NEW YORK INSTITUTE OF TECHNOLOGY

College of Engineering and Computing Science

Project Report

Measurement of Network Delay between Internet Hosts

NIRAJ RAJ – 1310530
MANN PATEL – 1316627
SYED MENAJ – 1318374

Term: Spring 2023
CSCI 690 / EENG 755 – Computer Networks

Professor:
Dr. Ziqian Dong

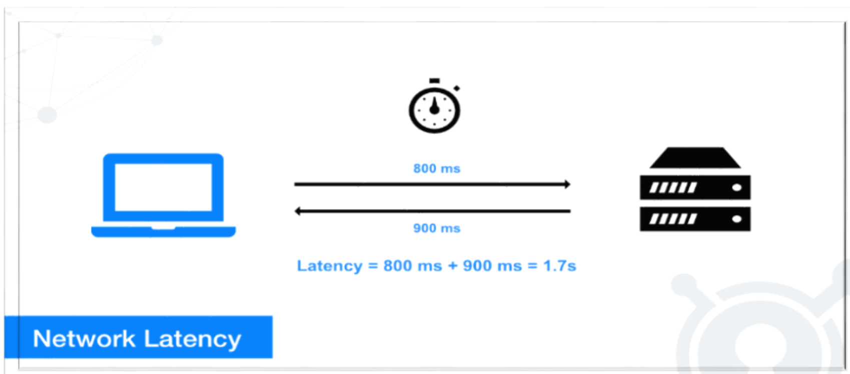
Table of Content

1. Abstract

Ping, MTR, and iPerf are essential network diagnostic tools. The round-trip time is measured using ping, which aids in confirming connectivity and locating problems. In order to analyze network pathways and identify bottlenecks, MTR combines the traceroute and ping commands. To help with performance optimization and congestion troubleshooting, iPerf measures throughput, bandwidth, and capacity using simulated traffic. In network diagnostics, these tools have specific functions that help administrators and technicians improve the efficiency and dependability of the network.

2. Objective

The information stack flow time, which measures how long it takes for data to go from a sender to a destination, might experience delays when the two sites are far apart. These noticeable delays can have an influence on user happiness and the effectiveness of computer-human collaboration. One can determine how long it takes for data to flow from one internet host to another in order to quantify network latency between hosts.



One can monitor the amount of time it takes for data to flow from one internet host to another in order to calculate the network latency between hosts. The ping command can be used to accomplish this by sending an ICMP echo request packet to a given address. Ping rates of 100ms or less are typically regarded as acceptable, whereas latency levels between 30 and 40ms are ideal for best performance.

3. What's Latency?

When data or a signal is transmitted from its source to its destination through a system or network, there is a temporal delay known as latency. It symbolizes the amount of time needed for a data packet to transit from one location to another. Latency is frequently expressed in milliseconds(ms) and is influenced by several variables, including network infrastructure, location, traffic, and processing delays.

The responsiveness and performance of applications and services in networking can be impacted by latency. Lower latency is preferred since it results in faster data transmission and less delay. Real-time applications like online gaming, video conferencing, and financial transactions can be negatively impacted by high latency due to delayed or sluggish communication between devices. [1]

3.1 Latency can be categorized into different types:

Network Congestion: High network traffic volumes can cause congestion, which can slow down packet transmission and increase latency. Data packets may undergo waiting and buffering when network resources are exhausted, increasing latency.
Distance: The source and destination's physical separation might cause latency. Over vast distances, signals must travel slowly, and this propagation delay adds to overall latency. Distance-related delay, for instance, becomes more noticeable in wide-area networks (WANs) or connections between physically far locations.
Network Equipment and Infrastructure: Latency can be affected by the functionality and capacity of routers, switches, cables, and other network hardware. Data packet processing and forwarding may be further delayed by outdated or overburdened equipment.
Network Protocol Overhead: TCP/IP and other data transfer methods add some overhead that may impact latency. Data transmission times might be impacted by handshaking, error checking, and other protocol-related operations.
Quality of Service (QoS) Policies: Latency can be affected by Quality of Service (QoS) algorithms used in networks to prioritize types of traffic. For instance, increasing the priority of some traffic may result in increased latency for other traffic.
Network Topology: The physical configuration and architecture of the network might affect latency. Additional latency may be introduced by longer, more complicated network pathways with many hops or ineffective routing.
Wireless Networks: Signal interference, signal propagation delays, and competition for wireless resources are just a few examples of the variables that might impact latency in wireless networks. [2]

