Designing a Secure network architecture for organisation

Course: Cyber Security & Forensics

Table of Contents

Abstract

Building a secure, available and resilient network is crucial in today's time. In this project, I aim to build a networking simulation of an organisation, where I will be configuring VLANs, IP subnets, switching, bonding and network segmentation via open-source tools. With the ever-growing cyber-attacks, organisations put prime focus on building and managing secure network infrastructure.

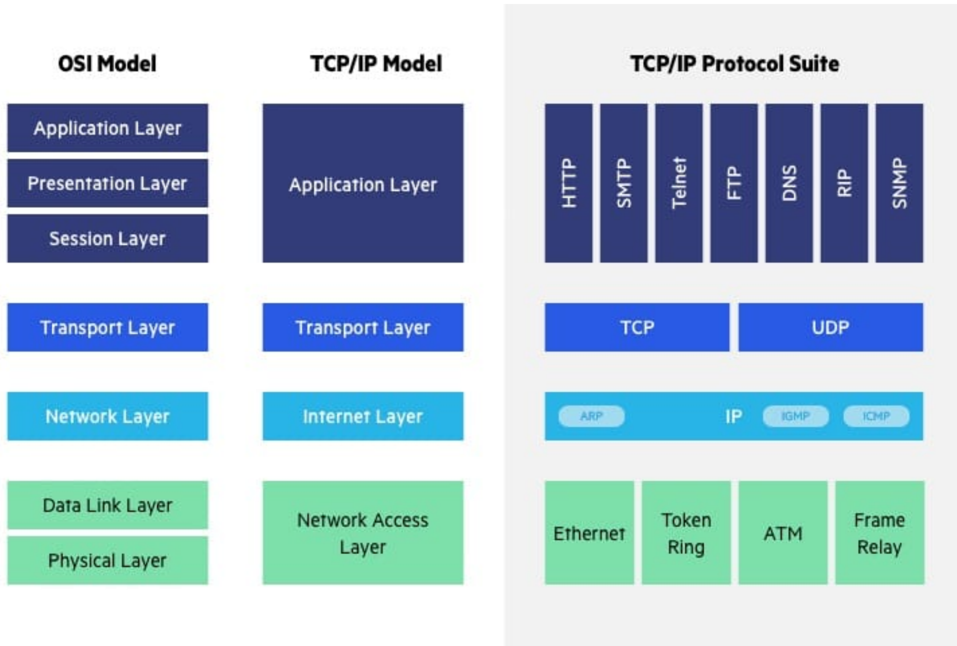
Introduction

The boom and dependence on digital devices have led to complex networks. With complex networks comes an even more complex topic, network security to ensure the CIA triad of security. Cyber security has seen a 12% increase in company spending, in 2021 as compared to last year, to put efforts to merely slow down the attacks. (Sense On)

A network security breach can lead to the loss of money, data, reputation and much more. Hence network engineers face a variety of challenges in order to keep their assets and resources with high availability, throughput, and security. Securing your network consists of many configurations and protocol placements at each layer of networking. Each OSI or TCP layer have their own functionality and its own unique ways to secure these functionalities. In this experiment, we will be focusing on layer 2, the data link layer, implementation and security.

Literature Review

At each networking layer of our OSI or TCP/IP model we implement various tools and protocols to secure its functionality. The first step in building a network architecture is the appropriate linking of devices and placing protocols and configurations to direct the traffic flow on each device. Tier-3 and tier-2 architecture are the current most resilient and scalable hierarchical architectures. New-age solutions such as VLANs, firewalls, VPNs, SIEM, IPS/IDS, zero trust policy, authentication parameters and many more are placed at each layer of the network to ensure confidentiality, integrity and availability for an uptime of 99.9% (Imperva)



