Network Engineering Capstone Functionality Report

Introduction

Provide a functionality report detailing the ten test case scenarios used to verify the utility of your network project. Seven of the test case scenarios must be from the provided predefined list, with the remaining three test cases created by you. The functionality report should be written so that a networking peer could replicate the steps for a successful test of your networking solution.

Student Name	[redacted]
WGU Student ID	[redacted]
WGU Student Email	[redacted]

[redacted]

[redacted]

Test Case #1: Device Discovery and Reachability

Your network solution must include multiple network segments with access controls that allow traffic from a device on one network to access the resources of a device on another network. Similarly, there must be devices on one network that cannot access resources on a different network.

Functionality

*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

The network is divided into several networks, both internally, and in the mock internet. The internal networks include network device networks between network devices, and endpoint networks which are assigned VLANs and utilize DHCP to obtain IP addresses.

The internal network device networks are:
EdgeRouter1 <-> L3Switch1 10.0.0.4/30
EdgeRouter1 <-> L3Switch2 10.0.0.8/30
L3Switch1 <-> L3Switch2 10.0.0.40/30

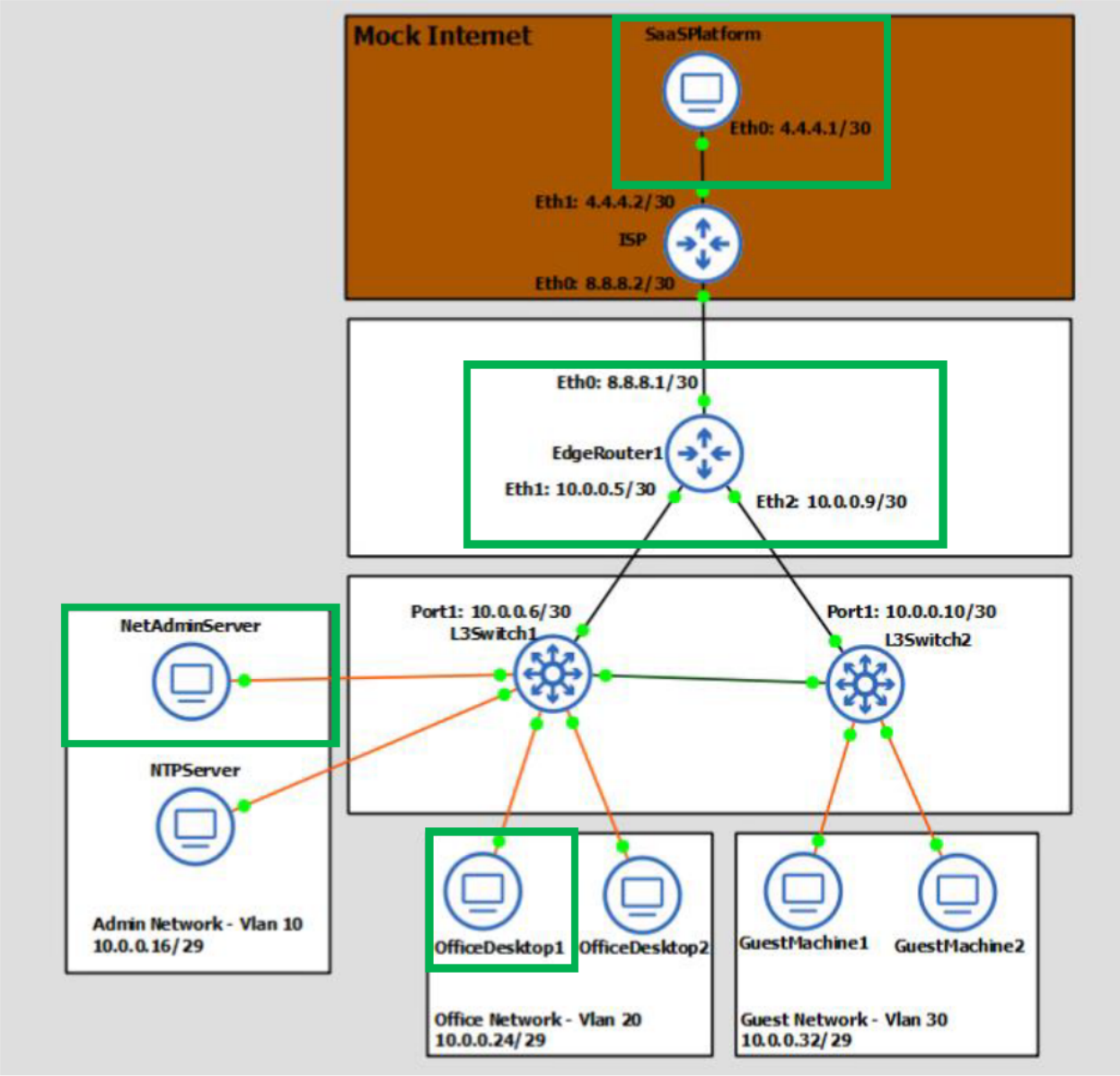
The internal endpoint networks are:
Admin Network 10.0.0.16/29 – VLAN 10
Office Network 10.0.0.24/29 – VLAN 20
Guest Network 10.0.0.32 - VLAN 30
L3Switch Tagging VLAN 40 10.0.0.40/30

The mock internet networks are:
ISP <-> EdgeRouter1 8.8.8.0/30
ISP <-> SasSPlatform 4.4.4.0/30

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*

All network devices are applicable to this test case, but the ones that are directly applicable to the testing method are enclosed in green boxes.



Legend

SaaS	Software as a Service
Eth*	Ethernet + port number
ISP	Internet Service Provider
L3	Layer 3
NetAdminServer	Network Administration Server
Admin	Administration
VLAN	Virtual Local Area Network

Testing Method

*Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.*

There are several ACLs in place that both deny access and allow access. To demonstrate access to another network, I will show that OfficeDesktop1 can access SaaSPlatform by creating a HTTP server on SaaSPlatform and connecting to it over port 80 on OfficeDesktop1. OfficeDesktop1 is on the 10.0.0.24/29 network, while SaaSPlatform is on the 4.4.4.0/30 network. This connectivity is enabled because traffic is only denied to other VLANs from OfficeDesktop1, and the ACL on EdgeRouter1 eth0 inbound allows traffic back from SaaSPlatform if a TCP connection has already been established.

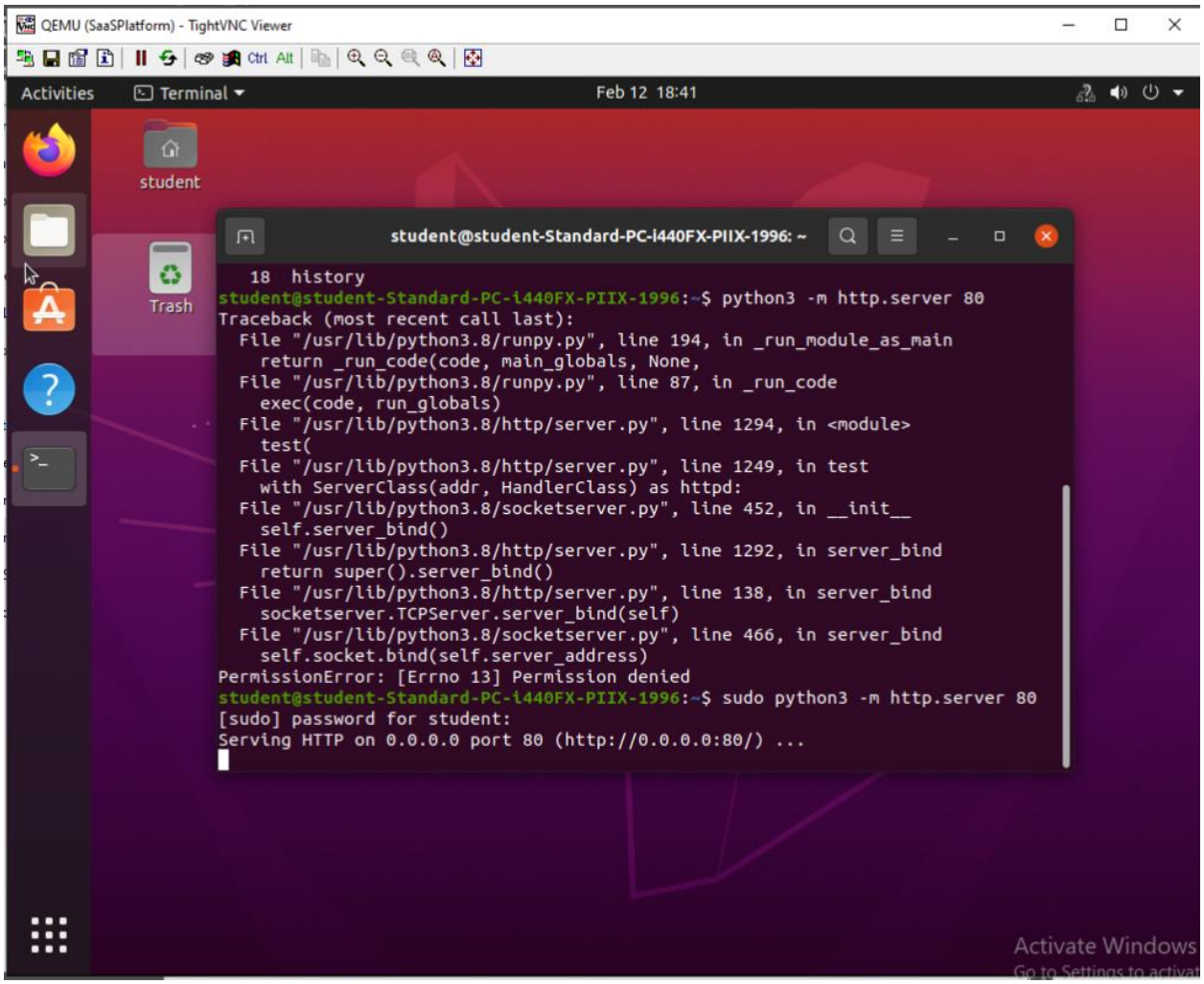
To demonstrate a case where resources is denied access to one on a different network, I will show that SaaSPlatform cannot access a HTTP server on NetAdminServer. NetAdminServer is on the 10.0.0.16/29 network and SaaSPlatform is on the 4.4.4.0/30 network. This connectivity is denied because EdgeRouter1 eth0 inbound denies all new TCP connections.

Process List

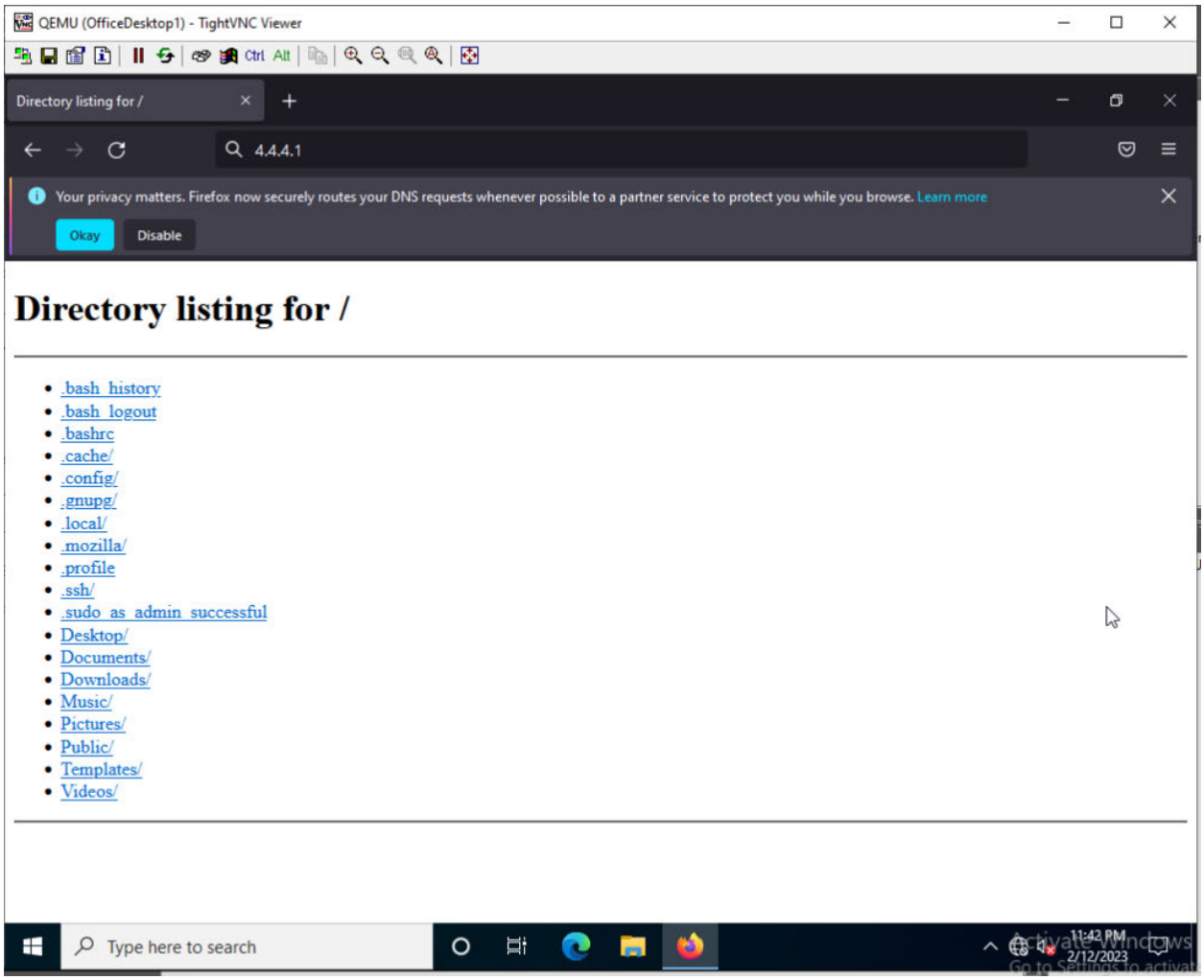
*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

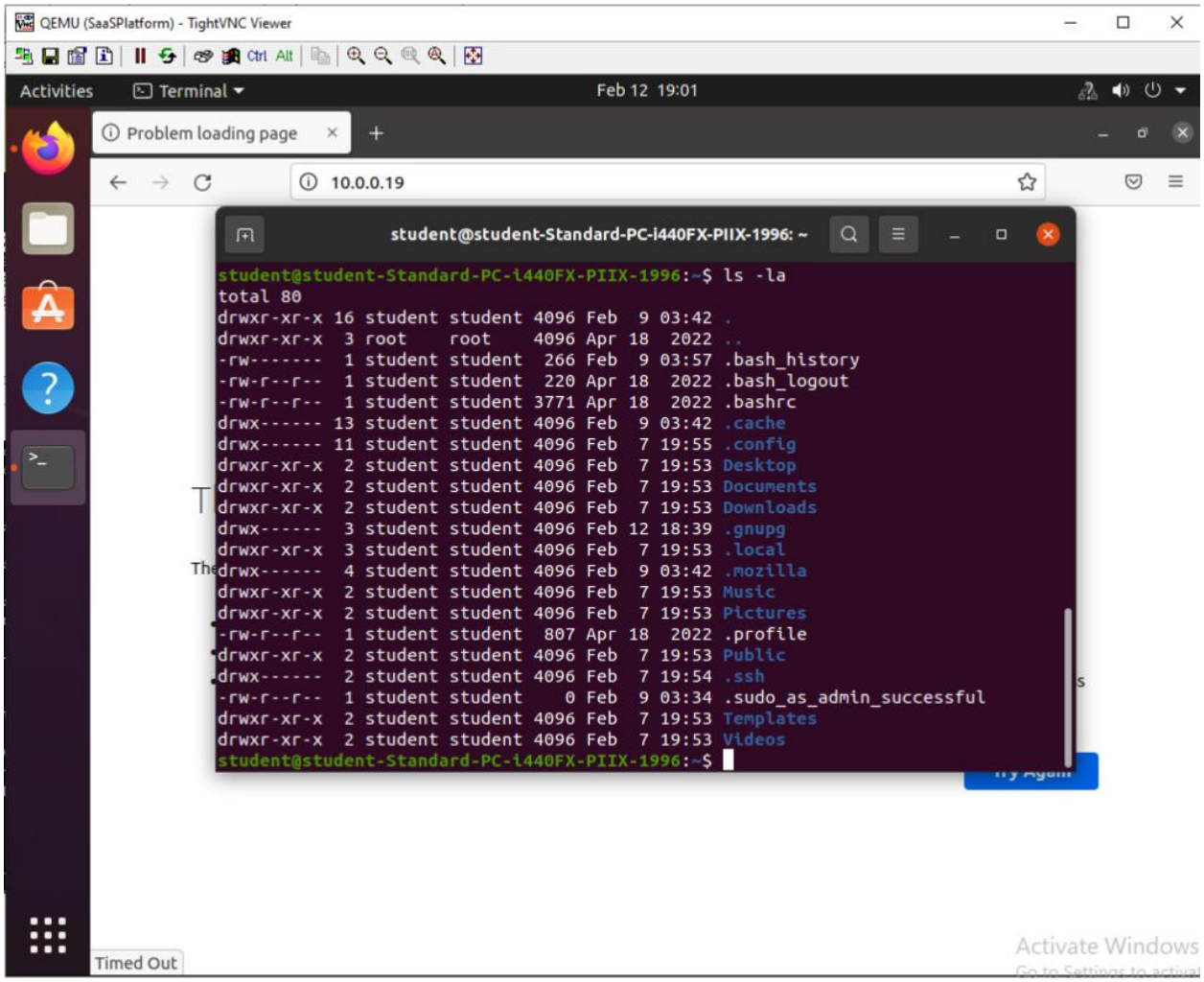
Access to resource on another network:

1. Login to SaaSPlatform.
2. Open a terminal.
3. Run “sudo python3 -m http.server 80” to start an http server.

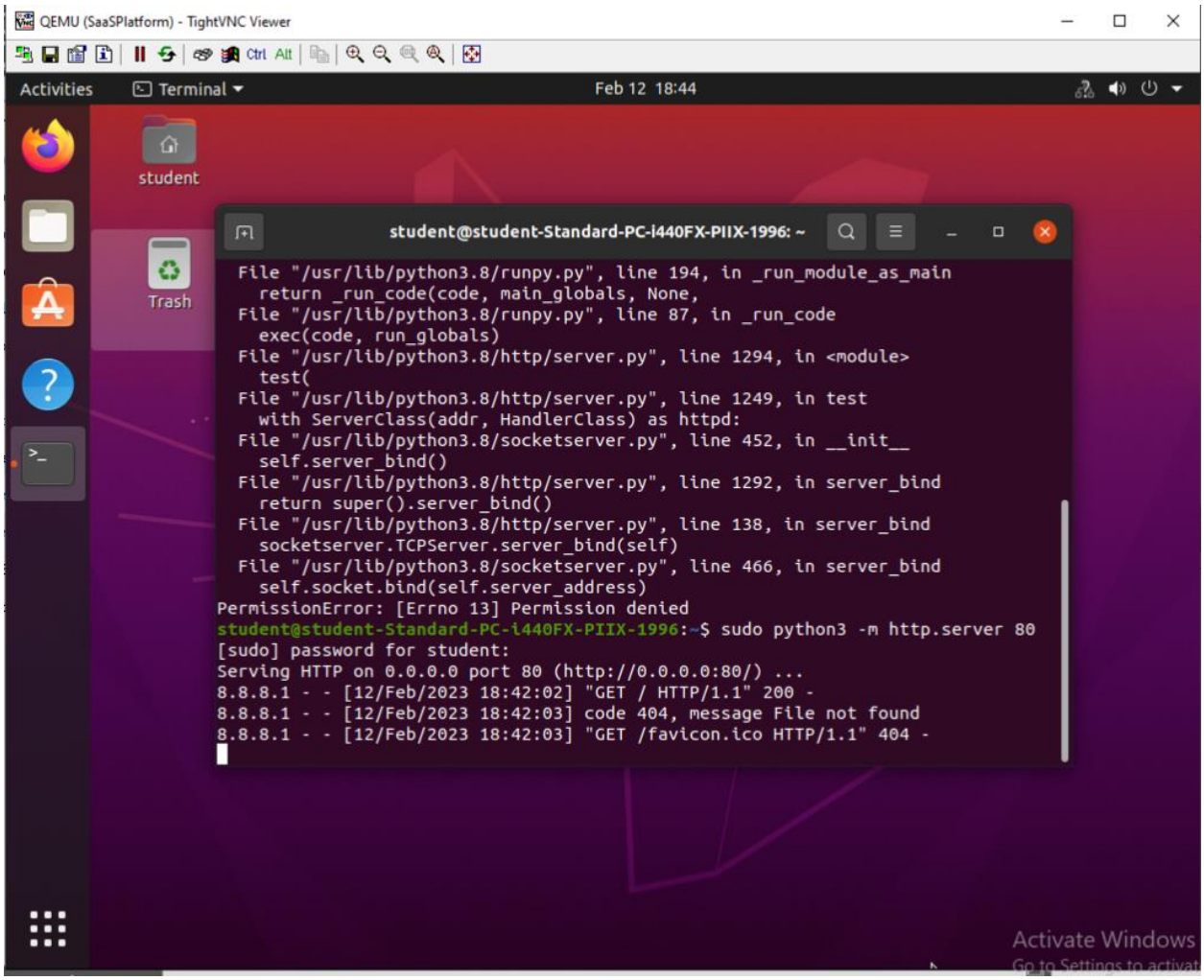


4. Login to OfficeDesktop1.
5. Open Firefox.
6. Connect to 4.4.4.1:80. It is successful and we can see the contents of the HTTP servers working directory.


QEMU (OfficeDesktop1) - TightVNC Viewer
Ctrl Alt
Directory listing for /
4.4.4.1
Your privacy matters. Firefox now securely routes your DNS requests whenever possible to a partner service to protect you while you browse. Learn more
Okay
Disable
Directory listing for /
.bash_history
.bash_logout
.bashrc
.cache/
.config/
.gnupg/
.local/
.mozilla/
.profile
.ssh/
.sudo_as_admin_successful
Desktop/
Documents/
Downloads/
Music/
Pictures/
Public/
Templates/
Videos/
Type here to search
11:43 PM
2/12/2023

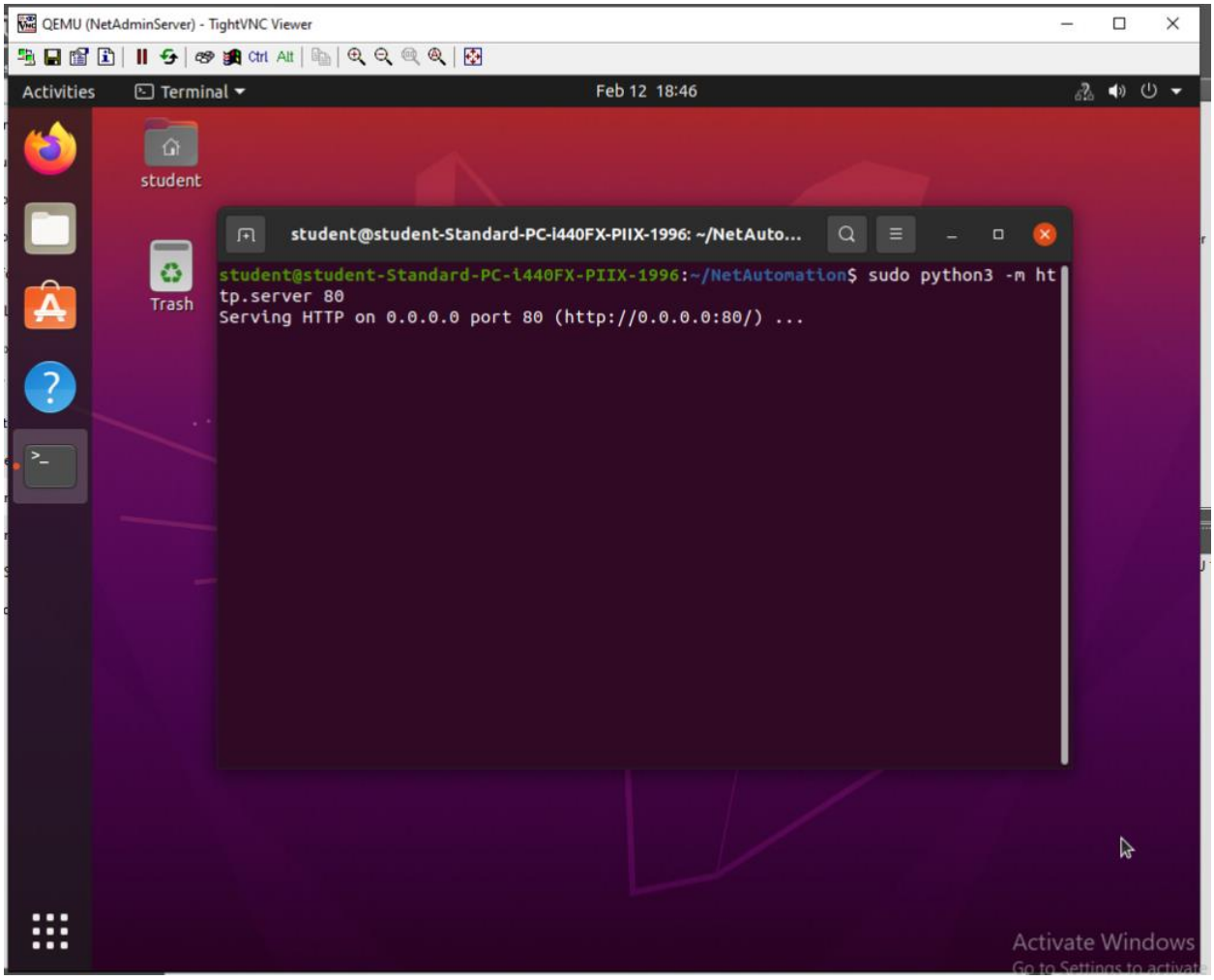


7. Connection is seen on 4.4.4.1 from the company's NAT public IP address 8.8.8.1.

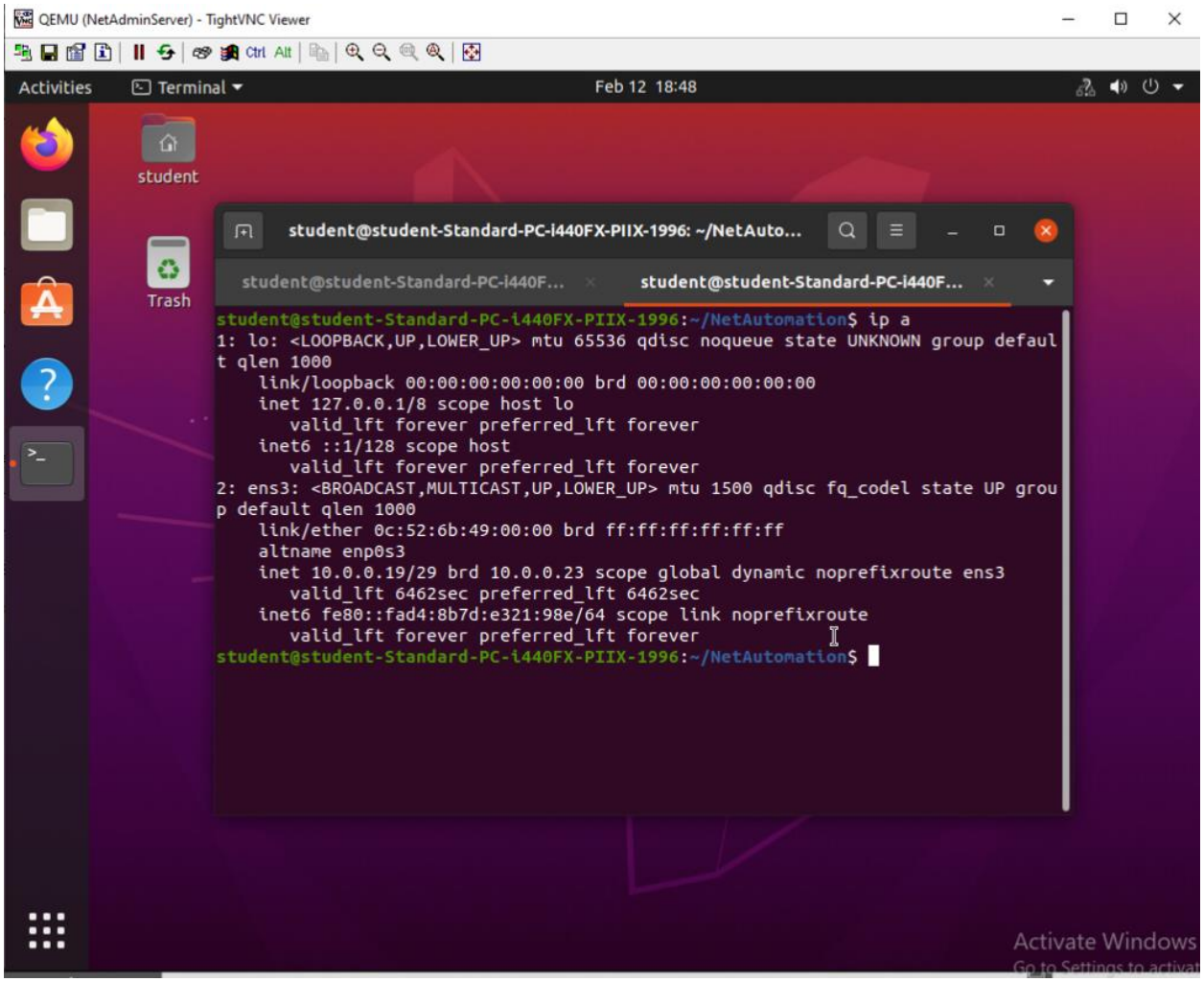


Deny access to another network:

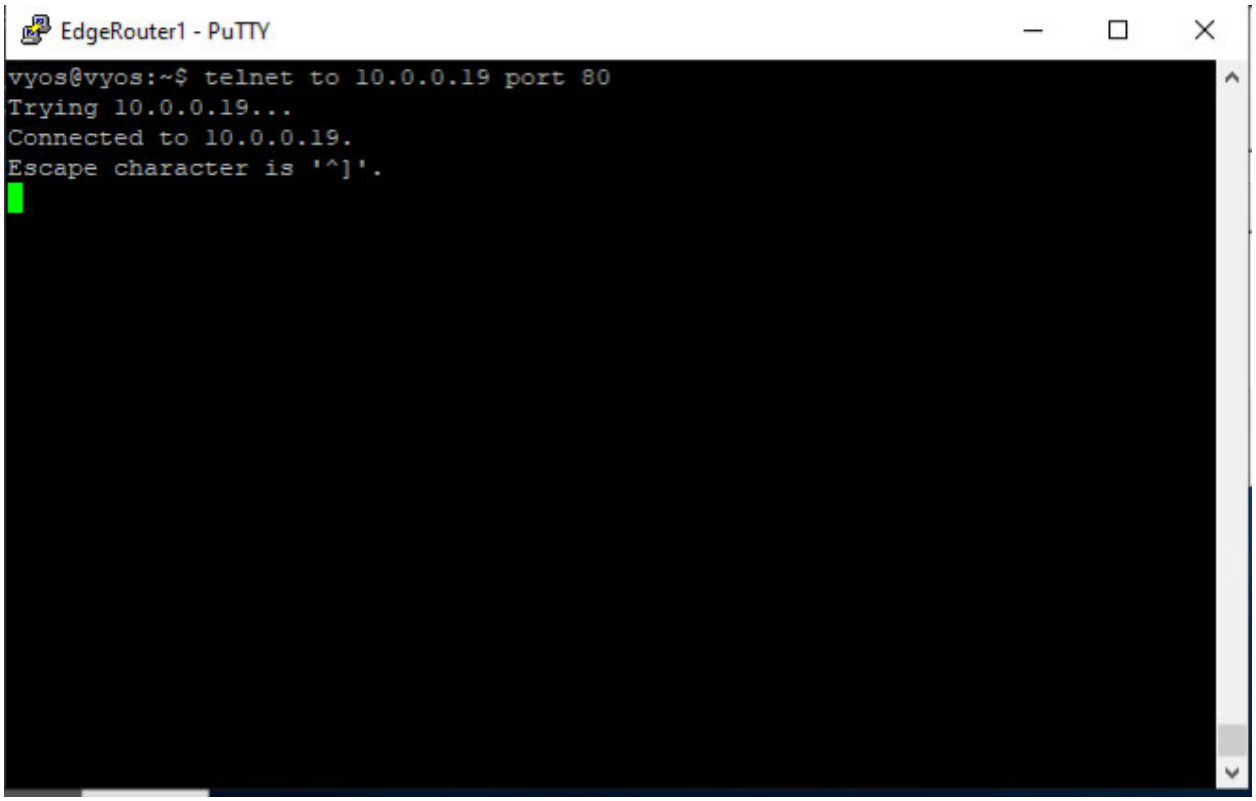
1. Login to NetAdminServer.
2. Open a terminal.
3. Run “sudo python3 -m http.server 80” to start an HTTP server.



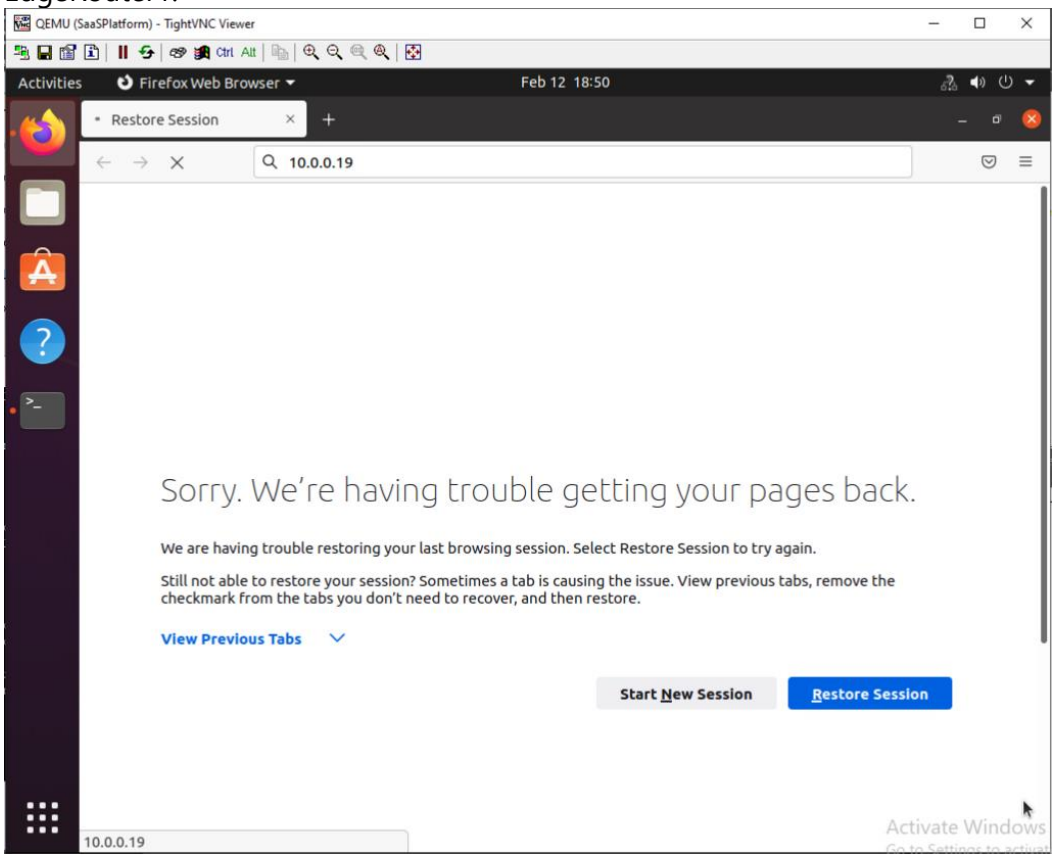
4. Get the IP address of NetAdminServer with "ip a".



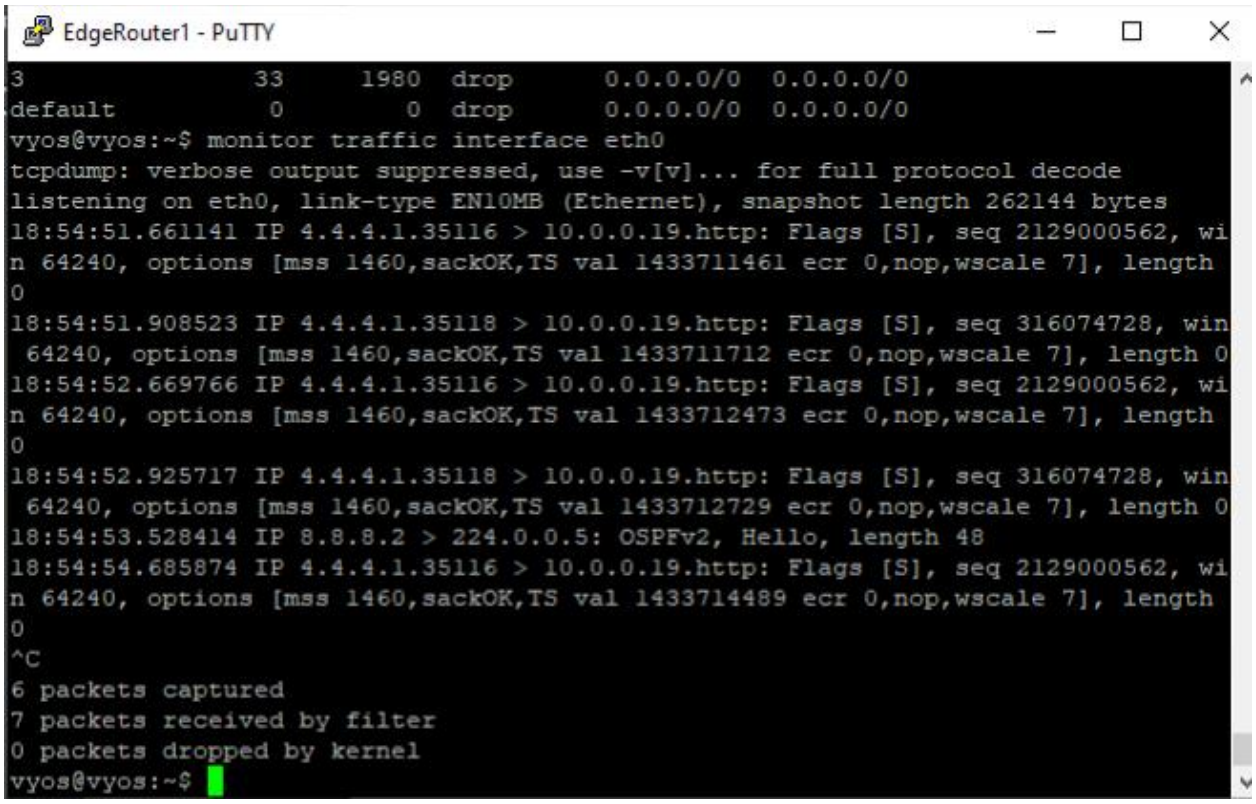
5. Login to SaaSPlatform.
6. Open Firefox.
7. Try to access the HTTP server on NetAdminServer's IP address at 10.0.0.19.
8. To verify that this HTTP server works, I run "telnet to 10.0.0.19 port 80" on EdgeRouter1. It successfully connects.


EdgeRouter1 - PuTTY
vyos@vyos:~$ telnet to 10.0.0.19 port 80
Trying 10.0.0.19...
Connected to 10.0.0.19.
Escape character is '^]'.

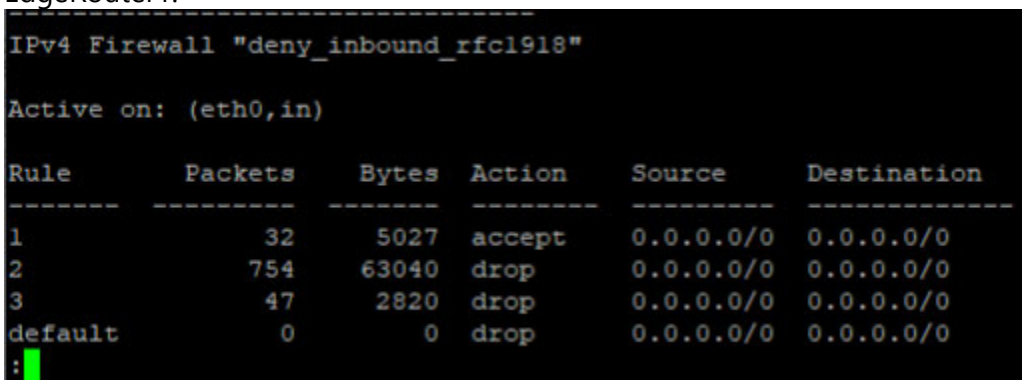
9. The connection from SaaSPlatform fails because of the ACL configured on EdgeRouter1.



10. To verify this, I run "monitor traffic interface eth0" on EdgeRouter1 which shows HTTP traffic from 4.4.4.1 to 10.0.0.19.



11. To verify that these packets hit the ACL, I run "show firewall statistics" on EdgeRouter1.



12. Lastly, I run "show firewall name deny_inbound_rfc1918" on EdgeRouter1 to see the rule conditions. We can see that rule 3 checks if the connection state is new, and if so, it drops the packets for any protocol.

```
---------------------------------
IPv4 Firewall "deny_inbound_rfc1918"

Active on: (eth0,in)

Rule     Action    Protocol      Packets    Bytes  Conditions
-------  --------  ----------  ---------  -------  ------------------------
1        accept    all              32     5027  ct state { established }
2        drop      icmp            754    63040  meta l4proto icmp
3        drop      all              61     3660  ct state { new }
default  drop      all               0        0
```

Test Case #2: Administering an Access Control List for Guest Access

Your network must utilize an Access Control List that allows guest access. Guest access should be limited to internet traffic only.

Functionality

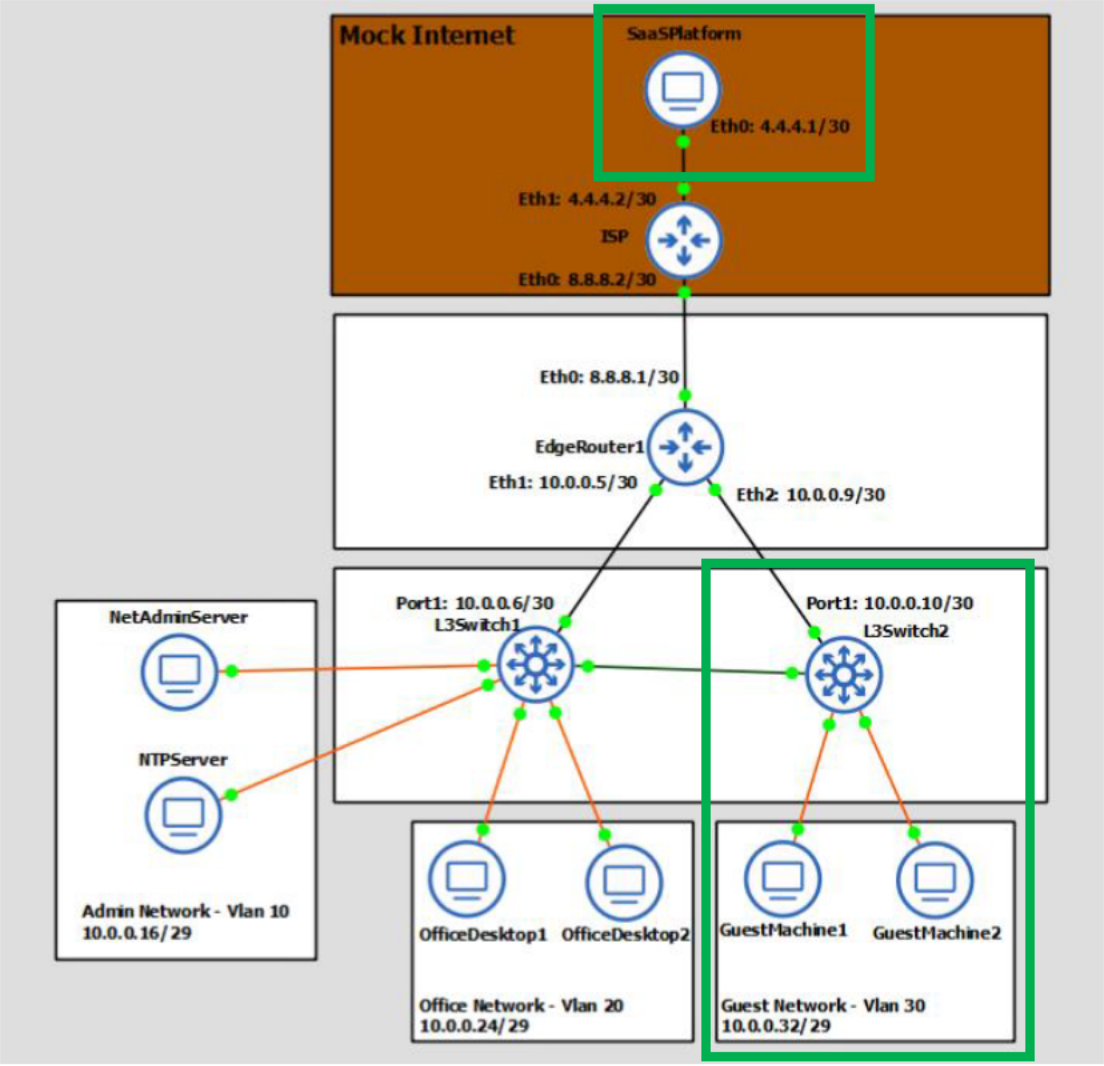
*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

There is a guest network configured on 10.0.0.32/29. There is an ACL configured on L3Switch2 ports 3 and 4 that only allow packets that have a destination IP address of the default gateway for the computers 10.0.0.33, 255.255.255.255 for DHCP, and the SaaSPlatform 4.4.4.1 in the Mock Internet.

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*

Devices that are directly applicable to the testing method are enclosed in green boxes.



Legend

SaaS	Software as a Service
Eth*	Ethernet + port number
ISP	Internet Service Provider
L3	Layer 3
NetAdminServer	Network Administration Server
Admin	Administration
VLAN	Virtual Local Area Network

Testing Method

*Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.*

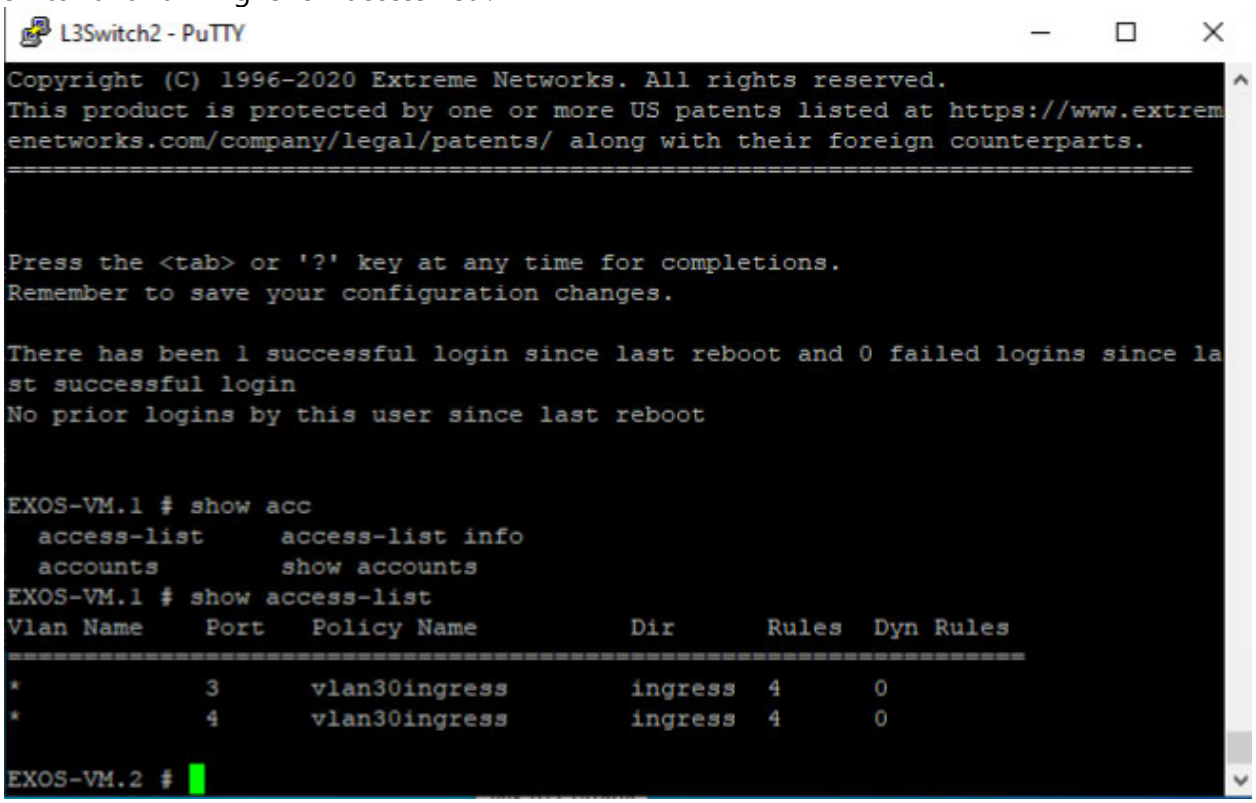
To verify that the ACL works properly for the Guest Network, I will perform a traceroute to 10.0.0.33 and 4.4.4.1 from GuestMachine1, both of which will be successful. To verify that I am

unable to reach any other devices, I will perform a traceroute destined to each hop returned by the traceroute that is not 10.0.0.33 and 4.4.4.1. This will fail because the ACL will deny packets not destined for those IP addresses.

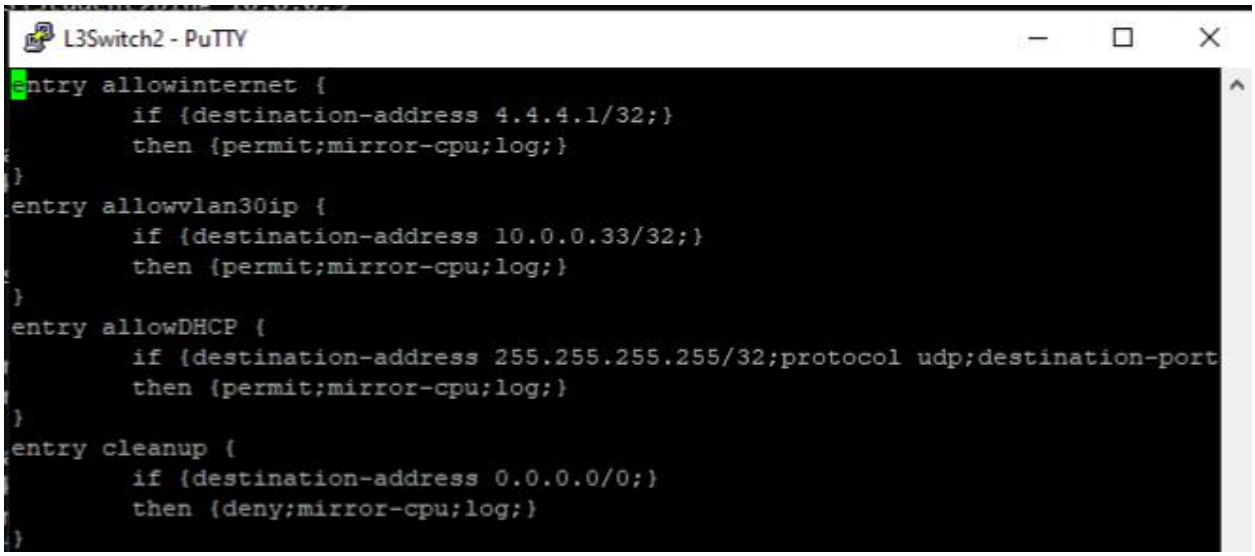
Process List

*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

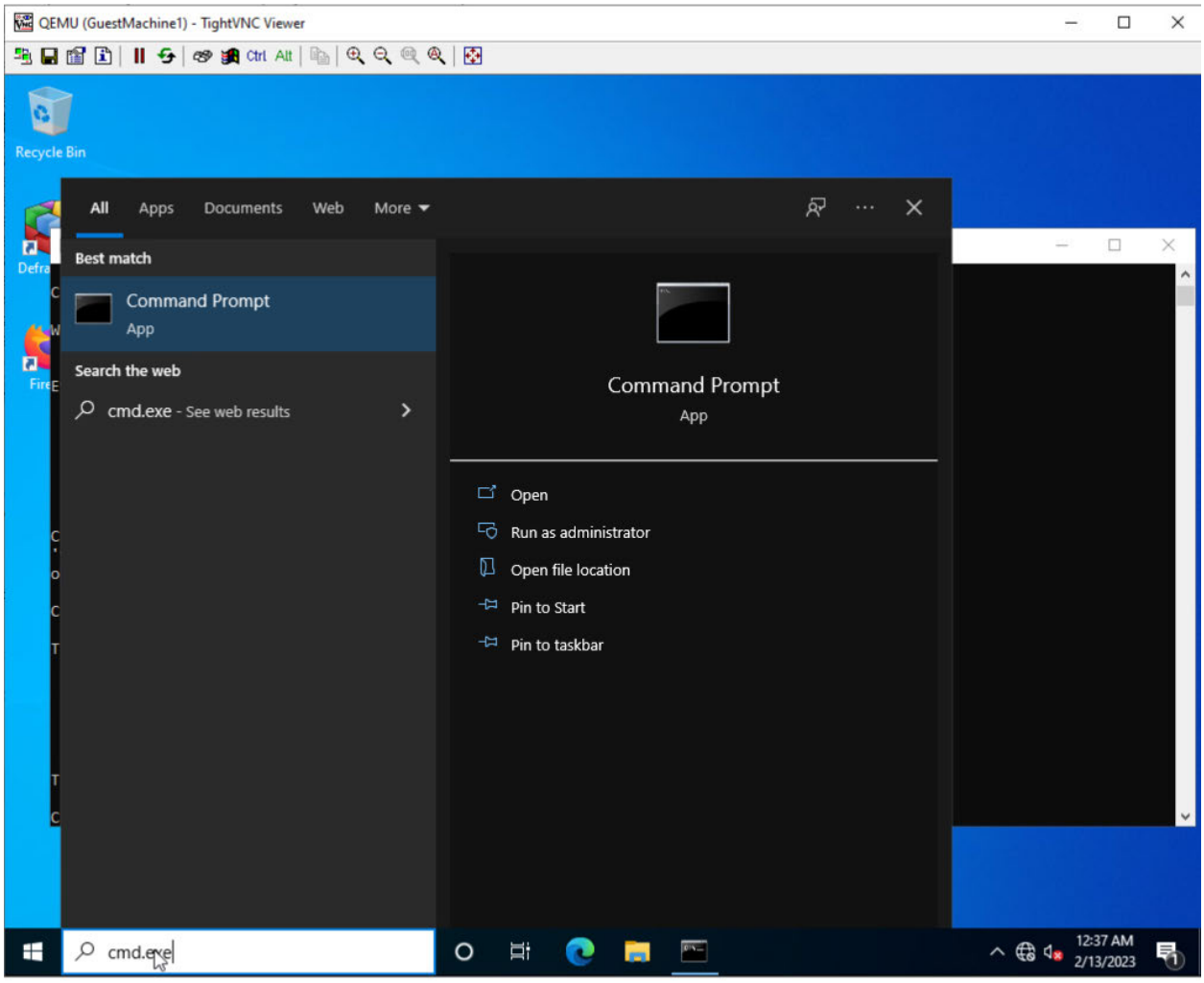
1. Verify the access lists are in place on L3Switch2 for ports 3 and 4 by logging into the switch and running "show access-list".