3.2 Why do we measure Latency?

Network Performance Monitoring: Administrators can maintain a positive user experience by proactively addressing latency-related issues by using proactive monitoring and issue identification provided by latency measurement.
Service Level Agreements (SLAs): Assuring service providers adhere to performance requirements through latency measurement in SLAs enables both parties to monitor and confirm the network's achievement of desired service levels.
Performance Optimization: By measuring latency, networks' bottlenecks and potential improvement areas can be found. In order to increase network efficiency and user experience, administrators can utilize this information to upgrade hardware, improve routing, introduce Quality of Service (QoS) methods, and improve network design. [3]
Troubleshooting: By assisting administrators in locating the root of performance issues including congestion, defective hardware, or ineffective network setups, latency

measurements are helpful for diagnosing network difficulties. As a result, problems can be identified and fixed quickly.

Capacity Planning: By forecasting how network resources will respond to a demand increase and identifying the need for more bandwidth, hardware improvements, or optimization techniques, latency measurement aids in capacity planning.

Application Performance Evaluation: The ability to quantify latency is essential for evaluating the performance of real-time applications like VoIP, video streaming, and online gaming. Administrators can assess the performance of applications and improve how they are delivered to users by analyzing latency. [3]

4. Ping

A network utility called Ping is used to check and confirm that a host or IP address can be reached on a network. It is frequently used to assess network connectivity problems and compute the RTT between a source and a destination. The Ping command sends a series of brief packets (ICMP Echo Request) to the host or IP address that is provided as the target. If accessible, the target answers with ICMP Echo Reply packets. Ping calculates the time it takes for packets to travel from their starting point to their destination and back, giving information on network latency and possible packet loss. [4]

For simple network troubleshooting, Ping is a straightforward yet efficient tool. It gives an indication of network performance and assists in determining whether a host is online, whether there is connectivity between the source and destination, and whether. Network managers can notice network congestion, packet loss, or high latency by examining the ping results, which might have an impact on the performance of an application.

Typically, ping instructions are run from a command prompt or terminal, and the output shows information like the minimum, maximum, and average round-trip times as well as the proportion of packets lost. Ping is a critical instrument for network diagnostics and monitoring that is extensively supported across a variety of operating systems. [5]