Imperva

Model Overview

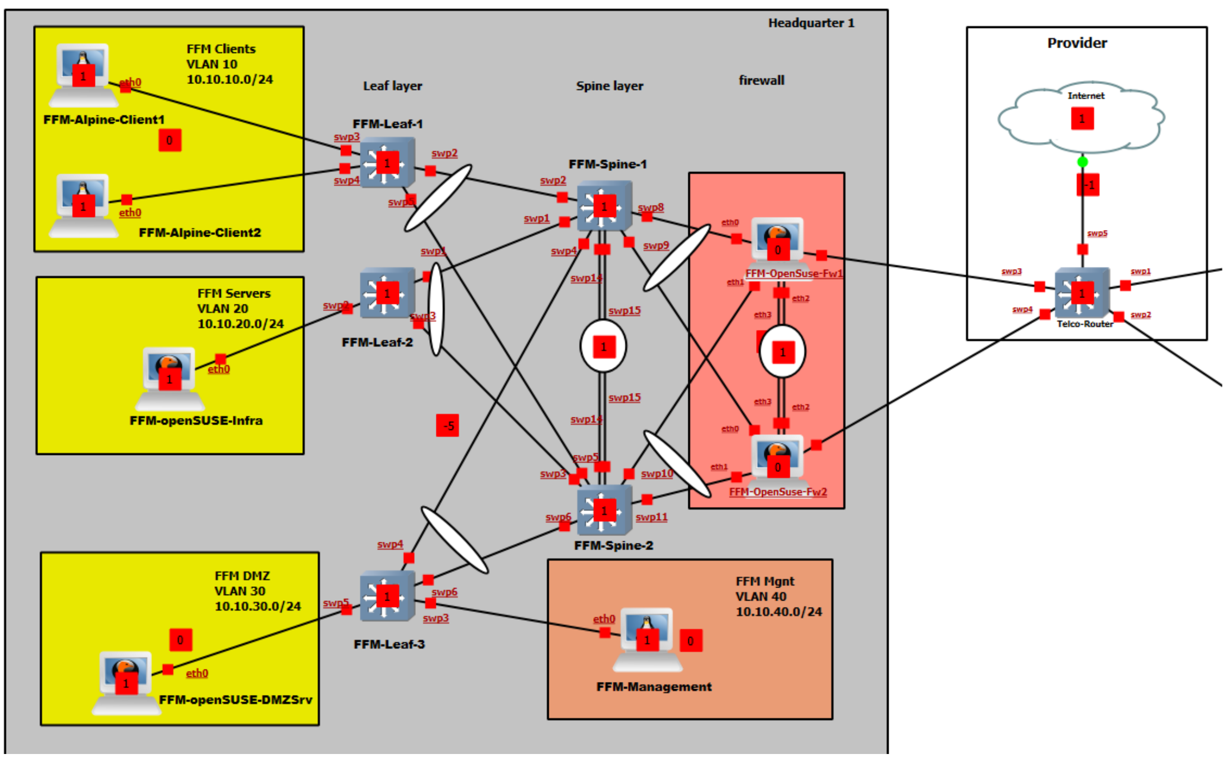
A company's network infrastructure will be replicated following tier-2, leaf-spine, architecture. For the endpoint devices, the network will be broken down into 4 segments which are clients, servers, internet-facing applications, and management respectively. Appropriate leaf-access layer, and spine-core layer configuration and linking will be done to build this. Then bridge mode will be established on the required switch ports so the devices can communicate via layer 2 switching. Measures will be taken to secure these assets and communication traffic, such as each segment will be assigned VLANs and IP subnets, to restrict the switch broadcasts. Connectivity tests will be done to verify this. Spanning Tree protocol will be enabled to prevent redundancy and unauthorized entry into the network and we will confirm this by network traffic monitoring tools such as tcpdump, a CLI alternative to wireshark. Layer 3 switching will be enabled by providing the management VLAN access to control and monitor the entire network traffic for security. Further, the security and efficiency of the network will be enhanced with link bondings to ensure availability and fault tolerance.

