MONASH University

ITO 4137: Architecture and Networks

Assessment 3: Technical Network Configuration Report

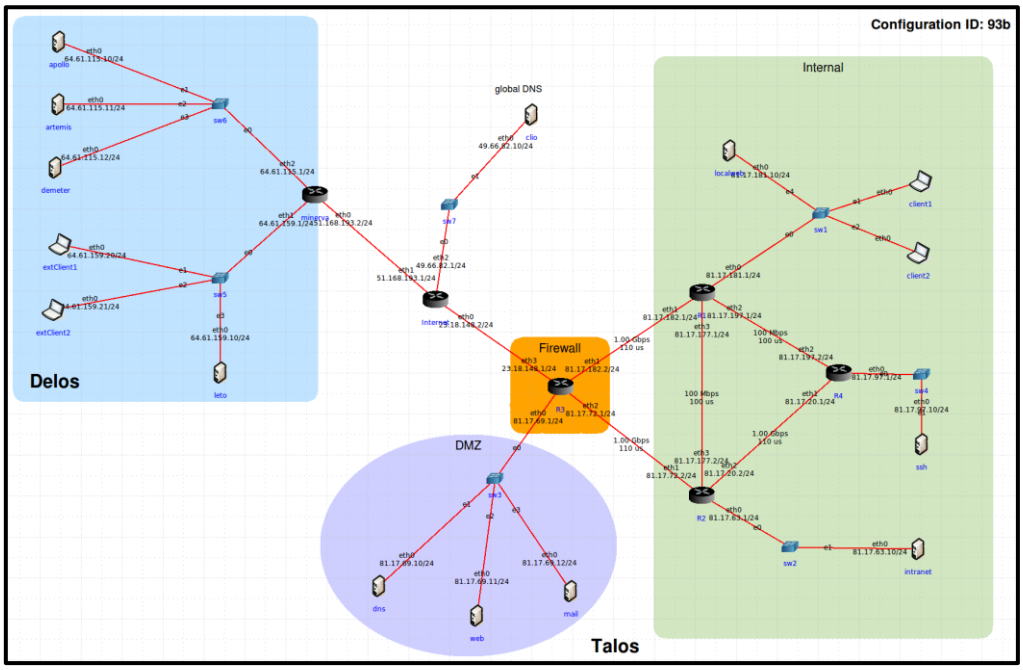
Student Name: Tristan Sim Yook Min
Student ID: 30428831

Date: 19 February 2025

Table of Contents

Task A: Routing

1) Methodology



The diagram above shows the network topology of the Talos and Delos networks. To determine the best static routes, one method for evaluating the most efficient path a router should take to forward packets to a destination is by using the Open Shortest Path First (OSPF) protocol (Moy, 1998). This protocol assigns costs to links based on bandwidth and then applies Dijkstra's Algorithm to calculate the shortest possible path to the destination. (Deep Medhi, 2018)

2) Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) leverages on taking advantage of the faster bandwidth speeds of a given media and interface. Prioritizing the faster bandwidths to maximize data throughput, hence faster links have lower cost and higher priority associated with them. (Moy, 1998)

The OSPF formula used to determine the cost of a link is given in *Equation (i)* below:

$$Cost = \frac{Reference\ Bandwidth}{Link\ Bandwidth} \sim \boldsymbol{Equation\ (i)}$$

$$where, the\ Reference\ Bandwidth = 100\ Mbps$$

Table 1 below: The Link Cost after resolving Equation (i)

Link Bandwidth	Cost
10 Mbps	10
100 Mbps	1
1 Gbps	0.1
10 Gbps	0.01

Task A: Routing

3) Dijkstra's Algorithm

Dijkstra's Algorithm finds the shortest path from a source node to all other nodes in a weighted graph and is also used by the OSPF protocol. (Dijkstra, 1959) It begins with the source node at a cost of 0, while all others are set to infinity. Each router is visited to update the shortest path based on calculated costs. If a new cost is lower than the recorded one and it is updated. The process repeats iteratively until all routers have been visited determine the lowest-cost path. (Deep Medhi, 2018) (Berenike Masinga, 2024)

4) Data Size Threshold Calculation

The Data Size Threshold determines the point at which an alternative path becomes more efficient than the configured route, based on transmission and propagation delays. For example, a lower-bandwidth path with a shorter delay may provide better latency for small data transfers. However, beyond a certain data threshold, a higher-bandwidth path with a longer delay will offer better overall transfer speed. (Shashank Khanvilkar, 2005) It is important to note that propagation delay is the cumulative sum of all delays across each hop in a route.

The Total Delay Formula is shown as *Equation (ii)* below:

$$T_{total} = T_{transmission} + T_{propagation} \quad \sim \boldsymbol{Equation\ (ii)}$$

$$where,$$

$$T_{transmission} = \frac{Data\ Size}{Link\ Bandwidth}$$

$$T_{propogation} = Sum\ of\ Propagation\ Delays\ Across\ all\ Hops$$

The Data Threshold Formula, shown as *Equation (iv)* below, is derived from the Total Delay Formula (Geeks for Geeks, 2024). For a sample calculation, please refer to ***Appendix 1: Data Threshold Sample Calculations for Router R1***.

$$\frac{Data\ Size}{Bandwidth_2} - \frac{Data\ Size}{Bandwidth_1} = T_{propagation\_2} - T_{propagation\_1}$$

$$Data\ Size\ \times \left(\frac{1}{Bandwidth_2} - \frac{1}{Bandwidth_1}\right) = T_{propagation\_2} - T_{propagation\_1}$$

$$\text{Data Threshold} = Data\ Size\ = \frac{T_{propogation2} - T_{propogation1}}{\left(\frac{1}{Bandwidth_2} - \frac{1}{Bandwidth_1}\right)} \quad \sim \boldsymbol{Equation\ (iii)}$$

$$\text{Data Threshold} = Data\ Size\ in\ bits$$

$$\text{Data Threshold} = \frac{Data\ Size\ in\ bits}{8\ bits} = Data\ Size\ Bytes$$

Task A: Routing

5.1) Router R1: Static Route & Data Threshold

Based on the information provided, the best course of action is for Router R1 to forward its network traffic to Router R3 to leverage the 1 Gbps bandwidth and lowest link cost.

Diagram 1 below: The Best Routes for Router 1

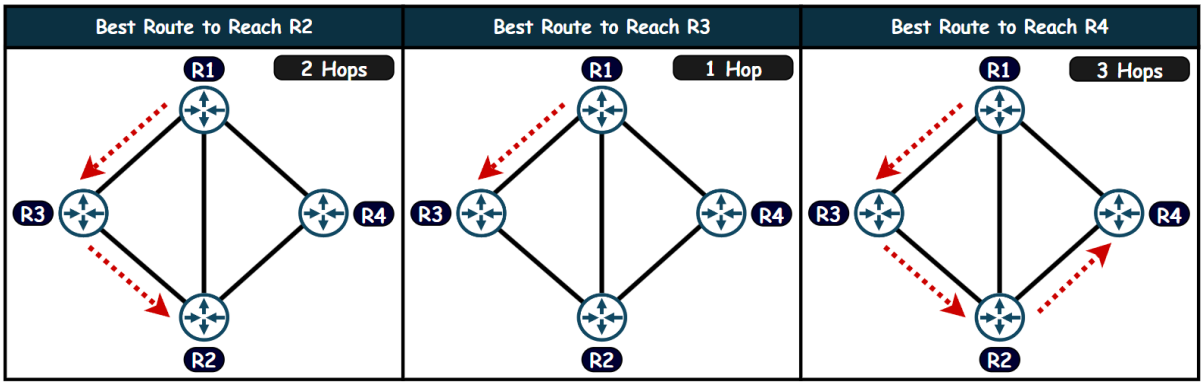


Table 2 below: The Total Link Cost after resolving Equation (ii)

Router	Possible Paths	Link Cost	Link Bandwidth	Propagation Delay	Remarks
R2	R1 → R2	1	100 Mbps	100 µs	-
	R1 → R3 → R2	0.2	1 Gbps	220 µs	Best Route
	R1 → R4→ R2	1.1	100 Mbps	210 µs	-
R3	R1 → R3	0.1	1 Gbps	110 µs	Best Route
	R1 → R2→ R3	1.1	100 Mbps	210 µs	-
	R1 → R4→ R2 → R3	1.2	100 Mbps	320 µs	-
R4	R1 → R4	1	100 Mbps	100 µs	-
	R1 → R2→ R4	1.1	100 Mbps	210 µs	-
	R1 → R3→ R2→ R4	0.3	1 Gbps	330 µs	Best Route

Table 3 below: The Data Threshold Calculation after resolving Equation (iv)

Best Route To R2	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R1 → R3 → R2	1000	220	R1 → R2	100	100	**1.67**
			R1 → R4→ R2	100	210	**0.14**

Route (R1 → R3 → R2) has the highest bandwidth and is better for data size above 1.67 KB. Since Route (R1 → R2) has a lower propagation delay than Route (R1 → R4→ R2), it is still more suitable for handling data smaller than 1.67 KB.