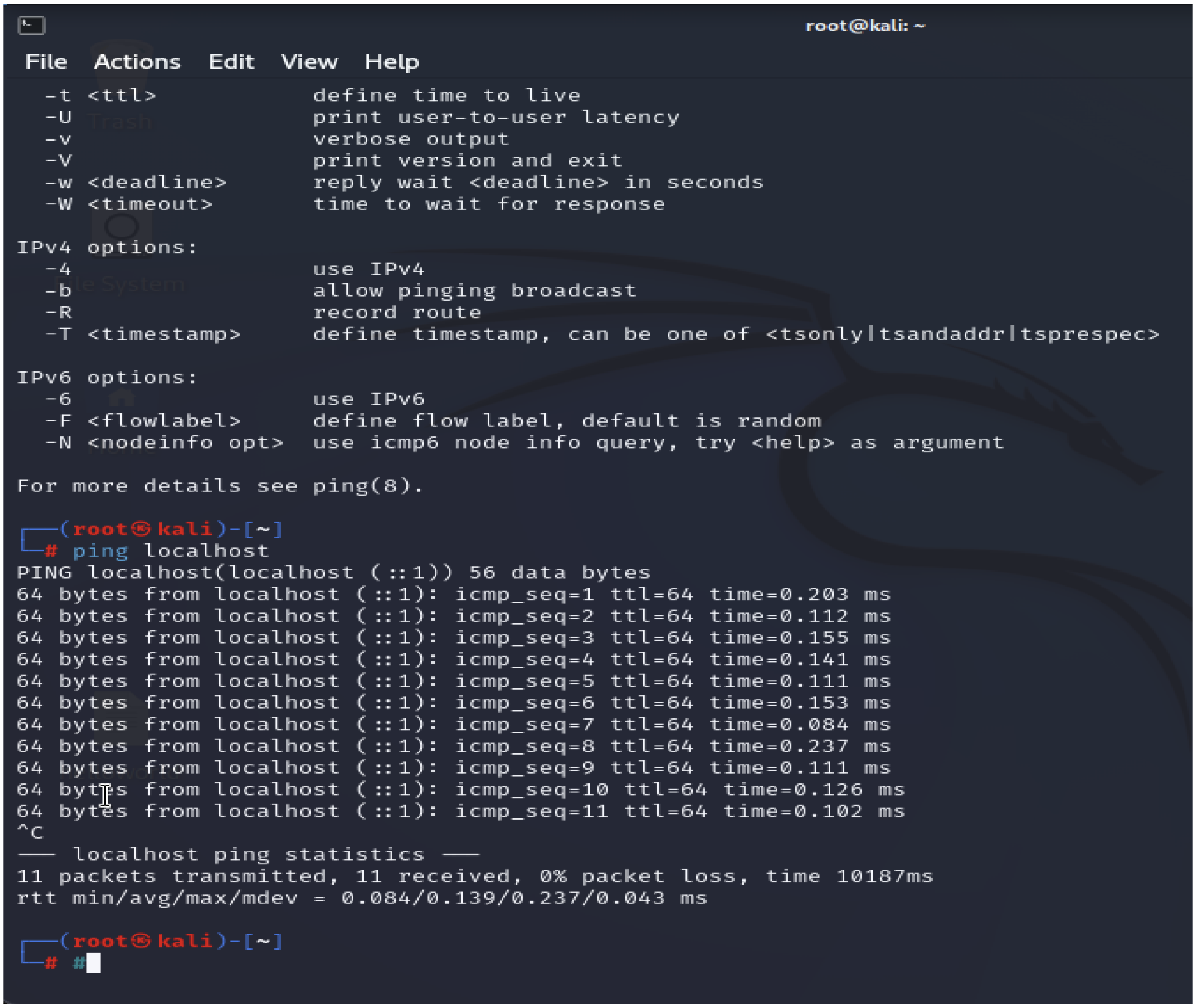
<table>
<tr><th colspan="5">IPv4 datagram</th></tr>
<tr><th></th><th>Bits 0–7</th><th>Bits 8–15</th><th>Bits 16–23</th><th>Bits 24–31</th></tr>
<tr><td rowspan="4">Header
(20 bytes)</td><td>Version/IHL</td><td>Type of service (ToS)</td><td colspan="2">Length</td></tr>
<tr><td colspan="2">Identification</td><td colspan="2">*flags* and *offset*</td></tr>
<tr><td>Time to live (TTL)</td><td>Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="4">Source IP address</td></tr>
</table>

	Destination IP address		
ICMP header (8 bytes)	Type of message	Code	Checksum
	Header data		
ICMP payload (*optional*)	Payload data		

4.1 **IPv4 datagram**

IPv6 datagram						
	Bits 0–3	**Bits 4–7**	**Bits 8–11**	**Bits 12–15**	**Bits 16–23**	**Bits 24–31**
Header (40 bytes)	Version	Traffic class		Flow label		
	Payload length				Next header	Hop limit
	Source address (128 bits)					
	Destination address (128 bits)					
ICMP6 header (8 bytes)	Type of message		Code		Checksum	
	Header data					
ICMP6 payload (*optional*)	Payload data					

