DHCP Server Configuration Report

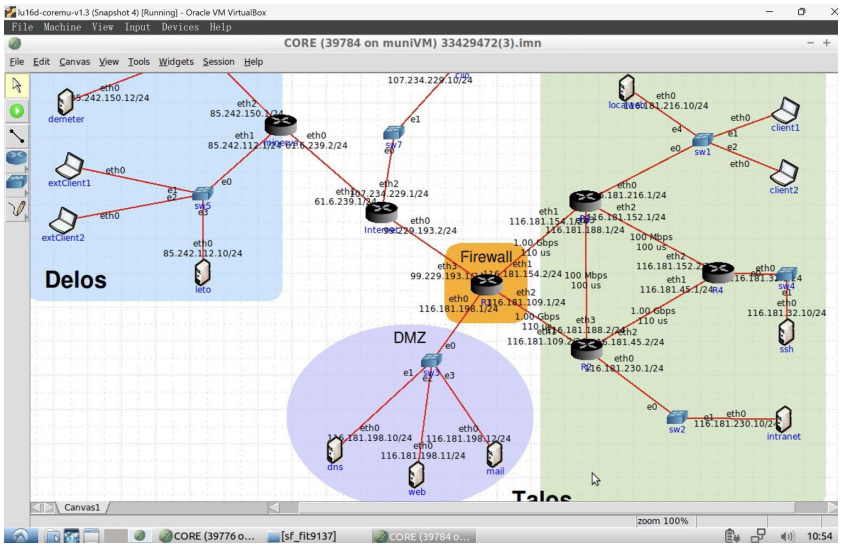
Student ID:33429472
Student Name: Ziqi Pei

Introduction
The Dynamic Host Configuration Protocol (DHCP) server is a service used to automatically assign IP addresses and other network configuration information. This report aims to explain how to configure a DHCP server and verify its proper functioning.

Task A: Routing Configuration

To fulfill the requirements of Task A, the objective is to configure routing and determine the optimal path:

Ensure that all hosts can connect with each other.
Add default routes for all connections.
Select an appropriate path for the Talos network, considering the balance between the minimum hop count and the maximum link speed.
Router R1:
I have configured router R1 as follows:



1) ip route add 116.181.32.0/24 via 116.181.152.2

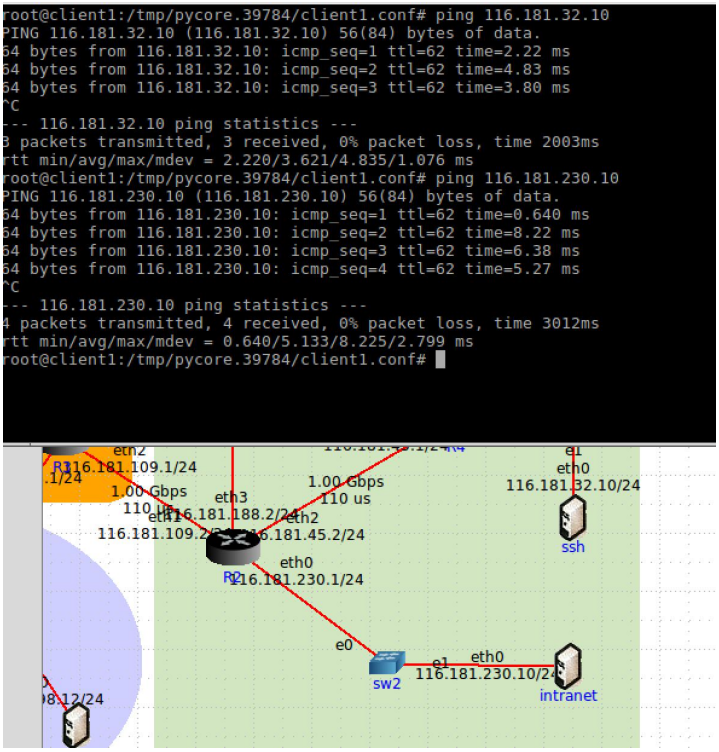
If I want to connect to the SSH network, I can connect to R4. Despite its 100Mbps link speed, it offers the shortest delay and hop count. Based on a calculation of 1500 bytes, the transmission time can be determined using the formula: Transmission Time = Data Size / Bandwidth. Therefore, the transmission time is approximately 0.000015 seconds, calculated as 1500 bits / 100,000,000 bits per second.

2) ip route add 116.181.230.0/24 via 116.181.188.2

If I want to connect to the intranet network, I can connect to R2. Despite its 100Mbps link speed, it also offers the shortest delay and hop count. Using the same calculation as above, the transmission time is approximately 0.000015 seconds.

3) ip route add default via 116.181.154.2

I choose to use a fixed route to transmit to R3. The reason for this choice is that R1 needs to forward traffic destined for the talos.edu network to R2 as the next hop router. From there, it will be transmitted to R3.



Router R2:

(1) ip route add 116.181.32.0/24 via 116.181.45.1

If I want to connect to the SSH network, I can directly connect to R4. It has a 1Gbps link with a delay of 110 microseconds, and only requires one hop. Calculating the transmission time for 1500 bytes, it can be determined as follows: Transmission Time = Data Size / Bandwidth + Total Delay. Therefore, the transmission time is approximately 0.012 milliseconds (12 microseconds) + 110 microseconds, which is approximately 0.122 milliseconds.

(2) ip route add 116.181.216.0/24 via 116.181.188.1

If I want to connect to the localweb network, the optimal path I choose is through R3. It has a 100Mbps link with a delay of 100 microseconds, and only requires one hop. Using the same calculation as above, the transmission time for 1500 bytes is approximately 0.12 milliseconds + 100

microseconds, which is approximately 0.22 milliseconds.

(3) ip route add default via 116.181.109.1 to R3.

If I want to set a default route to R3, I can use the command above to configure it. This default route will forward traffic to R3, allowing it to handle any outgoing traffic that does not match any specific route in the routing table.

Router R3:

(1) ip route add 116.181.230.0/24 via 116.181.109.2

If I want to connect to the intranet, I can connect to the route via R2. It has a 1Gbps link with a delay of 110 microseconds, and only requires one hop. Calculating the transmission time for 1500 bytes, it can be determined as follows: Transmission Time = Data Size / Bandwidth + Total Delay. Therefore, the transmission time is approximately 0.012 milliseconds (12 microseconds) + 110 microseconds, which is approximately 0.122 milliseconds.

(2) ip route add 116.181.216.0/24 via 116.181.154.1

If I want to connect to the localweb, I can connect to the route via R1. It has a 1Gbps link with a delay of 110 microseconds, and only requires one hop. Using the same calculation as above, the transmission time for 1500 bytes is approximately 0.012 milliseconds + 110 microseconds, which is approximately 0.122 milliseconds.

(3) ip route add default via 99.229.193.2

The default route in this case is to connect to the external Internet route. This command configures the default route for R3 to forward all traffic to the specified external gateway address.

Router R4:

(1) ip route add 116.181.216.0/24 via 116.181.152.1

If I want to connect to the localweb, I can connect via R1. It has a 100Mbps link with a delay of 100 microseconds, and only requires one hop. Calculating the transmission time for 1500 bytes, it can be determined as follows: Transmission Time = Data Size / Bandwidth + Total Delay. Therefore, the transmission time is approximately 0.12 milliseconds + 100 microseconds, which is approximately 0.22 milliseconds.

(2) ip route add 116.181.230.0/24 via 116.181.45.2

If I want to connect to the intranet, I can connect via R2. It has a 1Gbps link with a delay of 110 microseconds, and only requires one hop. Using the same calculation as above, the transmission

time for 1500 bytes is approximately 0.012 milliseconds + 110 microseconds, which is approximately 0.122 milliseconds.