Best Route To R3	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R1 → R3	1000	110	R1 → R2→ R3	100	210	**-1.39**
			R1 → R4→ R2 → R3	100	320	**-2.92**

Route (R1 → R3) will always be the best route for any data size since this route has the highest bandwidth and lowest propagation delay. The negative data threshold on the alternative routes indicate they are never optimal compared with Route (R1 → R3).

Best Route To R4	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R1 → R3→ R2→ R4	1000	330	R1 → R4	100	100	**3.20**
			R1 → R2→ R4	100	210	**1.67**

Route (R1 → R3→ R2→ R4) suitable for data sizes greater than 3.20 KB. However, Route (R1 → R4) will be suitable for data below 3.20 KB.

Task A: Routing

5.2) Router R2: Static Route & Data Threshold

Based on the following information, Router R2 should direct its network traffic to Router R3 and R4 to efficiently forward its network traffic to the intended destinations.

Diagram 2 below: The Best Routes for Router 2

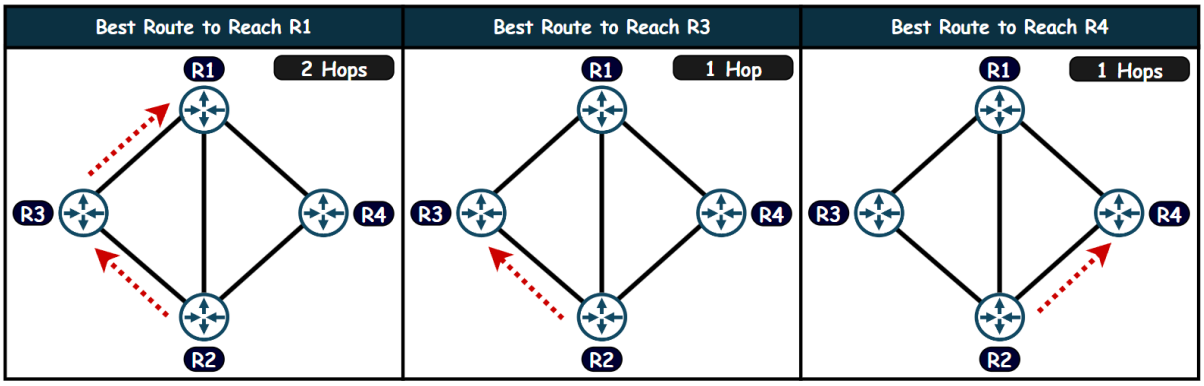


Table 4 below: The Total Link Cost after resolving Equation (ii)

Router	Possible Paths	Link Cost	Link Bandwidth	Propagation Delay	Remarks
R1	R2 → R1	1	100 Mbps	110 µs	-
	R2 → R3→ R1	0.2	1 Gbps	220 µs	Best Route
	R2 → R4 → R1	1.1	100 Mbps	210 µs	-
R3	R2 → R3	0.1	1 Gbps	110 µs	Best Route
	R2 → R1 → R3	1.1	100 Mbps	210 µs	-
	R2 → R4 → R1→ R3	1.2	100 Mbps	320 µs	-
R4	R2 → R4	0.1	1 Gbps	110 µs	Best Route
	R2 → R1 → R4	2	100 Mbps	200 µs	-
	R2 → R3 → R1→ R4	1.2	100 Mbps	320 µs	-

Table 5 below: The Data Threshold Calculation after resolving Equation (iv)

Best Route To R1	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R2 → R3→ R1	1000	220	R2 → R1	100	110	**1.53**
			R2 → R4 → R1	100	210	**0.14**

Route (R2 → R3→ R1) is best route for data size exceeding 1.53 KB. Whilst Route (R2 → R1) is suitable for data size smaller than 1.53 KB due to it having the lowest propagation delay.

Best Route To R3	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R2 → R3	1000	110	R2 → R1 → R3	100	210	**-1.39**
			R2 → R4 → R1→ R3	100	320	**-2.92**

Route (R2 → R3) will always be the best route for any data size since this route has the highest bandwidth and lowest propagation delay. The negative data threshold on the alternative routes indicate they are never optimal compared with Route (R2 → R3).

Best Route To R4	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R2 → R4	1000	110	R2 → R1 → R4	100	200	**-1.25**
			R2 → R3 → R1→ R4	100	320	**-2.92**

Route (R2 → R4) will always be the best route for any data size since this route has the highest bandwidth and lowest propagation delay.

Task A: Routing

5.3) Router R3: Static Route & Data Threshold

Like that of the other Routers, Router R3 also utilizes the faster 1 Gbps bandwidth to maximize network efficiency and direct its traffic to Router R1 and R2 to reach its destinations.

Diagram 3 below: The Best Routes for Router 3

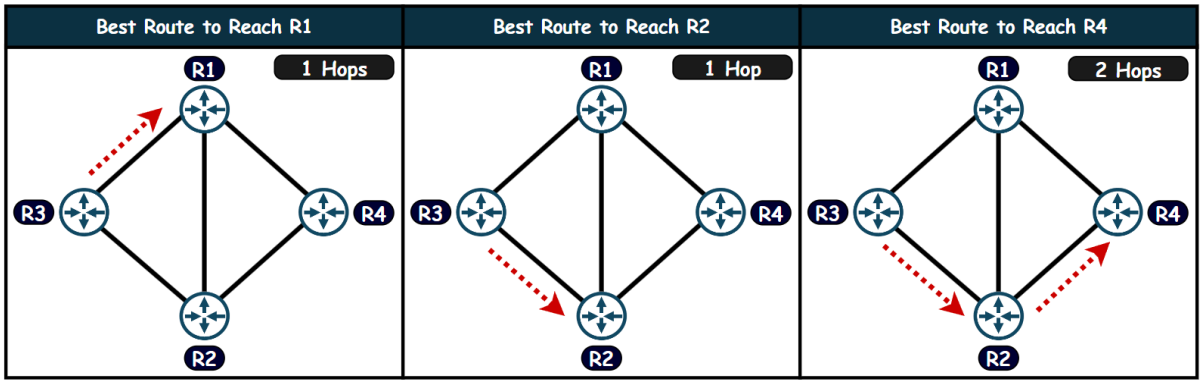


Table 6 below: The Total Link Cost after resolving Equation (ii)

Router	Possible Paths	Link Cost	Link Bandwidth	Propagation Delay	Remarks
R1	R3 → R1	0.1	1 Gbps	110 µs	Best Route
	R3 → R2→ R1	1.1	100 Mbps	210 µs	-
	R3 → R2 → R4→ R1	1.2	100 Mbps	320 µs	-
R2	R3 → R2	0.1	1 Gbps	110 µs	Best Route
	R3 → R1 → R2	1.1	100 Mbps	210 µs	-
	R3 → R1 → R4→ R2	1.2	100 Mbps	320 µs	-
R4	R3 → R2→ R4	0.2	1 Gbps	210 µs	Best Route
	R3 → R1 → R4	1.1	100 Mbps	210 µs	-
	R3 → R2 → R1→ R4	2.1	100 Mbps	310 µs	-

Table 7 below: The Data Threshold Calculation after resolving Equation (iv)

Best Route To R1	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R3 → R1	1000	110	R3 → R2→ R1	100	210	**-1.39**
			R3 → R2 → R4→ R1	100	320	**-2.92**

Route (R3 → R1) has the best bandwidth and lowest propagation delay giving it the best transfer speeds and latency. The negative data threshold on the other routes indicate they are never optimal compared with Route (R3 → R1).

