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:** | 924 |
| 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 |

**2.1P Task**

**Table of Content**

* [Introduction](#Intro)…………………………………………………………………………..05
* Network Topology
* [Network Diagram](#Netwokdiag)…………………………………………………………….06
* [Node and Interface detail](#NOdesandinter)…………………………………………………….11
* Connectivity Testing
* [Ping Testing](#ping)…………………………………………………………………..15
* Q&A
* [Question 01](#que01)…………………………………………………………………...17
* [Question 02](#que02)…………………………………………………………………...19
* [Question 03](#que03)…………………………………………………………………...20
* [Question 04](#que04)…………………………………………………………………...21
* [Conclusion](#concl) …………………………………………………………………...............22
* [Reference](#refe)…………………………………………………………………..................23

**Table of Acronyms**

|  |  |
| --- | --- |
| Acronyms | Full Form |
| VM | Virtual Machine |
| CRM | Customer Relationship Management |
| BGP | Border Gateway Protocol |
| ISP | Internet Service Provider |
| RIP | Routing Information Protocol |
| SDN | Software Define Network |

**Table of Figures**

[Figure 1](#figure1)………………………………………………………………………………………05

[Figure 2](#figure2)………………………………………………………………………………………06

[Figure 3](#figure3)………………………………………………………………………………………06

[Figure 4](#figure4)………………………………………………………………………………………07

[Figure 5](#figure5)………………………………………………………………………………………07

[Figure 6](#figure6)………………………………………………………………………………………08

[Figure 7](#figure7)………………………………………………………………………………………08

[Figure 8](#figure8)………………………………………………………………………………………09

[Figure 9](#figure9)………………………………………………………………………………………10

[Figure 10](#figure10)……………………………………………………………………………………..10

[Figure 11](#figure11)……………………………………………………………………………………..11

[Figure 12](#figure12)……………………………………………………………………………………...11

[Figure 13](#figure13)……………………………………………………………………………………...12

[Figure 14](#figure14)……………………………………………………………………………………...12

[Figure 15](#figure15)……………………………………………………………………………………...13

[Figure 16](#figure16)……………………………………………………………………………………...14

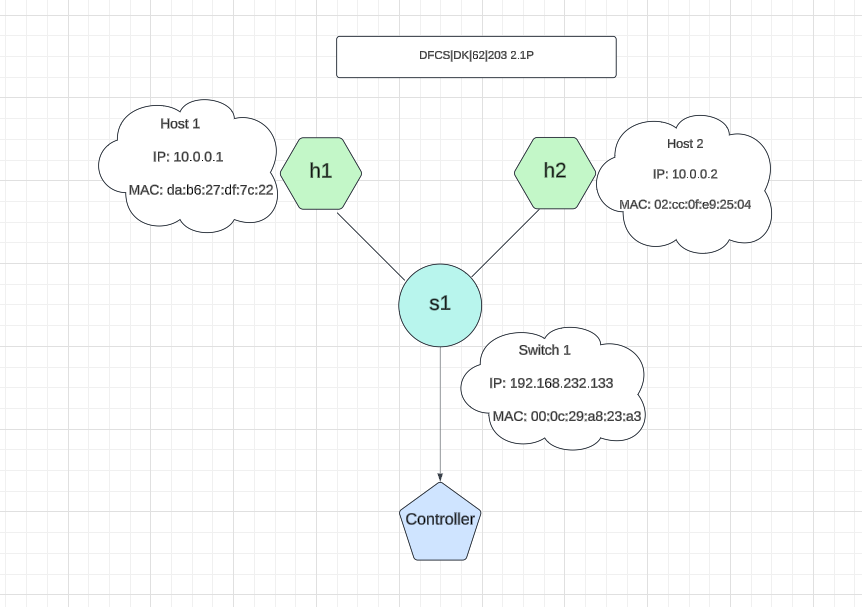
**Introduction**

Task 2.1P on SIT325: The topic of Advanced Network Security is presented in detail in this Assignment. To complete the challenge, Mininet must be used to create a network topology; host connectivity must be verified; and, there are questions about aspects of network theory. The relationship between Software-Defined Networking (SDN) and traffic.