While designing important thing to consider is the redundancy to limit any active link or component failure. I will be preventing this through means of switching and bonding. Another major factor would be to consider that if a VLAN spans across multiple departments and access layers switch, it can make all your switches and endpoint devices vulnerable to unauthorized access. Hence it's crucial to ensure that different VLANs are placed across switches and endpoints as per the required function. (Udemy) Below are the open source tools used in this simulation:

Tools	Version	Description
GNS3	Version 2.2.34	To host the simulation

Vmware workstation	16.2.3	To host the below tools (switch, servers) on GNS3 VM.
openSUSE	Qemu version leap 15.3	Used for storage and DMZ server
Alpine linux docker		To represent clients and management system
Cumulus Switch	VX 4.3.0	As the access and core switch
Tcpdump		For network traffic investigation

Research and Result



Bridge enabled on ports 2,3,4,5 for communication via Leaf-1

Above infrastructure is built for this simulation on GNS3. Going ahead with the Spine-leaf tier-2 architecture instead of the tier-3 architecture consisting of core, aggregation and access layer.
In tier-3, we have a core layer that acts as the backbone of the architecture; interconnecting distributed switches and forwarding packets reliably at high speed. Then the aggregation layer acts as a middleman between the core and access layer and performs functions such as routing, filtering, QoS on the traffic it receives. Lastly, the access layer forwards traffic to end-point devices in the hierarchy, such as printers, computers, and phones. Alternatively, in the spine-leaf architecture, the core layer and aggregation layer combine together to form one layer which we can call the spine or core layer. It's solely responsible for forwarding packets and managing routing, filtering, QoS prootocols. The access or leaf layer continues to manage endpoint devices. The spine and leaf together connect in a hierarchical mesh topology form. For

my simulated environment, I am going with this architecture due to its easiness of managing configurations, and improved redundancy with STP (Spanning tree protocol), also in the real world, this architecture is highly preferred in small-medium organizations due to its easiness, low cost, prevention of congestion, high bandwidth and scalability. (Study CCNA, 2021)

Firstly we make four different departments and assign them resources. We have the clients department with 2 client machines using Alpine docker machine. Then we have a servers department where servers such as DHCP, storage and NAC servers are kept. One internet-facing department has our DMZ server. Lastly, a management department to monitor and control the network. Using the spine and leaf structure we add switches and make connections to the endpoints, to build a physical path for communication. Currently, the two client machines cannot talk to each other. To enable communication we have to set bridge mode on the connection switch ports. (Fiber Optic Network) We do so by opening the **Leaf-1** console and running ***net add bridge bridge ports swp2-5***. Switching is now enabled on **Leaf-1** ports 2,3,4 and 5. (Udemy)

```
cumulus@cumulus:mgmt:~$
cumulus@cumulus:mgmt:~$
cumulus@cumulus:mgmt:~$ brctl show
bridge name     bridge id               STP enabled     interfaces
bridge          8000.0c542b9a0002       yes             swp2
                                                        swp3
                                                        swp4
                                                        swp5
cumulus@cumulus:mgmt:~$
```

Bridge enabled on ports 2,3,4,5 for communication via Leaf-1

While enabling switching on these ports, it's also important to distinguish these ports as access or trunk. All ports are by default trunk ports which is a security threat as these ports will allow all traffic to travel across them to reach the endpoint devices. To prevent this we change ports connected to the endpoint device into access ports, unless you want to allow all traffic to travel through it tagged like a firewall. Here we can see that ports 3 and 4 were connected to our clients and hence have been converted to access ports. Now any device connected to these access ports will be contained in the particular designated VLAN of the department. (Geeks for geeks, 2018)

```
Jser     Timestamp                   Command
------   -------------------------   ----------------------------------------
:umulus  2022-10-26 23:24:20.449402  net add interface swp3-4 bridge access 10
:umulus@cumulus:mgmt:~$ net show interface all
State  Name    Spd  MTU    Mode           LLDP  Summary
-----  ------  ---  -----  -------------  ----  -----------------
JP     lo      N/A  65536  Loopback             IP: 127.0.0.1/8
       lo                                       IP: ::1/128
DN     eth0    1G   1500   Mgmt                 Master: mgmt(UP)
ADMDN  swp1    N/A  1500   NotConfigured
JP     swp2    1G   9216   Trunk/L2             Master: bridge(UP)
JP     swp3    1G   9216   Access/L2            Master: bridge(UP)
JP     swp4    1G   9216   Access/L2            Master: bridge(UP)
JP     swp5    1G   9216   Trunk/L2             Master: bridge(UP)
ADMDN  swp6    N/A  1500   NotConfigured
ADMDN  swp7    N/A  1500   NotConfigured
ADMDN  swp8    N/A  1500   NotConfigured
ADMDN  swp9    N/A  1500   NotConfigured
ADMDN  swp10   N/A  1500   NotConfigured
ADMDN  swp11   N/A  1500   NotConfigured
ADMDN  swp12   N/A  1500   NotConfigured
ADMDN  swp13   N/A  1500   NotConfigured
ADMDN  swp14   N/A  1500   NotConfigured
ADMDN  swp15   N/A  1500   NotConfigured
JP     bridge  N/A  9216   Bridge/L2
JP     mgmt    N/A  65536  VRF                  IP: 127.0.0.1/8
       mgmt                                     IP: ::1/128

:umulus@cumulus:mgmt:~$
```