4.2 **IPv6 datagram**



```
root@kali: ~
File  Actions  Edit  View  Help
  -t <ttl>          define time to live
  -U                print user-to-user latency
  -v                verbose output
  -V                print version and exit
  -w <deadline>     reply wait <deadline> in seconds
  -W <timeout>      time to wait for response

IPv4 options:
  -4                use IPv4
  -b                allow pinging broadcast
  -R                record route
  -T <timestamp>    define timestamp, can be one of <tsonly|tsandaddr|tsprespec>

IPv6 options:
  -6                use IPv6
  -F <flowlabel>    define flow label, default is random
  -N <nodeinfo opt> use icmp6 node info query, try <help> as argument

For more details see ping(8).

┌──(root㉿kali)-[~]
└─# ping localhost
PING localhost(localhost (::1)) 56 data bytes
64 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.203 ms
64 bytes from localhost (::1): icmp_seq=2 ttl=64 time=0.112 ms
64 bytes from localhost (::1): icmp_seq=3 ttl=64 time=0.155 ms
64 bytes from localhost (::1): icmp_seq=4 ttl=64 time=0.141 ms
64 bytes from localhost (::1): icmp_seq=5 ttl=64 time=0.111 ms
64 bytes from localhost (::1): icmp_seq=6 ttl=64 time=0.153 ms
64 bytes from localhost (::1): icmp_seq=7 ttl=64 time=0.084 ms
64 bytes from localhost (::1): icmp_seq=8 ttl=64 time=0.237 ms
64 bytes from localhost (::1): icmp_seq=9 ttl=64 time=0.111 ms
64 bytes from localhost (::1): icmp_seq=10 ttl=64 time=0.126 ms
64 bytes from localhost (::1): icmp_seq=11 ttl=64 time=0.102 ms
^C
--- localhost ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10187ms
rtt min/avg/max/mdev = 0.084/0.139/0.237/0.043 ms

┌──(root㉿kali)-[~]
└─# #
```