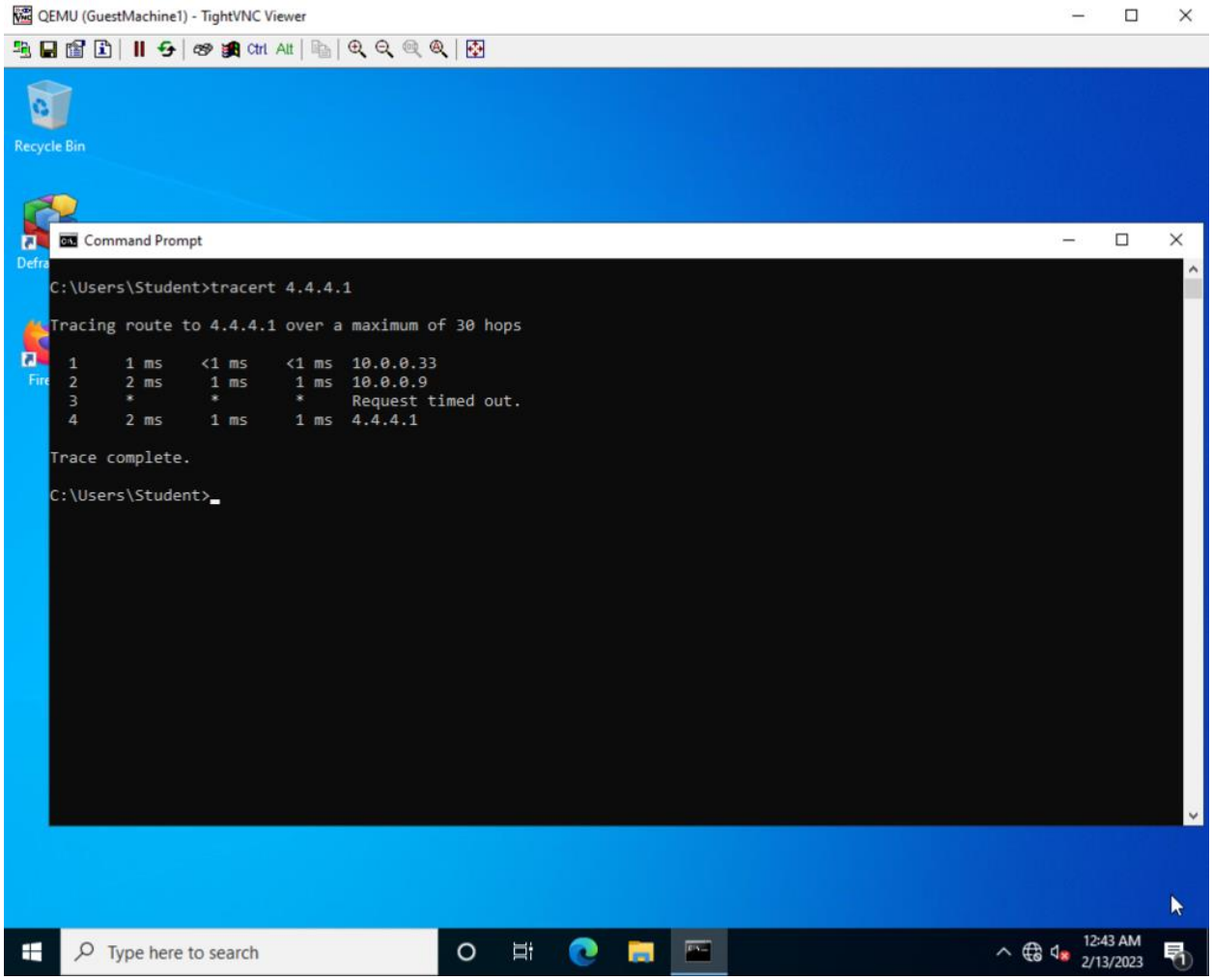
2. Verify the ACLs are blocking all traffic other than DHCP and destination addresses 10.0.0.33 (gateway) and 4.4.4.1 by opening the policy file by running "vi vlan30ingress.pol". We can see that this is correct.



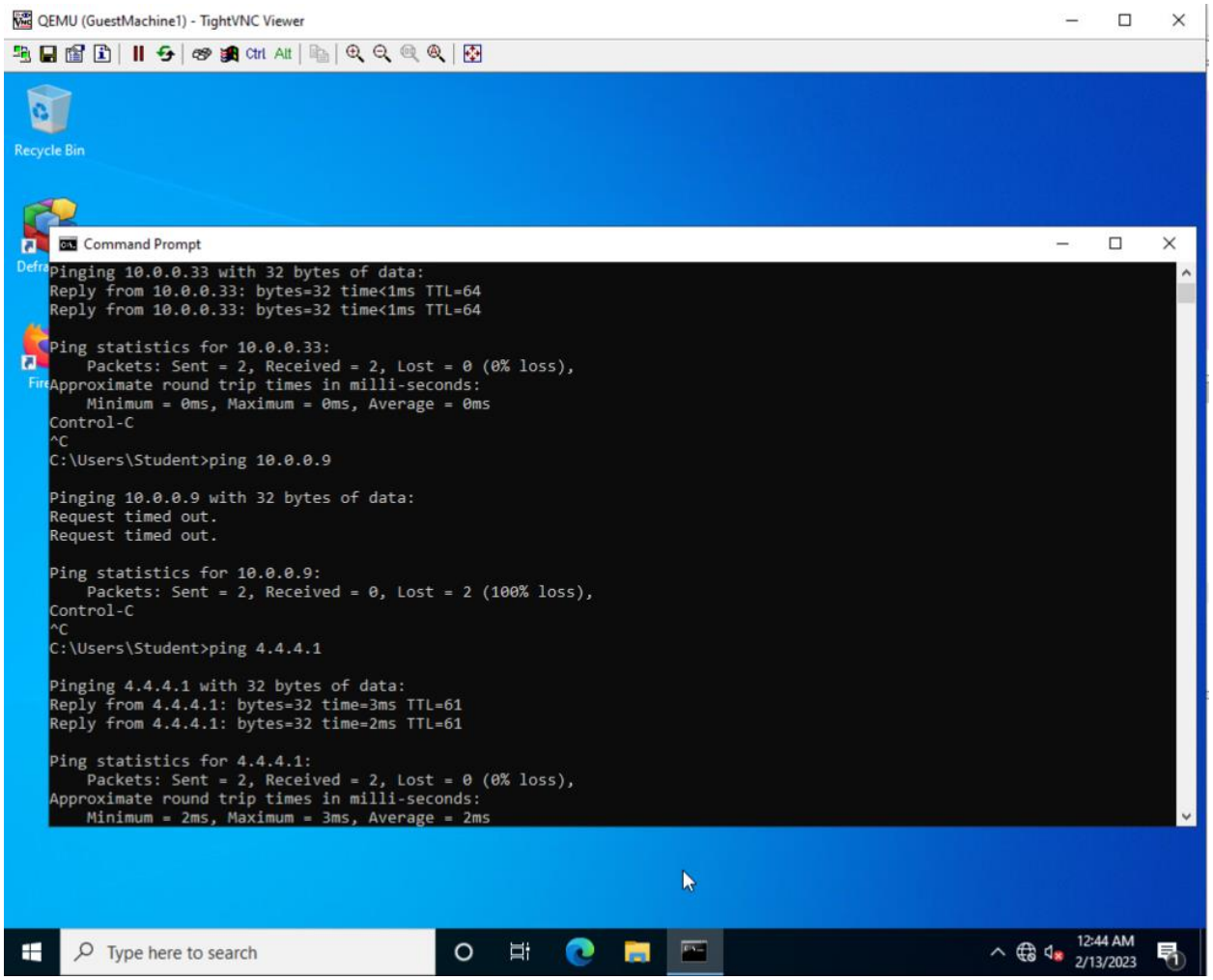
3. Login to GuestMachine1
4. Run cmd.exe



5. In the command prompt, run "tracert 4.4.4.1" to discover all layer 3 hops between GuestMachine1 and SaasPlatform. This shows that 10.0.0.33, 10.0.0.9, a device which blocks inbound ICMP traffic, and 4.4.4.1 are in between.



6. Run "ping 10.0.0.33" and let it complete. This will be successful because it is explicitly allowed in the ACL.
7. Run "ping 10.0.0.9" and let it complete. This will fail and is caught by the deny all rule because it is not explicitly allowed.
8. Run "ping 4.4.4.1" and let it complete. This will be successful because it is explicitly allowed in the ACL.


QEMU (GuestMachine1) - TightVNC Viewer
Ctrl Alt
Recycle Bin
Command Prompt
Pinging 10.0.0.33 with 32 bytes of data:
Reply from 10.0.0.33: bytes=32 time<1ms TTL=64
Reply from 10.0.0.33: bytes=32 time<1ms TTL=64
Ping statistics for 10.0.0.33:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Student>ping 10.0.0.9
Pinging 10.0.0.9 with 32 bytes of data:
Request timed out.
Request timed out.
Ping statistics for 10.0.0.9:
Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Users\Student>ping 4.4.4.1
Pinging 4.4.4.1 with 32 bytes of data:
Reply from 4.4.4.1: bytes=32 time=3ms TTL=61
Reply from 4.4.4.1: bytes=32 time=2ms TTL=61
Ping statistics for 4.4.4.1:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms
Type here to search
12:44 AM
2/13/2023

Test Case #3: Security Compliance—Log-in Banners and Automation

Display a log-in banner when accessing each device on the network. The log-in banner should notify users of an acceptable use policy (AUP) or other security-based policies when attempting to Login to the network.

Additionally, establish an automated process to update the log-in banner for multiple devices. Clearly identify the devices that will be updated, and provide a step-by-step guide for initiating the automated updates.

Note: Remove the banners from the devices that will be updated by your automation process prior to submission so the evaluators can run the process and verify the new configuration.

Functionality

*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

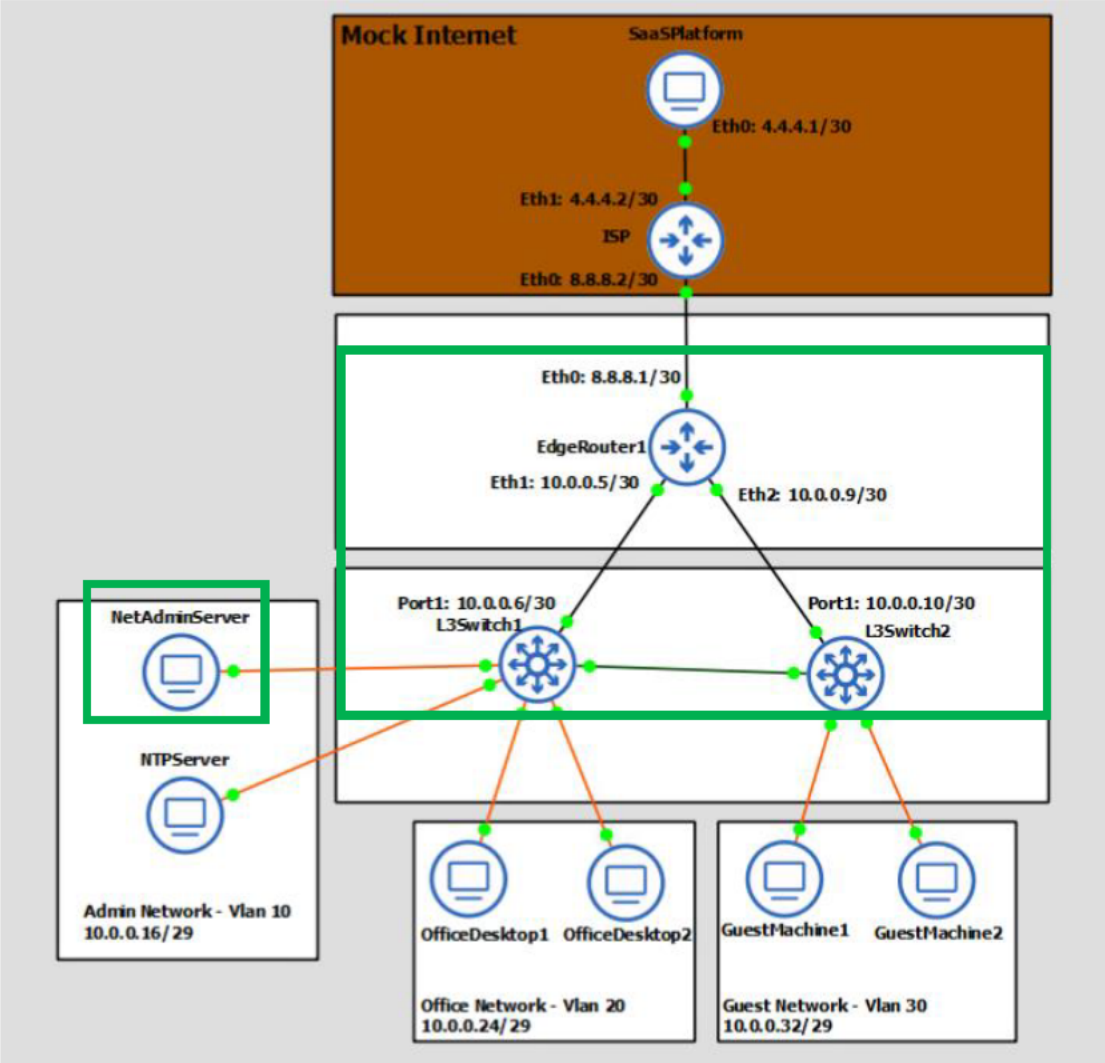
There are three network devices that would require banners on the network. EdgeRouter1, L3Switch1, and L3Switch2. The ISP router will not receive a banner because it is in the Mock Internet and would not be controlled by the customer. The login banner currently in the lab is based on the "Short-Form Banner" from Kellep Charles article on SecurityOrb.com "Warning banner sample for systems and network devices".

The banners are configured through a Python script hosted on NetAdminServer and located at "/home/student/NetAutomation/update_banner.py". This script utilizes the paramiko and netmiko libraries to handle SSH connections to the router and switches to update their banners. The banner that will be configured on the devices is stored as a constant in the Python script. The constant is named "BANNER" and is at the top of the script.

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*

Devices that are directly applicable to the testing method are enclosed in green boxes.



Legend

SaaS	Software as a Service
Eth*	Ethernet + port number
ISP	Internet Service Provider
L3	Layer 3
NetAdminServer	Network Administration Server
Admin	Administration
VLAN	Virtual Local Area Network

Testing Method

*Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.*

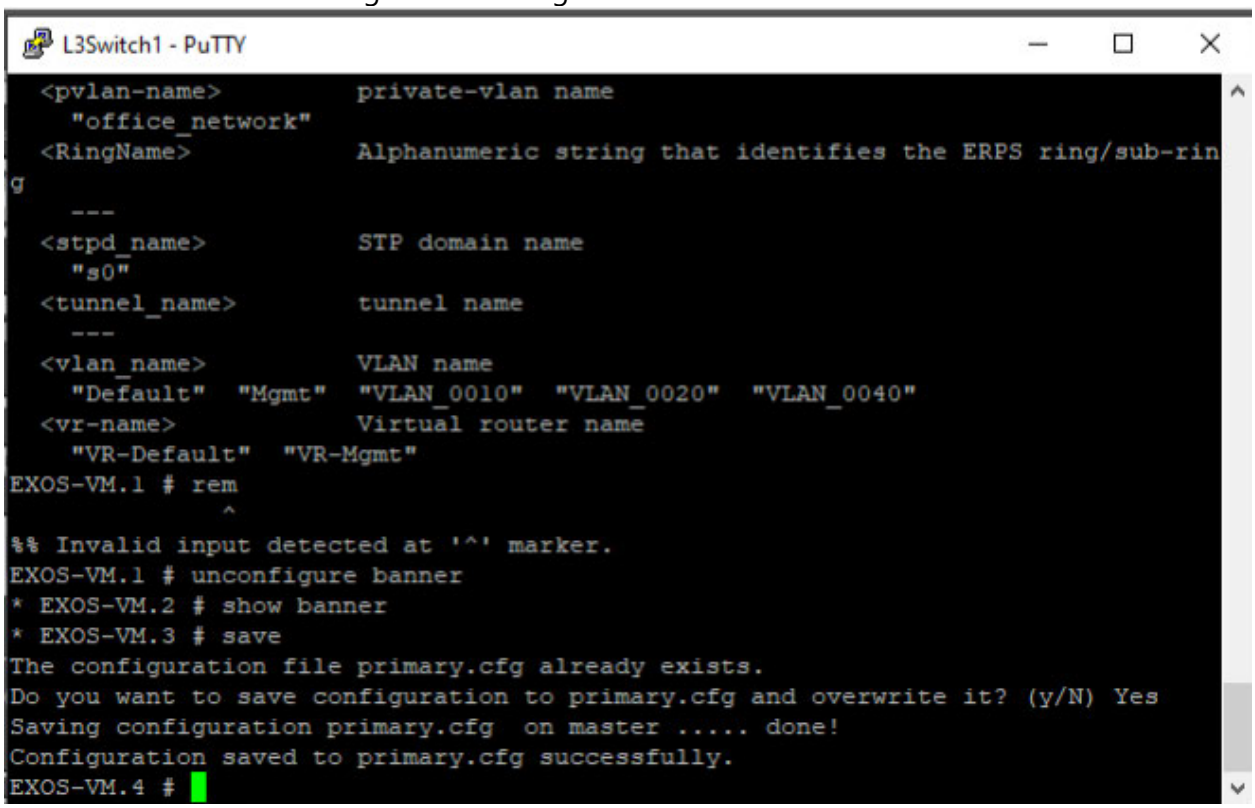
I will remove the banner from each device and save the configuration. I will then verify that there is no banner configured. I will then run the Python script to configure a banner that meets the requirements

stated in the test case on each device. I will then reboot each device and show the new banner to demonstrate that each device has the proper banner that persists after reboot.

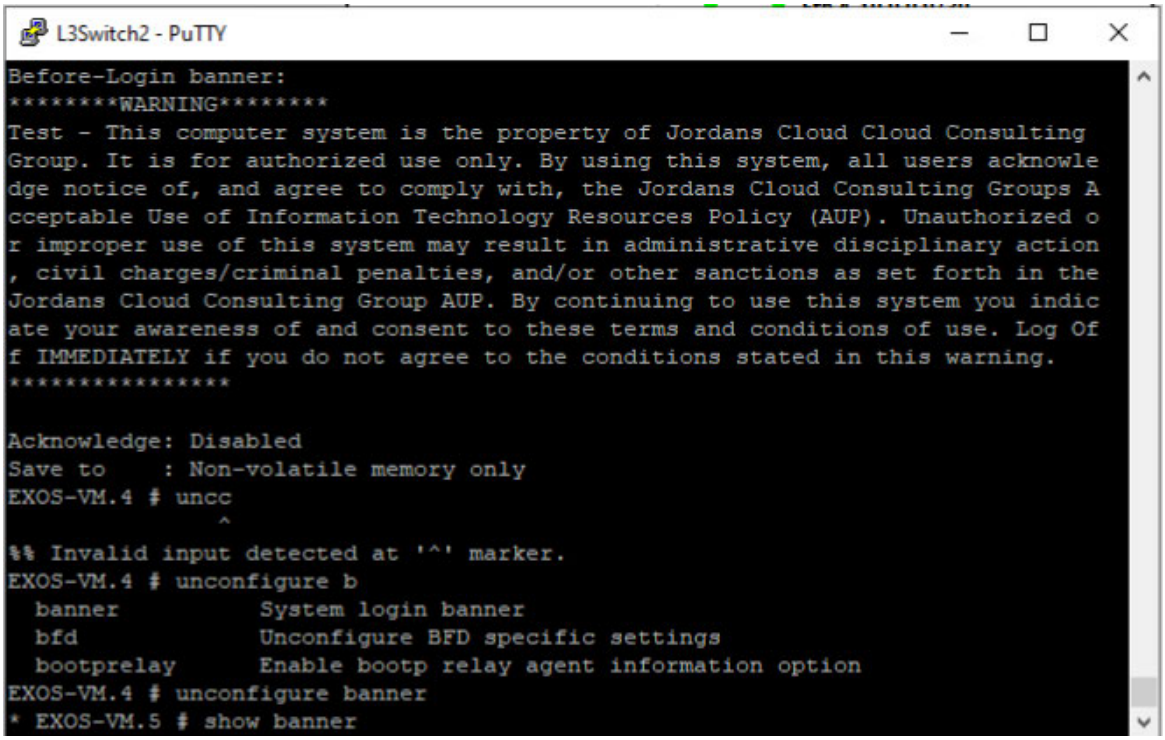
Process List

*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

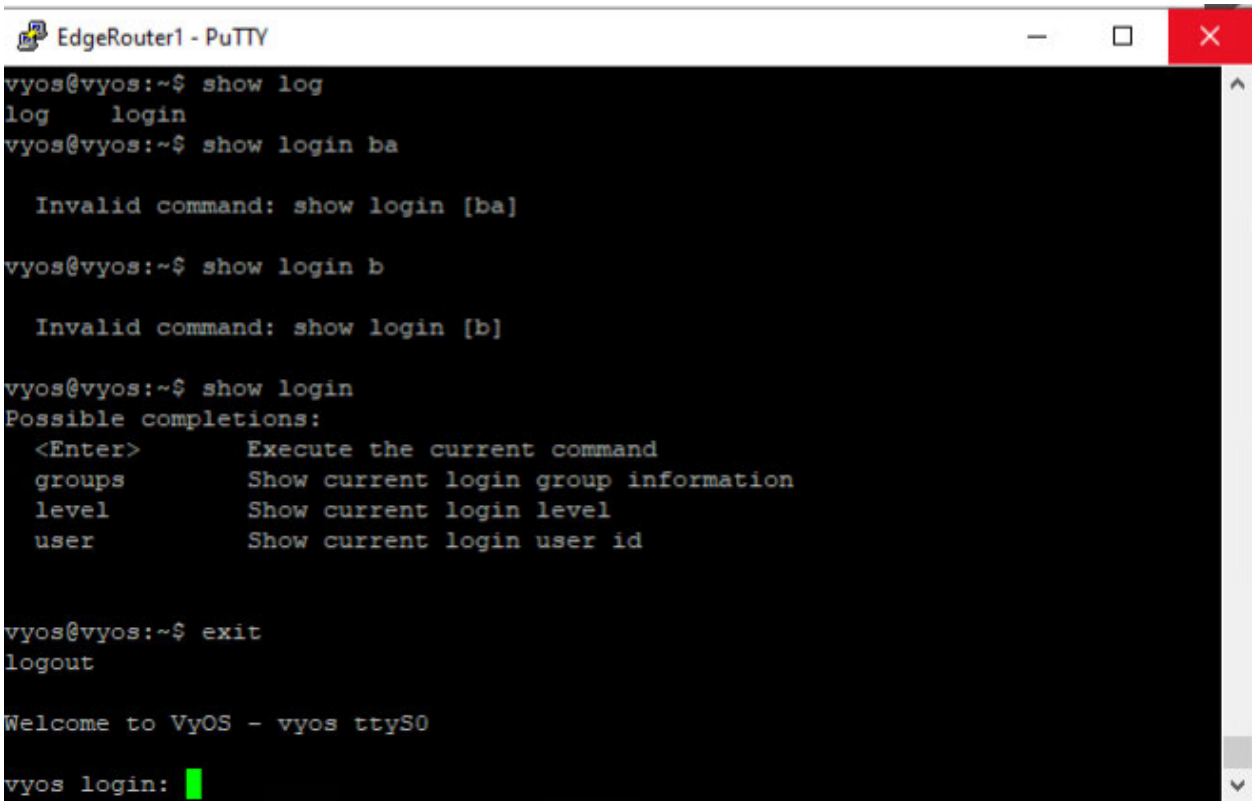
1. Login to L3Switch1.
2. Run "unconfigure banner" to remove any configured banners.
3. Run "show banner" to verify that this was successful.
4. Run "save" to save the configuration through reboot.