(3) ip route add default via 116.181.45.2

R4 needs to forward traffic to the minerva network via R3. This command sets the default route for R4 to forward all other traffic to the specified gateway address.

By configuring the routing table as described above, we ensure that all hosts in the talos.edu network can communicate with each other via the optimal paths. Additionally, R3 acts as the default gateway for the talos.edu network, forwarding all other traffic to the Internet through the default route.

Important Note: When configuring the routing table, it is important to avoid routing loops, as they can lead to network instability and excessive traffic. By carefully configuring static routes and ensuring the correct next-hop router is set, we can prevent routing loops and ensure efficient network communication.

Router Internet:

(1) ip route add 116.181.0.0/16 via 99.229.193.1

This command is added to establish connectivity with the 116.181.0.0 network segment on the right side.

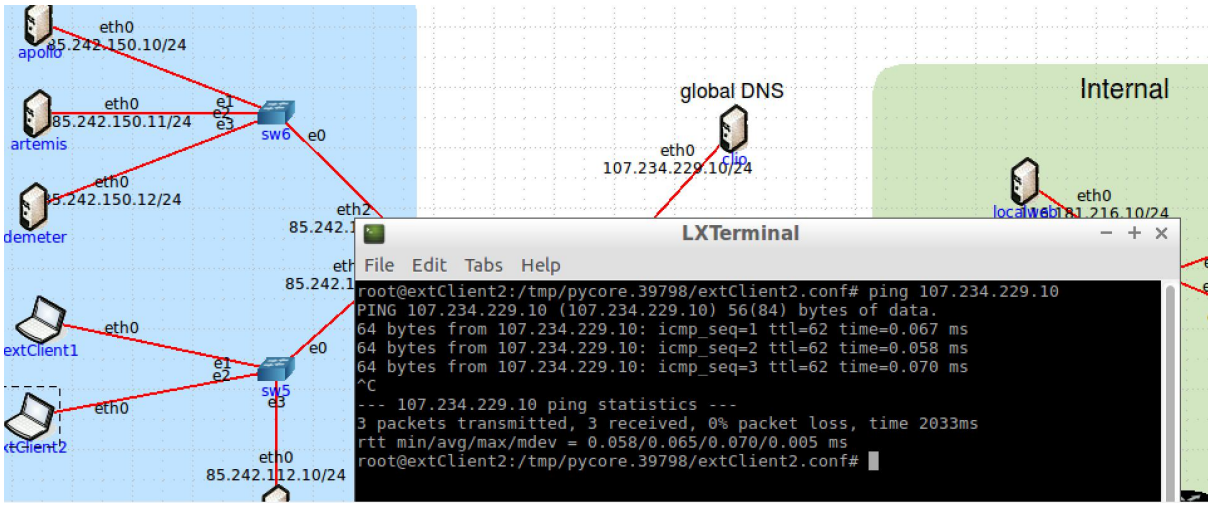
(2) ip route add 85.242.0.0/16 via 61.6.239.2

This command is added to establish connectivity with the Delos network segment on the left side.

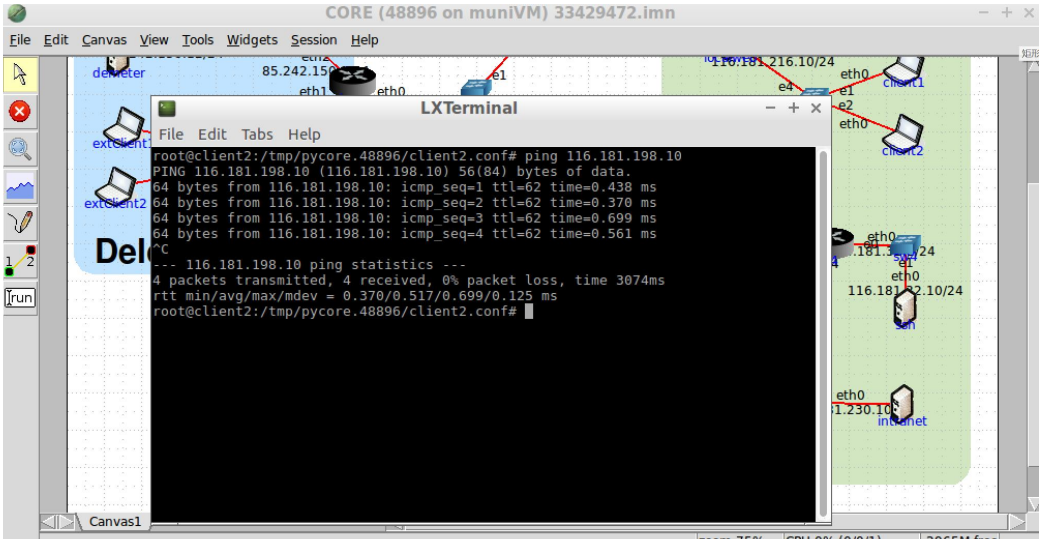
(3) ip route add 85.242.112.0/24 via 61.6.239.2

This command is added to establish connectivity with the minerva network segment on the left side.

We can test the connectivity by using exclient2 to connect to the global server hosted on the Internet and verify that the connection is successful.



Similarly, within the firewall, Client2 can also ping the external Delos IP address 85.242.250.10.



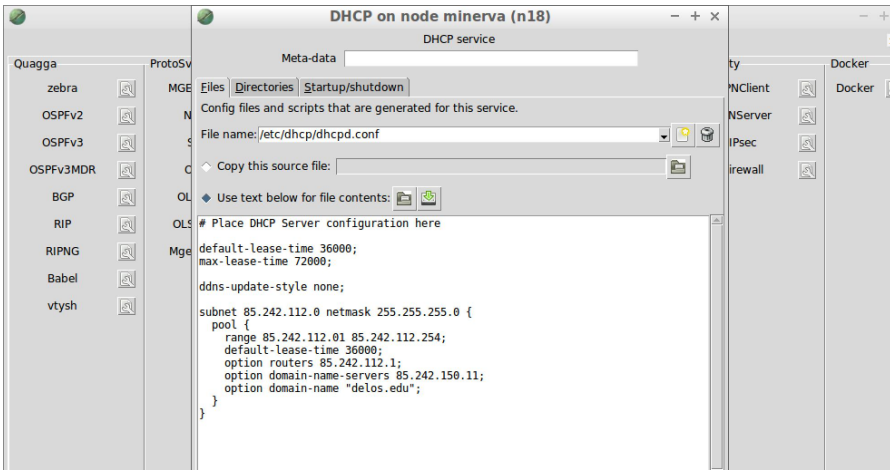
Client2 within the firewall can also successfully ping the external DNS server.