4.3 Output of Ping

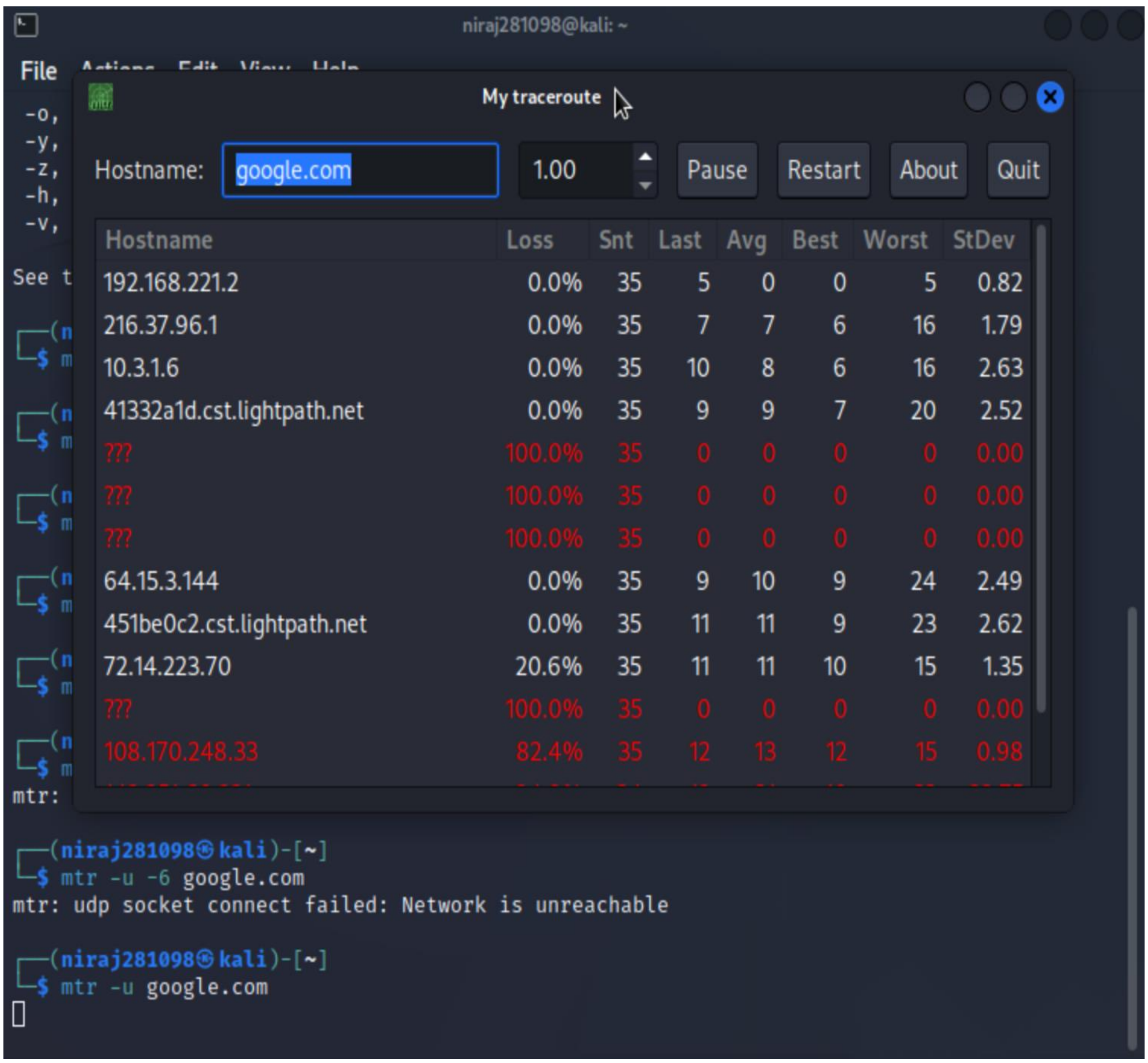
5. <u>Traceroute & MTR</u>

Traceroute: Traceroute operates by sending a string of ICMP or UDP packets with Time-to-Live (TTL) values that are increasing. The TTL value, which is assigned to each packet starting at 1, specifies the most hops it can go. A packet's TTL value is decreased when it reaches a router, and if it hits zero, the router discards the packet and sends an ICMP Time Exceeded message back to the originating host. The TTL value is increased each time this procedure is carried out, and it continues until the packet successfully reaches the destination host or has traveled the specified maximum number of hops.

Each router or "hop" along the route is identified by its IP address and round-trip times (RTTs) by Traceroute. Network administrators can examine the output to determine the order of routers used, assess delay at each hop, and spot any potential congestion or latency problems. [6]

MTR (My Traceroute): MTR is a Traceroute addon that combines the features of both Ping and Traceroute. It continually transmits packets to the target host and offers up-to-date information on the route and latency data in real time. The average, minimal, and maximal RTTs for each hop are shown by MTR in a tabular style as it continuously collects data. In addition to providing statistics on packet loss and jitter, it also offers a more thorough examination of network performance than the conventional Traceroute.
It enables network administrators to track the performance and course of network connections over a long period of time, assisting in troubleshooting and spotting patterns of network issues.

Providing information on network pathways, hop-by-hop delay, and potential bottlenecks, Traceroute and MTR are both useful tools for network diagnostics. They aid in locating network problems, improving routing settings, and resolving connectivity issues. [7]