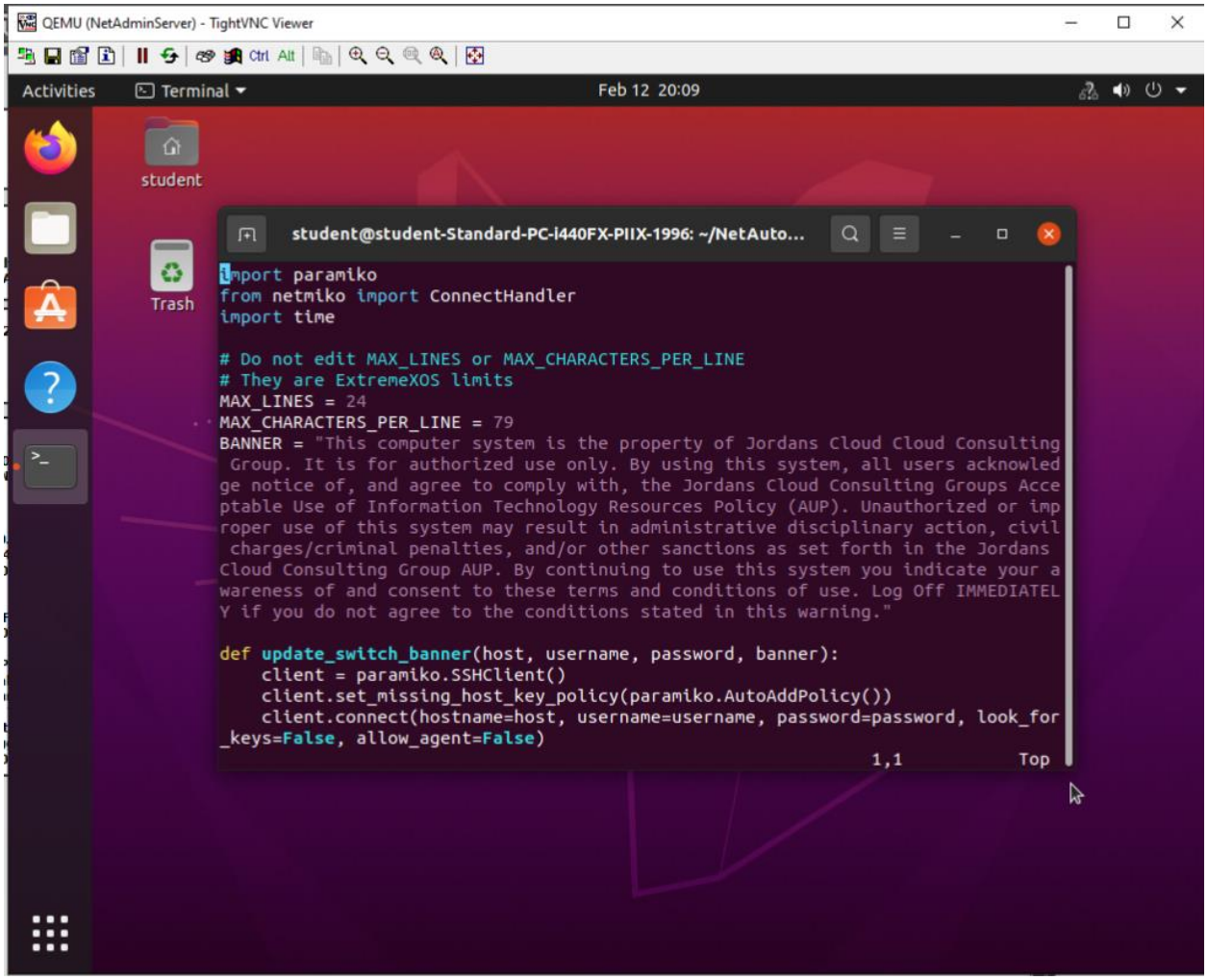
5. Repeat steps 1-3for L3Switch2



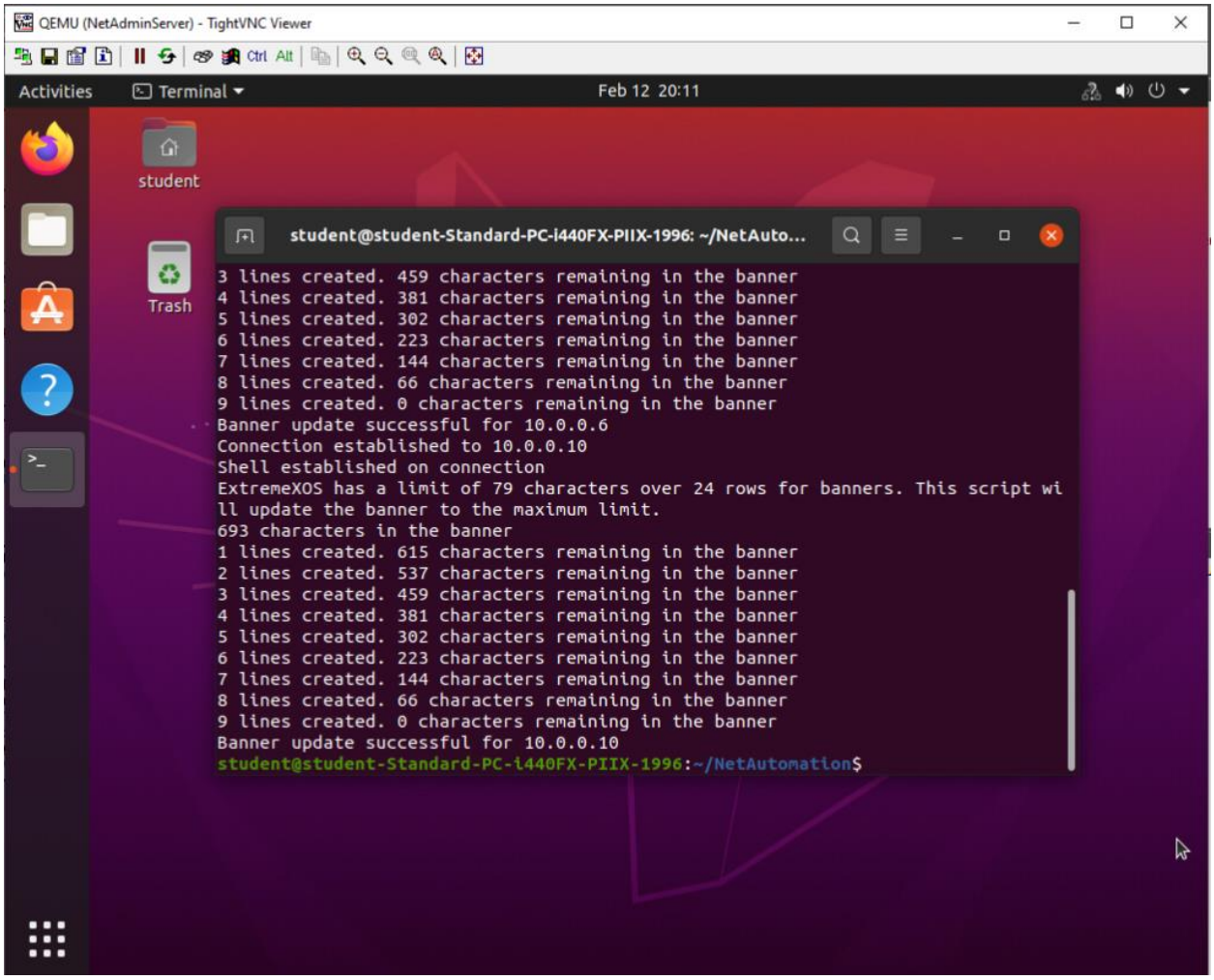
6. Login to EdgeRouter1.
7. Run “config” to enter configuration mode.
8. Run “delete system login banner” to delete any configured banners.
9. Run “commit” then “save” to save the configuration through reboot.
10. Run “exit” to leave configuration mode
11. Run “exit” again to log out. There should be no login banner.



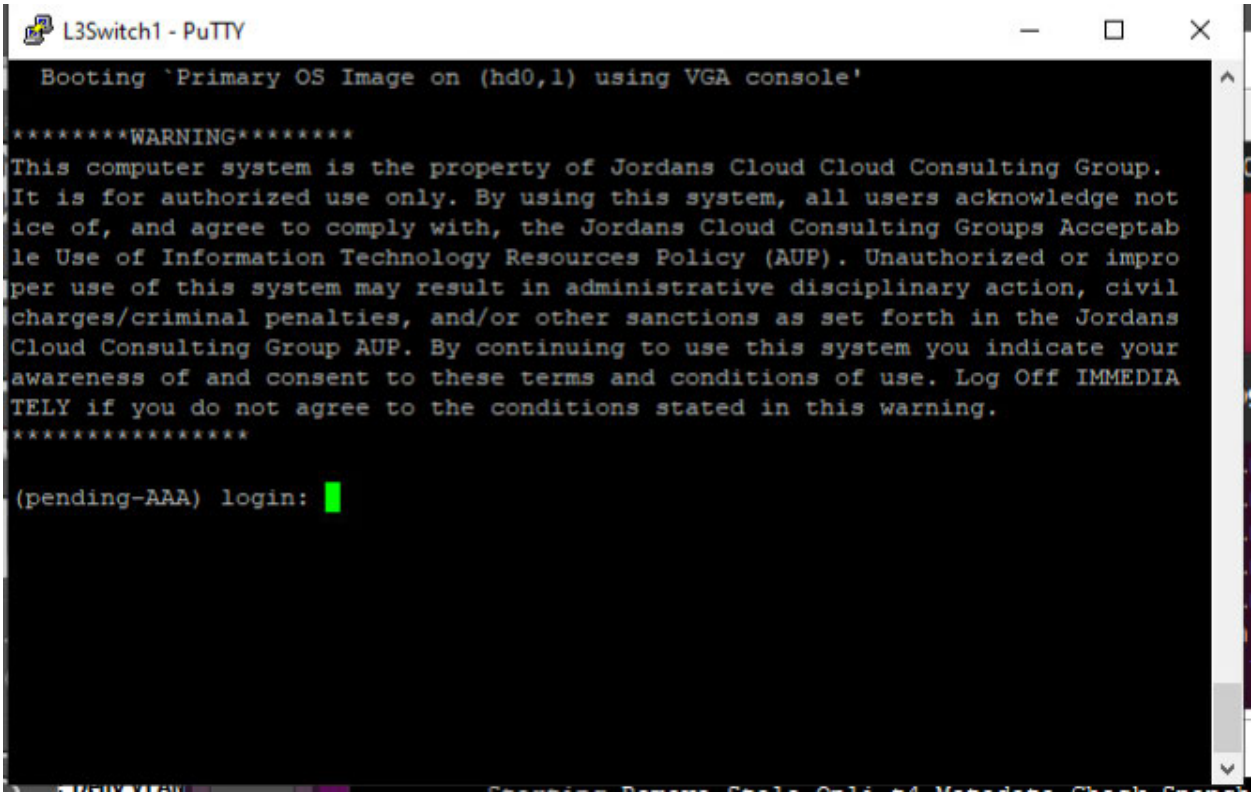
12. Login to NetAdminServer.
13. Open a terminal and run “cd /home/student/NetAutomation”.
14. Run “ls” to view available scripts. You should see “update_banner.py” which is the script we will use.
15. Use a text editor on “update_banner.py” to look at the banner that will be used on the network devices. The “BANNER” constant is on line 9 of the file.
16. Modify the banner to suit the organizations needs. Keep in mind that there are limitations on banner size, and characters. ExtremeXOS limits the allowed lines and characters, and VyOS has issues handling certain characters. The script handles ExtremeXOS’s limitations natively, but not VyOS because there is not a list I found of all excluded characters.

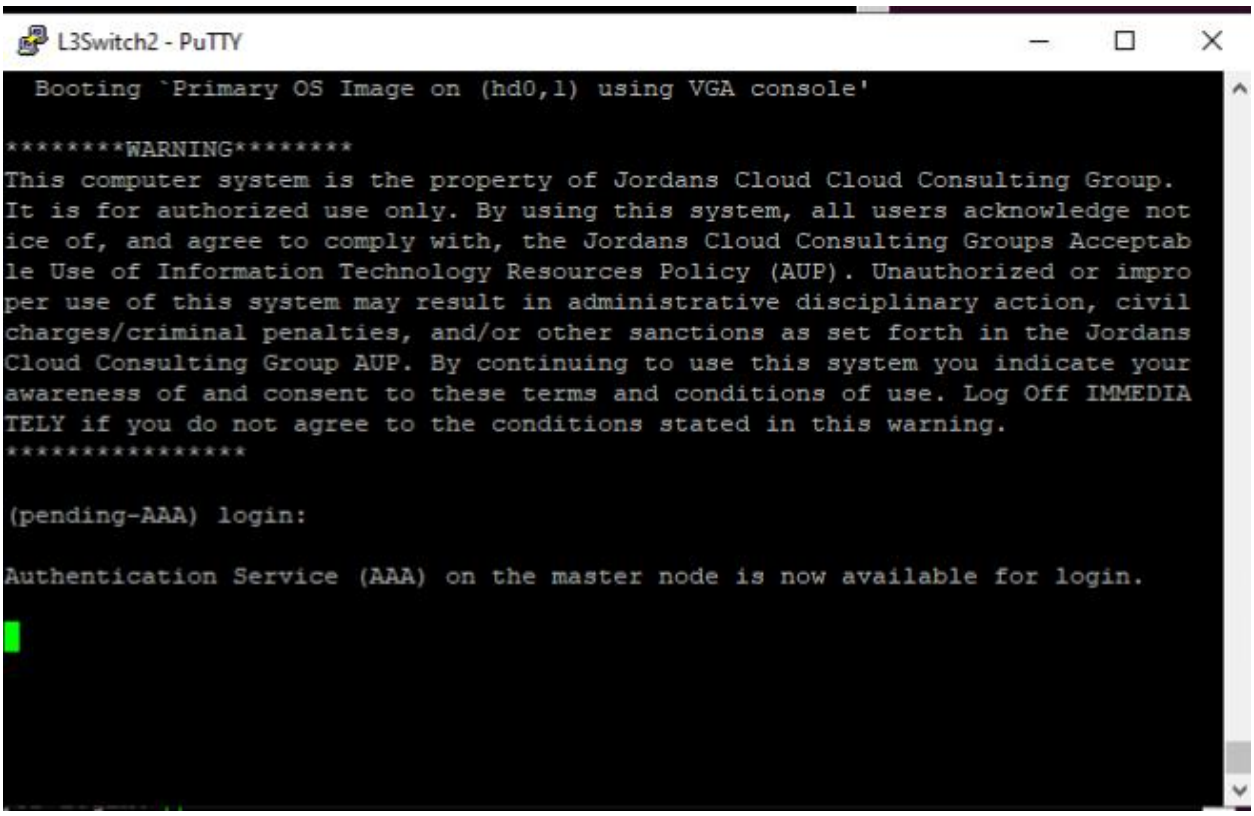


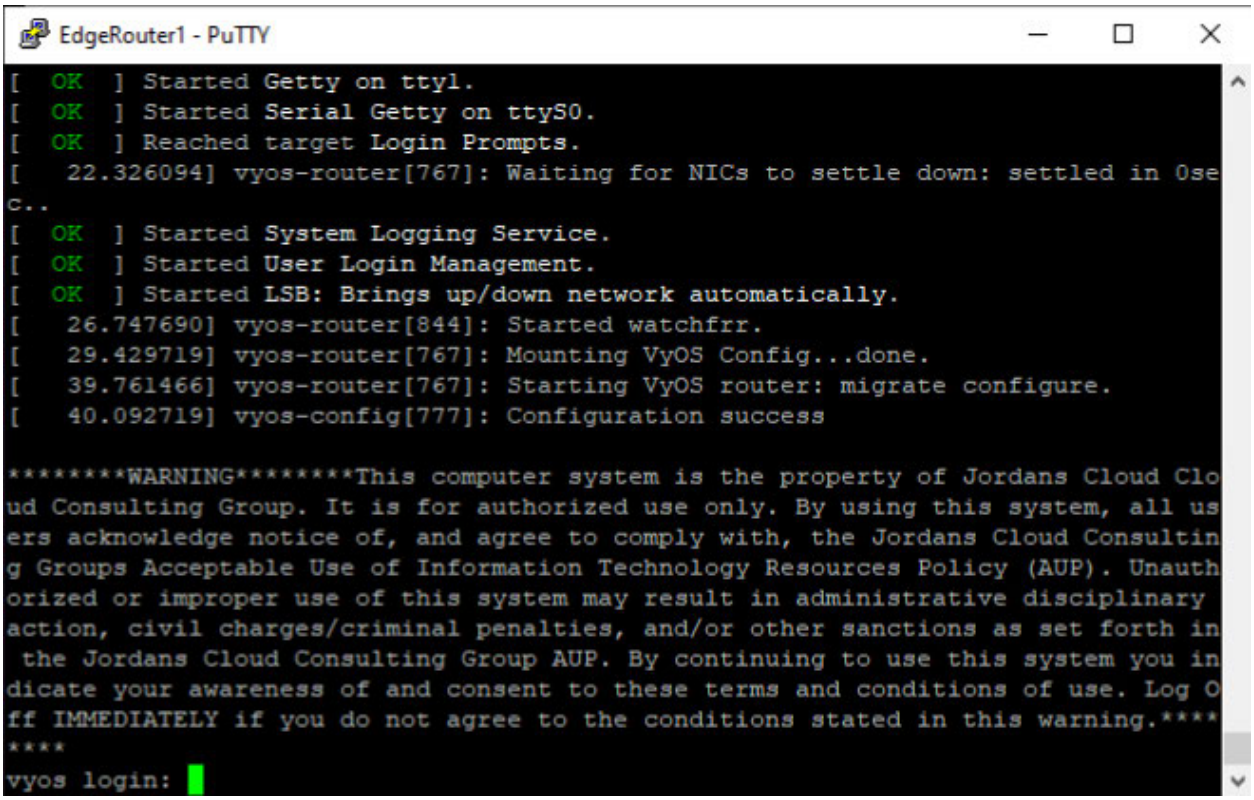
17. When you have created the banner to use, save and exit the file.
18. Run “python3 update_banner.py” to update the banners across the three network devices. It will show progress updates while it is running.



19. To verify that the script updated the devices successfully, reboot EdgeRouter1, L3Switch1 and L3Switch2 using the "reboot" command on each.
20. After rebooting each device, we can see that the banner configuration was successful. The banner will appear right after reboot, before login. No additional commands are needed.


L3Switch1 - PuTTY
Booting `Primary OS Image on (hd0,1) using VGA console'
********WARNING********
This computer system is the property of Jordans Cloud Cloud Consulting Group.
It is for authorized use only. By using this system, all users acknowledge not
ice of, and agree to comply with, the Jordans Cloud Consulting Groups Acceptab
le Use of Information Technology Resources Policy (AUP). Unauthorized or impro
per use of this system may result in administrative disciplinary action, civil
charges/criminal penalties, and/or other sanctions as set forth in the Jordans
Cloud Consulting Group AUP. By continuing to use this system you indicate your
awareness of and consent to these terms and conditions of use. Log Off IMMEDIA
TELY if you do not agree to the conditions stated in this warning.
****
(pending-AAA) login:


L3Switch2 - PuTTY
Booting `Primary OS Image on (hd0,1) using VGA console'
********WARNING********
This computer system is the property of Jordans Cloud Cloud Consulting Group.
It is for authorized use only. By using this system, all users acknowledge not
ice of, and agree to comply with, the Jordans Cloud Consulting Groups Acceptab
le Use of Information Technology Resources Policy (AUP). Unauthorized or impro
per use of this system may result in administrative disciplinary action, civil
charges/criminal penalties, and/or other sanctions as set forth in the Jordans
Cloud Consulting Group AUP. By continuing to use this system you indicate your
awareness of and consent to these terms and conditions of use. Log Off IMMEDIA
TELY if you do not agree to the conditions stated in this warning.
****
(pending-AAA) login:
Authentication Service (AAA) on the master node is now available for login.



*Banners have been removed after configuration in the lab per instructions

Test Case #4: Accessing External Resources—Routing and Traffic Security

User devices on your network should have dynamic addresses that are assigned through DHCP unless they provide a service that requires a static address. You must also have at least one network resource that requires a static address.

Functionality

*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

There are several interfaces that utilize static IP addresses and several networks that utilize DHCP. The static IP addresses configured are:
NTPServer eth0 10.0.0.18/29
L3Switch1 eth1 10.0.0.6/30
L3Switch2 eth1 10.0.0.42/30
L3Switch2 eth1 10.0.0.10/30
L3Switch2 eth2 10.0.0.41/30
EdgeRouter1 eth0 8.8.8.1/30 - eth1 10.0.0.5/30 - eth2 10.0.0.9/30
ISP eth0 8.8.8.2/30 - eth1 4.4.4.2/30
SaaSPlatform eth0 4.4.4.1/30

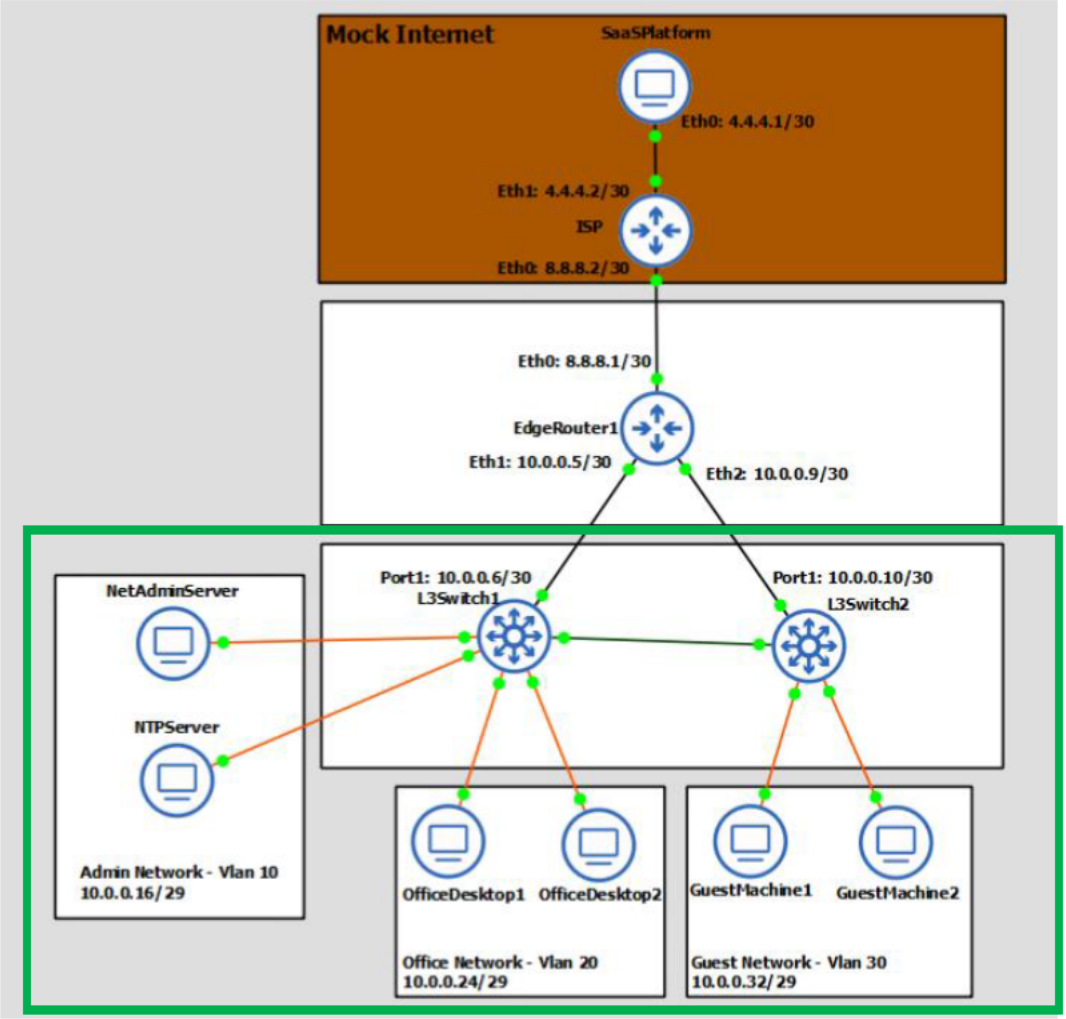
DHCP is configured on L3Switch1 and L3Switch2. DHCP will assign an IP address and default gateway to each device that requests a lease. The default gateway for each lease is the VLAN IP address for each VLAN. Example: 10.0.0.25/29 VLAN 20 – Default Gateway address is VLAN Address 10.0.0.25.

The switches assign IP addresses in the following ranges on the following ports:
L3Switch1 VLAN_0010 Ports 3 6 -10.0.0.19 - 10.0.0.22
L3Switch1 VLAN_0020 Ports 4 5 – 10.0.0.26 - 10.0.0.30
L3Switch2 VLAN_0030 Ports 3 5 – 10.0.0.34 - 10.0.0.38

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*

Devices that are directly applicable to the testing method are enclosed in green boxes.



Legend

SaaS	Software as a Service
Eth*	Ethernet + port number
ISP	Internet Service Provider
L3	Layer 3
NetAdminServer	Network Administration Server
Admin	Administration
VLAN	Virtual Local Area Network

Testing Method

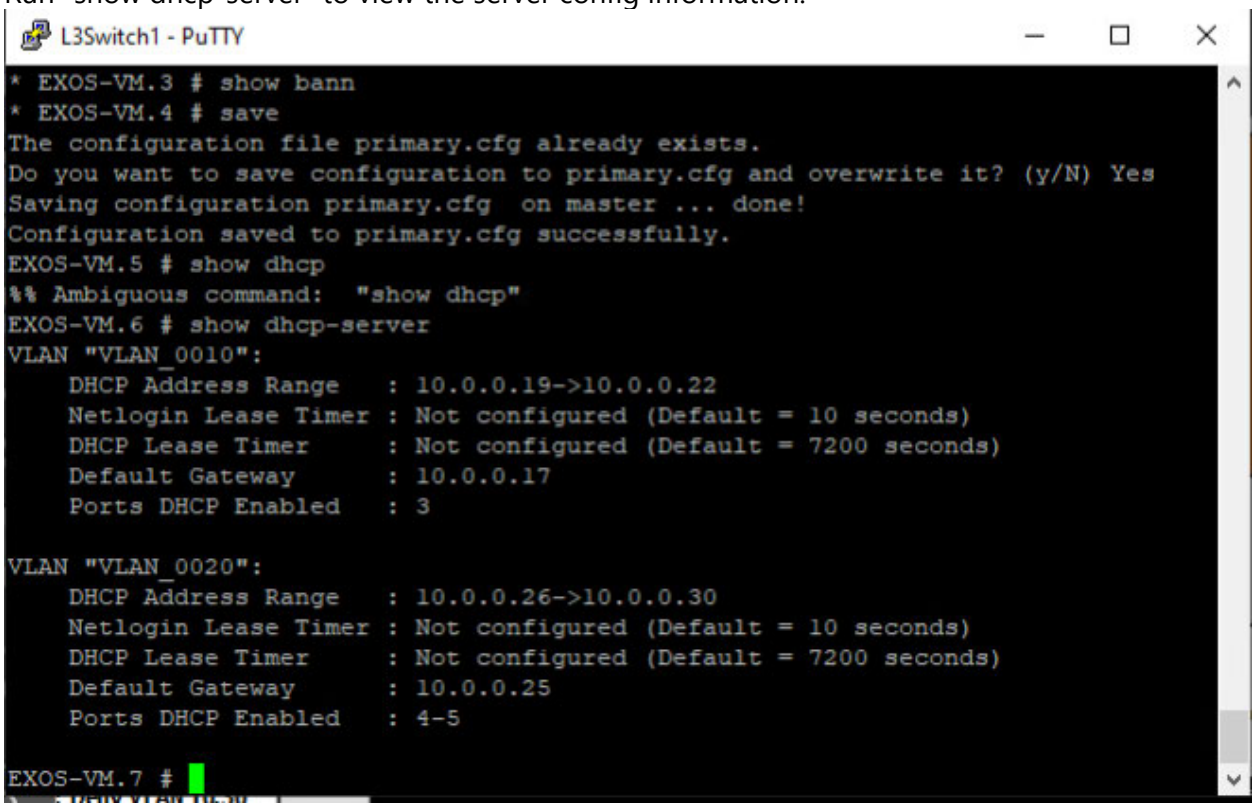
*Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.*

To demonstrate that DHCP is working as expected, I will show the DHCP service details on each switch. I will then log onto a computer from each network receiving a DHCP lease and verify that one has been received, and it falls within the configured range. I will also discuss NTPServer's static address and how it affects the DHCP address pool for VLAN 10.