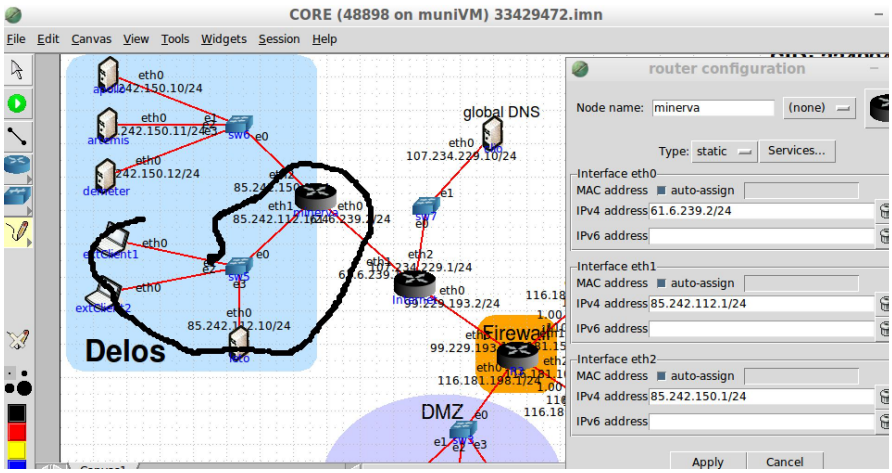
Task B: DHCP server configuration

To meet the requirements of Task B, we need to configure a DHCP server on the minerva node to assign dynamic IP addresses and other required settings to the client machines in the client subnet. In addition, we also need to enable the DHCP client service on the delos client. Here is the configuration for each part of the task:

Configure DHCP server on minerva:

1. Configure the DHCP server with the following settings: Here we can learn from the DHCP configuration of R1





The subnet is the network segment connected to minerva and exClient 85.242.112.0

- IP address range: Defines a range of IP addresses to be dynamically assigned to client machines in the client subnet. For example, the range can be set as 85.242.113.01 to 85.242.112.254

- Subnet Mask: Set the subnet mask to match the subnet of the client subnet. Set to 255.255.255.0.

- Default Gateway: Set the default gateway to the IP address of the minerva node or the IP address of a router connected to the client subnet.

- DNS server: Set the DNS server IP address to the appropriate DNS server that the client machine should use. According to the title, our Delos default DNS server is artemis, so we fill in the address here as 85.242.150.11

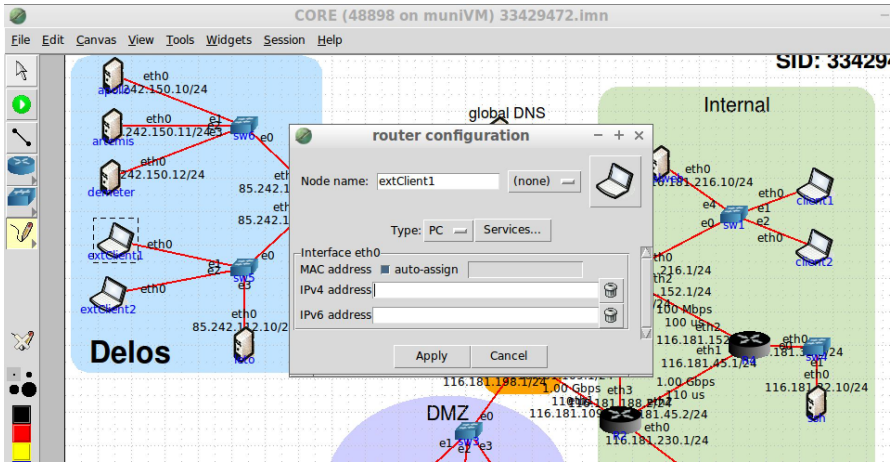
The specific operation is as follows

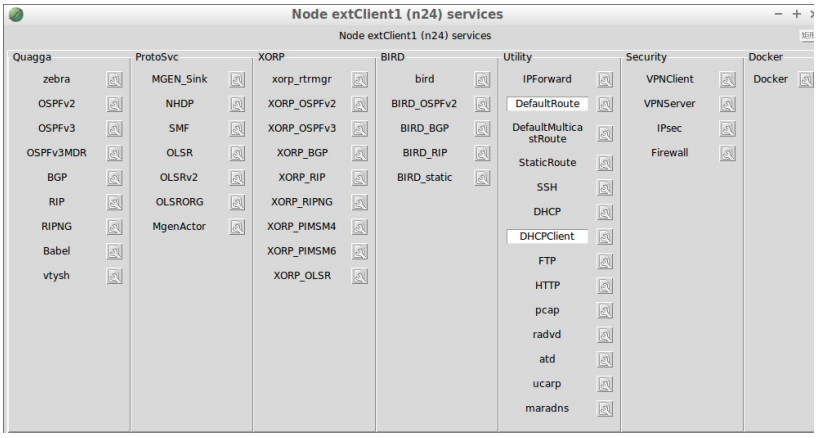
Save and apply the configuration changes for the DHCP server.

Enable the DHCP client service on the delos client:

1. Access each client machine on the client subnet.
2. Open the network settings or network configuration files on each client machine.
3. Find the network configuration for the Ethernet interface or Wi-Fi connection.
4. Change the network configuration from static IP address assignment to DHCP.
5. Save the network configuration changes and restart the network interface or client machine.

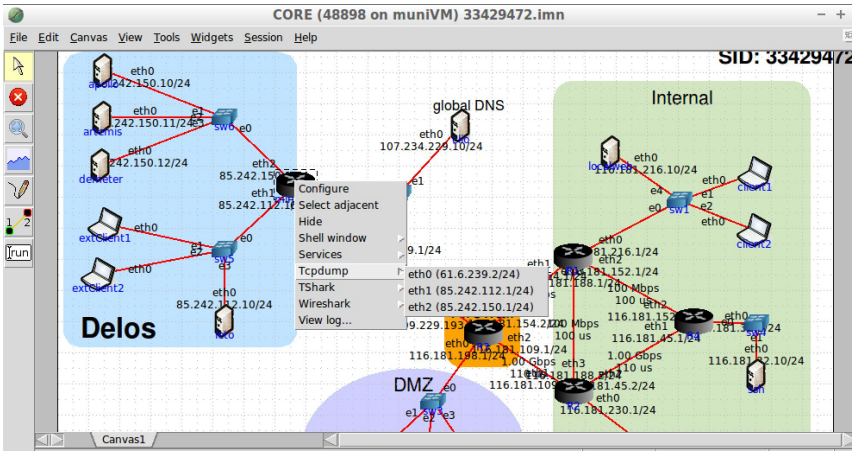
By configuring the DHCP server on minerva and enabling the DHCP client service on the delos clients, we ensure that client machines in the client subnet can automatically obtain dynamic IP addresses and other necessary network settings. This eliminates the need to manually assign static IP addresses and simplifies network management, and requires the DHCP Client in exClient1, 2 to be lit



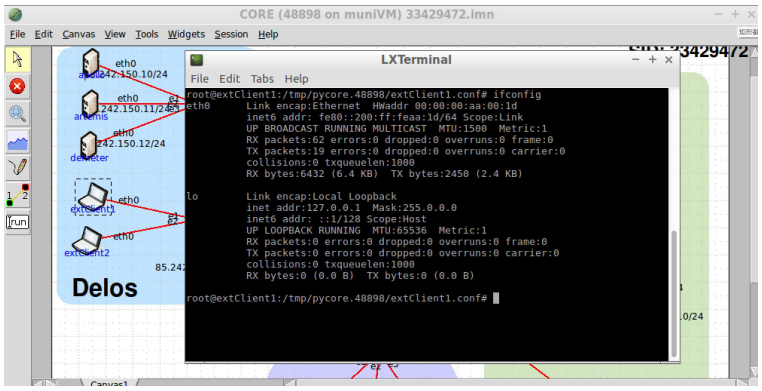


The third step is to start dynamically assigning IP addresses

1 Need to click eth1's tcpdump to find the line 85.242.112.1 connected by exclient1



2 We use the ifconfig command to check the IP address, this time we found that it has been cleared



We use the dhclient command to request an IP address, and we get a replay

19:56:14.233310 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 00:00:00:aa:00:1d, length 300

19:56:14.240837 IP 85.242.112.1.67 > 85.242.112.4.68: BOOTP/DHCP, Reply, length 300