5.1 Output of MTR

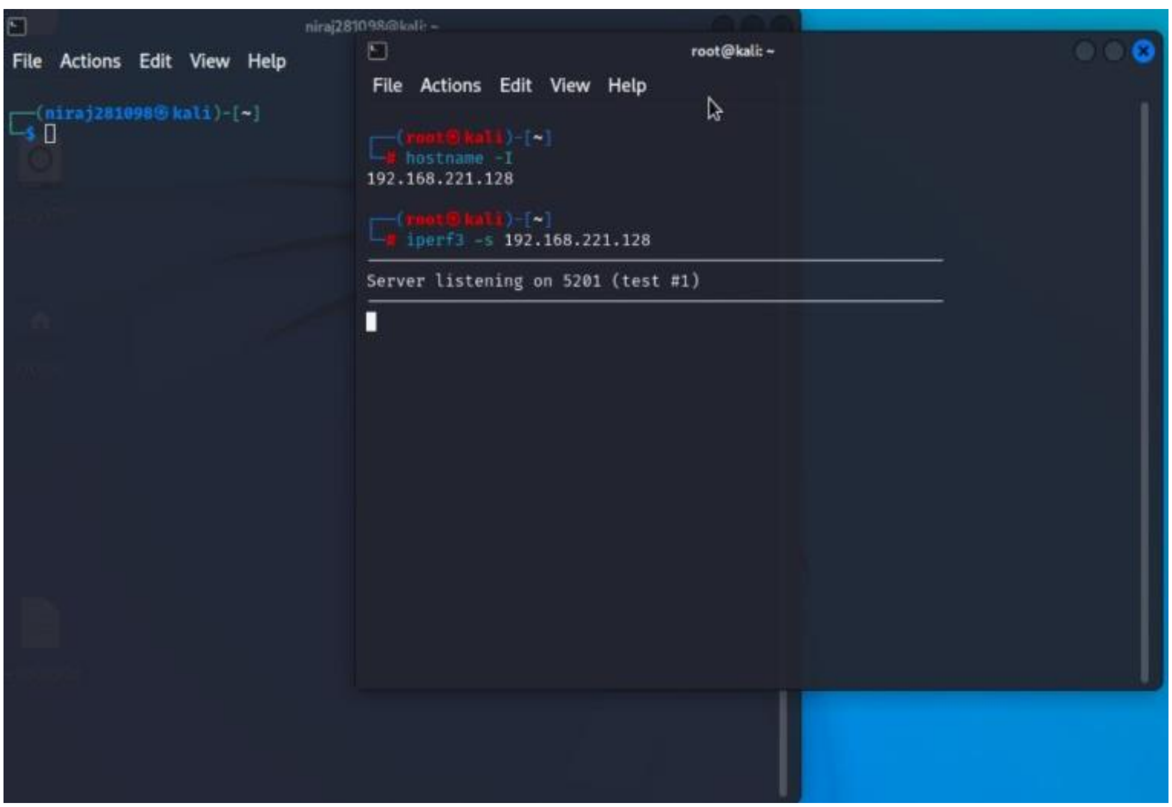
6. iPerf

iPerf stands for "Internet Protocol Performance". It is a frequently employed tool for evaluating the performance of networks that looks at the throughput, bandwidth, and capacity of a network. By simulating TCP or UDP traffic streams between a client and server, administrators can assess the performance and quality of a network connection.

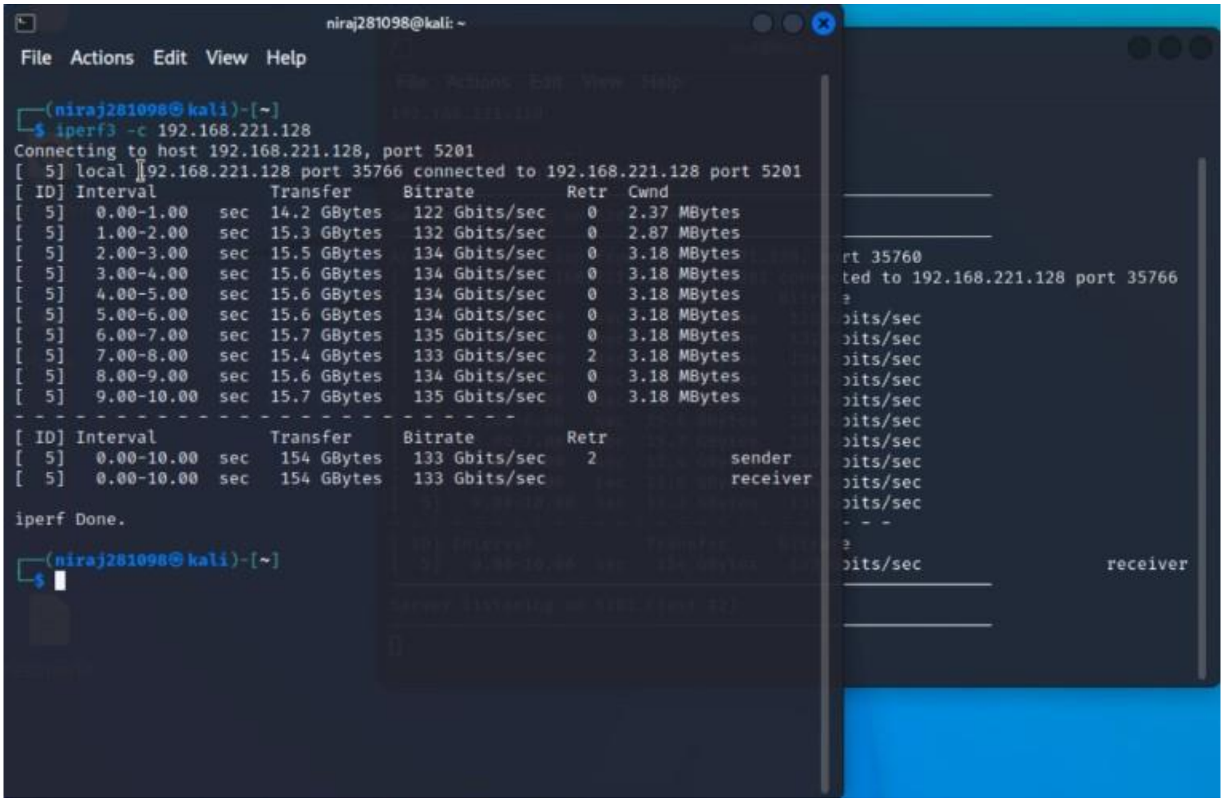
Perf offers a variety of options and tools for doing network performance assessments. Throughput, latency, packet loss, and jitter are just a few of the characteristics it can measure. By selecting the proper test length, packet size, and other factors, administrators can simulate real-world network conditions and evaluate how the network performs in various scenarios.