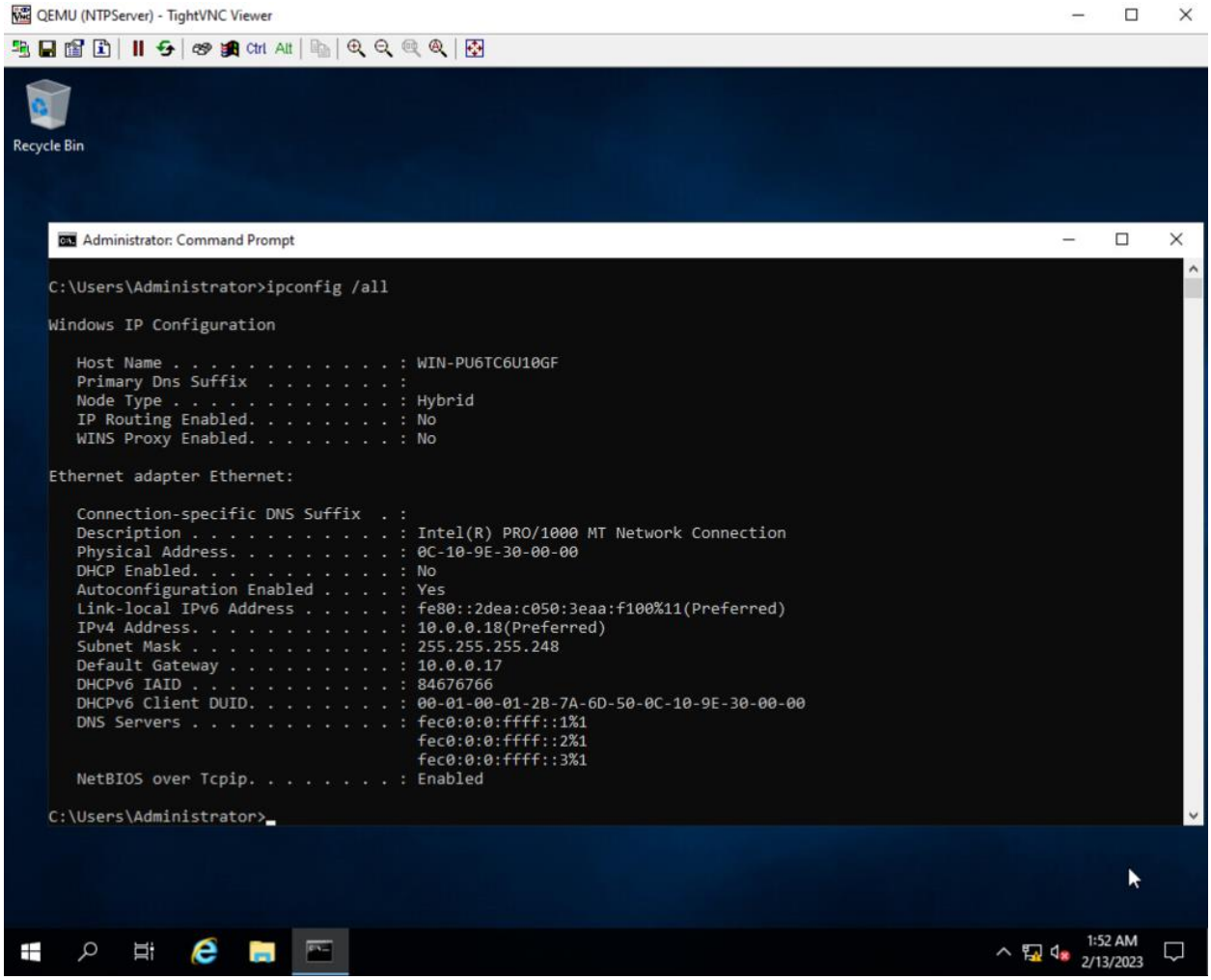
Process List

*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

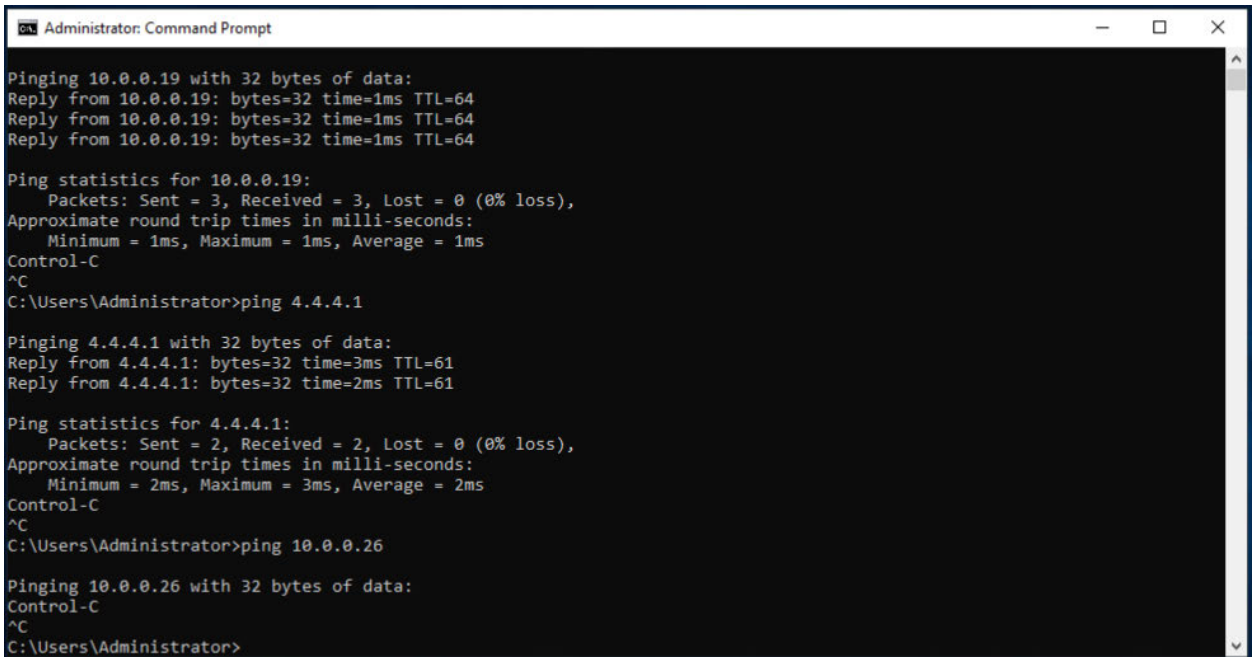
1. Login to L3Switch1.
2. Run "show dhcp-server" to view the server config information.



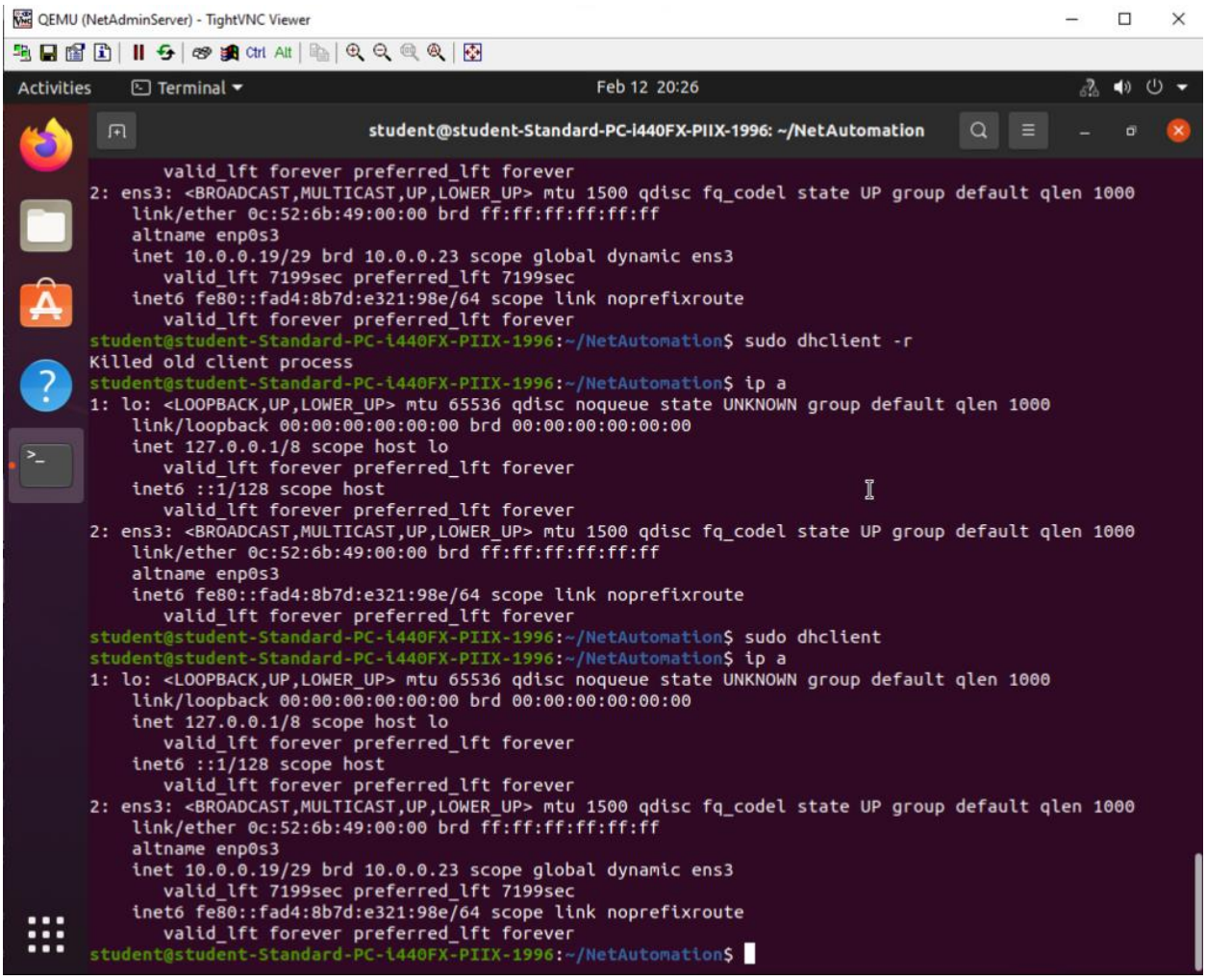
3. Login to NetAdminServer on VLAN 10. It is the only device receiving DHCP leases on the network. The reason for this is because NTPServer is configured statically as 10.0.0.18. This is why the DHCP address pool for VLAN 10 starts at 10.0.0.19. We can view the static address for NTPServer by opening "cmd.exe" and running "ipaddress /all". We can see that "DHCP Enabled" is "No". NTPServer uses a static address so network devices know where to reach it to receive NTP information.



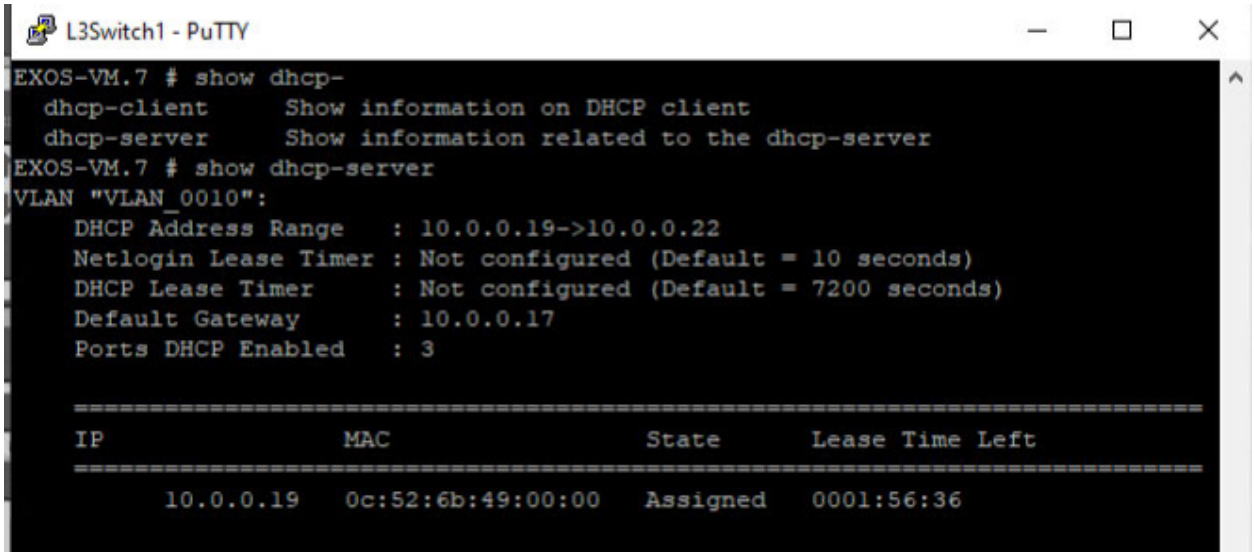
4. I run a ping to 10.0.0.19 and 4.4.4.1 to verify that even thought a static address is configured, internet access is still possible.



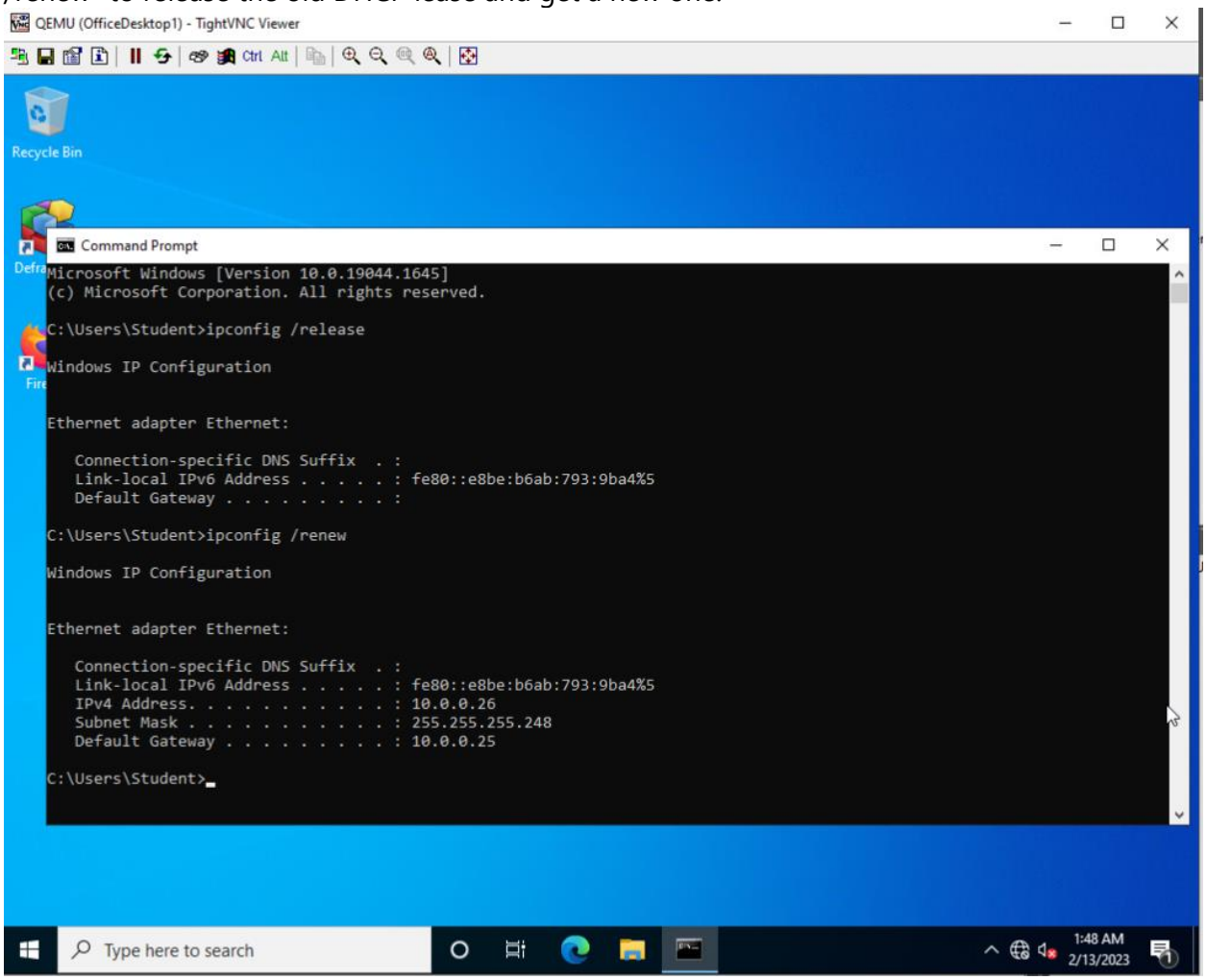
5. Open a terminal and run “ip a”. An IP address should have already been received by the DHCP server.
6. Release the DHCP lease by running “sudo dhclient -r”. You should no longer have an IP address after running “ip a”.
7. Obtain a DHCP lease by running “sudo dhclient”. You should now have an address after seeing the output of “ip a”.



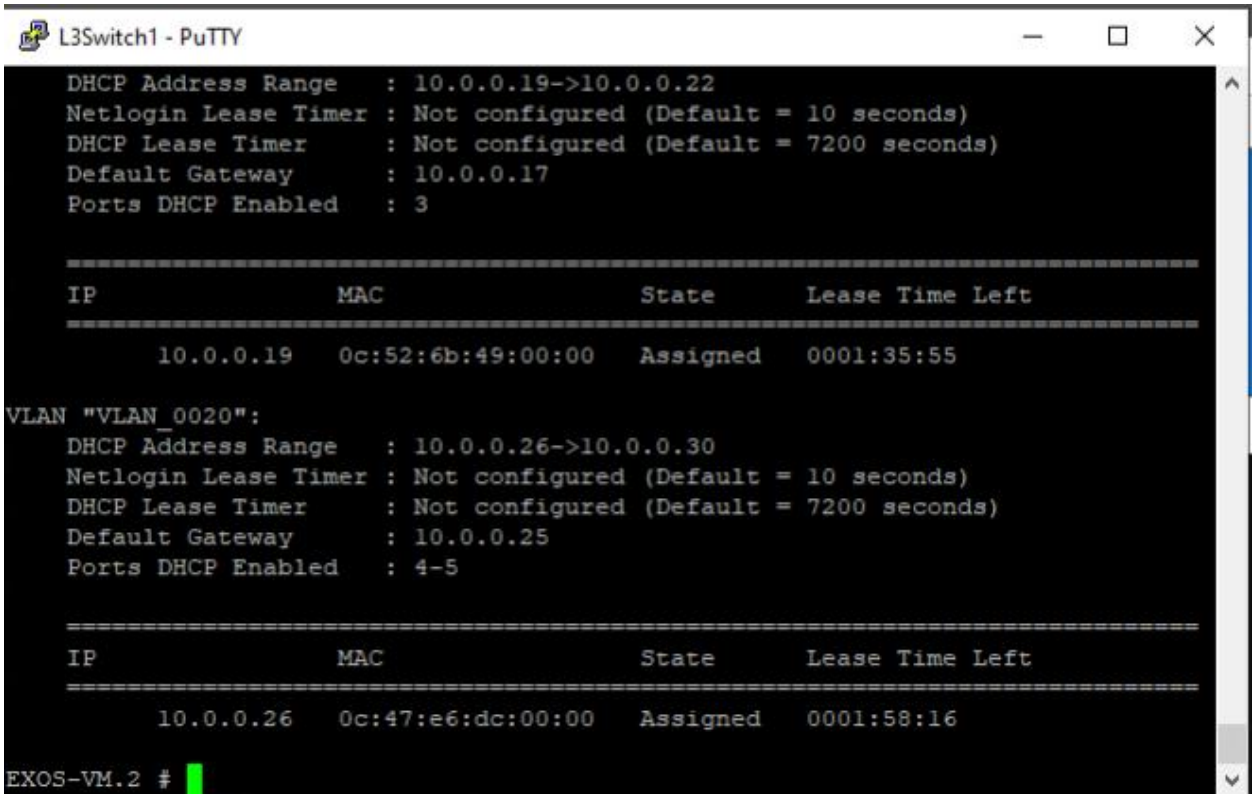
8. Verify the that L3Switch1 gave this lease by running "show dhcp-server" on it. We can see that the lease it (10.0.0.19) gave corresponds with the lease received on NetAdminServer and the interface's MAC address.



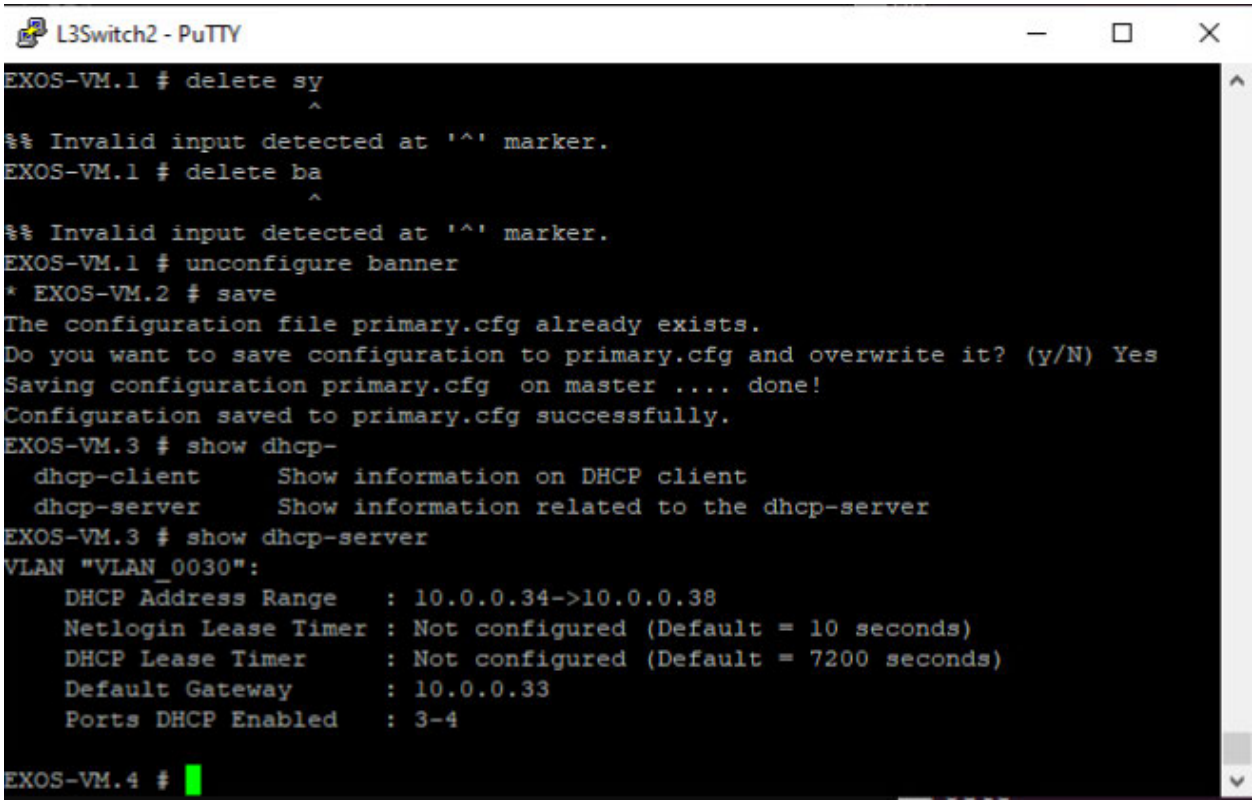
9. To verify DHCP is working correctly for VLAN 20, Login to a host on the VLAN. For this example, I will use OfficeDesktop1.
10. Run "cmd.exe" and in the command prompt run "ipconfig /release" and "ipconfig /renew" to release the old DHCP lease and get a new one.



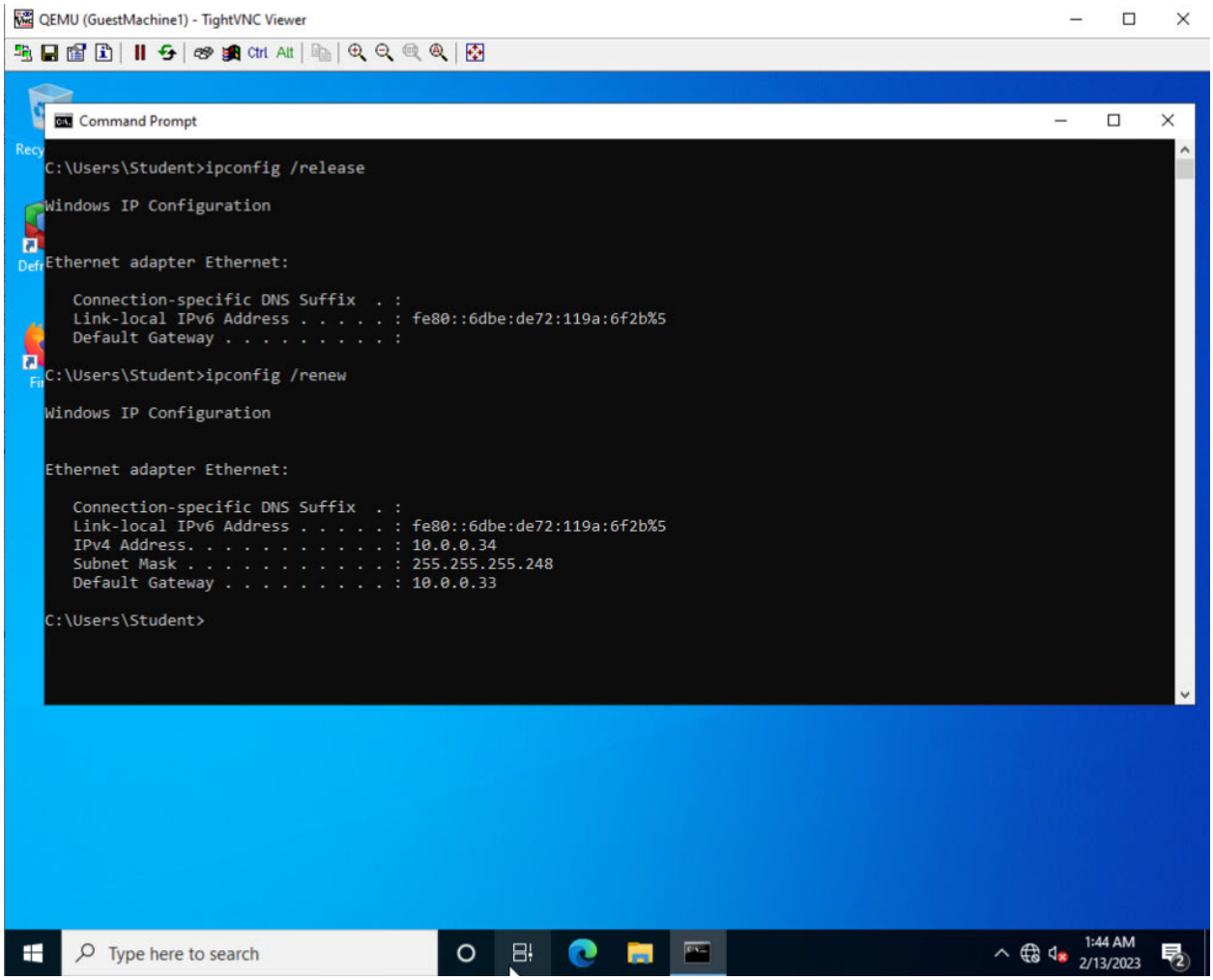
11. To verity this lease was given by L3Switch1, run "show dhcp-server" on the switch. This shows that the lease given to the host (10.0.0.26) was given by the server.



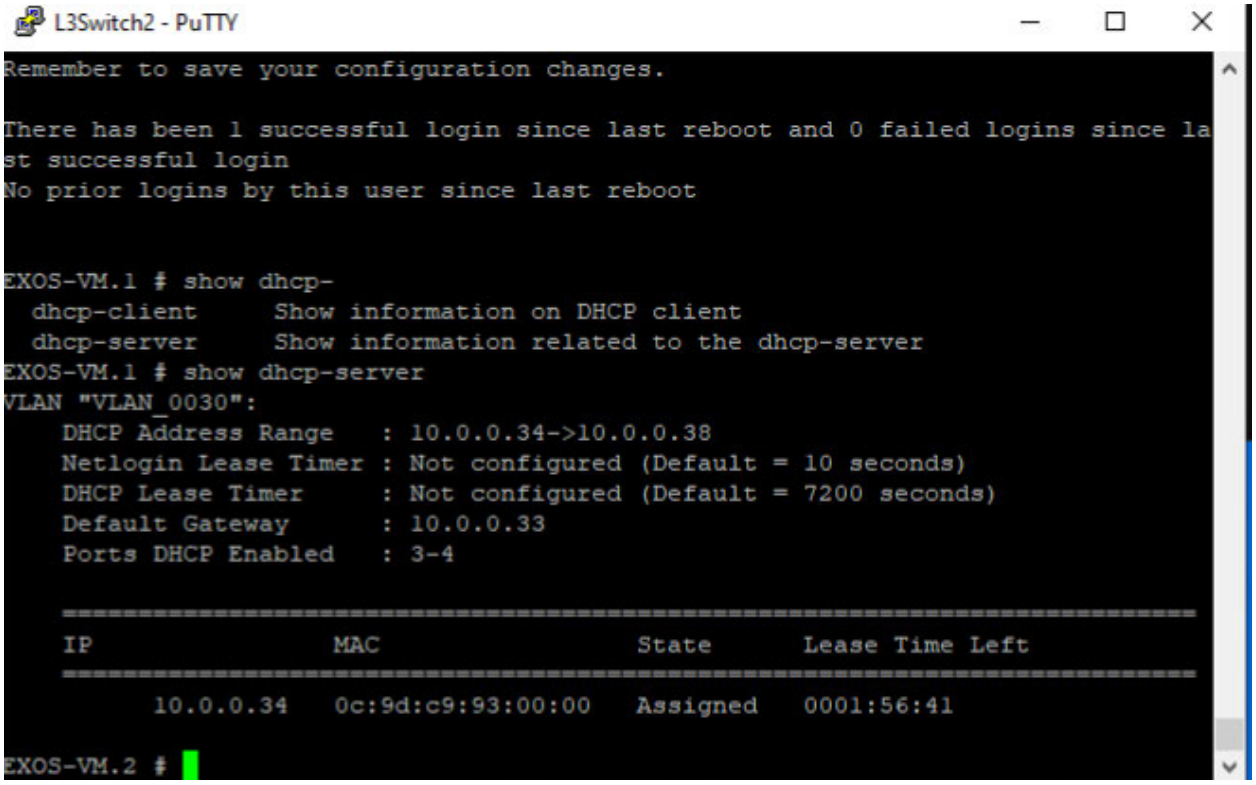
12. To verify L3Switch2's DHCP configuration, Login to L3Switch2 and run "show dhcp-server"



13. Login to a host on VLAN 30. For this example, I will use GuestMachine1.
14. Run "cmd.exe".
15. In the command prompt, run "ipconfig /release" and "ipconfig /renew" to release the old DHCP and receive a new one from the switch.