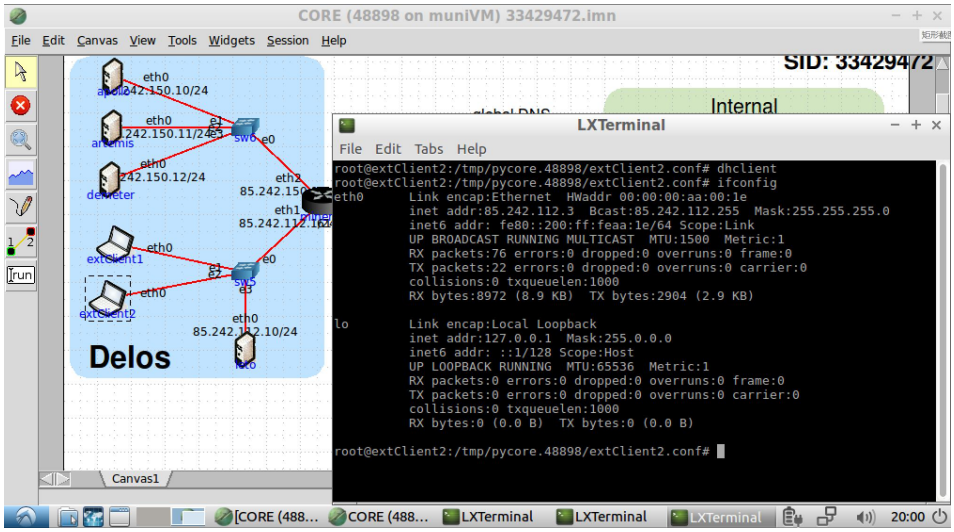
19:56:18.325384 ARP, Request who-has 85.242.112.4 tell 85.242.112.1, length 28

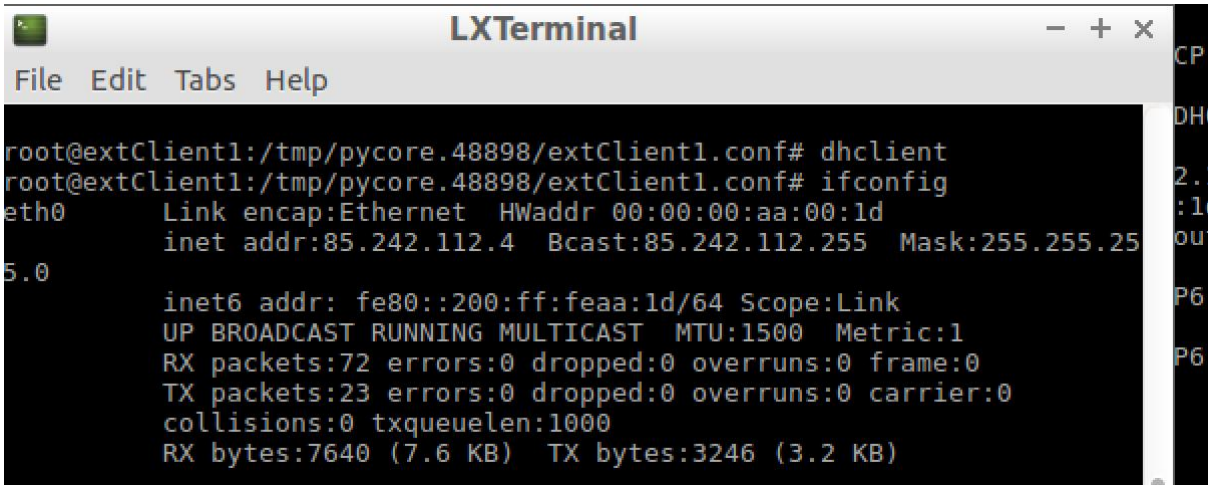
19:56:18.325510 ARP, Reply 85.242.112.4 is-at 00:00:00:aa:00:1d, length 28

19:57:36.916938 IP6 fe80::200:ff:feaa:1d > ff02::2: ICMP6, router solicitation, length 16

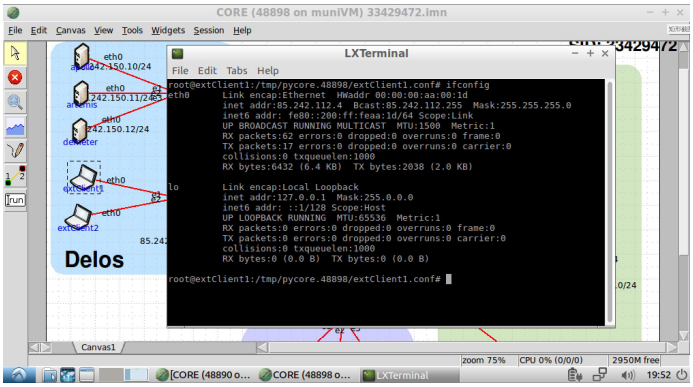
At this time we have obtained an IP address

Ask for our address again, and you'll get our IP address,



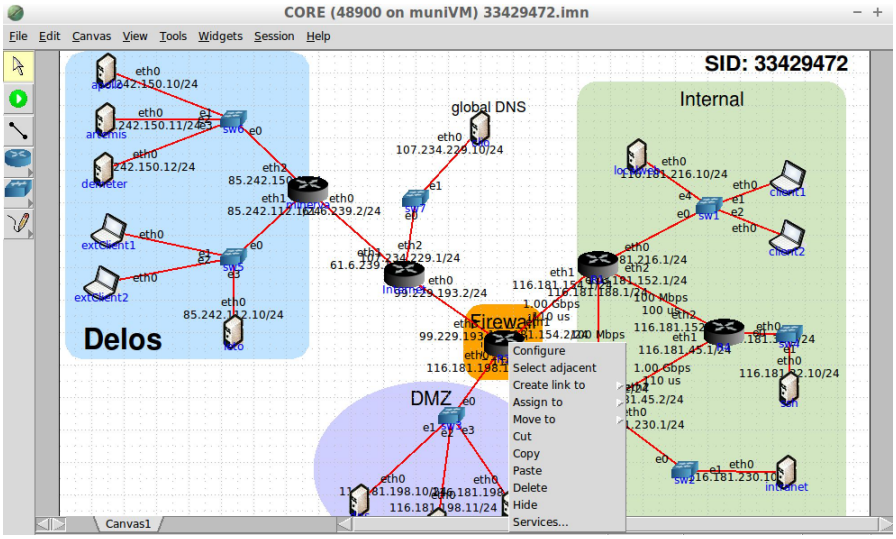


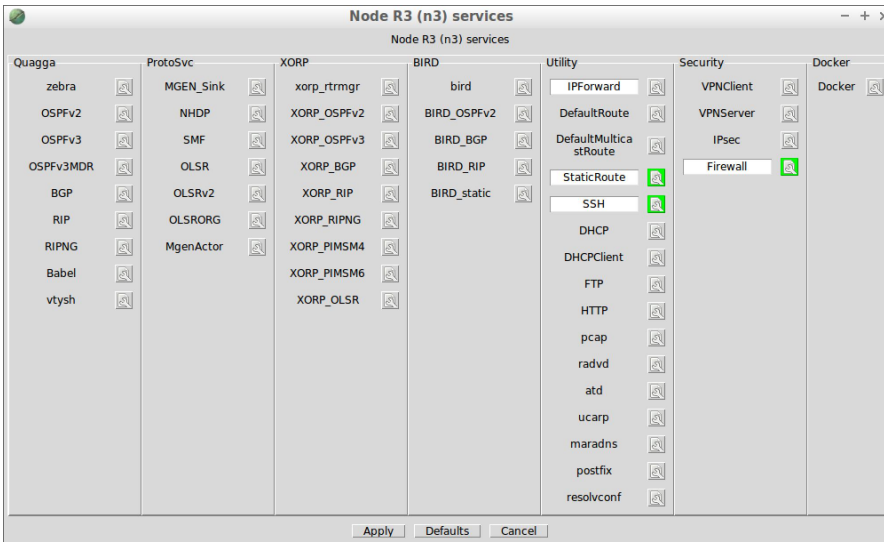
ExClien2 obtained the IP address in the same way



Task C: Firewall configuration

To meet the requirements of Task C, we need to configure the firewall service on the R3 node to meet the specified rules and restrictions. The following is the configuration of each requirement: The first step is to click on R3 Services and turn on FireWall





1. Allow traffic to the DMZ from anywhere, but only for public services (DNS, HTTP, SMTP) provided by each server (DMZ → External):

- Configure rules to allow from anywhere

traffic from all parties to the DMZ server, but restricted to specific public services (such as DNS, HTTP, SMTP).