iPerf is adaptable to many network topologies because it supports both client-server and peer-to-peer testing modes. It may be applied to both LANs and WANs, and it can help with capacity planning, network optimization, and troubleshooting.

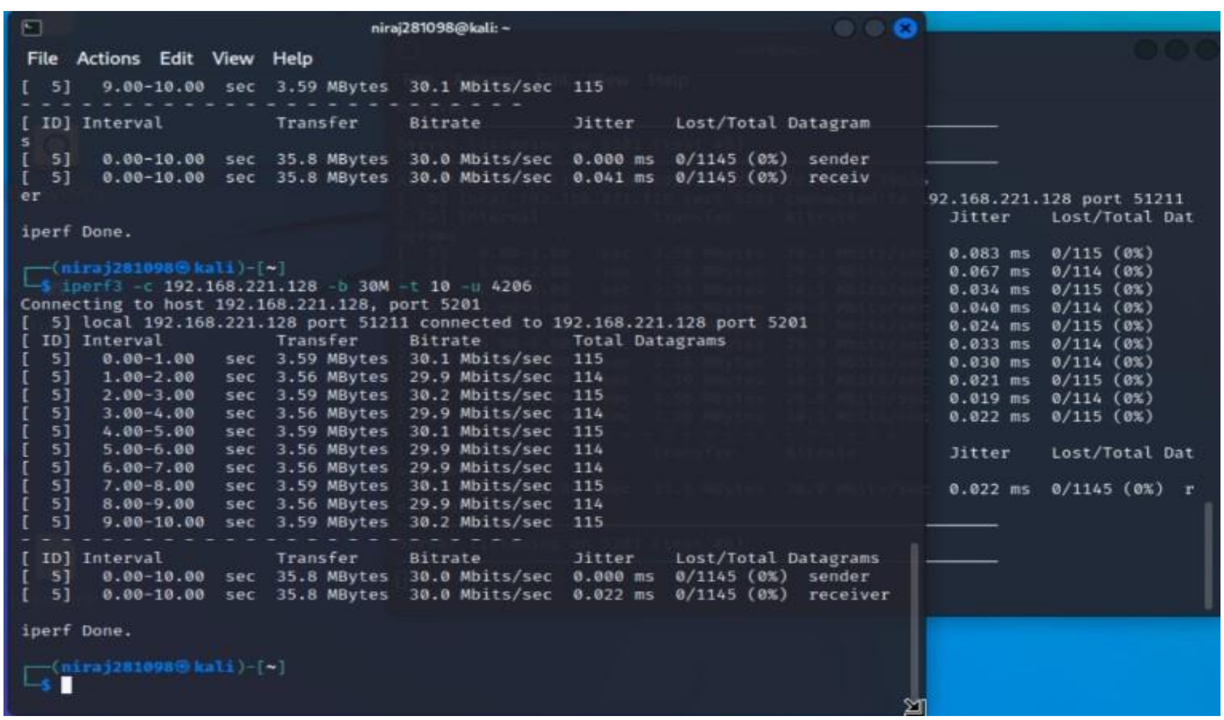
IPerf is compatible with Windows, Linux, and macOS thanks to its command-line interface and cross-platform functionality. It is widely used in the networking sector and serves as a useful tool for network managers, service providers, and researchers to assess performance and optimize networks. [7]



