 2600:9000:257a:6200:3:8785:fc0:93a1
rDNS record for 54.230.27.14: server-54-230-27-14.hyd57.r.cloudfront.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.86 seconds
rlt-admin@ritadmn:~$

```

Interpretation:

Key Information from the Scan:

1. Target Host: msrit.edu (resolved to IP address 54.230.27.14)
 - Hostname: msrit.edu maps to multiple IP addresses, including IPv6 addresses (like 2600:9000:257a:9600:3:8785:fc0:93a1).

2. Host Status:

- Host is up: This means that the IP address (54.230.27.14) is reachable and responding to requests. The latency to the host is 0.011s, which is quite low.

3. Reverse DNS (rDNS) Resolution:

- The rDNS entry for the IP address 54.230.27.14 resolves to server-54-230-27-14.hyd57.r.cloudfront.net. This indicates that the host is likely behind an AWS CloudFront distribution in the Hyderabad region (hyd57).

4. Open Ports:

- Port 80/tcp: Open, and this port is typically used for HTTP (unsecured web traffic).
- Port 443/tcp: Open, and this port is used for HTTPS (secured web traffic).
- These ports being open suggests that msrit.edu runs a web server that supports both regular and secure web access.

5. Filtered Ports:

- The message "Not shown: 998 filtered ports" means that a significant number of ports are being filtered by a firewall or some other network protection mechanism, preventing Nmap from determining their state.

Observations:

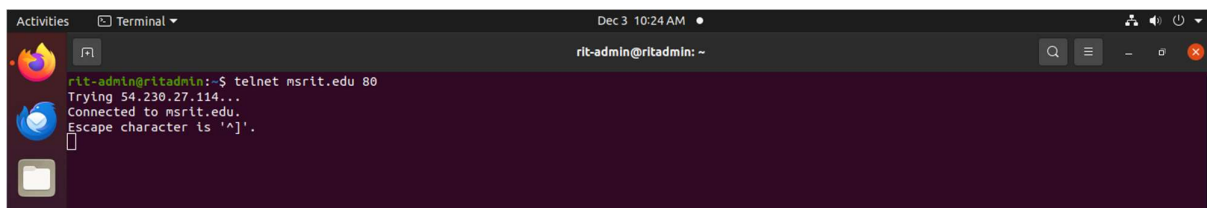
- The server hosting msrit.edu is live and is running a web server with open HTTP (port 80) and HTTPS (port 443) services.
- The IP address 54.230.27.14 is associated with CloudFront (Amazon Web Services), indicating the site might be using a CDN (Content Delivery Network) for optimized delivery of web content.
- A large number of ports are filtered (i.e., blocked or hidden by a firewall).

9) telnet

Syntax: telnet [hostname] [port], where [hostname] is the IP address or domain name of the remote host and [port] (optional) is the port to connect to (if omitted, telnet defaults to port 23).

Purpose: Telnet is a network protocol and client program used to establish a connection to remote systems over a TCP/IP network. It allows a user to log into another computer, often a server, and interact with it via a command-line interface.

Example Output:

A screenshot of a Linux terminal window. The title bar shows 'Activities', 'Terminal', and the date 'Dec 3 10:24 AM'. The terminal prompt is 'rit-admin@ritadmin: ~'. The user has entered the command 'telnet msrit.edu 80'. The output shows 'Trying 54.230.27.114...' followed by 'Connected to msrit.edu.' and 'Escape character is '^[''. The terminal background is dark purple with light blue text.

Interpretation:

The command telnet msrit.edu 80 is being executed. This attempts to establish a telnet connection to the msrit.edu server on port 80. The output shows that the connection is being established ("Trying 54.230.27.114...") and that the connection is successful ("Connected to msrit.edu."). The next line "Escape character is '^['." is a standard telnet prompt, informing the user that the escape

character to exit the telnet session is Ctrl+]. This type of output is typical when attempting to connect to a server using the telnet protocol. Telnet is an older protocol that allows a user to interact with a remote system in a text-based way, often used for diagnostic or administrative purposes. The information provided here indicates that the connection to the msrit.edu server on port 80 was successful, which could be useful for further troubleshooting or interacting with the server if needed.