- Limit the allowed traffic range to the specified ports and protocols for each service.
- Make sure only public services provided by servers in the DMZ are accessible from anywhere.

Our command is as follows

#rules for DNS server from external to DMZ

iptables -A FORWARD -i eth3 -o eth0 -p udp --dport 53 -d 116.181.198.10 -j ACCEPT

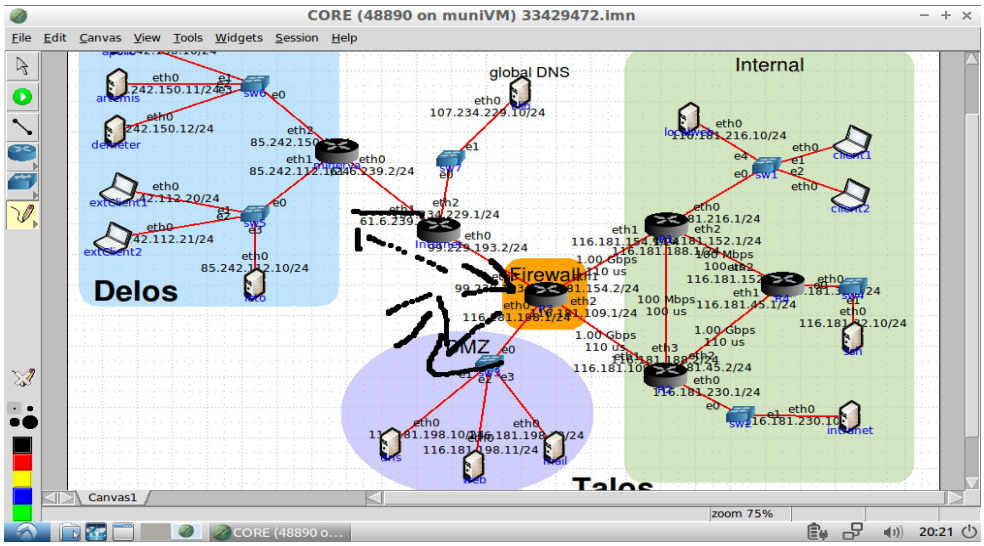
```
#rules for DNS server form DMZ to external

iptables -A FORWARD -i eth0 -o eth3 -p udp --dport 53 -s 116.181.198.10 -m state
 --state NEW -j ACCEPT
iptables -A FORWARD -i eth3 -o eth0 -p udp --sport 53 -d 116.181.198.10 -m state
 --state ESTABLISHED,RELATED  -j ACCEPT
```

Instructions destined for DNS 116.181.198.10 are allowed through the firewall

iptables -A FORWARD -i ehh0 -o eth3 -p udp --sport 53 -s 116.181.198.10 -j ACCEPT

The data allowed to enter the eho0 port can be output from the eth3 port, the protocol is udp, and the data is sent from the port 53

```
#rules for DNS server from external to DMZ

iptables -A FORWARD -i eth3 -o eth0 -p udp --dport 53 -d 116.181.198.10 -j ACCEP
T
iptables -A FORWARD -i eth0 -o eth3 -p udp --sport 53 -s 116.181.198.10 -j ACCEP
T
```



2. Allow the server in the DMZ to initiate communication by itself according to the service it provides, and only limited to the service (Stateful Inspection: DMZ → External):

- Configure stateful inspection rules to allow servers in the DMZ to initiate outbound communications for specific services they provide.

- Ensure that allowed outbound traffic is limited to only the ports and protocols required by each service.

#rules for DNS server form DMZ to external

iptables -A FORWARD -i eth0 -o eth3 -p udp --dport 53 -s 116.181.198.10 -m state --state NEW -j ACCEPT

Active internal and external requests are acceptable. Outgoing from the eth0 port and entering from the eth3 port are acceptable.

iptables -A FORWARD -i eth3 -o eth0 -p udp --sport 53 -d 116.181.198.10 -m state --state ESTABLISHED,RELATED -j ACCEPT

It still enters and exits through port 53, the information sent by dns is allowed to return, and the status is the allowed response of establish

#rules for web server from external to DMZ

是一个 tcp 协议，从 116.181.198.11 的端口，可以请求进出

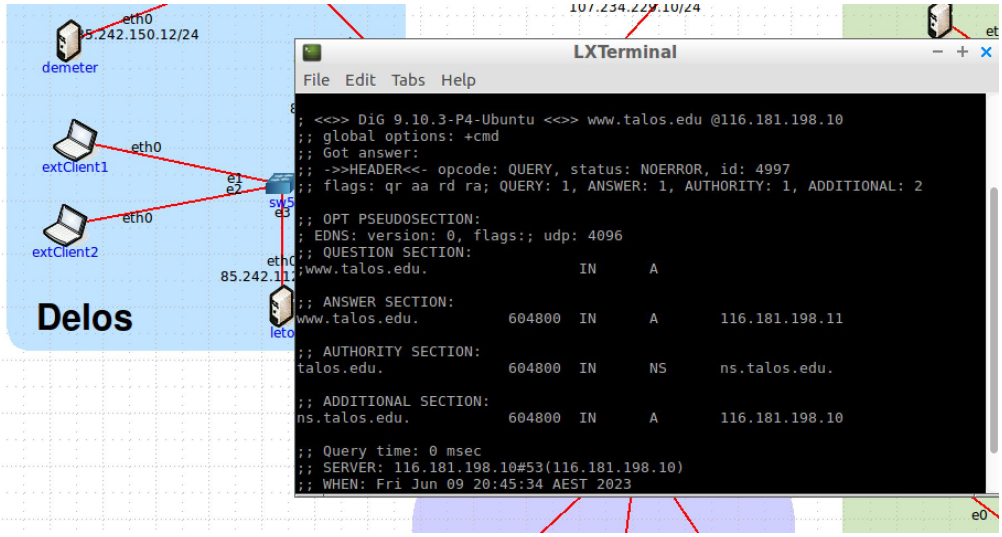
```
#rules for web server from external to DMZ

iptables -A FORWARD -i eth3 -o eth0 -p tcp --dport 80 -d 116.181.198.11 -j ACCEP
T
iptables -A FORWARD -i eth0 -o eth3 -p tcp --sport 80 -s 116.181.198.11 -j ACCEP
T
```

iptables -A FORWARD -i eth3 -o eth0 -p tcp --dport 80 -d 116.181.198.11 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth3 -p tcp --sport 80 -s 116.181.198.11 -j ACCEPT

