Statement and Confirmation of Own Work



***A signed copy of this form must be submitted with every assignment.***

***If the statement is missing your work may not be marked.***

**Student Declaration**

I confirm the following details:

|  |  |
| --- | --- |
| **Student Name:** | Johnson Kenisha Corera |
| **Student ID Number:** | c23020001@cicra.edu.lk |
| **Qualification:** | Bachelor in Cyber Security |
| **Unit:** | SIT325 Advanced Network Security |
| **Centre:** | CICRA Campus |
| **Word Count:** | 431 |
| I have read and understood both *Deakin* *Academic Misconduct Policy* and the *Referencing and Bibliographies* document. To the best of my knowledge my work has been accurately referenced and all sources cited correctly.  I confirm that I have not exceeded the stipulated word limit by more than 10%.  I confirm that this is my own work and that I have not colluded or plagiarized any part of it. | |
| **Candidate Signature:** |  |
| **Date:** | 03/12/2024 |

**Task 4.1P**

**Table of Content**

[Introduction](#into)…………………………………………………………………………………..05

[Part A](#PartA)…………………………………………………………………………………………06

[Part B](#PartB)…………………………………………………………………………………………09  
[Question 01](#Quest)…………………………………………………………………………………...10

[Conclusion](#conc)……………………………………………………………………………………11

[Reference](#refe)……………………………………………………………………………………..12

**Table of Figures**

[Figure 1](#Figure1)………………………………………………………………………………………06

[Figure 2](#Figure2)………………………………………………………………………………………06

[Figure 3](#Figure3)………………………………………………………………………………………07

[Figure 4](#Figure4)………………………………………………………………………………………07

[Figure 5](#Figure5)………………………………………………………………………………………07

[Figure 6](#Figure6)………………………………………………………………………………………08

[Figure 7](#Figure7)………………………………………………………………………………………08

[Figure 8](#Figure8)………………………………………………………………………………………08

[Figure 9](#Figure9)………………………………………………………………………………………09

**Table of Acronyms**

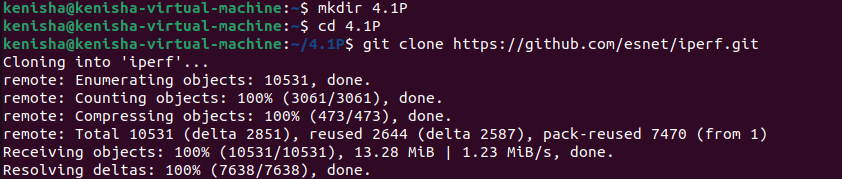
|  |  |
| --- | --- |
| SDN | Software Define Network |
| TCP | Transmission Control Protocol |
| IP | Internet Protocol |
| ICMP | Internet Control Message Protocol |
| LAN | Local Area Network |
| RTT | Real-time text |
| DPI | Dots Per Inch |
| TLS | Transport Layer Security |
| SSL | Secure Sockets Layer |
| NASDAQ | National Association of Securities Dealers Automated Quotations |
| VoIP | Voice over Internet Protocol |

**Introduction**

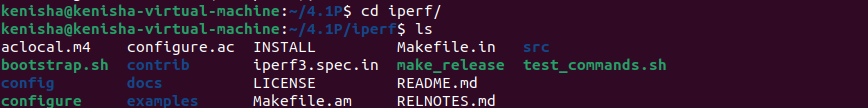
* Firstly, I installed Iperf to discover the throughput in TCP between the two hosts in the network. I created a second host that imitated it and the first host acted as the server of the purpose of imitation. I then made a request to pass data over the network to determine how much it could take in terms of load. This test gave information on functionality of the http network and how band width is utilized.
* I then pinged the same two hosts and used the round trip time of the ping to measure the network latency between them. Another part of this endeavor was an assessment of the network’s ability to deliver actual time data transfer, which is essential for applications that need the network to provide data in real quick time.