Best Route To R2	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R3 → R2	1000	110	R3 → R1 → R2	100	210	**-1.39**
			R3 → R1 → R4→ R2	100	300	**-2.64**

Route (R3 → R2) has the best bandwidth and lowest propagation delay giving it the best transfer speeds and latency.

Best Route To R4	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R3 → R2→ R4	1000	210	R3 → R1 → R4	100	210	**0**
			R3 → R2 → R1→ R4	100	310	**-1.39**

Route (R3 → R2→ R4) has the best bandwidth and lowest propagation delay giving it the best transfer speeds and latency.

Task A: Routing

5.4) Router R4: Static Route & Data Threshold

Router R4 should forward its packet to Router 2 as it is the route with the fastest network speeds and lowest latency to other Routers in the network.

Diagram 4 below: The Best Routes for Router 4

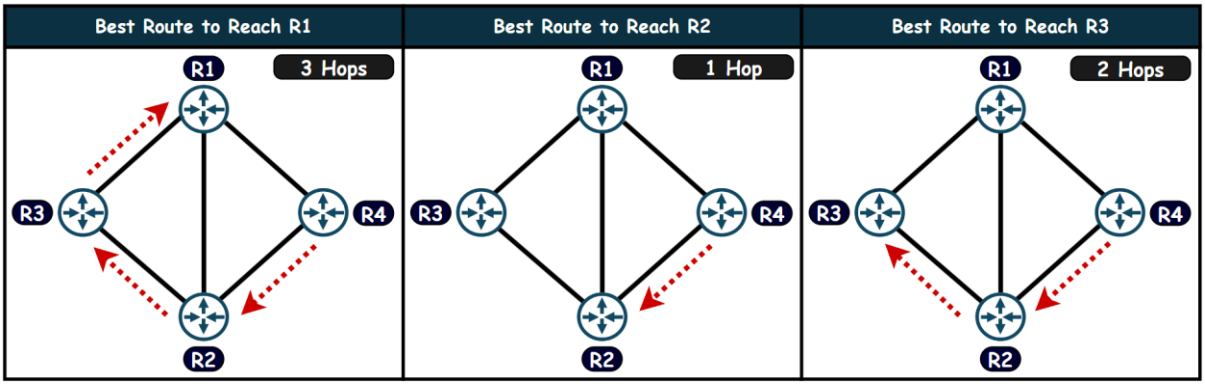


Table 8 below: The Total Link Cost after resolving Equation (ii)

Router	Possible Paths	Link Cost	Link Bandwidth	Propagation Delay	Remarks
R1	R4 → R1	1	100 Mbps	100 µs	-
	R4 → R2→ R1	1.1	100 Mbps	210 µs	-
	R4 → R2 → R3→ R1	0.3	1 Gbps	330 µs	Best Route
R2	R4 → R2	1	1 Gbps	110 µs	Best Route
	R4 → R1 → R2	2	100 Mbps	200 µs	-
	R4 → R1 → R4→ R2	1.2	100 Mbps	320 µs	-
R3	R4 → R2→ R3	0.2	1 Gbps	220 µs	Best Route
	R4 → R1 → R3	1.1	100 Mbps	210 µs	-
	R4 → R2 → R1→ R3	1.2	100 Mbps	320 µs	-

Table 9 below: The Data Threshold Calculation after resolving Equation (iv)

Best Route To R1	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R4 → R2 → R3→ R1	1000	330	R4 → R1	100	100	**3.20**
			R4 → R2→ R1	100	210	**1.67**

Route (R4 → R2 → R3→ R1) has the best bandwidth and is best for data sizes greater than 3.20 KB. Whilst Route (R4 → R1) has better latency for data size smaller than 3.20 KB.

Best Route To R2	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R4 → R2	1000	110	R4 → R1 → R2	100	200	**-1.25**
			R4 → R1 → R4→ R2	100	320	**-2.91**

Route (R4 → R2) has the best bandwidth and lowest propagation delay giving it the best transfer speeds and latency. The negative data threshold on the other route indicates it is never optimal compared with Route (R4 → R2).

Best Route To R3	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R4 → R2→ R3	1000	220	R4 → R1 → R3	100	210	**0.14**
			R4 → R2 → R1→ R3	100	320	**-1.39**

Route (R4 → R2→ R3) performs better when the data size is greater than 0.14 KB whilst Route (R4 → R1 → R3) has better performance with data smaller than 0.14 KB.

Task A: Routing

6) Router Configuration

After performing the analysis to determine the Best Routes, the best static route configurations are tabulated in *Table 10* below and configured persistently on the respective Routers.

Table 10 below: Static Route Configuration

Router	Configuration
R1	# To Default Gateway Router R3 /sbin/ip route add default via 81.17.182.2 # To Router R3 /sbin/ip route add 81.17.69.0/24 via 81.17.182.2 /sbin/ip route add 81.17.63.0/24 via 81.17.182.2 /sbin/ip route add 81.17.97.0/24 via 81.17.182.2 # For Inter-Router Connections /sbin/ip route add 81.17.72.0/24 via 81.17.182.2 /sbin/ip route add 81.17.20.0/24 via 81.17.182.2
R2	# To Default Gateway Router R3 /sbin/ip route add default via 81.17.72.1 # To Router R3 /sbin/ip route add 81.17.69.0/24 via 81.17.72.1 /sbin/ip route add 81.17.181.0/24 via 81.17.72.1 # To Router R4 /sbin/ip route add 81.17.97.0/24 via 81.17.20.1 # For Inter-Router Connections /sbin/ip route add 81.17.182.0/24 via 81.17.72.1 /sbin/ip route add 81.17.197.0/24 via 81.17.20.1
R3	# To Default Gateway Router Internet /sbin/ip route add default via 23.18.148.2 # To Router R1 /sbin/ip route add 81.17.181.0/24 via 81.17.182.1 # To Router R2 /sbin/ip route add 81.17.63.0/24 via 81.17.72.2 /sbin/ip route add 81.17.97.0/24 via 81.17.72.2 # For Inter-Router Connections /sbin/ip route add 81.17.177.0/24 via 81.17.182.1 /sbin/ip route add 81.17.197.0/24 via 81.17.182.1 /sbin/ip route add 81.17.20.0/24 via 81.17.72.2
R4	# To Default Gateway Router R2 to get to Router R3 /sbin/ip route add default via 81.17.20.2 # To Router R2 /sbin/ip route add 81.17.69.0/24 via 81.17.20.2 /sbin/ip route add 81.17.63.0/24 via 81.17.20.2 /sbin/ip route add 81.17.181.0/24 via 81.17.20.2 # For Inter-Router Connections /sbin/ip route add 81.17.182.0/24 via 81.17.20.2 /sbin/ip route add 81.17.72.0/24 via 81.17.20.2 /sbin/ip route add 81.17.177.0/24 via 81.17.20.2

Task A: Routing

7) Border Gateway and Internet Routers

The Router R3 and Minerva are Border Routers for their respective networks. Router R3 also acts as a Default Gateway and Firewall for the Talos Network. However, the Internet Router, situated between Router R3 and Minerva is not configured with any Static/Dynamic Routing Protocols and has been configured to establish connection between Talos and Delos.