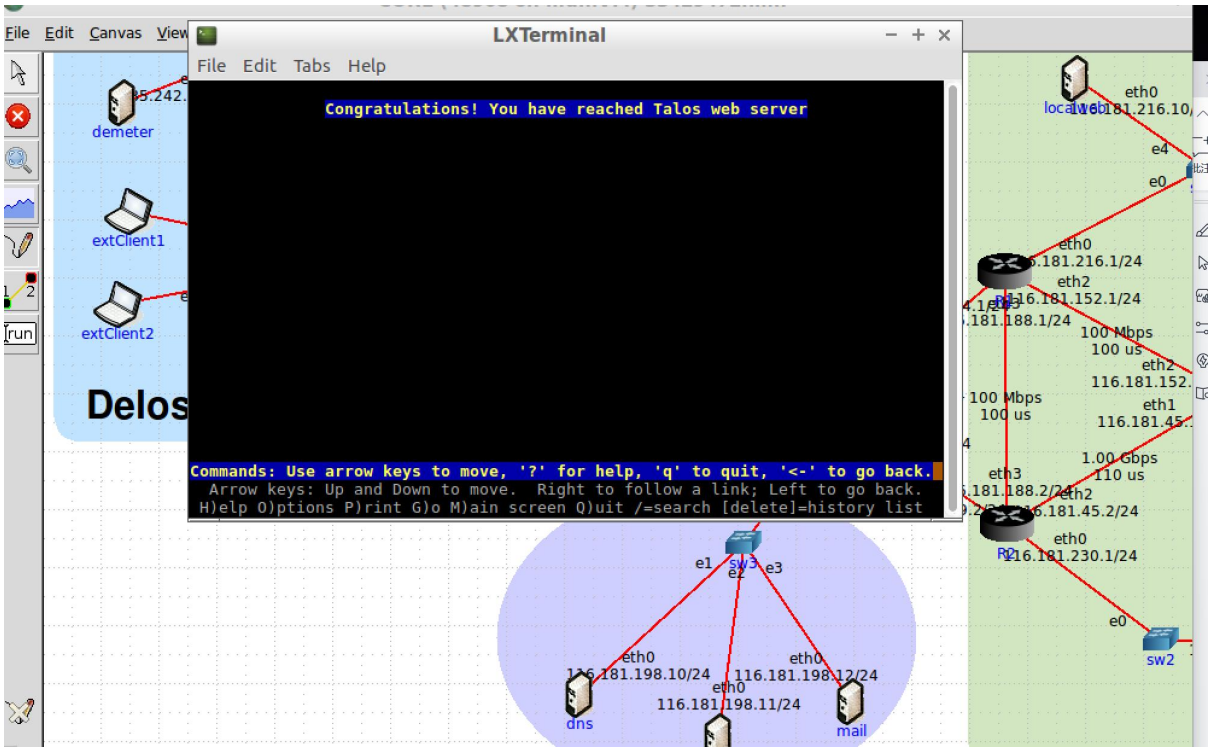
The mail server's outbound command is
#rules for mail server from external to DMZ
iptables -A FORWARD -i eth3 -o eth0 -p tcp --dport 25 -d 116.181.198.12 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth3 -p tcp --sport 25 -s 116.181.198.12 -j ACCEPT
Port is number 25

The outside world responds to the mail server
#rules for mail server from external to DMZ

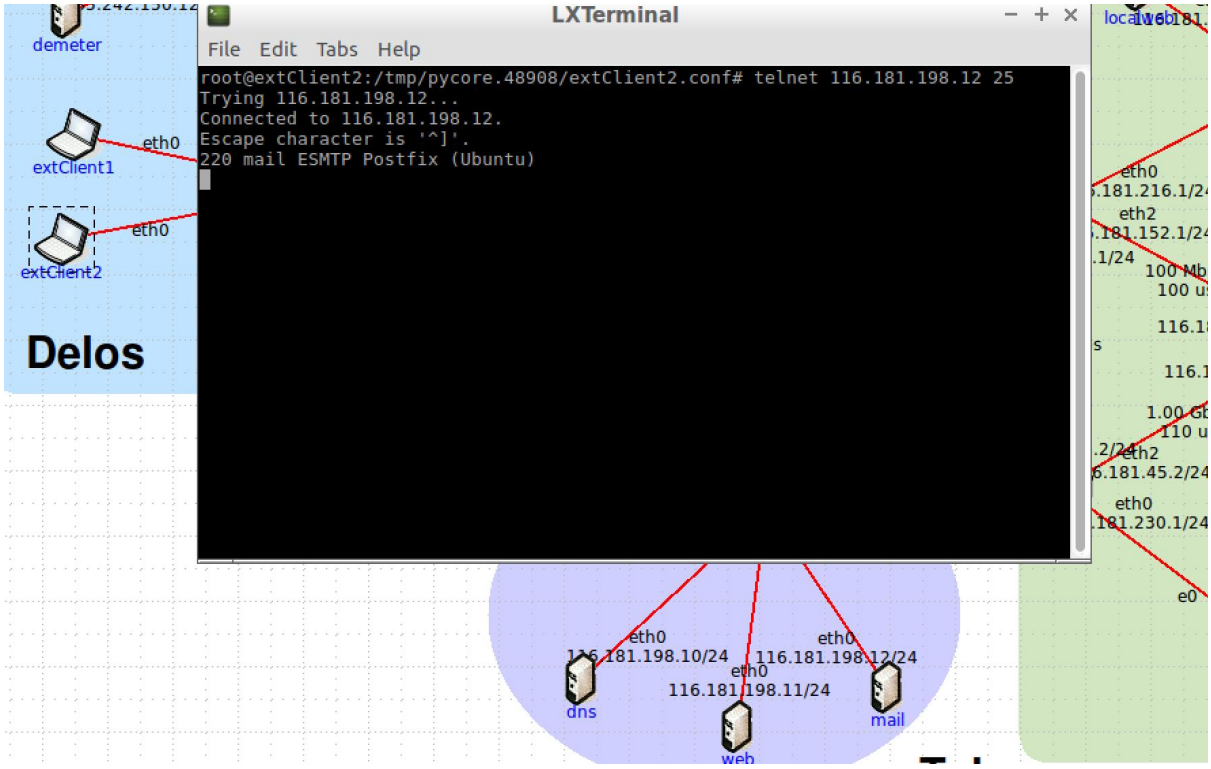
iptables -A FORWARD -i eth3 -o eth0 -p tcp --dport 25 -d 116.181.198.12 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth3 -p tcp --sport 25 -s 116.181.198.12 -j ACCEPT
Next we will test
Can't connect to dns externally
But we can see that the outside world can initiate requests with dns



Now we need to initiate a request to the web server, the command is lynx+ webIP lynx 116.181.198.11



Next, we can check whether we can access the e-mail server telnet + mailip address + 25 (port number)



All the proofs represent that our firewall is in effect, and the structure of the first two questions has been completed

3. Allow internal hosts to access all services provided by servers in the DMZ (Stateful Inspection: Internal → DMZ):

- Configure stateful inspection rules to allow internal hosts to access services provided by servers in the DMZ.
- Can be more lenient in the rules, allowing access using address ranges and all IP traffic to ensure internal hosts can access all DMZ services.
- Use SSH to connect to a host from the internal subnet to test the correctness of the rules.