**Part A**

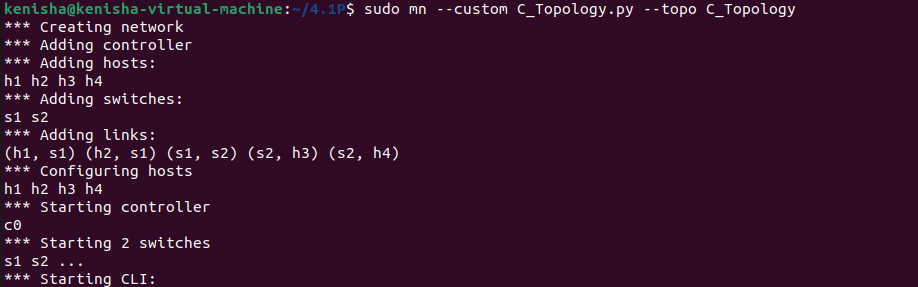
* I began by successfully using the **git clone** command to clone the iperf repository. <https://github.com/esnet/iperf.git>.



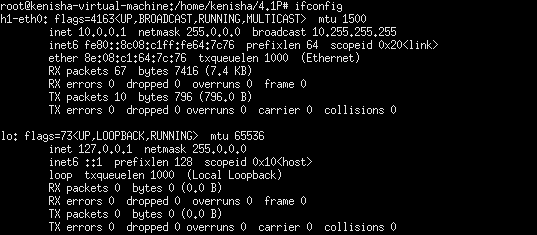
*Figure 1: iperf cloning*

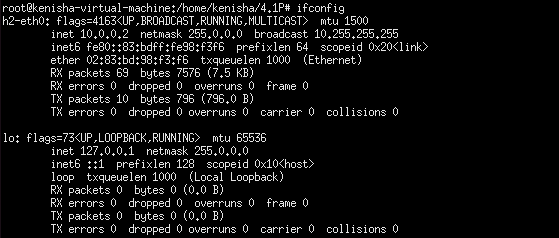


* After that, I typed the command sudo mn –custom C\_Topology.py –topo C\_Topology to start the environment of mininet.

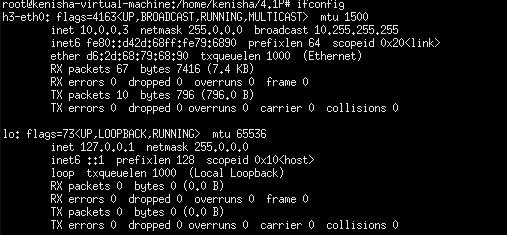


*Figure 2: Running Mininet*

* More specifically, when the Mininet environment was set up, I initiated the xterm terminals of hosts h1 and h3. After that, using the ifconfig command, I checked that they were assigned proper IPs and are ready for the testing. It proved valuable because in the next stages I had to connect to the host and the IP address was necessary to this operation.

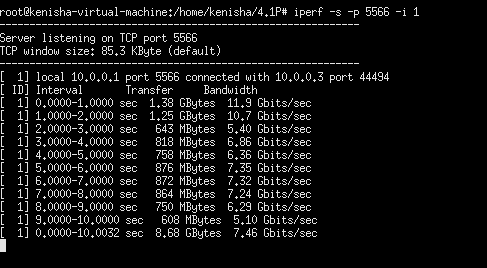
  
*Figure 3: Open xterm terminal in h1*

*Figure 4: Open xterm terminal in h2*

**

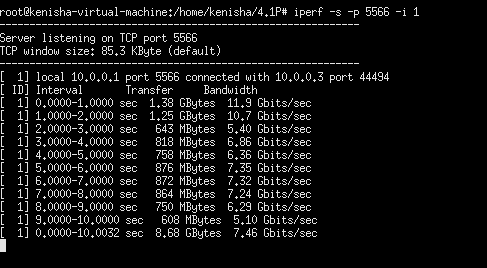
*Figure 5: Open xterm terminal in h3*

* In host h1, I started the Iperf TCP server with the command “iperf -s -p 5566 -i 1”.

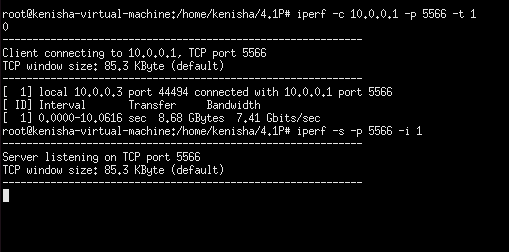


*Figure 6: h1 server stared*

* Then, I went to host h3 continuing the experiment by running the TCP client command, “iperf -c 10.0.0.1 -p 5566 -t 15’.” This command will start a TCP connection to h1 and send data to this host so as to measure throughput for the next 15 seconds.