Table 11 below: Border/Internet Router Configuration

Router	Roles	Configuration
R3	Firewall, Default Gateway, Border Router	# To Default Gateway Router Internet /sbin/ip route add default via 23.18.148.2
Minerva	Border Router	# To Default Gateway Router Internet /sbin/ip route add default via 51.168.193.1
Internet	Internet Service Provider Router	# Static Route to Talos Network /sbin/ip route 81.17.0.0/16 via 23.18.148.1 # Static Router to Delos Network /sbin/ip route add 64.61.0.0/16 via 51.168.193.2

Task B: Dynamic Host Configuration Protocol (DHCP)

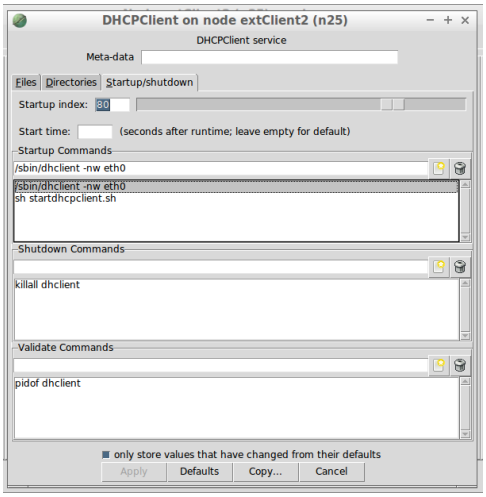
1) Configuration of the DHCP Server

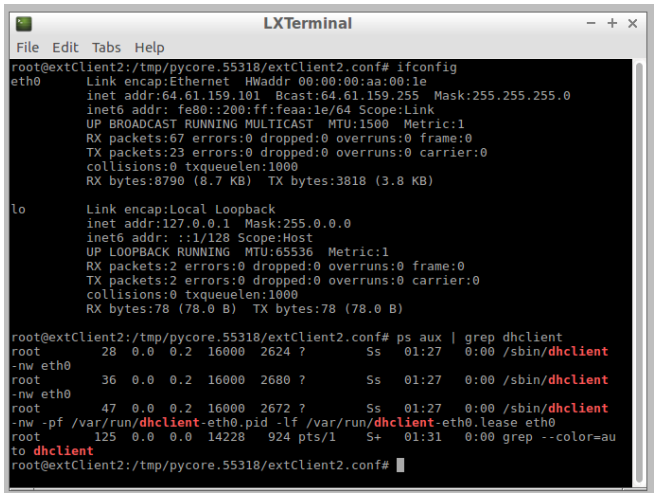
The Minerva router has been configured as the DHCP server for the Delos network. It has been assigned an IP range from 64.61.159.100 to 64.61.159.254 for dynamic allocation, reserving addresses below 100 for static assignment to servers. Therefore, statically assigned addresses, such as Leto (64.61.169.10), will not be affected by the DHCP service. The DHCP server configuration is as follows:

```
log-facility local6;
default-lease-time 36000;
max-lease-time 72000;
ddns-update-style none;

subnet 64.61.159.0 netmask 255.255.255.0 {     # DHCP Service Configuration
  range 64.61.159.100 64.61.159.254;           # Assignable IP range
  option routers 64.61.159.1;                  # Minerva's eth1 as default gateway
  option domain-name-servers 64.61.115.11;     # Artemis (DNS Server)
  option domain-name "delos.edu";
}
```

2) DHCP Service for Client Workstations

The static IP addresses assigned to the Delos clients were removed, but they did not receive an IP address from the DHCP server because the "*dhclient*" service was not running. This service is required for clients to obtain an IP address; however, it did not start automatically when the workstation booted. To resolve this, the command "*/sbin/dhclient -nw eth0*" was added to the Startup Commands of each client to ensure that the DHCP service runs properly. The status of the "*dhclient*" service can be verified by running "*ps aux | grep dhclient*", which retrieves the process ID (PID) of the running service. The required commands are shown below.





Task C: Firewall Configuration

1) Enforce Firewall Default Policy

The first step is to enforce the firewall's default policy, which is to drop all incoming and outgoing traffic. Afterward, based on network requirements, specific rules can be added to allow permitted services to function based on the iptables chain rules. (netfilter, 2024)

```
# Firewall Policy

# Block All Network Traffic
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

2) Internet to Talos De-Militarized Zone (DMZ)

Firewall R3 is configured to allow only intended external traffic from the Internet to access specific services on designated DMZ servers. For example, a web request to “www.talos.edu” triggers a DNS query, which is sent to the Global DNS server and forwarded to the Root DNS server in the Talos DMZ. Only UDP traffic is allowed to reach the DNS server. Once the domain resolves to an IP address, the firewall permits TCP traffic on port 80 for HTTP requests to the web server. A stateful firewall policy ensures that only authorized protocol requests from the Internet are allowed, whilst related responses are permitted back, blocking any unsolicited traffic that does not match an established session.

The firewall chain rule snippet is as follows:

```
# Task C.1: Allow External (Internet) to Access DMZ (DNS, HTTP, SMTP)

# Incoming Rule (Stateful): Allow HTTP Packets to be Forwarded to Web Server
iptables -A FORWARD -i eth3 -o eth0 -d 81.17.69.11 -p tcp --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Outgoing Rule (Stateful): Allow HTTP Packets to be Forwarded to the Internet
iptables -A FORWARD -i eth0 -o eth3 -s 81.17.69.11 -p tcp --sport 80 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Incoming Rule (Stateful): Allow SMTP Packets to be Forwarded to Mail Server
iptables -A FORWARD -i eth3 -o eth0 -d 81.17.69.12 -p tcp --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Outgoing Rule (Stateful): Allow SMTP Packets to be Forwarded to Mail Internet
iptables -A FORWARD -i eth0 -o eth3 -s 81.17.69.12 -p tcp --sport 25 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Incoming Rule (Stateful): Allow UDP Packets to be Forwarded to DNS Server
iptables -A FORWARD -i eth3 -o eth0 -d 81.17.69.10 -p udp --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Outgoing Rule (Stateful): Allow UDP Packets to be Forwarded to DNS Internet
iptables -A FORWARD -i eth0 -o eth3 -s 81.17.69.10 -p udp --sport 53 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Task C: Firewall Configuration

3) Talos De-Militarized Zone (DMZ) to the Internet

Similarly to the first set of rules, Firewall R3 is configured to restrict DMZ servers to initiating only service-specific connections to external servers. For example, the web server can establish HTTP sessions with other HTTP endpoints but cannot access unrelated services such as SMTP or SSH. The firewall enforces a stateful policy, allowing only established connections initiated by DMZ servers whilst blocking any unsolicited traffic.

The firewall chain rule snippet is shown below:

```
# Task C.2: Allow DMZ to Initiate Communication to Internet (Stateful)

# Allow only DMZ Web Server (81.17.69.10) to make HTTP requests
iptables -A FORWARD -i eth0 -o eth3 -s 81.17.69.11 -p tcp --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Allow responses from external web servers back to the DMZ Web Server
iptables -A FORWARD -i eth3 -o eth0 -d 81.17.69.11 -p tcp --sport 80 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow only DMZ Mail Server (81.17.69.11) to send SMTP emails
iptables -A FORWARD -i eth0 -o eth3 -s 81.17.69.12 -p tcp --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Allow responses from the External Mail Server back to the DMZ Server
iptables -A FORWARD -i eth3 -o eth0 -d 81.17.69.12 -p tcp --sport 25 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow only DMZ DNS Server (81.17.69.12) to query external DNS servers
iptables -A FORWARD -i eth0 -o eth3 -s 81.17.69.10 -p udp --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Allow responses from the External DNS Server back to the DMZ Server
iptables -A FORWARD -i eth3 -o eth0 -d 81.17.69.10 -p udp --sport 53 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

4) Talos Internal to Talos De-Militarized Zone (DMZ)

The endpoints of the Talos internal network are granted access to all services provided by the DMZ servers under a more permissive policy, allowing protocols such as ICMP and SSH. However, access is restricted to only three known subnets within the Talos internal network. If a new subnet is added in the future, the firewall rules must be reviewed and updated based on the subnet's authority to ensure proper control and governance. A stateful firewall policy is enforced, allowing internal endpoints to initiate connections to DMZ servers whilst permitting only established responses. However, DMZ servers are strictly prohibited from initiating connections to the Talos internal network, preventing unauthorized access and reducing potential attack surfaces.

The firewall chain rule snippet is as follows:

```
# Task C.3: Allow Internal Hosts of Talos to Reach DMZ (Stateful)

# Allow Internal Subnet 81.17.181.0/24 to Access the DMZ
iptables -A FORWARD -i eth1 -o eth0 -s 81.17.181.0/24 -d 81.17.69.0/24 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Allow responses from DMZ servers back to Internal Subnet
iptables -A FORWARD -i eth0 -o eth1 -s 81.17.69.0/24 -d 81.17.181.0/24 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow Internal Subnet 81.17.97.0/24 to Access the DMZ
iptables -A FORWARD -i eth2 -o eth0 -s 81.17.97.0/24 -d 81.17.69.0/24 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Allow responses from DMZ servers back to the Internal Subnet
iptables -A FORWARD -i eth0 -o eth2 -s 81.17.69.0/24 -d 81.17.97.0/24 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow Internal Subnet 81.17.63.0/24 to Access the DMZ
iptables -A FORWARD -i eth2 -o eth0 -s 81.17.63.0/24 -d 81.17.69.0/24 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Allow responses from DMZ servers back to the Internal Subnet
iptables -A FORWARD -i eth0 -o eth2 -s 81.17.69.0/24 -d 81.17.63.0/24 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Task C: Firewall Configuration

5) Talos Internal Network

A stateless firewall policy has been implemented to facilitate communication within the Talos internal network. It permits a wider range of subnets and larger pool of protocols, ensuring internal connectivity whilst ensuring basic traffic filtering.