This question requires Talos to connect to all servers through the firewall

#rules for internal to DMZ

iptables -A FORWARD -s 116.181.0.0/16 -d 116.181.198.0/24 -j ACCEPT

Here, 116.181.0.0 includes all ip addresses of talos and the location of DMZ, and all traffic can enter and exit

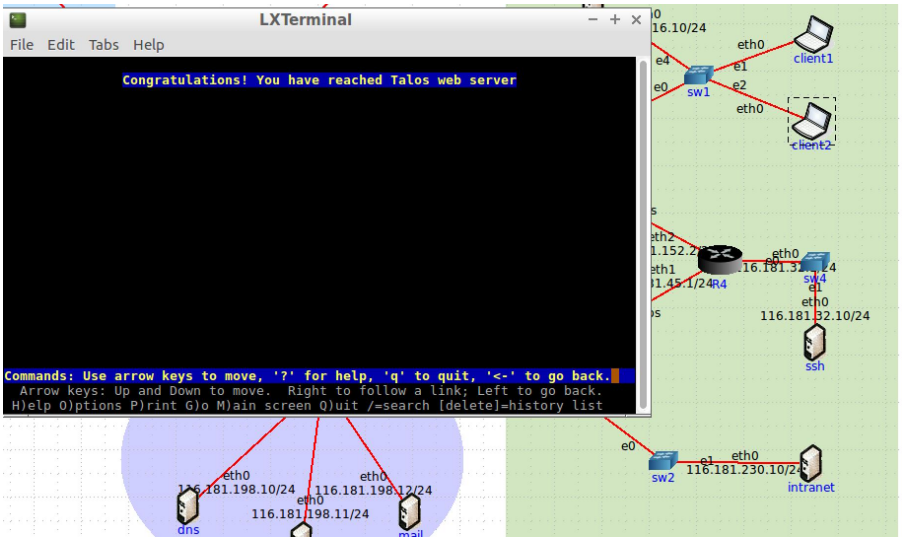
iptables -A FORWARD -d 116.181.0.0/16 -s 116.181.198.0/24 -j ACCEPT

```
#rules for internal to DMZ
iptables -A FORWARD -s 116.181.0.0/16 -d 116.181.198.0/24 -j ACCEPT
iptables -A FORWARD -d 116.181.0.0/16 -s 116.181.198.0/24 -j ACCEPT
```

Next we test we can choose the client

root@client2:/tmp/pycore.48916/client2.conf# lynx 116.181.198.11

After instructing the Client, we found that it is possible to connect to the DMZ web server



4. Allow internal hosts to access other internal hosts (if traffic goes through R3) (Internal → Internal):

- Configure rules to allow all traffic between internal hosts since this is internal to internal communication.

The core question of this question is how the internal host connects to the internal server through the firewall

#internal to internal

intables -A FORWARD -i eth1 -o eth2 -j ACCEPT

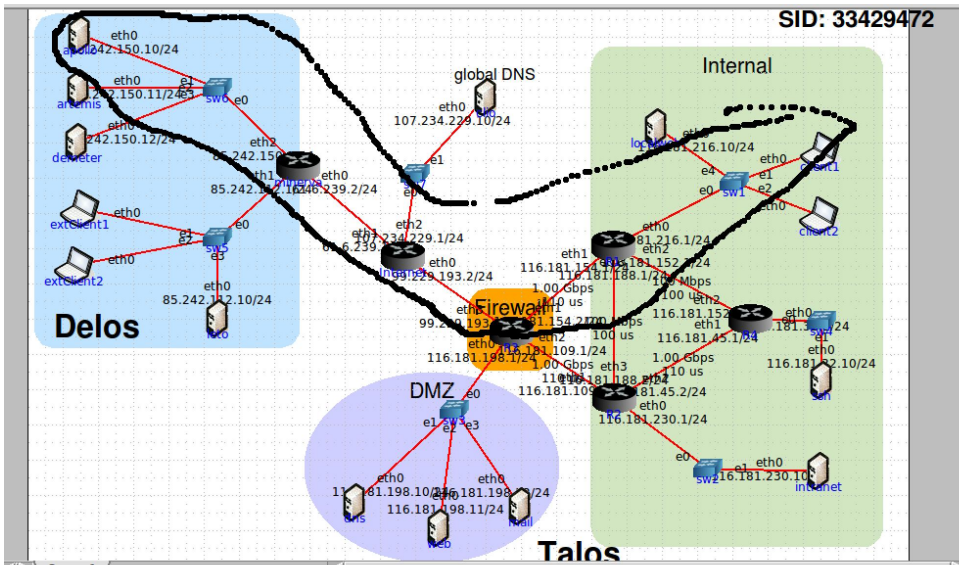
intables -A FORWARD -i eth2 -o eth1 -j ACCEPT

eth1 port in and eth2 port out

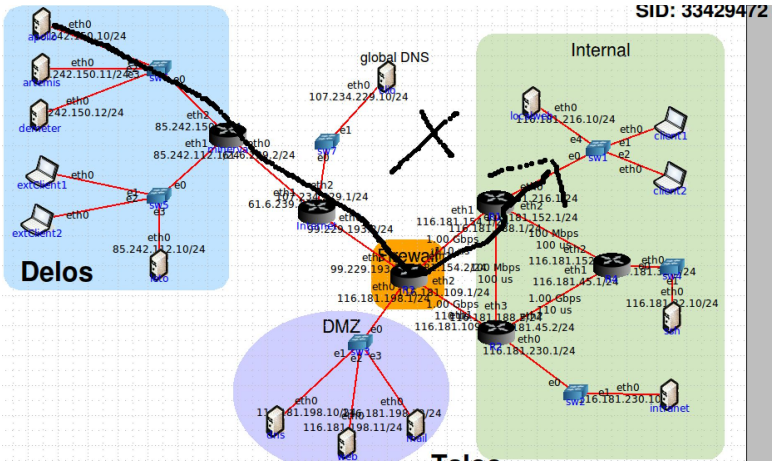
The eth2 port goes out and the eth1 port goes in and runs through

5. Allow internal nodes to access external servers, but only allow response packets from internal to initiate communication (Stateful Inspection: Internal → External):

- Configure stateful inspection rules to allow internal nodes to access external servers.
- Only allow packets from external servers in response to internally initiated communications.

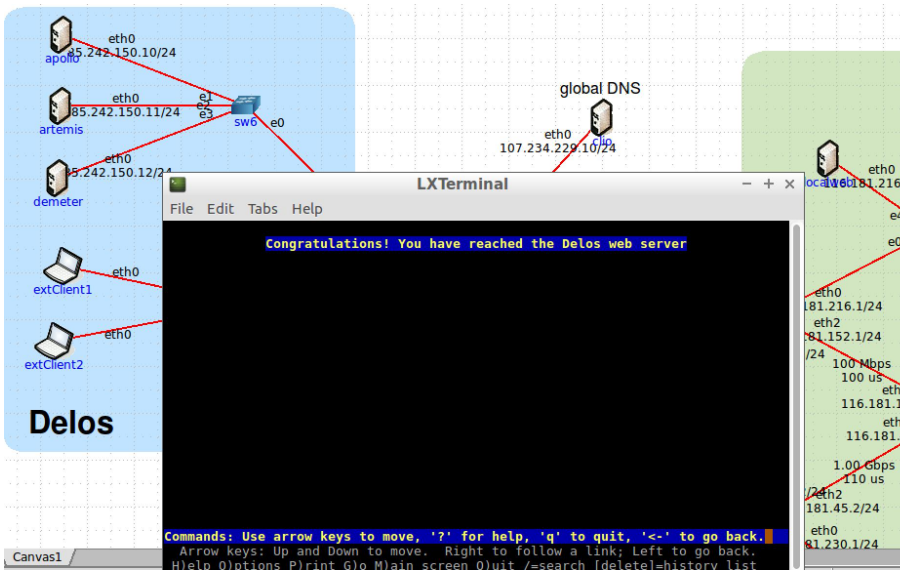


#internal to external



iptables -A FORWARD -i eth1 -o eth3 -j ACCEPT
iptables -A FORWARD -i eth2 -o eth3 -j ACCEPT
Internal to external information can be sent
iptables -A FORWARD -i eth3 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth3 -o eth2 -m state --state ESTABLISHED,RELATED -j ACCEPT
The state is that only the state of establish can be entered

Next, we will conduct a test. Use the command Client 1 to send the command lynx 148.130.78.10 to apollo, and you can send



exClient1 issued a command to local but ,there was no response.lynx 116.181.216.10.the initiative is new type, not establish

6. Allow nodes in the client subnet of talos to access R3 via SSH (any host connected to the R1.eth0 subnet):

- Configure rules to allow nodes in the client subnet of talos to access R3 via SSH.
- Make sure that the nodes in the client subnet of talos can successfully establish an SSH connection to R3.