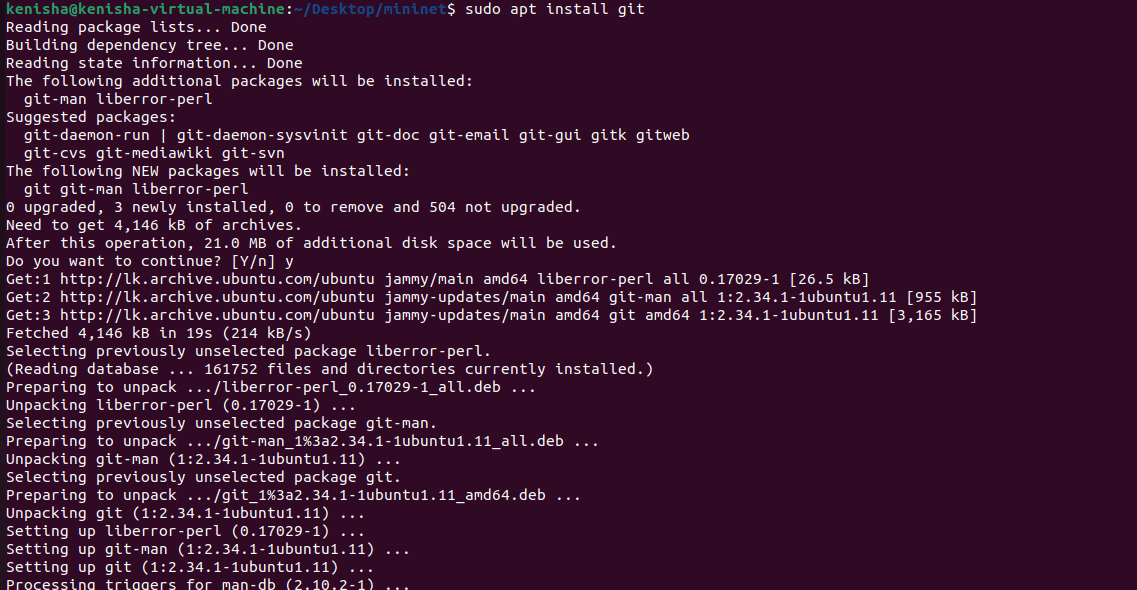
**Network Topology**

**Network diagram**

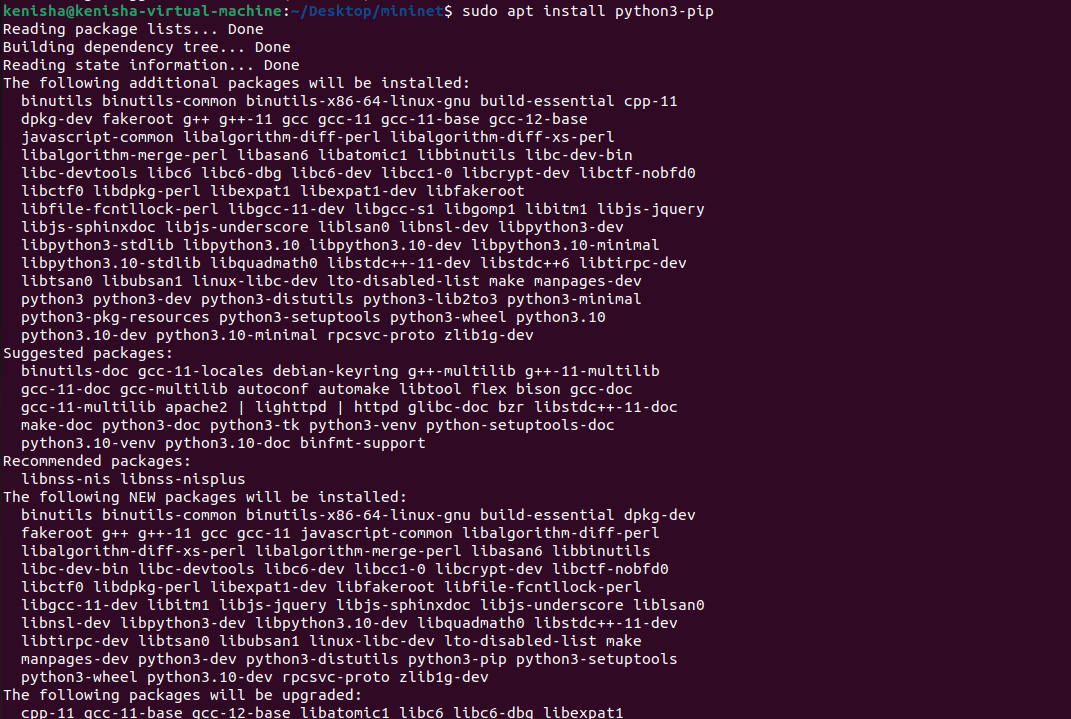
I built the network topology plan that incorporate MAC and IP addresses of switch and hosts. I labeled the switch ports to which the controller and the hosts are connected to. From the result, it was easy to understand the network setups and connections if there was a visualization like this one.