The firewall chain rule snippet is shown below:

```
# Task C.4: Allow Internal Host to reach other Internal Host (Stateless)
iptables -A FORWARD -i eth1 -o eth2 -s 81.17.0.0/16 -d 81.17.0.0/16 -j ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 81.17.0.0/16 -d 81.17.0.0/16 -j ACCEPT
```

6) Talos Internal Network to the Internet

For each of the three subnets in the Talos internal network, separate stateful firewall policies have been enforced to ensure stricter governance. Only three services are permitted (HTTP, SMTP and DNS) for outbound traffic to the Internet. These connections must be initiated from the internal network, with the firewall allowing only corresponding established responses back to the endpoints, preventing unsolicited inbound traffic.

The firewall chain rule snippet is as follows:

```
# Task C.5: Allow Internal Nodes to Access Internet Services (Stateful)

# Allow Internal Subnet 81.17.181.0/24 to Initiate Connections to the Internet
iptables -A FORWARD -i eth1 -o eth3 -s 81.17.181.0/24 -p tcp --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth3 -s 81.17.181.0/24 -p tcp --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth3 -s 81.17.181.0/24 -p udp --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Allow Responses from the Internet to Internal Subnet (Stateful)
iptables -A FORWARD -i eth3 -o eth1 -d 81.17.181.0/24 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow Internal Subnet 81.17.97.0/24 to Access Internet Services (Stateful)
iptables -A FORWARD -i eth2 -o eth3 -s 81.17.97.0/24 -p tcp --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth2 -o eth3 -s 81.17.97.0/24 -p tcp --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth2 -o eth3 -s 81.17.97.0/24 -p udp --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Allow Responses from the Internet to Internal Subnet (Stateful)
iptables -A FORWARD -i eth3 -o eth2 -d 81.17.97.0/24 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow Internal Subnet 81.17.63.0/24 to Access Internet Services (Stateful)
iptables -A FORWARD -i eth2 -o eth3 -s 81.17.63.0/24 -p tcp --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth2 -o eth3 -s 81.17.63.0/24 -p tcp --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth2 -o eth3 -s 81.17.63.0/24 -p udp --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Allow Responses from the Internet to Internal Subnet (Stateful)
iptables -A FORWARD -i eth3 -o eth2 -d 81.17.63.0/24 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

7) Talos Internal (81.17.181.0/24) to Secure Shell into Router R3

Endpoints on subnet 81.17.181.0/24, connected to Router R1's eth0 interface, are permitted to establish Secure Shell (SSH) access to Router R3 for configuration. A stateful firewall policy has been enforced, allowing Router R3 to accept SSH connections from 81.17.181.0/24 and respond with the corresponding packets.

The firewall rule appends INPUT and OUTPUT chain rules, as shown below:

```
# Task C.6: Allow the nodes in subnet 81.17.181.0/24 Secure Shell (SSH) to R3
iptables -A INPUT -i eth1 -s 81.17.181.0/24 -p tcp --dport 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -o eth1 -d 81.17.181.0/24 -p tcp --sport 22 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Task C: Firewall Configuration

8) Router R3 ICMP Echo Messages

ICMP echo messages are permitted across the Talos Internal and DMZ network to test reachability across the network. The firewall chain rule snippet is as follows:

```
# Task C.7: Allow the R3 to send and receive ICMP messages

# Allow ICMP Echo Request from Internal Network
iptables -A INPUT -i eth1 -s 81.17.181.0/24 -p icmp -j ACCEPT
iptables -A INPUT -i eth2 -s 81.17.97.0/24 -p icmp -j ACCEPT
iptables -A INPUT -i eth2 -s 81.17.63.0/24 -p icmp -j ACCEPT

# Allow ICMP Echo Reply from Internal Network
iptables -A OUTPUT -o eth1 -d 81.17.181.0/24 -p icmp -j ACCEPT
iptables -A OUTPUT -o eth2 -d 81.17.97.0/24 -p icmp -j ACCEPT
iptables -A OUTPUT -o eth2 -d 81.17.63.0/24 -p icmp -j ACCEPT

# Allow ICMP Echo Request from DMZ
iptables -A INPUT -i eth0 -s 81.17.69.0/24 -p icmp -j ACCEPT
iptables -A OUTPUT -o eth0 -d 81.17.69.0/24 -p icmp -j ACCEPT
```

9) Firewall Configuration Test

Firewall policies on Router R3 were tested across Delos, Talos DMZ, and the Talos Internal Network. Alongside manual testing, a shell script was used for automation, with its source code included in ***Appendix 2: Firewall Test Shell Scripts***. To use the shell script, create it using "*nano FirewallTest.sh*", paste the source code inside, and confirm the changes. Next, grant execute permissions with "*chmod +x FirewallTest.sh*", then run the script using "*./FirewallTest.sh*". For more details on the test results, including Wireshark packet captures, please refer to ***Appendix 3: Snapshot of Firewall Tests***.

The firewall successfully permits traffic from Delos to the Talos DNS, Web Server, and Mail Server, verified by successful DNS queries and 3-way TCP handshakes. It enforces role-based restrictions on DMZ servers, ensuring that only designated services are accessible. Unauthorized traffic to the Talos internal network is blocked, with unsolicited SSH and ICMP Echo Requests discarded and is confirmed by the missing of responses from Router R3 eth3.

Designated DMZ servers can initiate connections only within their permitted service roles. As verified by the test script, the Web Server successfully connected to the Delos Web Server over HTTP, whilst its SMTP request to the Delos Mail Server was blocked. The Web Server was unable to initiate connections to the higher-trust Talos Internal Network, maintaining internal security. However, ICMP Echo messages to the router were allowed.

Endpoints in the Talos Internal Network can initiate connections to the Internet only over whitelisted ports (DNS, HTTP, and SMTP), whilst all other traffic, such as SSH and ICMP, is blocked. Since the DMZ is a lower-trust zone, Talos Internal has full access to DMZ servers, including SSH and ICMP, in addition to other authorized services. Talos internal endpoints can freely access services, following a more permissive stateless firewall policy, ensuring broader communication within the trusted environment. Only endpoints in subnet 81.17.181.0/24 can SSH into Router R3, all other subnets are dropped.

References

Berenike Masinga, N. L. E. B., 2024. *Computing All Shortest Passenger Routes with a Tropical Dijkstra Algorithm.* [Online]
Available at: https://arxiv.org/abs/2412.14654
[Accessed 16 February 2025].

Deep Medhi, K. R., 2018. Chapter 2 - Routing Algorithms: Shortest Path, Widest Path, and Spanning Tree. In: *Network Routing Algorithms, Protocols, and Architecture.* s.l.:Elsevier Inc., pp. 30-63.

Dijkstra, E., 1959. A note on two problems in connexion with graphs. In: *Numerische Mathematik, .* s.l.:Springer, pp. 269-271.

Geeks for Geeks, 2024. *Delays in Computer Network.* [Online]
Available at: https://www.geeksforgeeks.org/delays-in-computer-network/
[Accessed 16 February 2025].