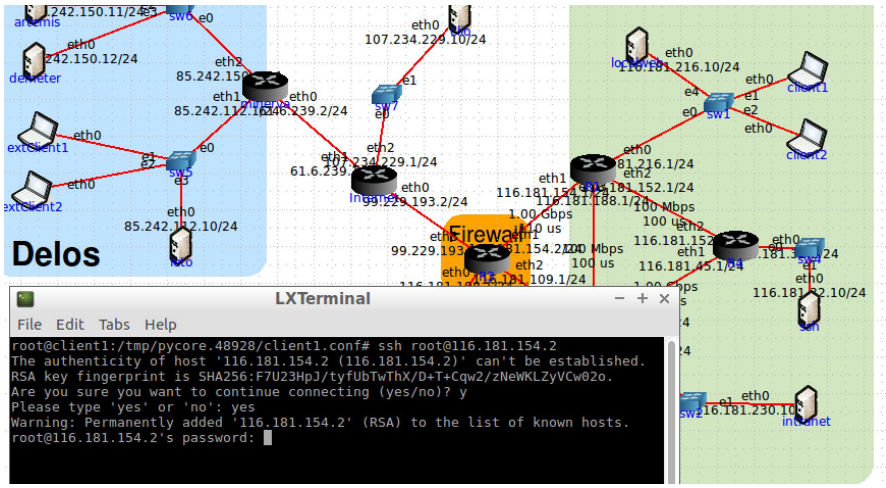
#client to R3

iptables -A INPUT -s 116.181.216.0/24 -p tcp --dport 22 -j ACCEPT

iptables -A OUTPUT -d 116.181.216.0/24 -p tcp --sport 22 -j ACCEPT

Only port 22 can send and respond

Next, we test the Client ssh roote@+R3 IP address to access the firewall



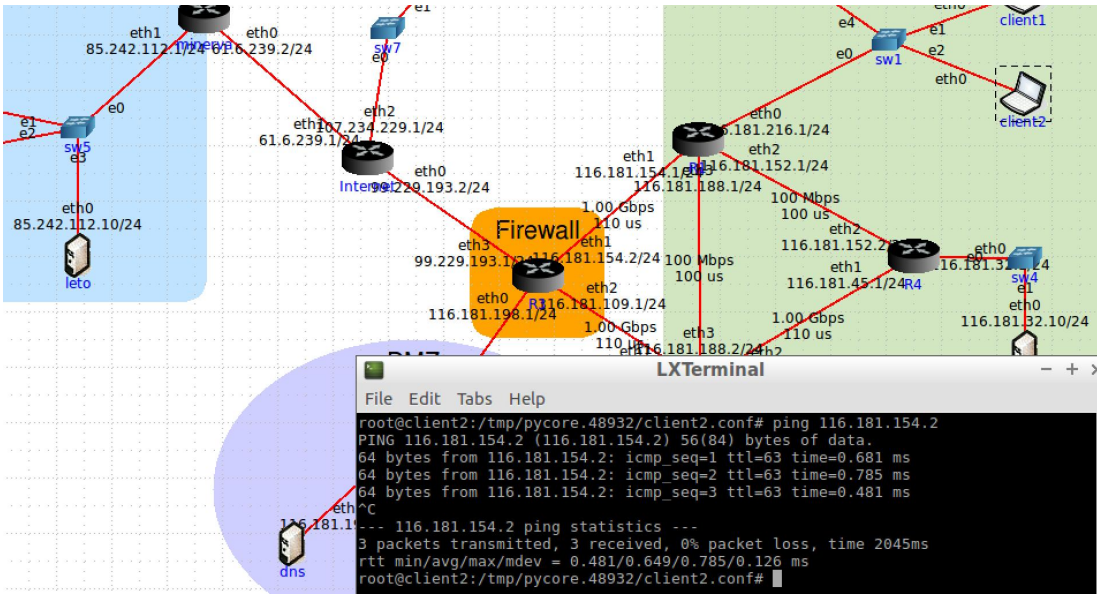
7. Allow the R3 node to send and receive ICMP echo messages with internal nodes and DMZ servers:

- Configure rules to allow R3 nodes to send and receive ICMP echo messages (ping) with internal nodes and DMZ servers.

- Ensure that R3 nodes can successfully send and receive ICMP echo messages for troubleshooting and network diagnostics.

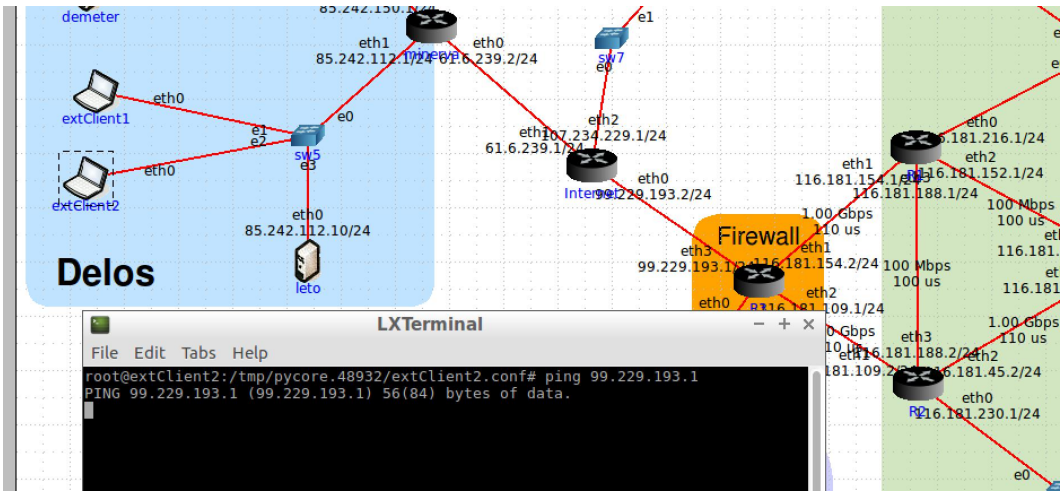
#R3 ICMP message

iptables -A OUTPUT -d 116.181.0.0/16 -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -s 116.181.0.0/16 -p icmp --icmp-type echo-reply -j ACCEPT
We can send this command to all pingDMZs of R3 on line 116.181. This command is sent first and then accepted.
iptables -A INPUT -s 116.181.0.0/16 -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -d 116.181.0.0/16 -p icmp --icmp-type echo-reply -j ACCEPT
This command is first received and then given in response.



Next, test that client2 can pass the ping to the firewall

Commands issued by external exClient to the firewall cannot pass through



8. Drop all other traffic:

- Configure a default rule to drop all traffic that does not match the above rules.
- This ensures that only the allowed traffic specified previously is allowed through and all other traffic is blocked

Our command is

#Default rules

iptables -P FORWARD DROP, for forward traffic drop

iptables -P INPUT DROP, for Input traffic drop

iptables -P OUTPUT DROP drops traffic for output