The interface of leaf-1: Trunk ports are 2,5 and access ports are 3,4

Now to protect our network from cyber attacks, we assign different VLAN IDs for each department. VLANs provide a segmentation to switch ports to share packets in a secure, tagged and contained manner. It reduces the packet congestion in the links and unauthorized access. Each VLAN is assigned a specific IP subnet, hence they provide the basic control of the network and packet identification via the VLAN IDs we assign them. It's important to assign different VLANs to switch ports connected to different departments, rather than using the default or native VLAN. Native VLANs will make the network vulnerable, as any machine in the network can access any endpoint device. (Udemy and Juniper Networks)

```
cumulus@FFM-Leaf-1:mgmt:~$ net show bridge vlan

Interface  VLAN  Flags
---------  ----  ---------------------
swp3         10  PVID, Egress Untagged
swp4         10  PVID, Egress Untagged
bond1         1  PVID, Egress Untagged
             10
             20
             30
             40
```

VLAN ID 10 was assigned to leaf-1 ports

Now we have to enable layer 2 protocol STP (spanning tree protocol) on the switch. It performs fault tolerance and eliminates network looping. STP checks for redundant links and blocks them, in the entire network so there are no closed loops performed. Also, in case of any active link failing, STP takes over. STP is enabled by default on cumulus switches and no configuration is required unless one wants to deliberately block some ports or set a rule on some ports. A security issue here can be, if a machine comes into our department and connects to its access ports it can affect the network. It can take up root access and perform elevation of privilege or open a backdoor into your network. Hence, STP allows us to enable admin-edge-port and BPDU guard so that if any unrecognized machine starts sending packets to the access port, the port will be taken down. (Tech Target and Geeks for geeks)

```
cumulus@FFM-Leaf-1:mgmt:~$ net add interface swp3,4 stp portadminedge
cumulus@FFM-Leaf-1:mgmt:~$ net com
--- /etc/network/interfaces     2022-10-26 23:24:26.611000000 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp  2022-10-27 01:19:30.059000000 +0000
@@ -8,24 +8,28 @@
 iface lo inet loopback

 # The primary network interface
 auto eth0
 iface eth0 inet dhcp
     vrf mgmt

 auto swp3
 iface swp3
     bridge-access 10
+    mstpctl-bpduguard yes
+    mstpctl-portadminedge yes

 auto swp4
 iface swp4
     bridge-access 10
+    mstpctl-bpduguard yes
+    mstpctl-portadminedge yes

 auto bridge
 iface bridge
     bridge-ports swp2 swp3 swp4 swp5
     bridge-vids 10 20 30 40
     bridge-vlan-aware yes

 auto mgmt
 iface mgmt
     address 127.0.0.1/8


net add/del commands since the last "net commit"
================================================

User     Timestamp                  Command
-------  -------------------------  ----------------------------------------
cumulus  2022-10-27 01:19:17.341885  net add interface swp3,4 stp bpduguard
cumulus  2022-10-27 01:19:27.518070  net add interface swp3,4 stp portadminedge
cumulus@FFM-Leaf-1:mgmt:~$ mstpctl showportbridge
```

Bpduguard and portadminege enabled on access ports 3 and 4.

```
cumulus@FFM-Leaf-1:mgmt:~$ mstpctl showport bridge
   bond1 8.003 forw 8.000.0C:54:2B:9A:00:02 8.000.0C:54:2B:9A:00:02 8.003 Desg
 E swp3  8.001 forw 8.000.0C:54:2B:9A:00:02 8.000.0C:54:2B:9A:00:02 8.001 Desg
 E swp4  8.002 forw 8.000.0C:54:2B:9A:00:02 8.000.0C:54:2B:9A:00:02 8.002 Desg
cumulus@FFM-Leaf-1:mgmt:~$
```

STP has designated forwarding status to these ports, which can be blocked if a networking loop is found.