Network Topology with Mininet

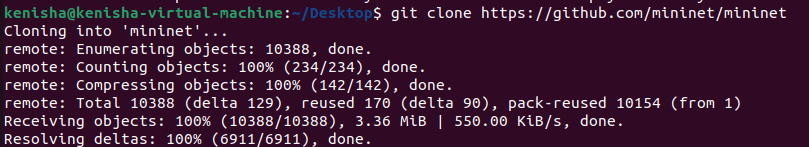
*Figure 1: Network diagram*



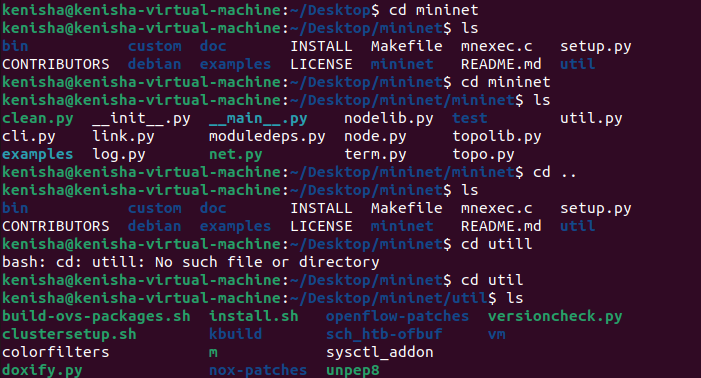
*Figure 2: git clone Installation*



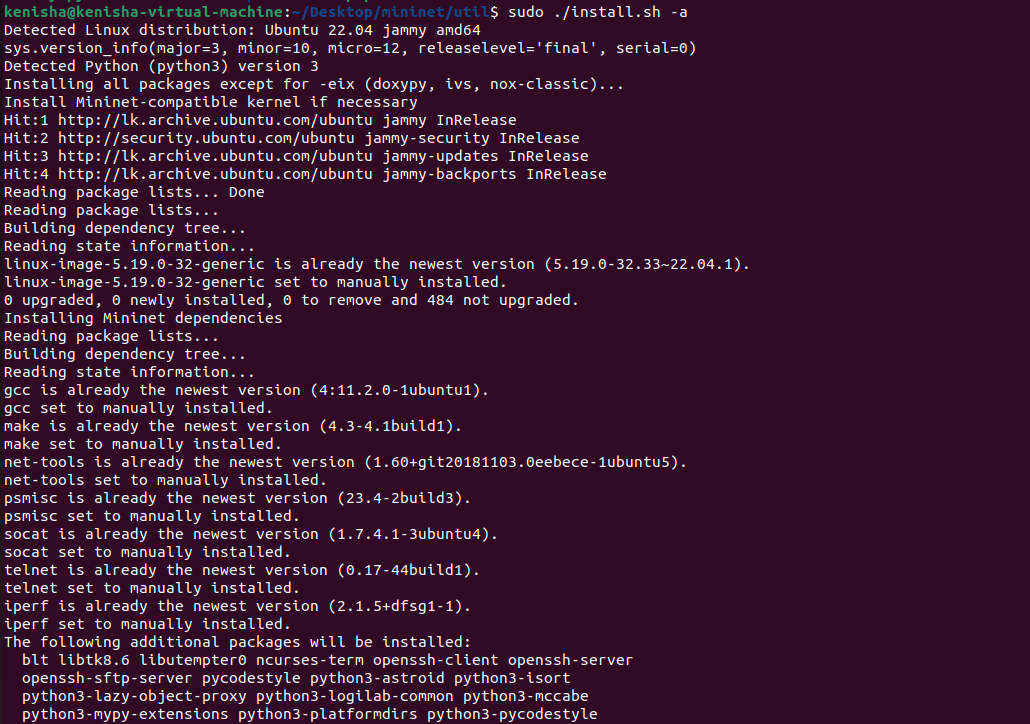
*Figure 3: python3-pip Installation*



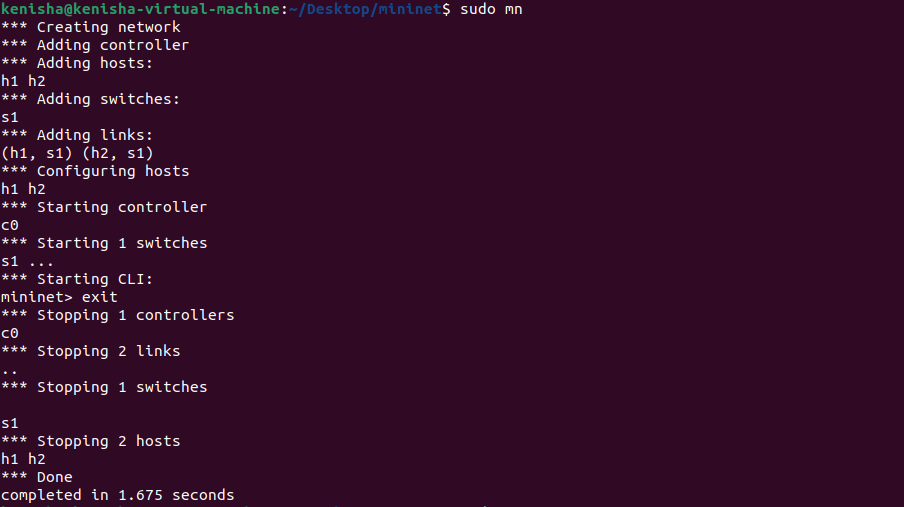
*Figure 4: git clone*



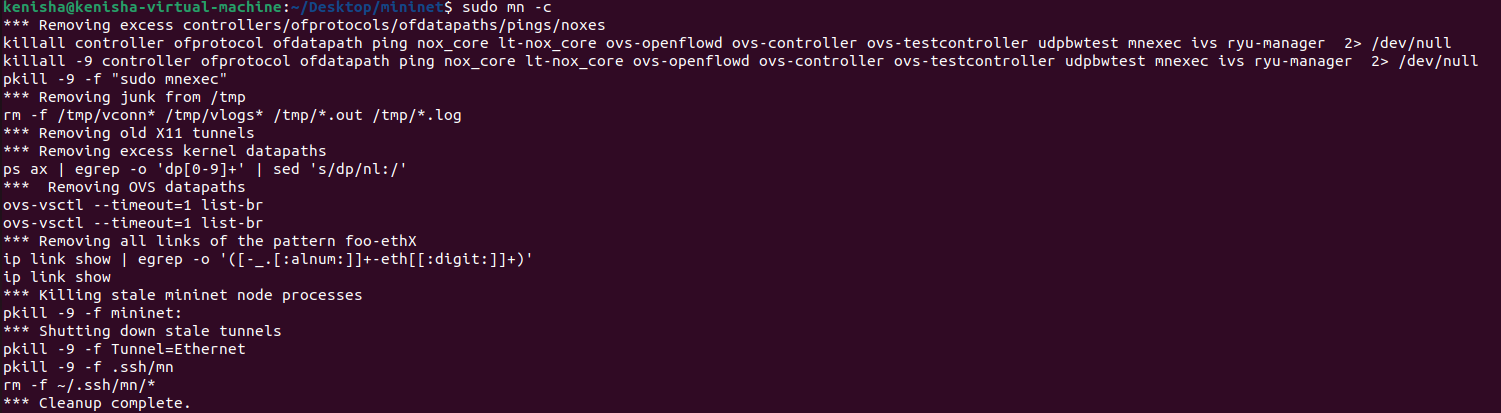
*Figure 5: Navigating Through mininet*



*Figure 6: Running an Executable*



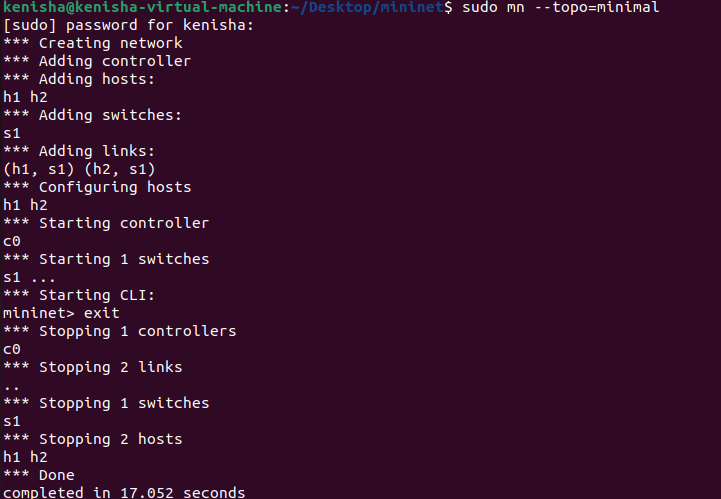
*Figure 7: Creating a Network Topology*