Moy, J., 1998. *OSPF Version 2. RFC 2328, Internet Engineering Task Force.* [Online]
Available at: https://datatracker.ietf.org/doc/html/rfc2328
[Accessed 16 February 2025].

netfilter, 2024. *Configuring chains.* [Online]
Available at: https://wiki.nftables.org/wiki-nftables/index.php/Configuring_chains
[Accessed 16 February 2025].

Shashank Khanvilkar, F. B. D. S. A. K., 2005. Chapter 7 - Multimedia Networks and Communication. In: W. CHEN, ed. *The Electrical Engineering Handbook.* s.l.:Elsevier Inc., pp. 401- 425.

Appendix 1: Data Threshold Sample Calculations for Router R1

Data Threshold Calculation for Router R1 to reach Router R2:

Best Route To R2	Bandwidth (Mbps)	Propagation Delay (µs)	Other Routes	Bandwidth (Mbps)	Propagation Delay (µs)	Data Threshold (Kilo Bytes)
R1 → R3 → R2	1000	220	R1 → R2	100	100	**1.67**
			R1 → R4→ R2	100	210	**0.14**

Sample Calculations comparing route R1 → R3 → R2 to R1 → R2:

$$\text{Data Threshold} = \textit{Data Size} = \frac{T_{propogation2} - T_{propogation1}}{\left(\frac{1}{Bandwidth_2} - \frac{1}{Bandwidth_1}\right)} \sim \boldsymbol{Equation\ (iii)}$$

$$\text{Data Threshold} = \frac{220 \times 10^{-6} - 100 \times 10^{-6}}{\left(\frac{1}{1000 \times 10^{6}} - \frac{1}{100 \times 10^{6}}\right)}$$

$$\text{Data Threshold} = \frac{120 \times 10^{-6}}{9 \times 10^{-9}}$$

$$\text{Data Threshold} = 13.33 \times 10^{3}\ bits = 13.33 Kilo\ Bits$$

$$\text{Data Threshold} = \frac{13.33 \times 10^{3}\ bits}{8\ bits} = \boldsymbol{1.67\ Kilo\ Bytes\ (Answer)}$$

Sample Calculations comparing route R1 → R3 → R2 to R1 → R4 → R2:

$$\text{Data Threshold} = \textit{Data Size} = \frac{T_{propogation2} - T_{propogation1}}{\left(\frac{1}{Bandwidth_2} - \frac{1}{Bandwidth_1}\right)} \sim \boldsymbol{Equation\ (iii)}$$

$$\text{Data Threshold} = \frac{220 \times 10^{-6} - 210 \times 10^{-6}}{\left(\frac{1}{1000 \times 10^{6}} - \frac{1}{100 \times 10^{6}}\right)}$$

$$\text{Data Threshold} = \frac{10 \times 10^{-6}}{9 \times 10^{-9}}$$

$$\text{Data Threshold} = 1.11 \times 10^{3}\ bits = 1.11\ Kilo\ Bits$$

$$\text{Data Threshold} = \frac{1.11 \times 10^{3}\ bits}{8\ bits} = \boldsymbol{0.14\ Kilo\ Bytes\ (Answer)}$$

Appendix 2: Firewall Test Shell Scripts

Delos Client Endpoint Firewall Test Script:

```
#!/bin/bash
# Change Read/Write/Execute Permission to Run: chmod +X FirewallTest.sh
# To Execute: ./FirewallTest.sh

echo ""
echo "Endpoint IP Address: $(hostname -I | awk '{print $1}')"
echo "Executing Delos to Firewall Test Script..."
echo ""

check_connection() {
    local EXPECTED_BLOCKED=$3
    echo -n "$1: "
    eval "timeout 5 $2" &> /dev/null
    if [ $? -eq 0 ]; then
        if [ "$EXPECTED_BLOCKED" == "yes" ]; then
            echo "❌ Test Failed"
        else
            echo "☑ Success"
        fi
    else
        if [ "$EXPECTED_BLOCKED" == "yes" ]; then
            echo "☑ Successfully Blocked"
        else
            echo "❌ Test Failed"
        fi
    fi
}

# Task C.1: External → DMZ Services
echo "Testing Delos → DMZ Servers"
check_connection "Delos → DMZ Web Server (HTTP) using Lynx" "lynx -dump www.talos.edu"
check_connection "Delos → DMZ Mail Server (SMTP) using Netcat" "nc -zv mail.talos.edu 25"
check_connection "Delos → DMZ DNS Server (DNS Query)" "dig @49.66.82.10 talos.edu"
# Expected to be Blocked by Firewall
check_connection "Delos → DMZ SSH" "ssh -o ConnectTimeout=5 muni@81.17.69.11" "yes"
check_connection "Delos → DMZ ICMP" "ping -c 5 81.17.69.11" "yes"
echo ""

# Task C.2: Delos → Delos Internal Servers
echo "Testing Delos → Delos Servers"
check_connection "Delos → Delos Web Server (HTTP) using Lynx" "lynx -dump www.delos.edu"
check_connection "Delos → Delos Mail Server (SMTP) using Netcat" "nc -zv mail.delos.edu 25"
check_connection "Delos → Delos DNS Query using Dig" "dig @49.66.82.10 delos.edu"
echo ""

# Task C.3: Delos → Talos Internal Servers (Blocked by Firewall)
echo "Testing Delos → Talos Internal Servers"
check_connection "Delos → Talos Intranet Server (HTTP) using Lynx" "lynx -dump 81.17.63.10" "yes"
check_connection "Delos → Talos Local Web Server (HTTP) using Lynx" "lynx -dump 81.17.181.10" "yes"
# SSH Access (Blocked by Firewall)
check_connection "Delos → Talos Intranet Server (SSH)" "ssh -o ConnectTimeout=5 muni@81.17.63.10" "yes"
check_connection "Delos → Talos Local Web Server (SSH)" "ssh -o ConnectTimeout=5 muni@81.17.181.10" "yes"
check_connection "Delos → Talos Router R3 (SSH)" "ssh -o ConnectTimeout=5 muni@81.17.182.2" "yes"
# Ping Tests (Blocked by Firewall)
check_connection "Delos → Talos Intranet Web Server (ICMP)" "ping -c 5 81.17.63.10" "yes"
check_connection "Delos → Talos Local Web Server (ICMP)" "ping -c 5 81.17.181.10" "yes"
check_connection "Delos → Talos Router R3 Server (ICMP)" "ping -c 5 81.17.182.2" "yes"

echo ""
echo "☑ Firewall Test Completed."
echo ""
```

Appendix 2: Firewall Test Shell Scripts

DMZ Web Server Firewall Test Script:

```
#!/bin/bash
# Change Read/Write/Execute Permission to Run: chmod +X FirewallTest.sh
# To Execute: ./FirewallTest.sh

echo ""
echo "Endpoint IP Address: $(hostname -I | awk '{print $1}')"
echo "Executing DMZ to Firewall Test Script..."
echo ""

check_connection() {
    local EXPECTED_BLOCKED=$3
    echo -n "$1: "
    eval "timeout 5 $2" &> /dev/null
    if [ $? -eq 0 ]; then
        if [ "$EXPECTED_BLOCKED" == "yes" ]; then
            echo "❌ Test Failed"
        else
            echo "☑ Success"
        fi
    else
        if [ "$EXPECTED_BLOCKED" == "yes" ]; then
            echo "☑ Successfully Blocked"
        else
            echo "❌ Test Failed or Timed Out"
        fi
    fi
}

# Internal DMZ
echo "Testing  DMZ → DMZ Servers"
check_connection "DMZ → DMZ Web Server (HTTP) using Lynx" "lynx -dump www.talos.edu"
check_connection "DMZ → DMZ Mail Server (SMTP) using Netcat" "nc -zv mail.talos.edu 25"
check_connection "DMZ → DMZ DNS Server (ICMP)" "ping -c 5 81.17.69.10"
check_connection "DMZ → DMZ Mail Server (ICMP)" "ping -c 5 81.17.69.12"
echo ""

# External Services (Allowed by Firewall)
echo "Testing DMZ → External Services"
check_connection "DMZ → Delos Web Server (HTTP) using Lynx" "lynx -dump www.delos.edu"
check_connection "DMZ → Delos Mail Server (SMTP) using Netcat" "nc -zv mail.delos.edu 25" "yes"
echo ""

# Talos Internal Servers (Blocked by Firewall)
echo "Testing DMZ → Talos Internal Servers"
check_connection "DMZ → Talos Intranet Server (HTTP) using Lynx" "lynx -dump 81.17.63.10" "yes"
check_connection "DMZ → Talos Local Web Server (HTTP) using Lynx" "lynx -dump 81.17.181.10" "yes"
# SSH Access (Blocked by Firewall)
check_connection "DMZ → Talos Intranet Server (SSH)" "ssh -o ConnectTimeout=5 muni@81.17.63.10" "yes"
check_connection "DMZ → Talos Local Web Server (SSH)" "ssh -o ConnectTimeout=5 muni@81.17.181.10" "yes"
check_connection "DMZ → Talos Router R3 (SSH)" "ssh -o ConnectTimeout=5 muni@81.17.182.2" "yes"
# Ping Tests (Blocked by Firewall)
check_connection "DMZ → Talos Intranet Web Server (ICMP)" "ping -c 5 81.17.63.10" "yes"
check_connection "DMZ → Talos Local Web Server (ICMP)" "ping -c 5 81.17.181.10" "yes"
check_connection "DMZ → Talos Router R3 Server (ICMP)" "ping -c 5 81.17.69.1"

echo ""
echo "☑ Firewall Test Completed."
echo ""
```