Verify the same via Tcpdump, a network traffic monitoring tool. If any unrecognized inbound packet is received at the access port for connection then the port will go down. Below we can see no such inbound packets are coming from the clients at port3, but if they did access port would be down. Outbound packets are not blocked but unrecognised inbound packets are blocked via STP. (Udemy)

```
cumulus@FFM-Leaf-1:mgmt:~$ sudo tcpdump -i swp3,4 not icmp and outbound
[sudo] password for cumulus:
tcpdump: swp3,4: No such device exists
(SIOCGIFHWADDR: No such device)
cumulus@FFM-Leaf-1:mgmt:~$ sudo tcpdump -i swp3 not icmp and outbound
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on swp3, link-type EN10MB (Ethernet), capture size 262144 bytes
01:26:08.037750 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.0c:54:2b:9a:00:02.8002, length 36
01:26:10.038466 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.0c:54:2b:9a:00:02.8002, length 36
01:26:12.038190 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.0c:54:2b:9a:00:02.8002, length 36
01:26:14.037548 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.0c:54:2b:9a:00:02.8002, length 36
^C
4 packets captured
5 packets received by filter
0 packets dropped by kernel
cumulus@FFM-Leaf-1:mgmt:~$ sudo tcpdump -i swp3 not icmp and inbound
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on swp3, link-type EN10MB (Ethernet), capture size 262144 bytes




^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
cumulus@FFM-Leaf-1:mgmt:~$
```

Tcpdump logs

To design our management VLAN, we will perform layer 3 switching. So it can access all devices via SSH and perform host jumping via its designated management VLAN only. For this, we assign IP addresses to our switches, and all subnets will be connected to the management VLAN. Now management VLAN can access all devices under the IP subnets in the environment.

```
cumulus@cumulus:mgmt:~$ net add vlan 40 ip address 10.10.40.102/24
cumulus@cumulus:mgmt:~$ net pen
--- /etc/network/interfaces     2022-10-27 01:06:27.645000000 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp  2022-10-27 02:41:43.377000000 +0000
@@ -22,10 +22,17 @@
 iface bridge
     bridge-ports swp1 swp2 swp3
     bridge-vids 10 20 30 40
     bridge-vlan-aware yes

 auto mgmt
 iface mgmt
     address 127.0.0.1/8
     address ::1/128
     vrf-table auto
+
+auto vlan40
+iface vlan40
+    address 10.10.40.102/24
+    vlan-id 40
+    vlan-raw-device bridge
+



net add/del commands since the last "net commit"
================================================

User     Timestamp                   Command
-------  --------------------------  -------------------------------------------
cumulus  2022-10-27 02:41:41.071395  net add vlan 40 ip address 10.10.40.102/24
cumulus@cumulus:mgmt:~$
```

IP subnet of leaf-2 switch now connects to management VLAN 40

To eliminate single point of failure and increase availability, bandwidth and fault tolerance of our network will perform bonding via LACP, Link Aggregation Control Protocol, and MLAG, Multi Chasis Link aggregation protocol. For LACP we use the 802.3ad mod 4, as it utilizes all slaves, links within the bonding we form, equally and operates them at the same speed, unlike other mods provided by IEEE, for the leaf layer links. For the core layer linking, we used MLAG protocol as it allows two ports on different switches to act as one single interface for bonding, and assign one switch as the backup interface in case of failure further securing our spine-leaf switches. (Nvidia and Udemy)

For a secure network, we have to keep many factors in mind such as limiting unauthorized access to resources, blocking links in case of suspicious traffic flows, and high availability, resilience, throughput of our network. These are achieved by appropriately configuring and placing protocols at the most basic components in our network. In this experiment with the help of open-source tools I have used concepts of VLAN, access and trunk port declaration, STP and bonding protocols on the leaf-spine layer architecture to achieve the most essential and basic network security needed in an organisation.