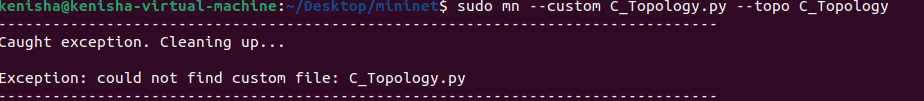
*Figure 8: Cleaning the Topology*

**Node and interface detail**

* First, I set up a simple network scenario of Mininet. By typing the command **sudo mn –topo=minimal,** the topology comprising of one OpenFlow kernel switch connected to two hosts and the OpenFlow reference controller was created. However, the clear design gave me an opportunity to think about the basics of the networks and their setups.

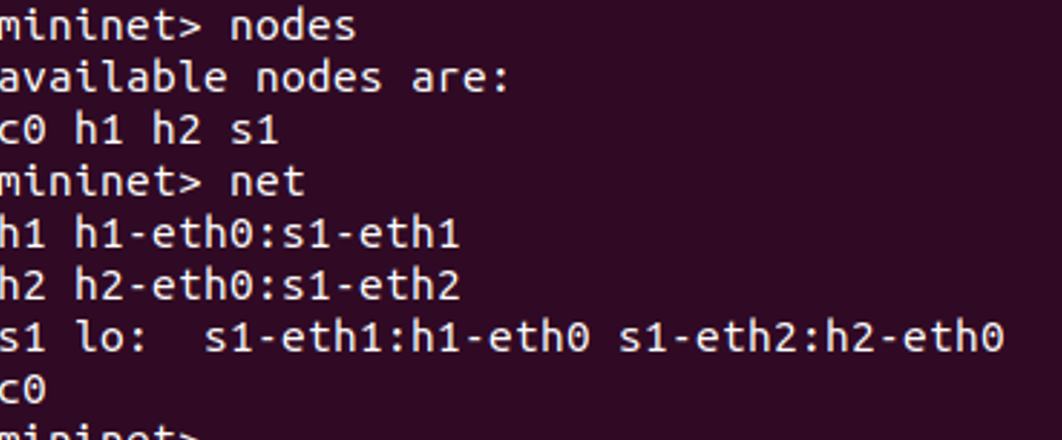


*Figure 9: Started the Topology*



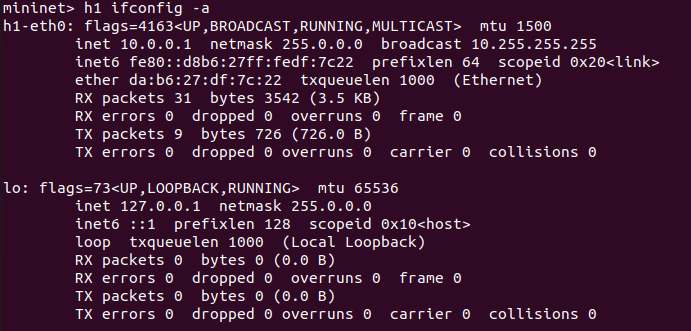
*Figure 10: Cleaning the Topology*

* In order to get a list of nodes in my network, I used the **mininet> nodes** command that gives details of each node that was present. I implemented the aspects of the network topology using **mininet> net**. With such instructions, I was able to confirm the details of the topology configuration. I copied and pasted the above outputs so that you can have a visual feel of the actual network topology.