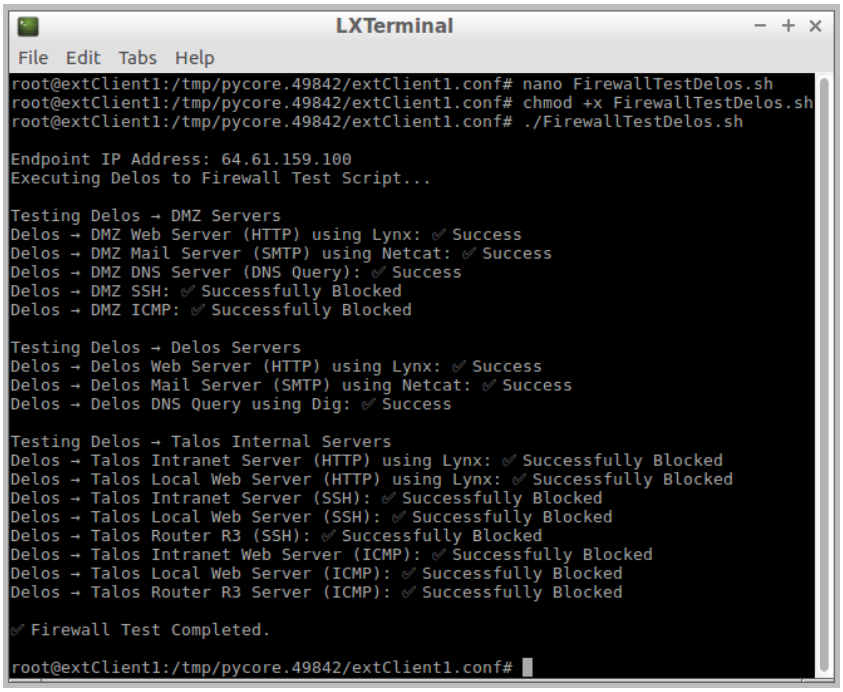
Appendix 2: Firewall Test Shell Scripts

Talos Internal Client Firewall Test Script:

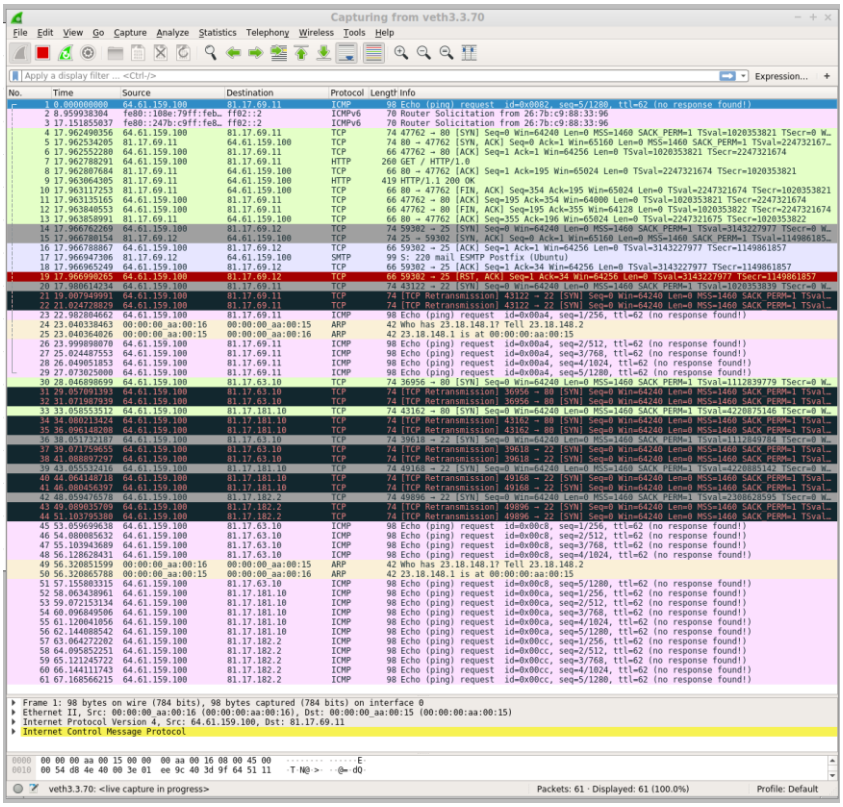
```
#!/bin/bash
# Change Read/Write/Execute Permission to Run: chmod +X FirewallTest.sh
# To Execute: ./FirewallTest.sh

echo ""
echo "Endpoint IP Address: $(hostname -I | awk '{print $1}')"
echo "Executing Talos Internal to Firewall Test Script..."
echo ""

check_connection() {
    local EXPECTED_BLOCKED=$3
    echo -n "$1: "
    eval "timeout 5 $2" &> /dev/null
    if [ $? -eq 0 ]; then
        if [ "$EXPECTED_BLOCKED" == "yes" ]; then
            echo "❌ Test Failed"
        else
            echo "☑ Success"
        fi
    else
        if [ "$EXPECTED_BLOCKED" == "yes" ]; then
            echo "☑ Successfully Blocked"
        else
            echo "❌ Test Failed"
        fi
    fi
}

# Internal → DMZ Services (Allowed by Firewall)
echo "Testing Internal → DMZ Servers"
check_connection "Internal → DMZ Web Server (HTTP) using Lynx" "lynx -dump www.talos.edu"
check_connection "Internal → DMZ Mail Server (SMTP) using Netcat" "nc -zv mail.talos.edu 25"
check_connection "Internal → DMZ DNS Server (ICMP)" "ping -c 5 81.17.69.10"
check_connection "Internal → DMZ Web Server (SSH - Port Check)" "nc -zv 81.17.69.11 22"
check_connection "Internal → DMZ Mail Server (SSH - Port Check)" "nc -zv 81.17.69.12 22"
echo ""

# Internal → External Services (Allowed by Firewall)
echo "Testing Internal → External Services"
check_connection "Internal → Delos Web Server (HTTP) using Lynx" "lynx -dump www.delos.edu"
check_connection "Internal → Delos Mail Server (SMTP) using Netcat" "nc -zv mail.delos.edu 25"
check_connection "Internal → Delos Web Server (ICMP)" "ping -c 5 www.delos.edu" "yes"
check_connection "Internal → Delos Maileb Server (ICMP)" "ping -c 5 mail.delos.edu" "yes"
check_connection "Internal → Delos Web Server (SSH - Port Check)" "nc -zv www.delos.edu" "yes"
check_connection "Internal → Delos Mail Server (SSH - Port Check)" "nc -zv mail.delos.edu" "yes"
echo ""

# Internal → Talos Internal Servers (Blocked by Firewall)
echo "Testing Internal → Talos Internal Servers"
check_connection "Internal → Talos Intranet Server (HTTP)" "lynx -dump 81.17.63.10"
check_connection "Internal → Talos Local Web Server (HTTP)" "lynx -dump 81.17.181.10"
# SSH Access (Allowed or Blocked by Firewall)
check_connection "Internal → Talos SSH Server (SSH - Port Check)" "nc -zv 81.17.97.10 22"
check_connection "Internal → Talos Local Web Server (SSH - Port Check)" "nc -zv 81.17.181.10 22"
check_connection "Internal → Talos Router R3 (SSH - Port Check)" "nc -zv 81.17.182.2 22"
# Ping Tests (Blocked by Firewall)
check_connection "Internal → Talos Intranet Web Server (ICMP)" "ping -c 5 81.17.63.10"
check_connection "Internal → Talos Local Web Server (ICMP)" "ping -c 5 81.17.181.10"
check_connection "Internal → Talos Router R3 Server (ICMP)" "ping -c 5 81.17.69.1"

echo ""
echo "☑ Firewall Test Completed."
echo ""
```