16. We can verify that this lease was given by L3Switch2 by running "show dhcp-server" on it. We can see that the lease given by the switch matches the one received by the computer.



Test Case #5: Layer 2 Link Redundancy and Spanning-Tree Protocol (802.1w)

Enable and manage the Spanning-Tree Protocol to establish redundant Layer 2 paths while avoiding possible loops and broadcast storms. Identify the Layer 2 devices that will become the Root Bridge.

Functionality

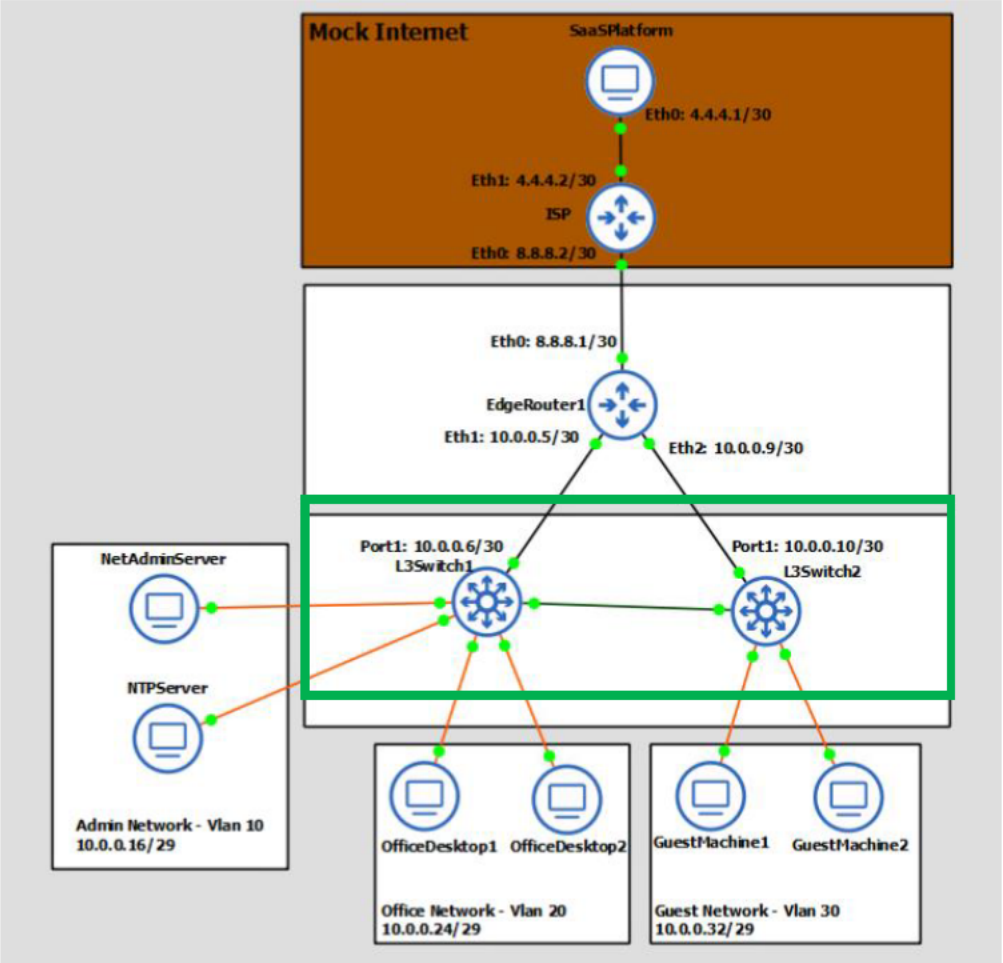
*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

There are two switches on the network, L3Switch1 and L3Switch2. There are no switching loops in the architecture since there are only 2 switches only connected by 1 link. STP is enabled on both switches.

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*

Devices that are directly applicable to the testing method are enclosed in green boxes.



Legend

SaaS	Software as a Service
Eth*	Ethernet + port number
ISP	Internet Service Provider
L3	Layer 3
NetAdminServer	Network Administration Server
Admin	Administration
VLAN	Virtual Local Area Network

Testing Method

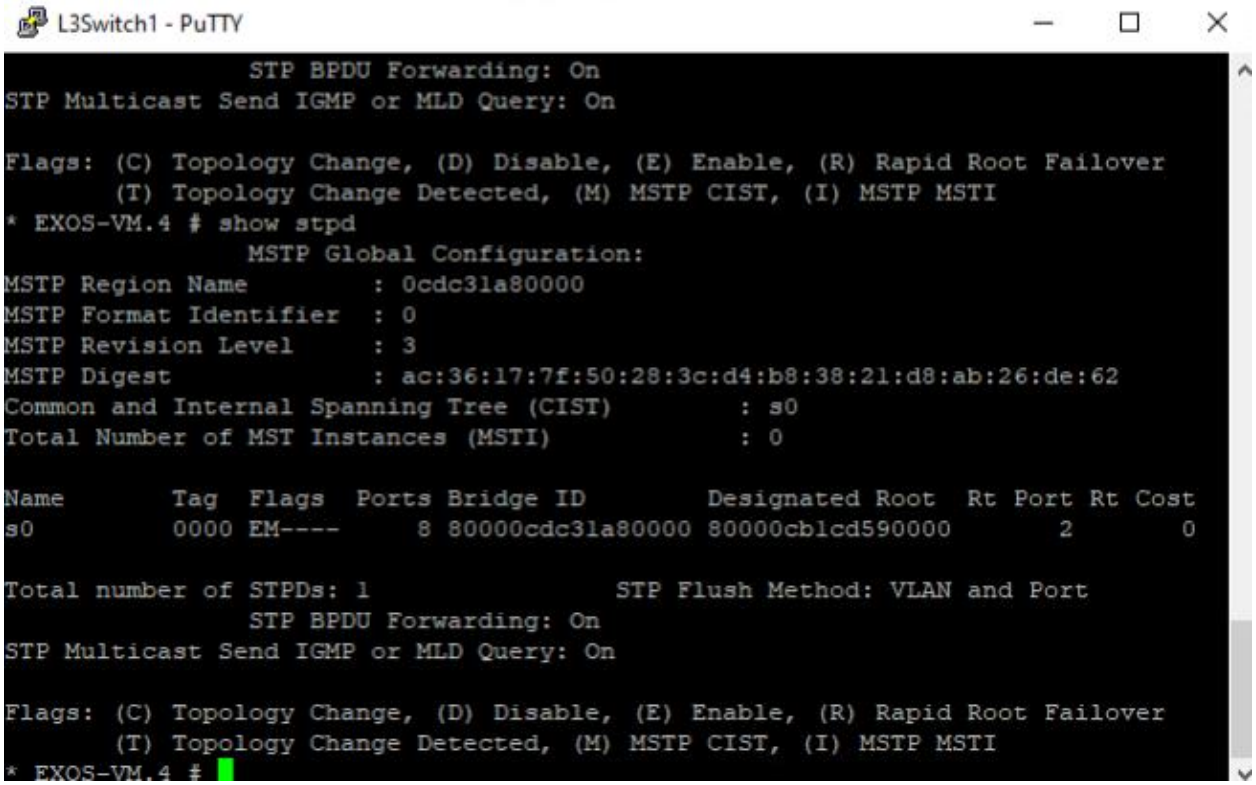
*Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.*

To demonstrate that STP is working as expected, I will show the STP configuration on each switch. Viewing the configuration, I will be able to see the elected root bridge. I will also capture packets on the link between L3Switch1 and L3Switch2 to view the exchange of STP information.

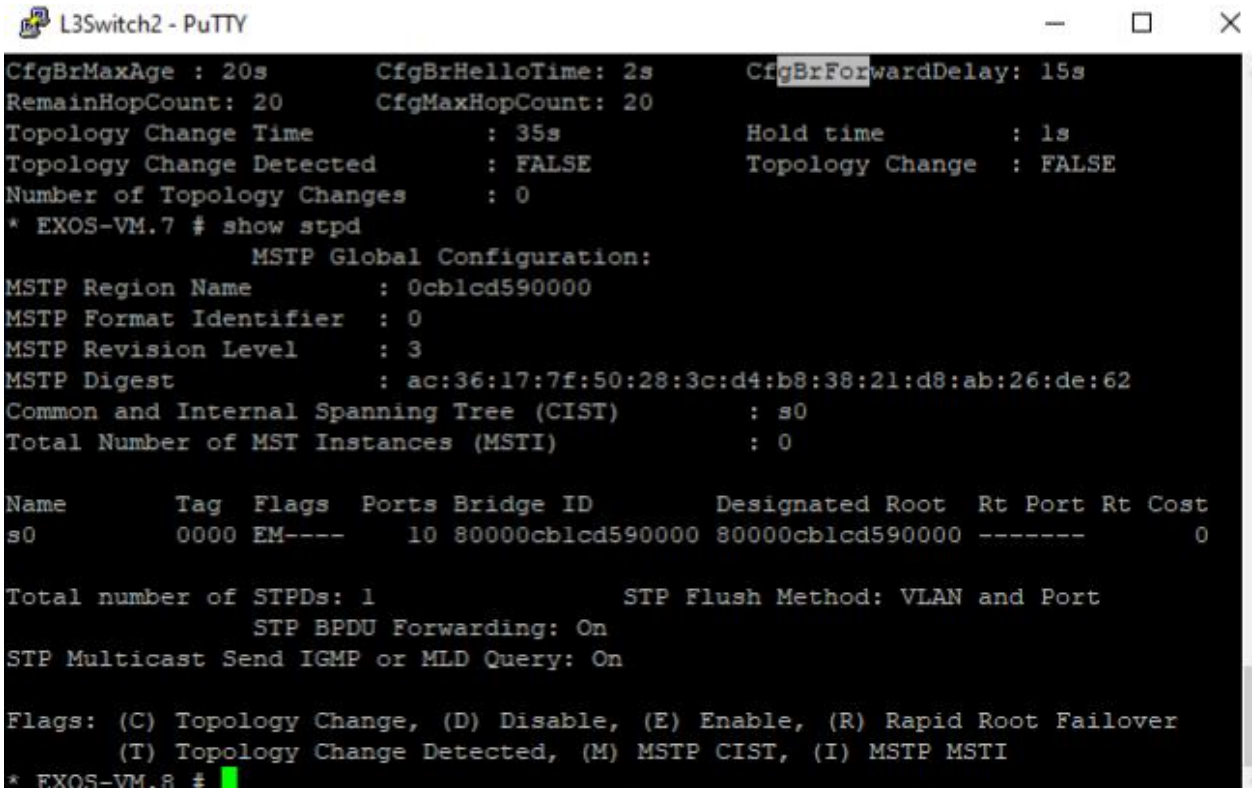
Process List

*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

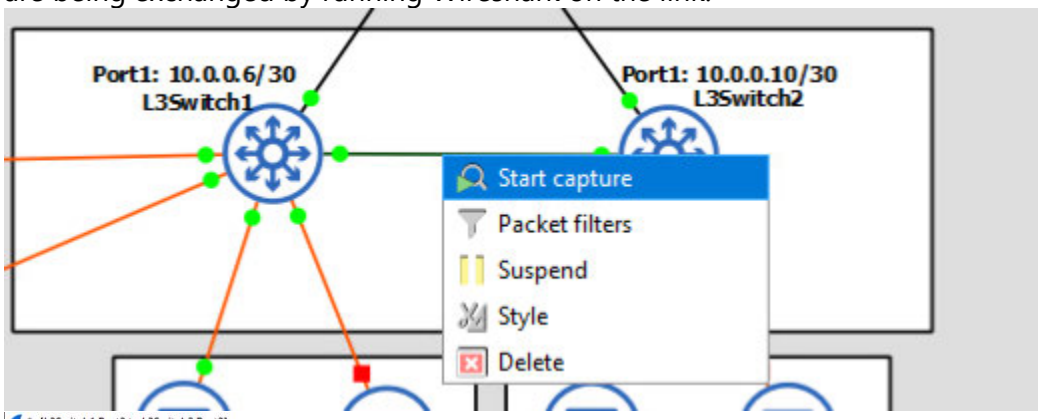
1. Login to L3Switch1
2. Run "show stud". We can see that STP is not selecting L3Switch1 as the root bridge.

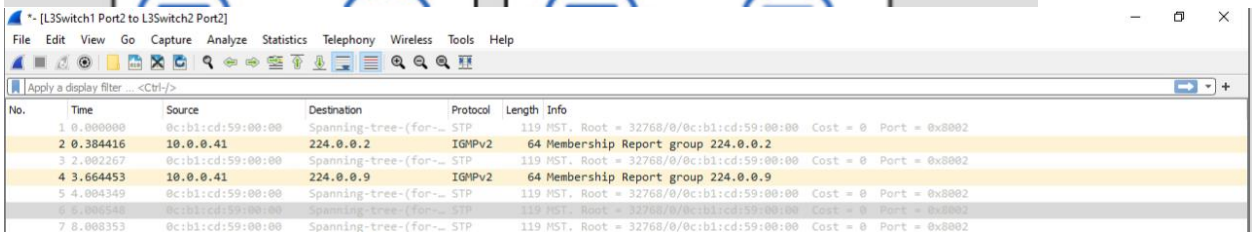


3. Login to L3Switch2
4. Run "show stpd". We can see that STP is selecting L3Switch2 as the root bridge.



5. We can also see on the link from L3Switch1 eth2 to L3Switch2 eth2 that STP packets are being exchanged by running Wireshark on the link.





Test Case #6: Edge Device Syslog and NTP

Configure perimeter devices to generate system logs that capture unwanted traffic. Additionally, those perimeter devices should utilize Network Time Protocol (NTP) for clock synchronization.

Functionality

*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

EdgeRouter1, L3Switch1, and L3Switch2 have ACLs configured which generate logs. A Windows 2019 Server is configured to be an NTP server which the three network devices use. The Windows Server has a static IP address of 10.0.0.18.

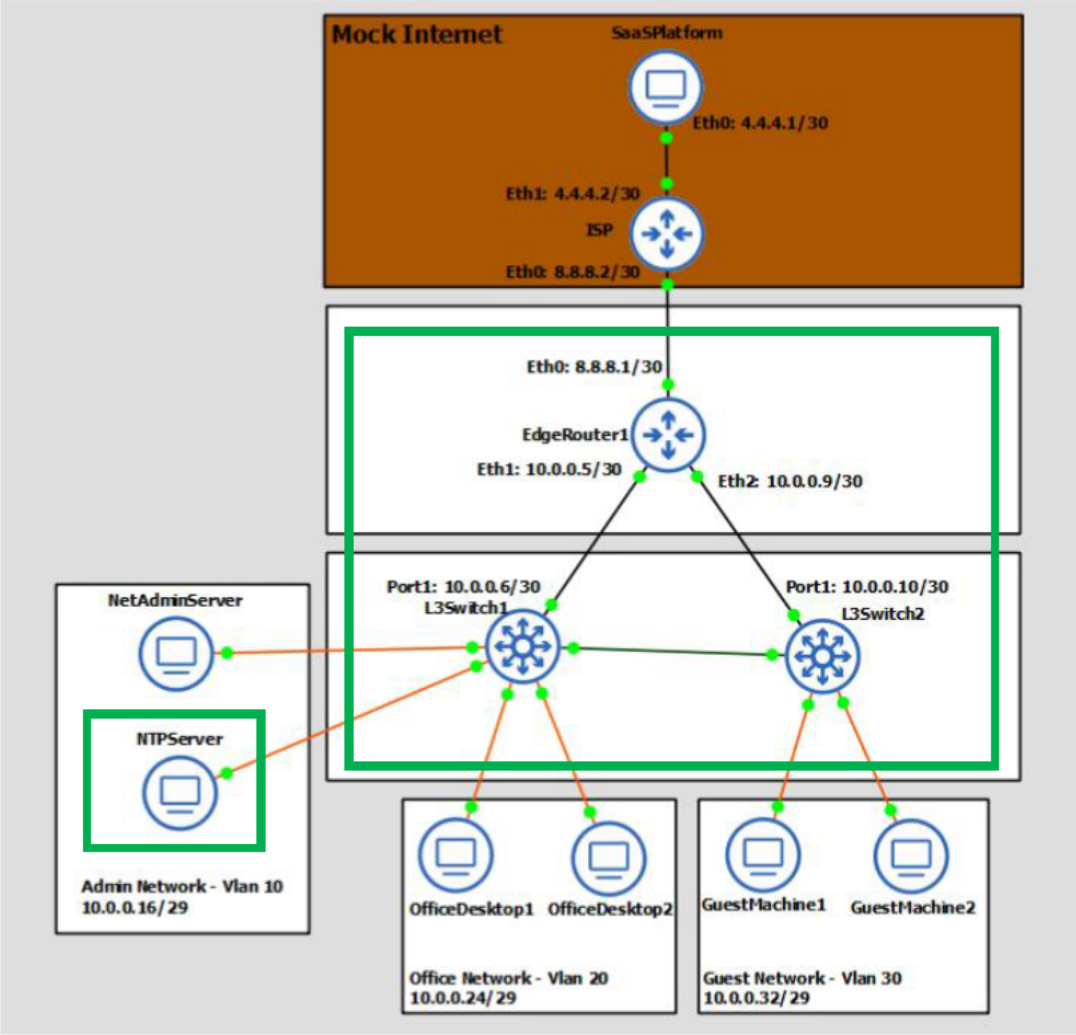
The only traffic allowed to EdgeRouter1 itself is OSPF. The only traffic allowed to EdgeRouter1 from the internet is traffic from established TCP connections which would have to be initiated from the internal network.

L3Switch1 blocks traffic from VLAN 10 to VLANs 20 and 30 on ports 3 and 6. It also blocks traffic from VLAN 20 to VLANs 10 and 30 on ports 4 and 5.
L3Switch1 blocks traffic from VLAN 30 to VLANs 10 and 20 on ports 3 and 4.

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*

Devices that are directly applicable to the testing method are enclosed in green boxes.



Legend

SaaS	Software as a Service
Eth*	Ethernet + port number
ISP	Internet Service Provider
L3	Layer 3
NetAdminServer	Network Administration Server
Admin	Administration
VLAN	Virtual Local Area Network

Testing Method

*Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.*

To show that NTP is configured and being utilized on the three network devices, I will show the NTP server configuration, and show the traffic statistics to the server on the switches, and force a sync to the NTP service on the router.

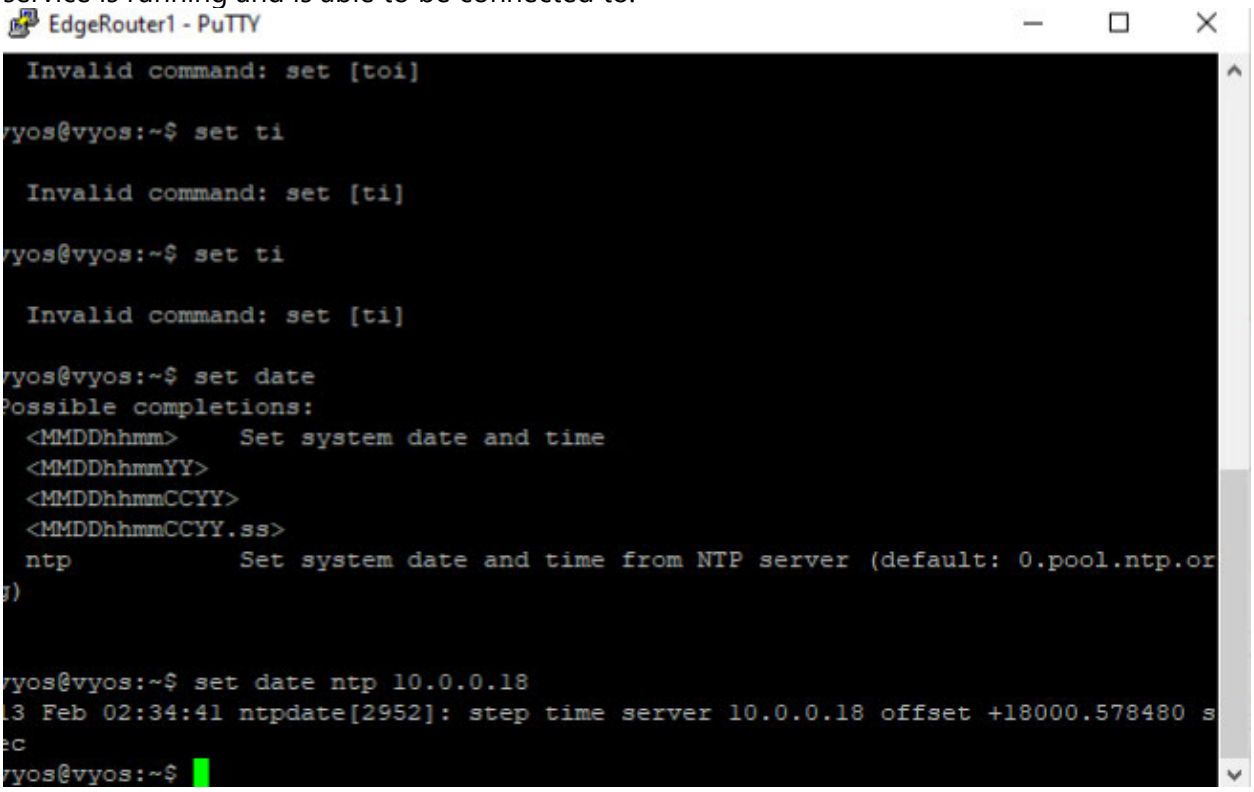
To show that the ACLs are working on each device and logging, I will generate unwanted traffic from:
VLAN 10 to VLAN 20
VLAN 20 to VLAN 10
VLAN 30 to VLAN 10
SaaSPlatform to NetAdminServer

and show the associated logging on the relevant network device.

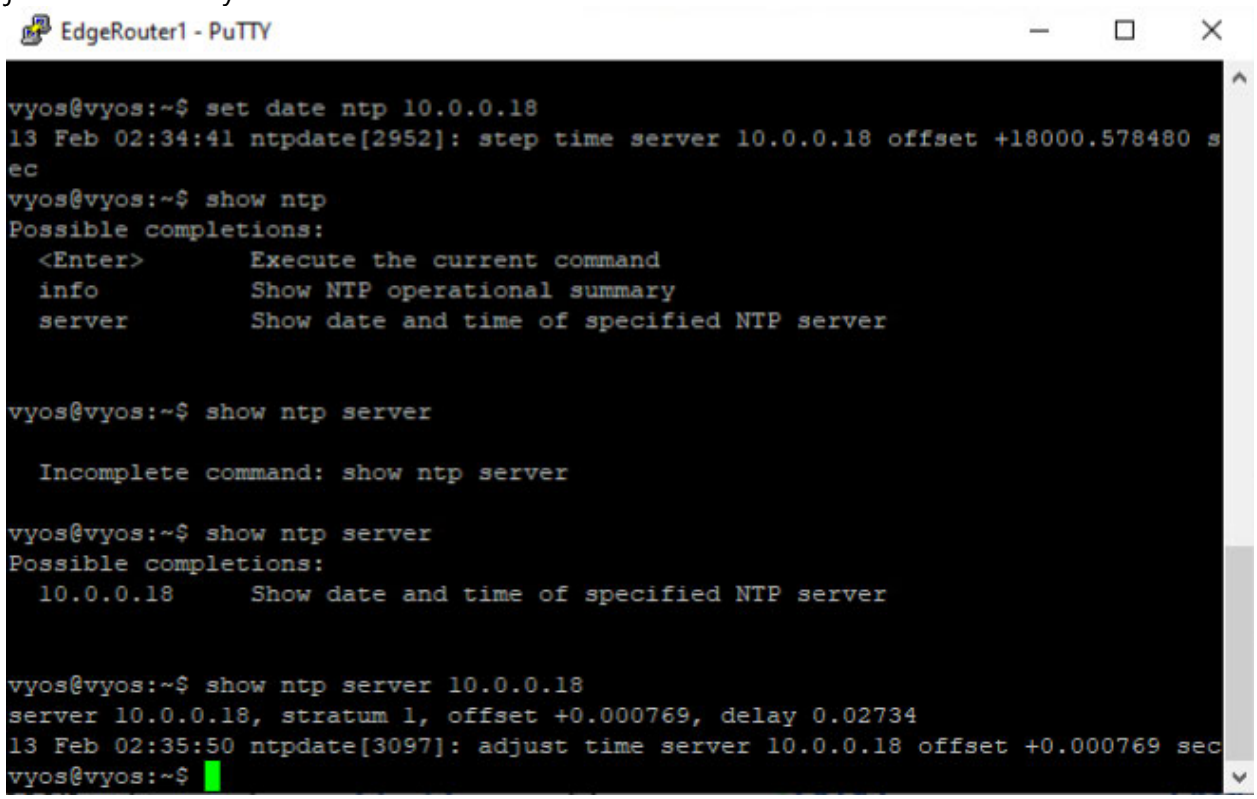
Process List

*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

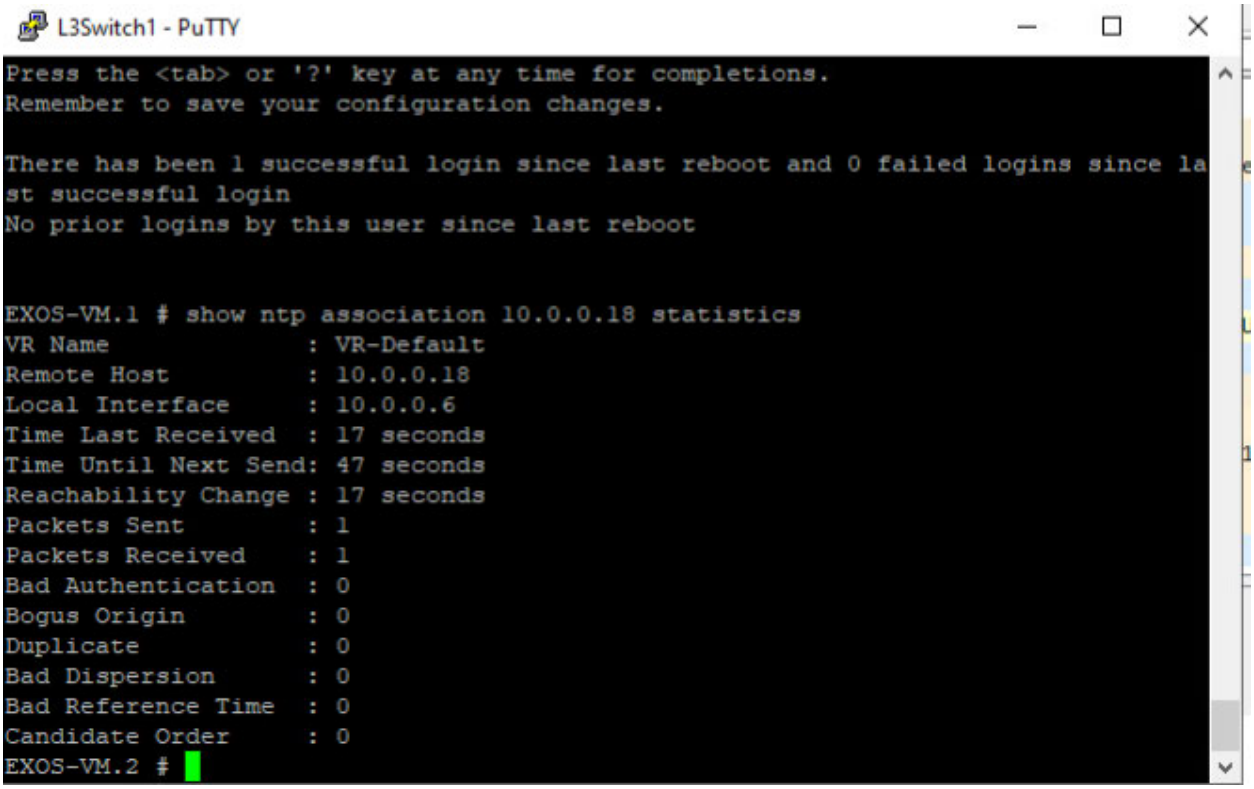
1. Login to EdgeRouter1.
2. Run "set date ntp 10.0.0.18". This will force a sync with NTPServer to demonstrate the service is running and is able to be connected to.