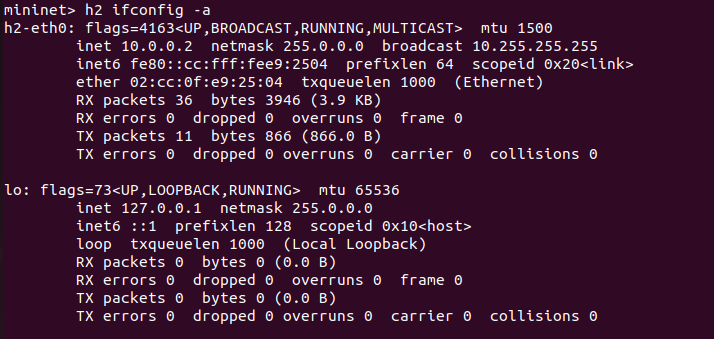


*Figure 11: nodes in the mininet*

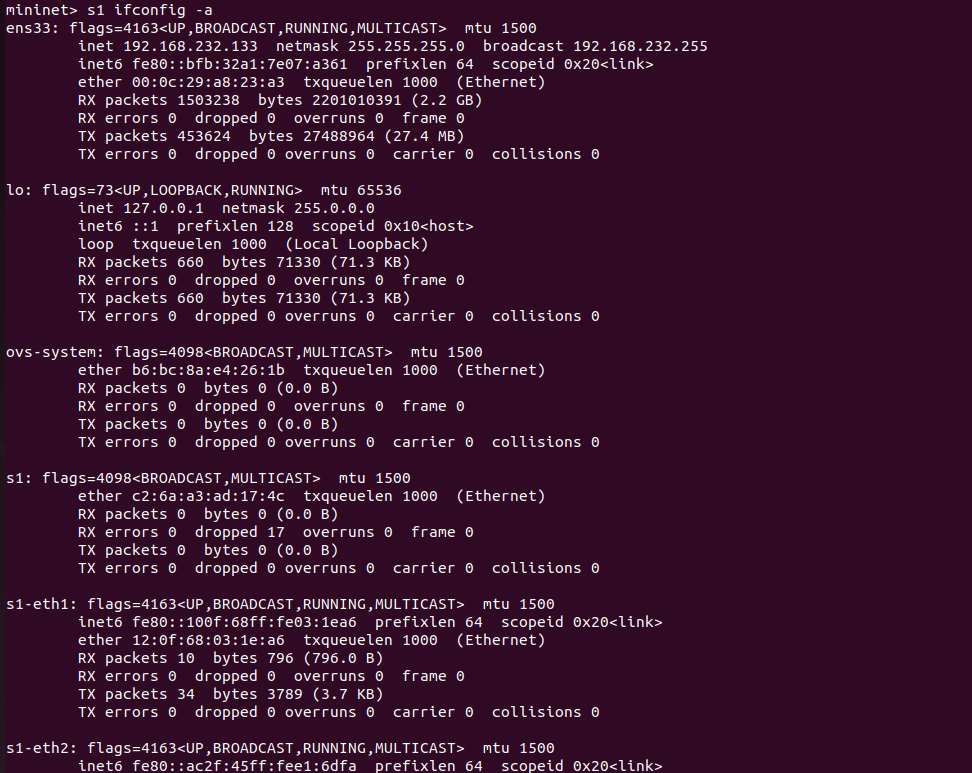
* Hosting mininet, using **mininet>h1 ifconfig -a**, I confirmed that the network interfaces of the hosts and the switch was **mininet>s1 ifconfig -a**. In addition, by typing this command, **mininet> h1 ps –a**. I was able to review the processes running within the host h1. The instructions also provided detailed description of the network settings and host processes. It is why I included related screen grabs to enhance the message’s comprehension.