Appendix 3: Snapshot of Firewall Tests

Delos Client Endpoint Firewall Test Results (Shell Script):

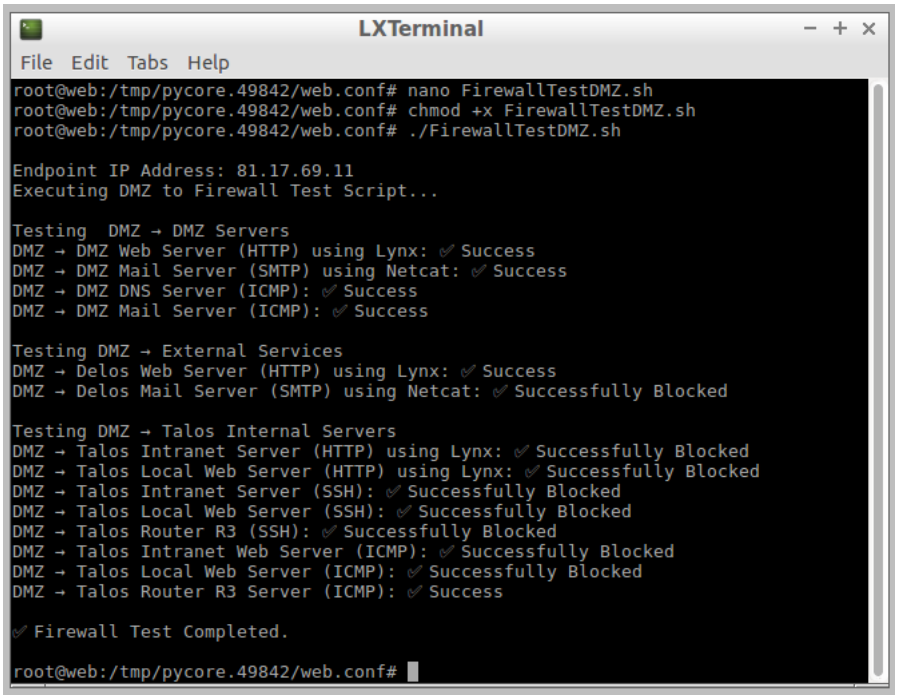


Firewall R3 eth3 Test Results (Wireshark):

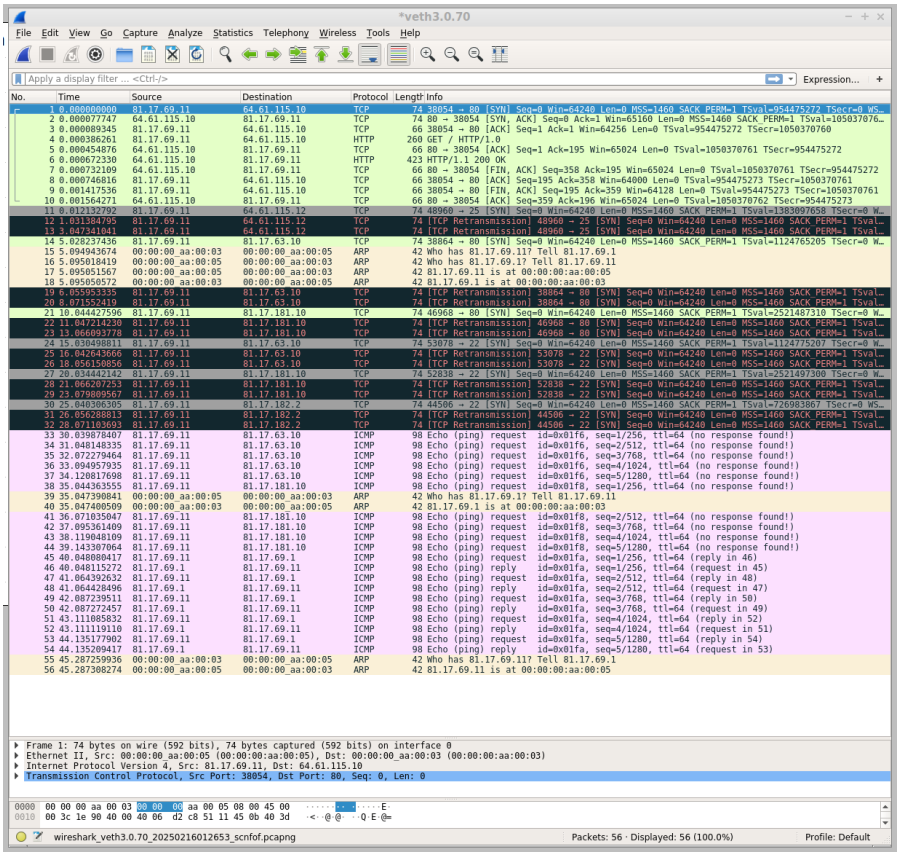


Appendix 3: Snapshot of Firewall Tests

DMZ Web Server Firewall Test Results (Shell Script):

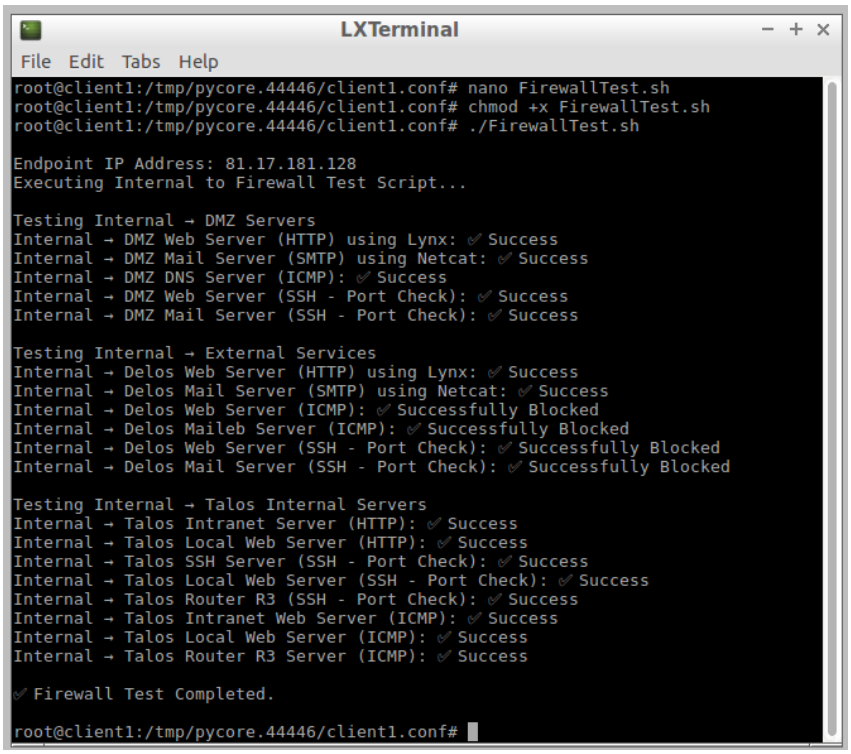


Firewall R3 eth0 Test Results (Wireshark):



Appendix 3: Snapshot of Firewall Tests

Talos Internal Endpoint Firewall Test Results (Shell Script):



Firewall R3 eth1 Test Results (Wireshark):