Conclusion & Future Work

Designing the network requires one to keep many aspects of security and feasibility in mind. In this experiment, we have built a scalable, secure, resilient and available network via switches and end-point devices. Investigated and placed protocols to enable layer 2 and 3 switching.

In present times there are several more essential components that are needed in a network such as Firewall for managing and controlling the traffic entering and leaving our leaf-spine architecture, and managing your own routing table. VPN to accommodate secure connection between an organization's branch offices across geographic locations. NAC servers and authentication parameters for our endpoints devices, and assets. Build protocols around how a remote worker can access these organisations' resources. This project will grow into incorporating all these additional and highly needed security components. Afterwards, we can even perform penetration tests to find vulnerabilities and eliminated them.

References

1) Study CCNA. (2021). Collapsed Core and Three-Tier Network Architectures. [online] Available at: https://study-ccna.com/collapsed-core-and-three-tier-architectures/.
2) Study CCNA. (2021). What is Spine and Leaf Network Architecture? [online] Available at: https://study-ccna.com/spine-and-leaf-architecture/.
3) SenseOn. (n.d.). How Much Should a Business Spend on Cybersecurity? [online] Available at: https://www.senseon.io/resource/how-much-should-a-business-spend-on-cybersecurity/.
4) Fiber Optic Network Products. (2018). Bridge vs. Switch: What's the Difference. [online] Available at: https://www.fiberopticshare.com/bridge-vs-switch-whats-the-difference.html.
5) www.juniper.net. (n.d.). Bridging and VLANs | Junos OS | Juniper Networks. [online] Available at: https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/topic-map/bridging-and-vlans.html [Accessed 28 Oct. 2022].
6) GeeksforGeeks. (2018). Access and trunk ports - GeeksforGeeks. [online] Available at: https://www.geeksforgeeks.org/access-trunk-ports/.
7) docs.nvidia.com. (n.d.). Bonding - Link Aggregation | Cumulus Linux 4.0. [online] Available at: https://docs.nvidia.com/networking-ethernet-software/cumulus-linux-40/Layer-2/Bonding-Link-Aggregation/#:~:text=Linux%20bonding%20provides%20a%20method [Accessed 28 Oct. 2022].
8) docs.nvidia.com. (n.d.). Multi-Chassis Link Aggregation - MLAG | Cumulus Linux 4.2. [online] Available at: https://docs.nvidia.com/networking-ethernet-software/cumulus-linux-42/Layer-2/Multi-Chassis-Link-Aggregation-MLAG/ [Accessed 28 Oct. 2022].
9) SearchNetworking. (n.d.). What is Spanning Tree Protocol? [online] Available at: https://www.techtarget.com/searchnetworking/definition/spanning-tree-protocol. [Accessed 28 Oct. 2022]
10) GeeksforGeeks. (2021). What is BPDU Guard and How to Configure BPDU Guard? [online] Available at: https://www.geeksforgeeks.org/what-is-bpdu-guard-and-how-to-configure-bpdu-guard/. [Accessed 28 Oct. 2022]
11) Secure Networking - A Company Network Project on Open-Source (2022), Udemy Available at: https://www.udemy.com/course/secure-networking-a-company-network-project-on-open-source/ (Accessed: 18 Oct. 2022)
12) Umair (n.d.). OSBoxes - Virtual Machines for VirtualBox & VMware. [online] OSBoxes - Virtual Machines. Available at: https://www.osboxes.org/ [Accessed 20 Oct. 2022].
13) Ali, Md. Nadir & Rahman, M. & Hossain, Syed. (2013). Network architecture and security issues in campus networks. 1-9. 10.1109/ICCCNT.2013.6726595. [Accessed 26 Oct. 2022].
14) Al Hayajneh, A. et al. (2020) Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). Computers. [Online] 9 (1), 8. [online]. Available from: http://dx.doi.org/10.3390/computers9010008. [Accessed 26 Oct. 2022].
15) www.xmodulo.com. (n.d.). Linux TCP/IP networking: net-tools vs. iproute2. [online] Available at: https://www.xmodulo.com/linux-tcpip-networking-net-tools-iproute2.html [Accessed 28 Oct. 2022].