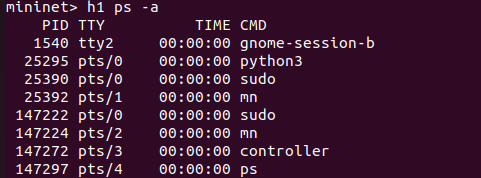
*Figure 12: IP configuration of Host 1*



*Figure 13: IP configuration of Host 2*



*Figure 14: IP configuration of switch 1*

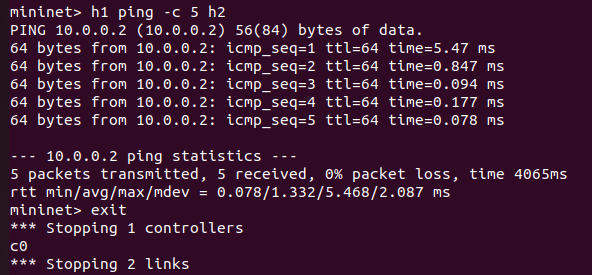


*Figure 15: Processes running in the host*

**Connectivity Testing**

**Ping Testing**

* The connectivity between the two hosts was as determined by the **‘mininet > h1 ping -c5 h2’** command. I entered this command to send five ping requests to host h2. On each try, I noted the ping values in the table below and captured the screenshots of the output results. The results of the test showed the ability of the hosts to interact with each other.



*Figure 16: Pinging test from Host 1 to Host 2*

* It is possible to observe variability in ping times in the figure due to a network delay. Network delay refers to the time taken for a data packet to go from one device and back. It could arise from a number of factors, including:
* In a network with high traffic, it can be filled up with too many traffic that will slow down transfer of data packets. The more cars are on the road the longer time each car they take to get to the intended or required destination.
* Of course, a data packet travelling a longer distance will do this in a longer time. Signal has to travel a longer physical distance and this is what causes this.
* Transmitted data must be understandable by routers and other network devices during the data packets’ travel. Depending on duration of time taken in this process it might add on to total time taken.
* In addition, the dynamics of the selected network equipment may also influence communication latency. This might be arising from hardware that is either overworked, or the computers which are outdated.

**Answer the following Questions**

**Question 01**

1. **Provide three examples of east-west traffic and three examples of north-south traffic in a modern data centre.**

* **East – West Traffic**

The definition also shows that data transport operating in the east-west direction concerns traffic that transverses within the same data centre. For instance, take into account:

**Data Replication**: Data replication in storage devices within a particular data centre ensures redundant data and availability is achieved while data consistency, and disaster recovery is promoted.

**Inter**- **Service Communication:** In a micro services architecture, a large number of services often interact with other services. For example if a payment processing company is using an authentication service to confirm the transaction data there could be lot of internal east-west traffic.

**VM**-**to-VM Communication:** Communication between VMs is the transfer of information between Virtual machines which are living on the same physical host. An application server virtual machine may talk to a database server VM in order to acquire data.

* **North-South Traffic**

The movement of data into or out of a data centre is called north-south traffic. Some examples are as follows:

**Cloud Data Backup:** It is much common already for data centres to contract out from external service providers in the cloud to contain copies of crucial data. This is a type of traffic known as North-South traffic where data is shifted from the data centre to cloud.

**User Access to Cloud Service:** Employees contribute to the formation of north-south traffic if they apply their smart mobile devices to obtain data from cloud applications oriented to the company. An employee working from home having accessed a company’s cloud stored CRM database.

**Client Request to Web Servers:** North-south traffic occurs when a user asks for a website; information goes from the user’s device to the web server at the data centre externally.