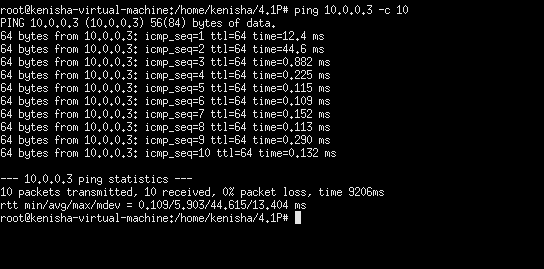


*Figure 7: Sending TCP connection from h2*



*Figure 8: h3 acting as server*

**Part B**

* To start with I tried to perform the ping activity from the host h3 to the host h2 in order to determine the time taken for transmitting the data from the transmitting host to the receiving host. I did this by log in into the h3 console and using command ping 10. 0. 0. 2 The size in bytes of 10 ICMP echo enquiries sent and received was also determined by this command.

*Figure 9: Ping from h2 to h3*

* The average latency was measured to be 0. 313 ms, indicating an extremely quick connection and likely little to no delay over the network link between the two hosts. A few factors that affect transmission delay in a network are system bandwidth, system distance from one another, network equipment quality, and network traffic volume.
* Because it connects with the hosts on different local Area Networks (LAN), the average latency in this case is very low – indicating that there are few if any intermediaries between the server computers so as to facilitate fast transfer of data. Hypotheses of low RTT values where they range between 0.147 and 0.888 ms indicate an unvarying network link with no jitter and lost packets.
* Hence, low latency is well tolerant in every application type that is related to the transfer of real time data, as implied by online gaming, Voip, as well as trading systems. Since there was no packet drop through the packets’ testing then it was proven that the Network connection is stable.

**Question 01**

**How network security and network latency are related?**

* Due to the fact that the delay rate is affected by the inclusion of layers of security then security and latency are highly correlated and in most instances can be understood as the same thing. The number of layers also has another drawback; they slow down the network because protocols like Transport Layer Security/Secure Socket Layer TLS/SSL encryption, for instance, require an additional time to encode and decode messages. Similarly, the method of deep packet inspection (DPI) thwarts threats by reducing traffic speed, and packets that are examined before they reach their predetermined destination. (Schotsal, 2023)
* The exemplification of latency and security is particularly precious in VoIP or online gaming in which even the smallest delays can become unbearable sometimes. These effects can be slightly reduced by methods such as attempting to outsource most of the encryption work to the lower layers or further tweaking of the network paths. However, difficulties arise in reaching the secure system design that would provide the needed level of security while not getting too far from optimal latency for the best network performance. (Dhingra, 2023)

(181 Words)

**Conclusion**

* In this Task, I carried out a Minenet like study and investigated about the network throughputs and latency in detail using german Iperf and ping tools. The trials were great at demonstrating potential network performance such as latency, stability, and efficiency of transferring data are all valuable stuff during real-time apps. The throughput test which provided understanding of how bandwidth is shared between two hosts proved to be informative for identifying the capacity of the network to handle data load. On the ping latency measurement, the round-trip time was 0.313 ms, and there was no jitter and no packet loss. The low latency of the network makes it suitable for latency sensitive applications such as VoIP, online gaming and other real time data transfer systems such as NASDAQ.
* Furthermore, the analysis explored the criticality of the trade-off between response time and network protection. More enhanced security elements which enhance the level of protection of the network to include Transport Layer Security/Secure Socket Layer (TLS/SSL) and deep packet inspection (DPI) take their time hence slowing down the speed. Security, especially in real time applications, is an important issue, yet delays may be an issue regarding signals so a kind of balance between security and signal delays should be made. Such approaches include reduction of the measures it takes to encrypt data, and the reduction of the number of channels that exist in the network. In total the trials demonstrated the important and unique proposition of Networks which are to provide the most effective mean to maintain high overall system safety, stability and performance to fit specific necessities of practical applications. Low latency organizational security coupled with a high through put is necessary in maintaining modern day network standards while ensuring safe communication is upheld.

**Reference**

* How do you balance network security and network performance?

<https://www.linkedin.com/advice/0/how-do-you-balance-network-security-performance>

* Encryption and Network Security

<https://www.thefastmode.com/technology-solutions/30066-encryption-and-network-security-striking-a-balance-between-data-protection-and-network-visibility>