6.1 Provide Server & Client network



6.2 Run the simple test between the source host to destination host



6.3output of Jitters & Packet losses using iPerf3.

7. Difference between tools

	No.	PROS	CONS
PING	**1**	Ping is a basic network utility used to test the reachability and round-trip time (RTT) of a network host or IP address.	Limited in-depth information about network performance.
	2	Helps identify basic network issues like packet loss and latency.	Doesn't provide detailed hop-by-hop analysis.
MTR	**1**	Provides hop-by-hop analysis of network paths.	Some networks may block ICMP or UDP packets, limiting its effectiveness.
	2	Helps identify bottlenecks and network performance issues.	Limited support on certain operating systems.
iPerf 3	**1**	Flexibility: iPerf is a versatile tool that can be used to test a wide range of network configurations, including TCP and UDP protocols.	Command-line interface may not be user-friendly for some users, particularly those who are not familiar with the command line.
	2	Customization: iPerf allows for the customization of various parameters such as the packet size, data transfer rate, and the duration of the test.	Lack of graphical user interface may make it difficult for users who prefer a visual representation of their test results.
	3	Open-source: iPerf is an open-source tool, which means that it is free to use and can be modified to suit specific testing needs.	Requires two hosts, one acting as the server and the other as the client, which may be a limitation for some users who want to test their network without having access to multiple devices.

8. Conclusion

In conclusion, there are various uses for iPerf3, Ping, and MTR in network diagnostics and performance assessment.

By creating simulated TCP or UDP traffic streams, **iPerf3** focuses on analyzing network performance, bandwidth, and capacity. In addition to being helpful for capacity planning, network optimization, and troubleshooting, it gives detailed performance measurements. [7]

A ping is a straightforward tool that calculates the RTT between a source and a destination host. It is helpful for basic network troubleshooting and for determining whether a network can be reached. [2]

Traceroute and Ping's features are combined in **MTR** (My Traceroute). It provides insights into latency, packet loss, and network congestion by giving a hop-by-hop study of network pathways. MTR is very helpful for identifying sporadic network problems and tracking network performance over time. [6]

Network technicians and administrators can select the best tool for their unique needs by being aware of the distinctions between these technologies. Network reliability, efficiency, and troubleshooting skills can be considerably improved by integrating iPerf3, Ping, and MTR into network diagnostics and performance evaluation processes.

9. References

[1]"Latency." Hackapedia. Accessed May 7, 2023. https://web.archive.org/web/20210422025642/https://hackapedia.com/term.

[2] Souders, Steve. "Velocity and the Bottom Line." Radar – O'Reilly. Accessed May 7, 2023. https://radar.oreilly.com/2009/07/velocity-making-your-site-fast.html

[3] *Rappaport, Theodore S. (2002). Wireless communications: principles and practice (2 ed.). Upper Saddle River, NJ: Prentice Hall PTR. ISBN 0-13-042232-0.*

[4] Mike Muuss. "The Story of the PING Program". Archived My original impetus for writing PING for 4.2a BSD UNIX came from an offhand remark in July 1983 by Dr. Dave Mills.

[5]*Postel, J. (September 1981).* "RFC 792 - Internet Control Message Protocol". *Tools.ietf.org.* doi:10.17487/RFC0792. Retrieved 2 February 2014.

[6] " *Traceroute*. (2002, February 25). Wikipedia, the free encyclopedia. Retrieved May 7, 2023, from https://en.wikipedia.org/wiki/Traceroute#cite_note-1

[7] " GUEANT, V. (n.d.). iPerf - The TCP, UDP, and SCTP network bandwidth measurement tool. https://iperf.fr/