(278 words)

1. **Premise of SDN is that the plethora of control plane protocols (discussed in the week 2’s lecture slides 14-18) creates complexity that is not necessary in all networks. Give an example of a network where the complexity is unnecessary and explain why this is so.**

* Small office networks employ complex routing protocols such as; BGP that are normally a preserve of ISPs or large organization networks. Small networks, with less number of devices and less complicated topology, can well use RIP routing or static routing in its true sense**.**
* If BGP is employed further cost is incidental to configuration, maintenance, as well as problem solving. BGP-compatible gear costs higher than a standard gear and they need specialized personnel and operational costs are also high. Also, the administration of network is somehow more complex due to the complexity that is incurred by BGP. Small office managers may not have the knowledge on how to solve the BGP problems, which sometimes may result to network downtime.
* Using RIP or static routing and other similar routing, small organization can suffice their network requirement without incurring further expenses or introducing more sophistication.
* This makes it possible for the network to always be both dependable and effective, relatively cheap to maintain, and easy to manage. It is unadvisable to complicate network solutions because it only leads to discouraging complications and coupled with improper management of resources.

1. words)
2. **What is OpenFlow?**

* Software Defined Networking calls for the application of a communication protocol known as OpenFlow. In implementation it enables the overall exchange of information between the data and the control plane within switches and routers amongst others. While remaining capable of deterministic forwarding, OpenFlow enables programmability and flexibility by giving a central controller the ability to dynamically manage and direct data paths. The graphical separation of the control and the data plane enables network managers to architect traffic flow patterns to suit unique demands thereby increasing ease of management and efficiency.
* Recognizing that the general techniques provided by OpenFlow can increases costs while providing tremendous benefits, using the ability to control the traffic, set up policies and react to alterations in the network instantaneously may help organizations to cut costs while increasing productivity. Its standardized methodology results in a more adaptable and transparent network environment for device interoperability among numerous suppliers. SDN is only possible with OpenFlow technology, which even in today’s complex network structures today enables simple network upgrades, more scalability, and better manageability.
* In summary, OpenFlow means the flexible network control and administration in accordance with key principles and protocols of network management. It assists the businesses to maintain their network operations within the optimum levels of effectiveness and versatility while minimizing the issues of the complexity of a network as well as the cost aspect. Being an important component of SDN, OpenFlow helps to progress from more static network control to a more flexible one.

1. Words)
2. **List essential characteristics of a network to be considered as an SDN network.**

* **Centralised Control:** Software-defined networking rely in a centralised controller that act as the control point for the whole system. This unburdens the network management and optimizes the usage of the resources available for other purposes.
* **Flexibility and Scalability:** By implementation of SDN, there is an increase in the abilities of networks to expand and develop. More devices and services can be readily integrated into the network without causing much interruption while the flow of traffic can also change quickly to meet the new demands.
* **Separation of Control and Data Planes**: SDN separates the control plane that is responsible of deciding where traffic should be forwarded and the data plane that is responsible of actually forwarding the traffic. This leads to more obtaining centralised control as well as affording more flexible administration.
* **Programmability**: Being as programmable as they are, it is quite probable for network managers to perform complex tasks, including repetitive ones, and create further complicated regulatory systems. This means that the amount of human configuration is minimized and the flexibility to change the network is enhanced.
* **Use of Standardised Protocols**: Standardised technologies such as OpenFlow and other protocols that makes it easier for end devices across numerous vendors and create more flexible and open environment for the network are used in SDN.

(213 words)

**Conclusion**

* In the conclusion, I carefully summarized the principal findings and conclusions derived from the completed assignments, giving particular emphasis to the primary roles that network security and SDN assume in the modern networking environments. I spoke on how SDN makes the network environments more flexible, scalable, and centralized apart from discussing on the importance of enhanced security measures that ensure data security and network sanctity.
* Furthermore, based on the intended learning outcomes achieved as part of the assignments, there were tasks such as understanding the nature of SDN architectural design, elements, and the protocols inherent in it. I also learned practical applications of networks security for instance identifying the vulnerabilities and coming up with ways to counter them.

**References**

* East-west Traffic  
  <https://www.pomerium.com/glossary/east-west-traffic>
* North-south Traffic   
  <https://www.pomerium.com/glossary/north-south-traffic>
* Wright, G. (2023) OpenFlow. <https://www.techtarget.com/whatis/definition/OpenFlow>
* Control Plane vs. Data Plane: What Are The Differences? <https://www.splunk.com/en_us/blog/learn/control-plane-vs-data-plane.html>