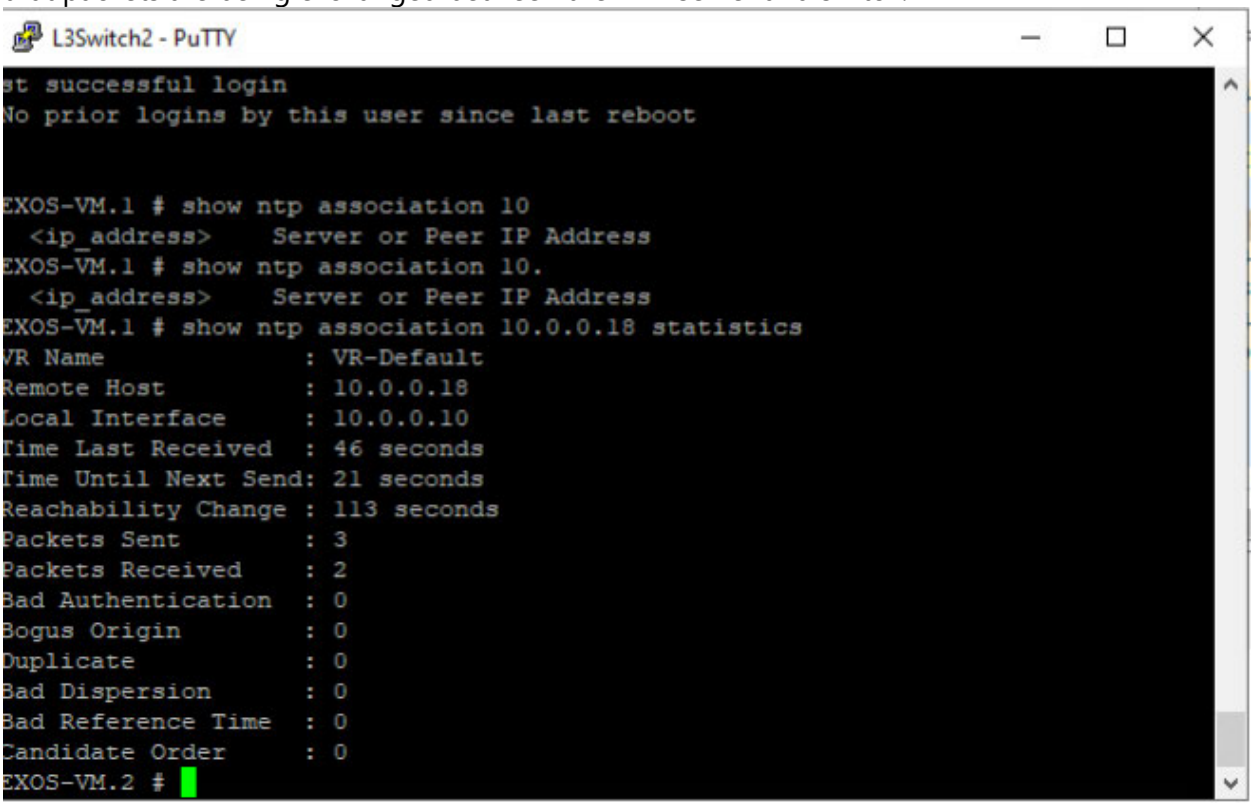
3. Run "show ntp server 10.0.0.18". This shows that the NTP configuration is persistent, not just a one-time sync.



4. Login to L3Switch1 and run "show ntp associations 10.0.0.18 statistics" which will show that packets are being exchanged between the NTP server and switch.

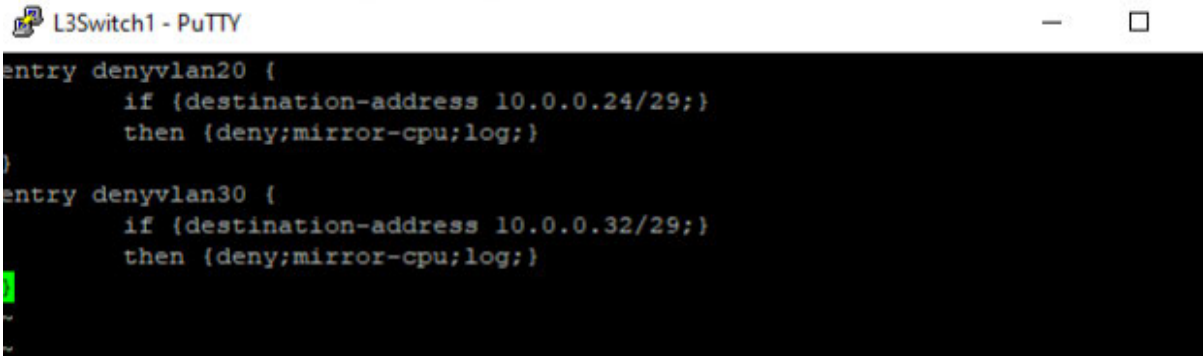


5. Login to L3Switch2 and run "show ntp associations 10.0.0.18 statistics" which will show that packets are being exchanged between the NTP server and switch.

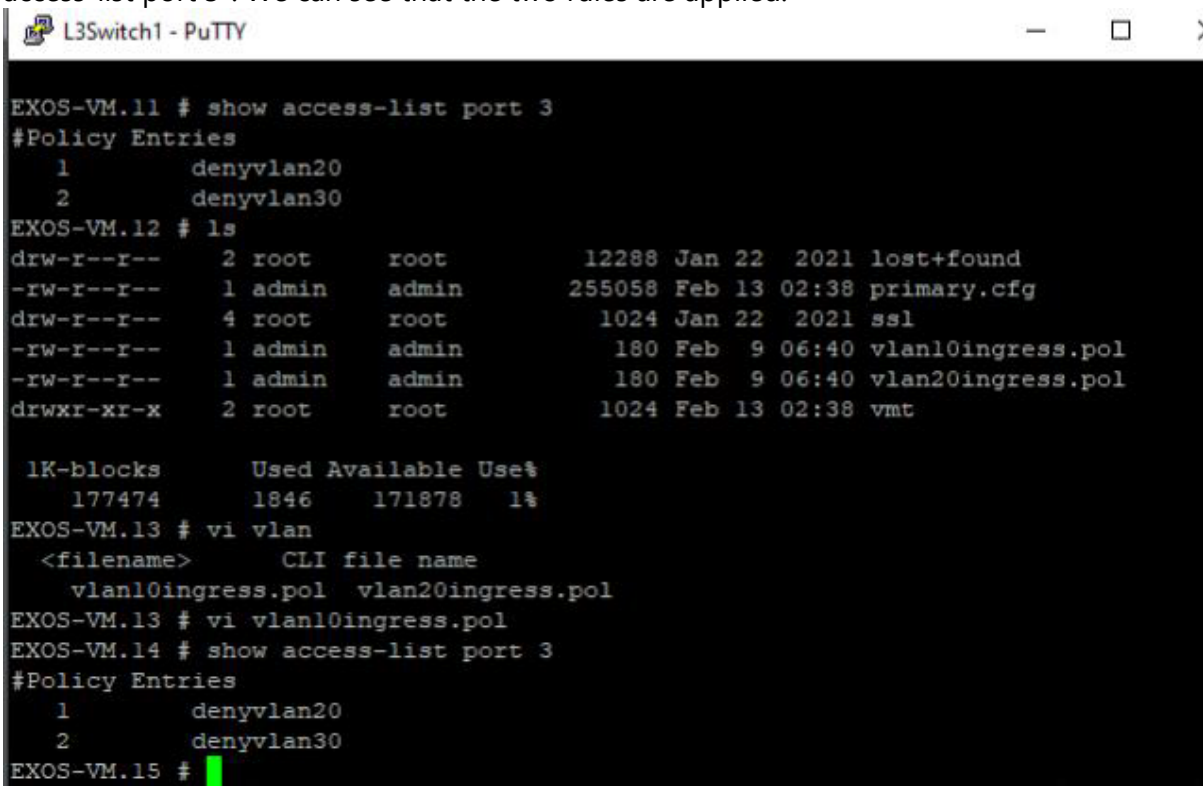


Viewing logs of unwanted traffic from VLAN 10 to VLAN 20:

1. Login to L3Switch1.
2. Run "vi vlan10ingress.pol" to view the ACL configured on VLAN 10. This shows the rules that will be triggered when sending traffic from VLAN 10 to VLAN 20.

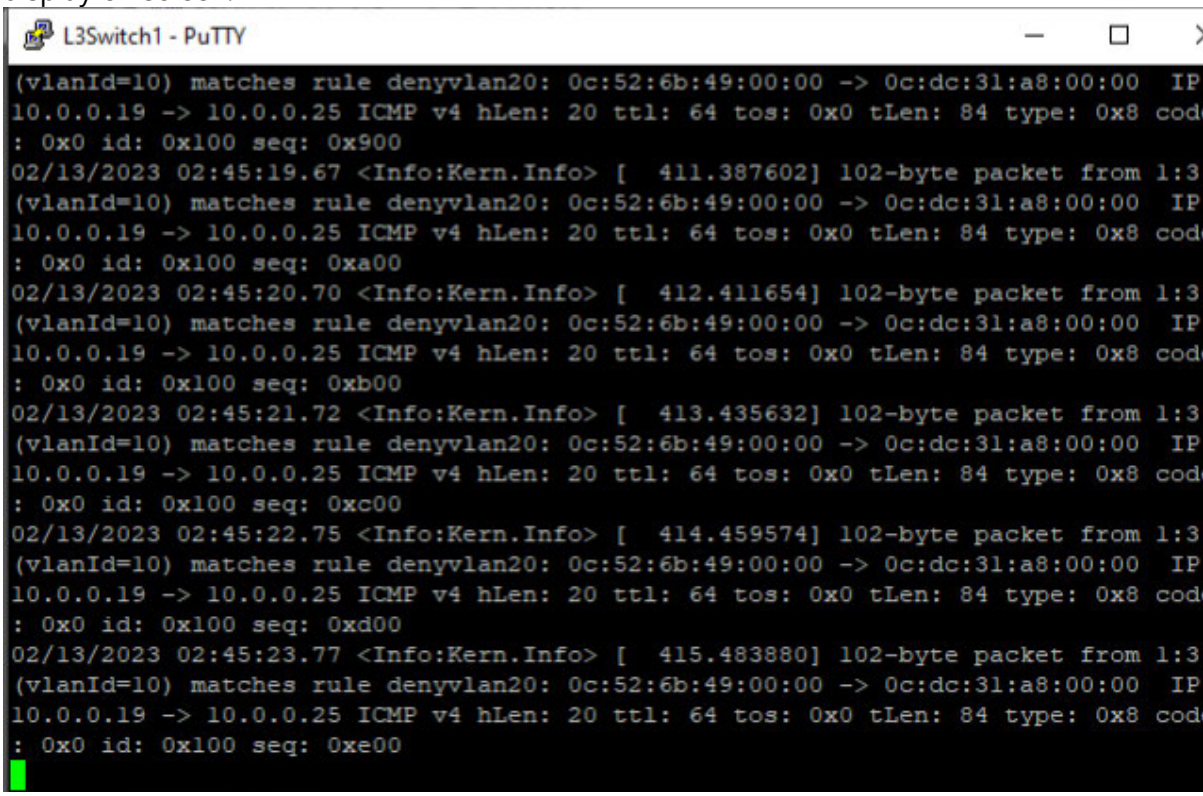


3. Verify that this rule is applied to the NetAdminServer port by running "show access-list port 3". We can see that the two rules are applied.



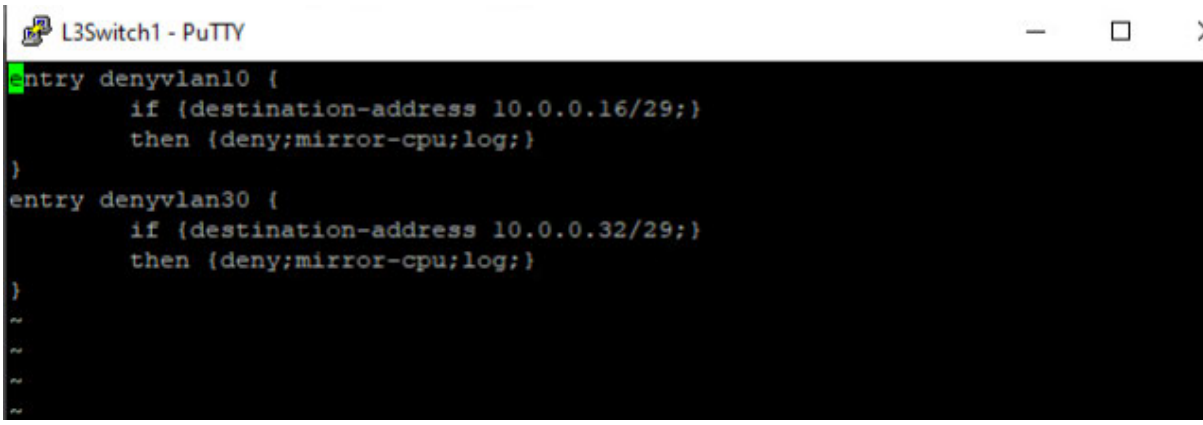
4. Run "enable log target session" to display system logs in the terminal
5. Login to NetAdminServer.
6. Open a terminal and ping the VLAN 20 IP address 10.0.0.25. We can see that the ICMP traffic is being denied by rule "denyvlan20" in the system logs that

display on screen.

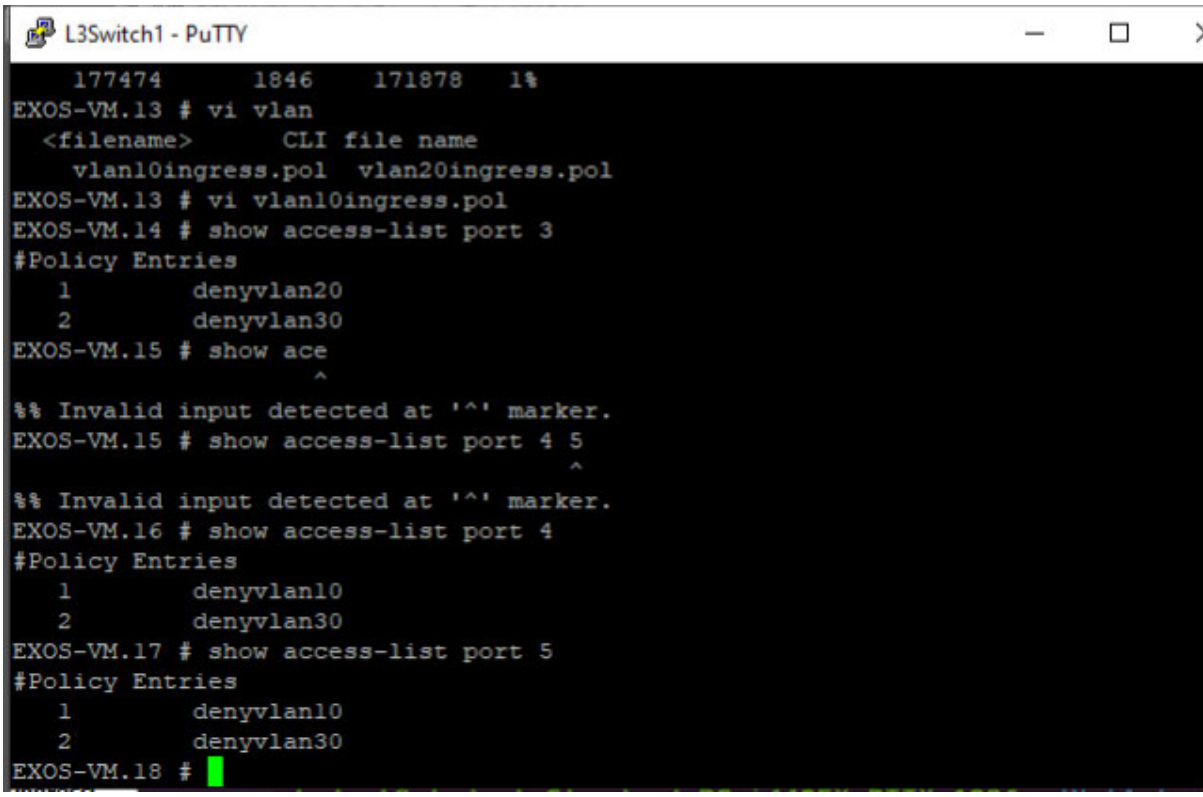


Viewing logs of unwanted traffic from VLAN 20 to VLAN 10:

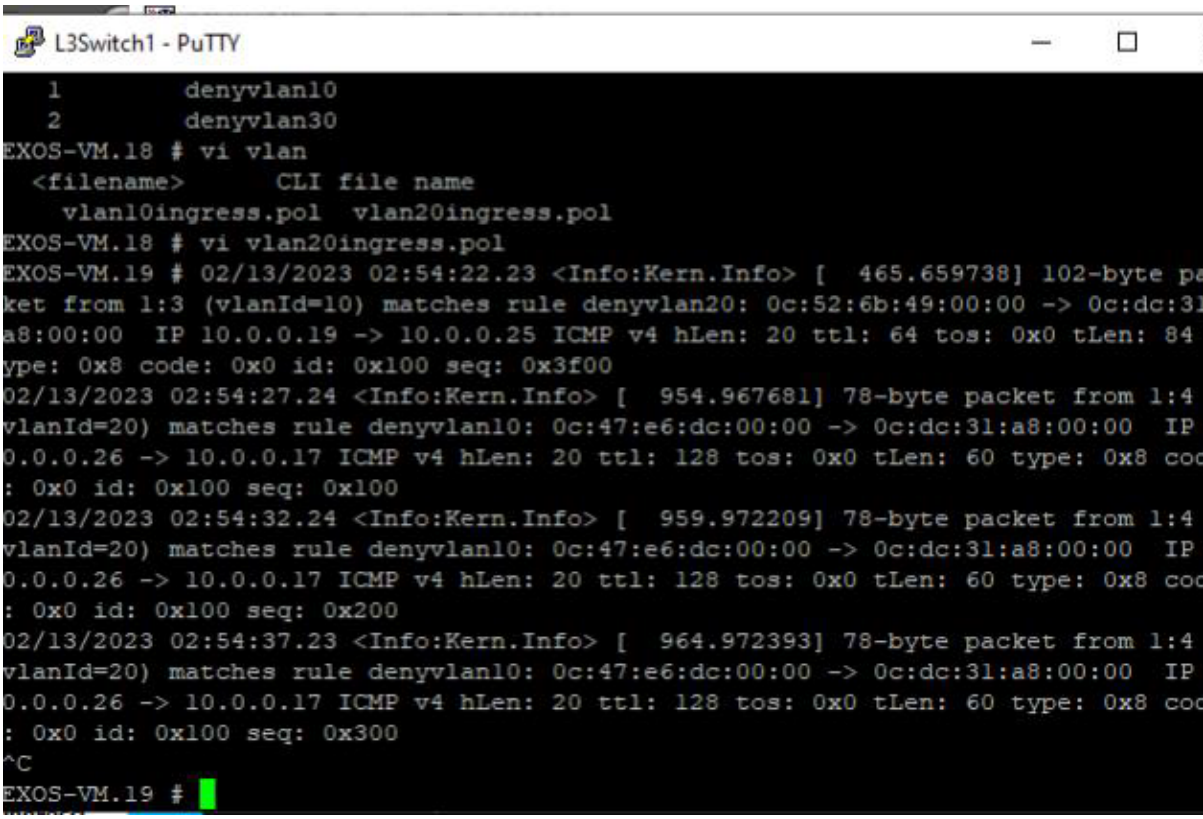
1. Login to L3Switch1
2. Run “vi vlan20ingress.pol” to view the ACL configured on VLAN 20. This shows the rules that will be triggered when sending traffic from VLAN 20 to VLAN 10.



3. Verify that this rule is applied to the NetAdminServer port by running “show access-list port 4” and “show access-list port 5”. We can see that the two rules are applied to both ports in VLAN 20.

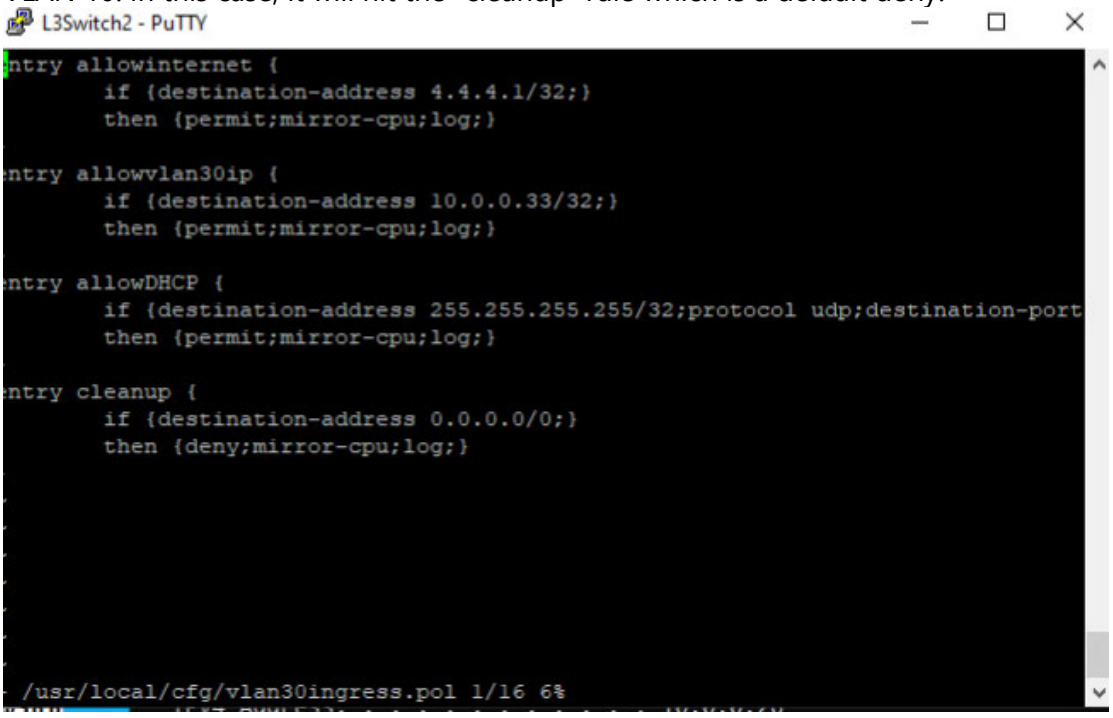


4. Run “enable log target session” to display system logs in the terminal
5. Login to a host on the VLAN 20, the Office Network.
6. Open a terminal and ping the VLAN 10 IP address 10.0.0.17. We can see that the ICMP traffic is being denied by rule “denyvlan10” in the system logs that display on screen.

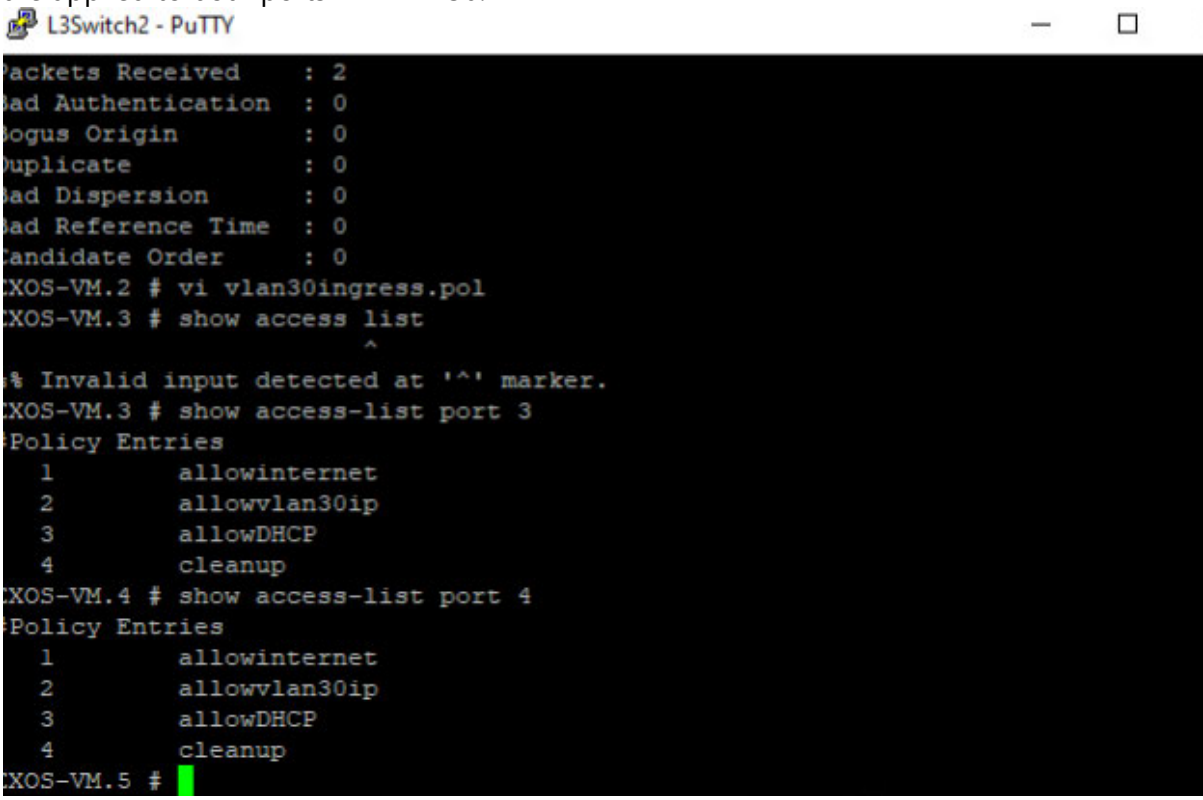


Viewing logs of unwanted traffic from VLAN 30 to VLAN 10:

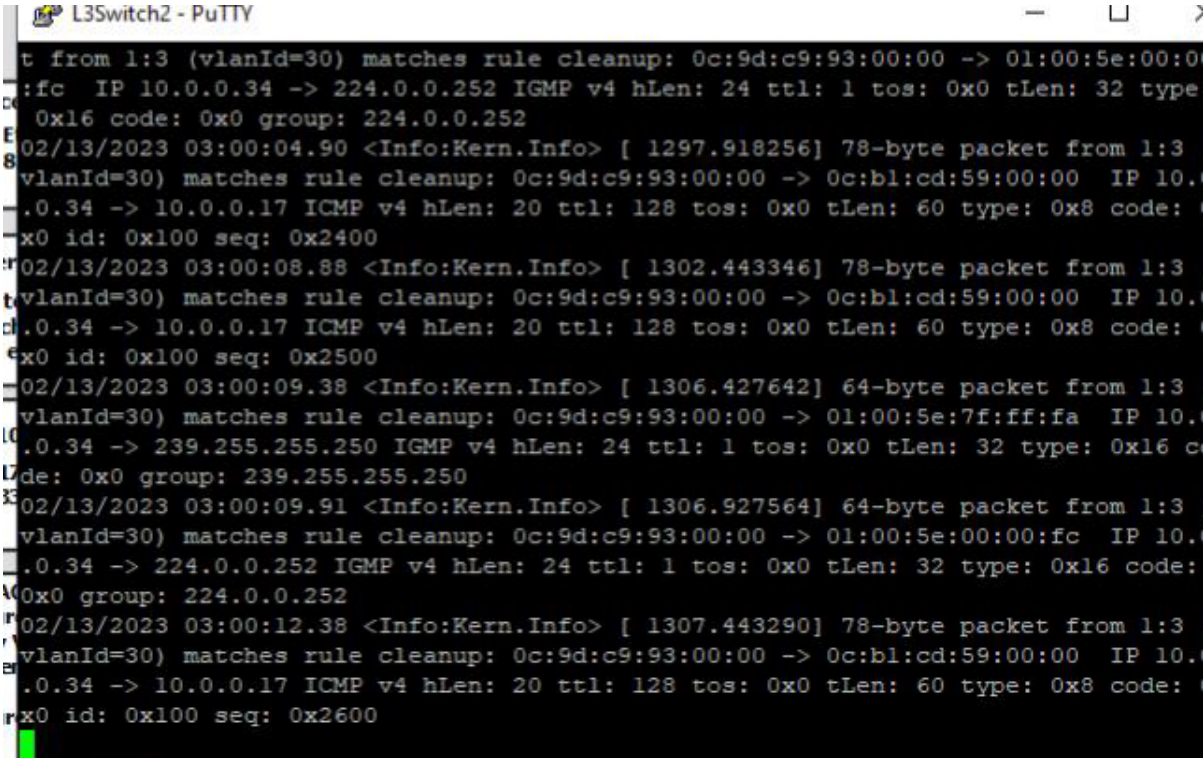
1. Login to L3Switch2
2. Run "vi vlan30ingress.pol" to view the ACL configured on VLAN 30. This shows the rules that will be triggered when sending traffic from VLAN 30 to VLAN 10. In this case, it will hit the "cleanup" rule which is a default deny.



3. Verify that this rule is applied to the NetAdminServer port by running "show access-list port 3" and "show access-list port 3". We can see that the two rules are applied to both ports in VLAN 30.

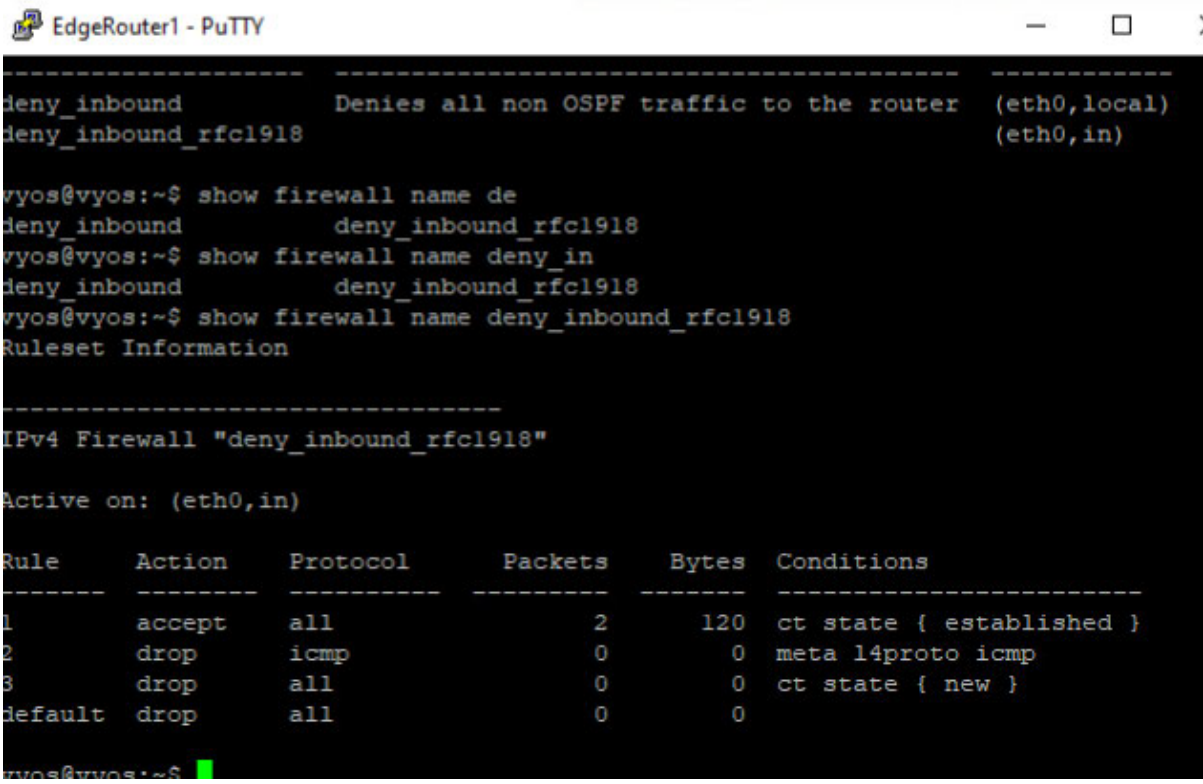


4. Run "enable log target session" to display system logs in the terminal
5. Login to a host on the VLAN 30, the Guest Network.
6. Open a terminal and ping the VLAN 10 IP address 10.0.0.17. We can see that the ICMP traffic is being denied by rule "cleanup" in the system logs that display on screen.

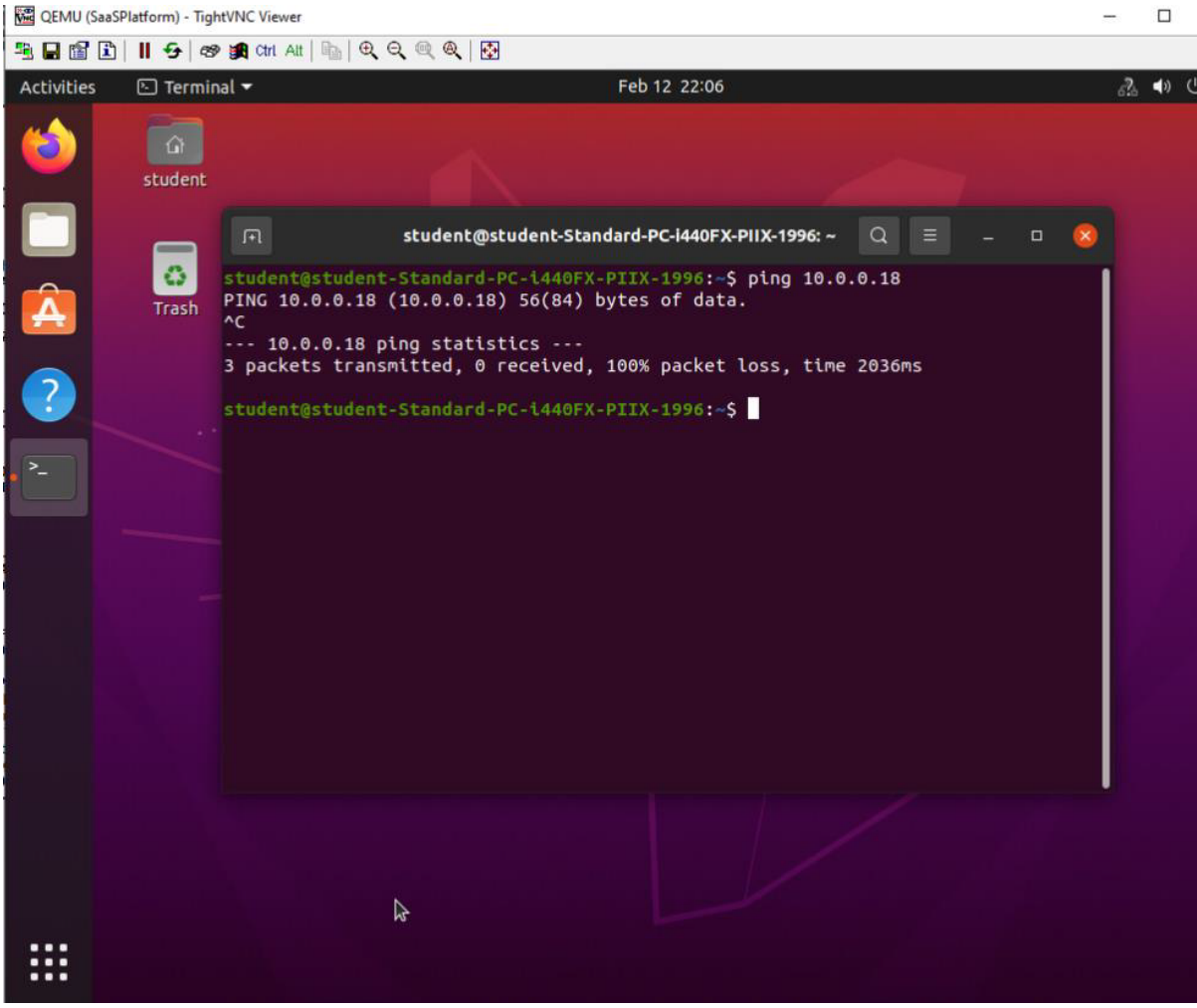


Viewing logs of unwanted traffic from SaaSPlatform to NetAdminServer:

1. Login to EdgeRouter1
2. Run "show firewall name deny_inbound_rfc1918" to view firewall rules active on the eth0 inbound interface. Notice that you can also see the logging of packets and bytes that each rule processes.

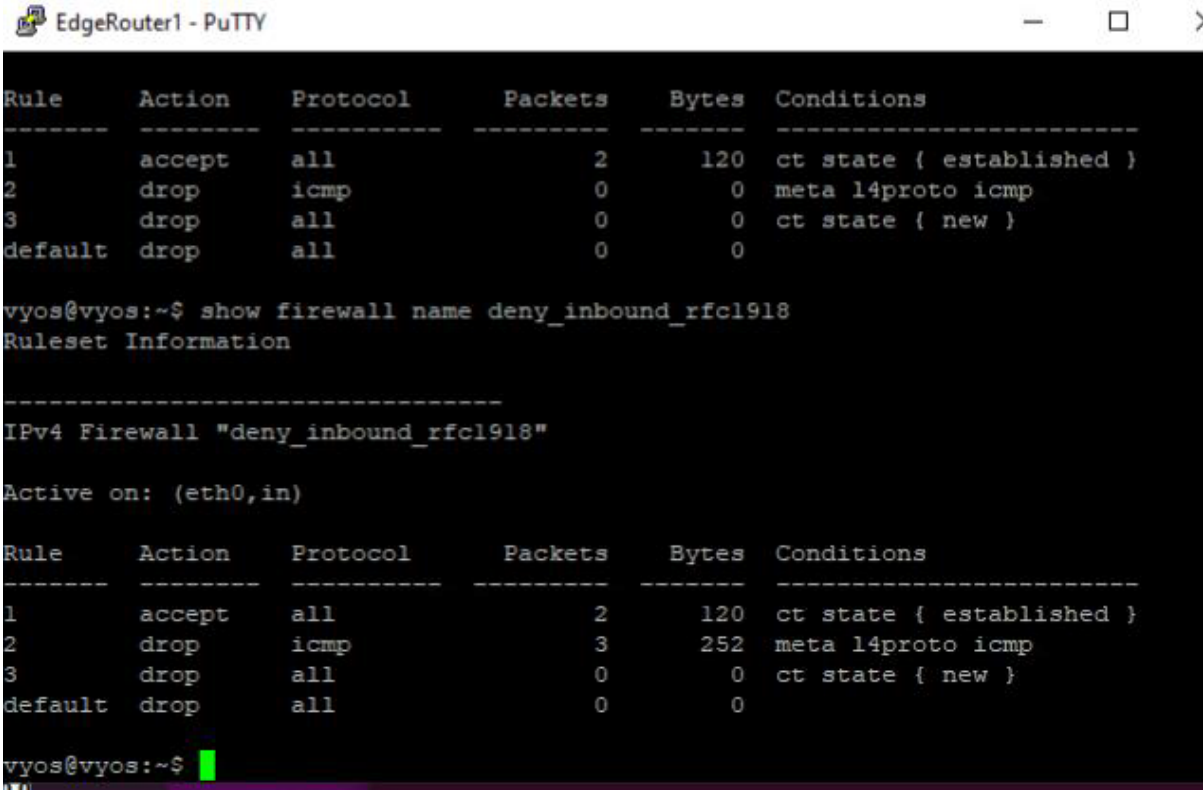


3. Login to SaaSPlatform.
4. Open a terminal and run “ping 10.0.0.18”. We can see that there was no response.



5. Run "show firewall name deny_inbound_rfc1918" to see if rule 2 dropped the ICMP packets. We can see that rule 2 logged and dropped the 3 packets that

SaaSPlatform sent and logged the number of bytes sent.



Test Case #7: Basic Network Segmentation at Layer 2 via VLANs and 802.1q

Your network traffic should be segmented per department or service function at Layer 2 to enhance security and reduce network congestion at the switching layer while allowing segmented traffic to traverse between switches (VLAN trunking).

Functionality

*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

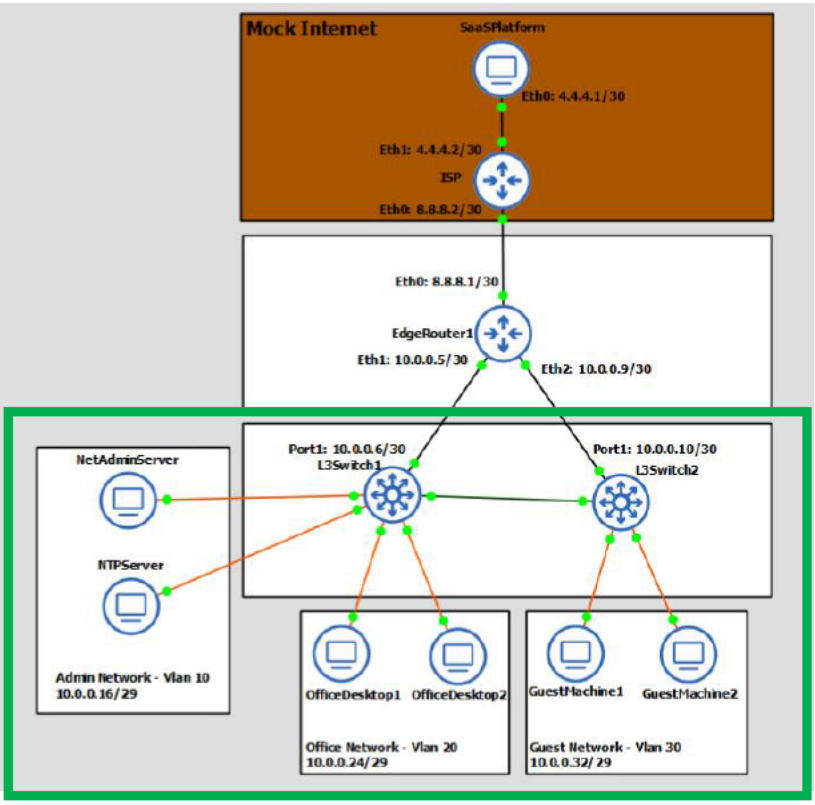
There are 3 VLANs configured:
L3Switch1 Admin Network VLAN 10 10.0.0.16/29
L3Switch1 Office Network VLAN 20 10.0.0.24/29
L3Switch2 Guest Network VLAN 30 10.0.0.32/29

On L3Switch1, port 2 is connected to L3Switch2 and is configured as a tagged port.
On L3Switch2, port 2 is connected to L3Switch1 and is configured as a tagged port.

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*

Devices that are directly applicable to the testing method are enclosed in green boxes.



Legend

SaaS	Software as a Service
Eth*	Ethernet + port number
ISP	Internet Service Provider
L3	Layer 3
NetAdminServer	Network Administration Server
Admin	Administration
VLAN	Virtual Local Area Network

Testing Method

*Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.*

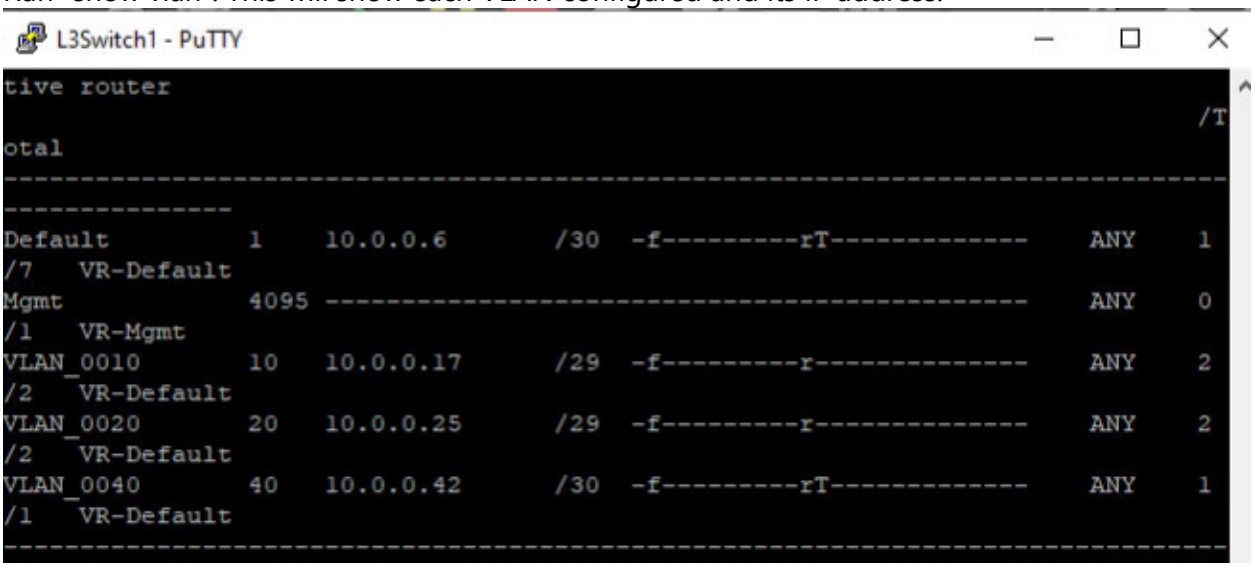
To demonstrate that VLANs are configured, I will show the VLAN that each port on the switches is assigned to, the VLANs IP addresses and tagged ports.

To verify that VLAN trunking works, I will capture the packets sent on VLAN 40 between L3Switch1 eth2 and L3Switch2 eth2. This will contain an 802.1q tag in the packet.

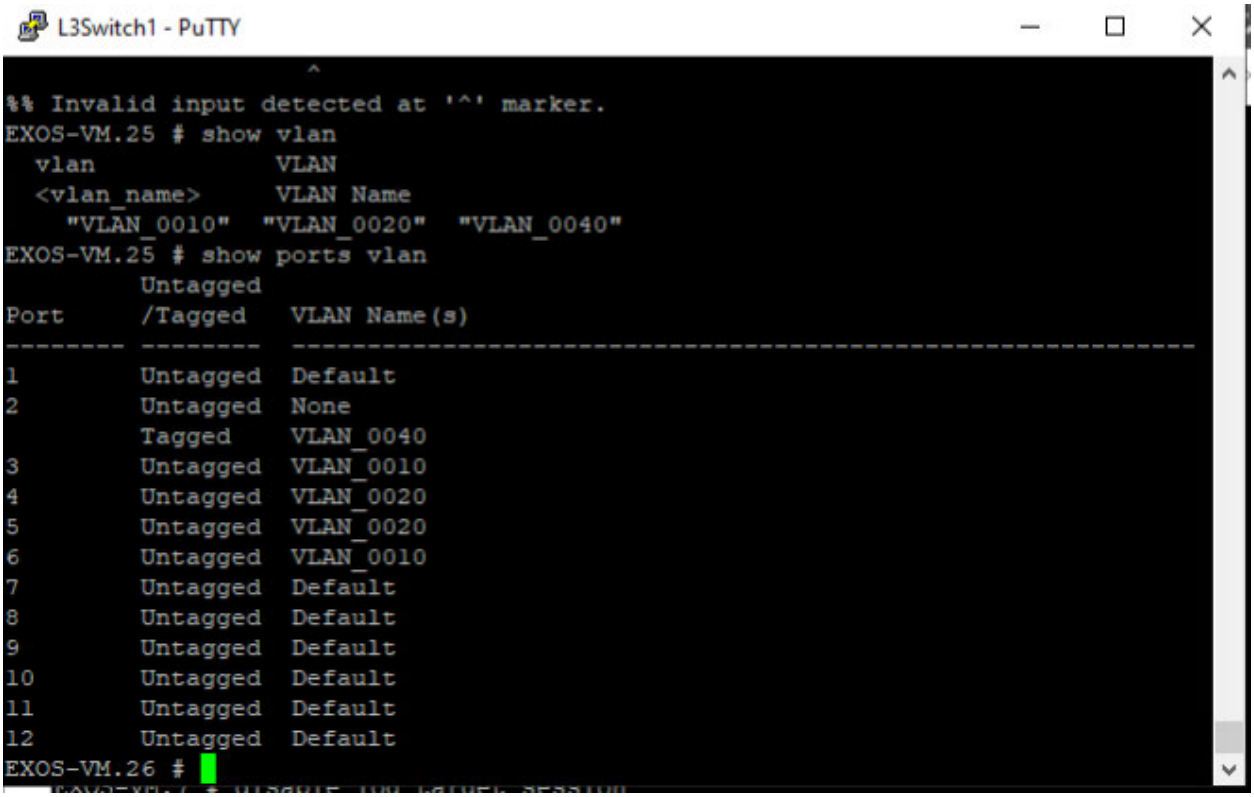
Process List

*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

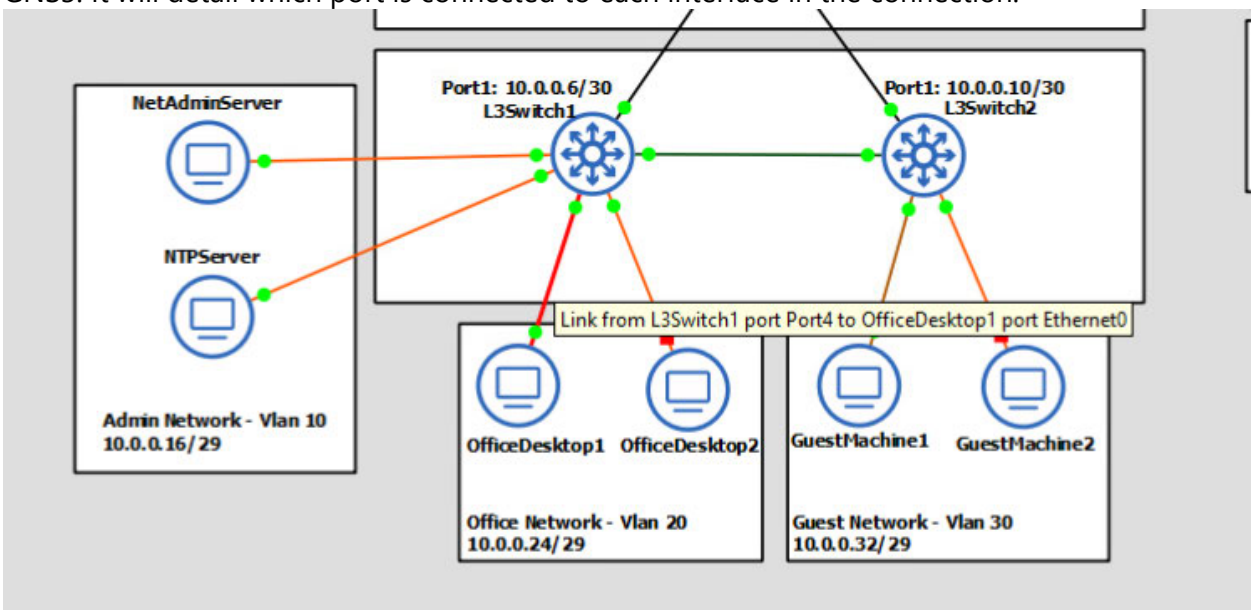
1. Login to L3Switch1
2. Run "show vlan". This will show each VLAN configured and its IP address.



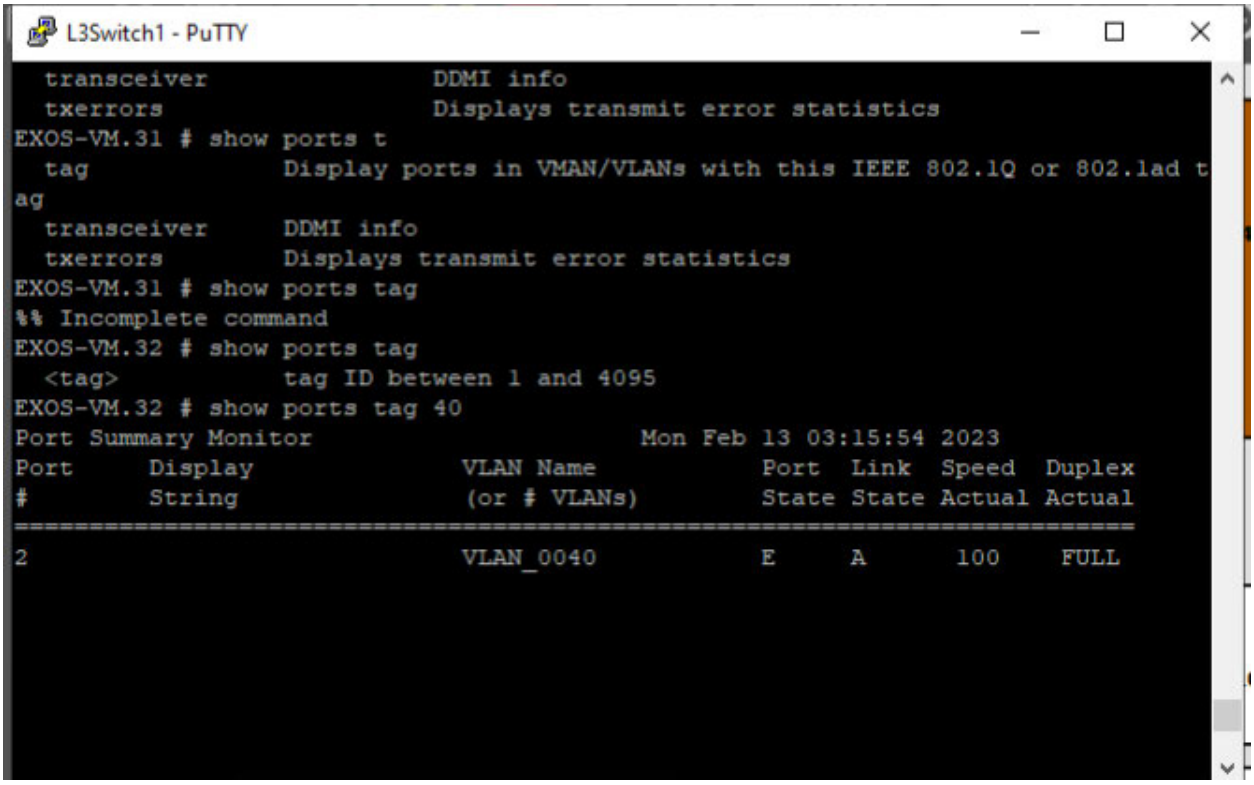
3. Run "show ports vlan" to show which VLAN each port is assigned to. We can see that



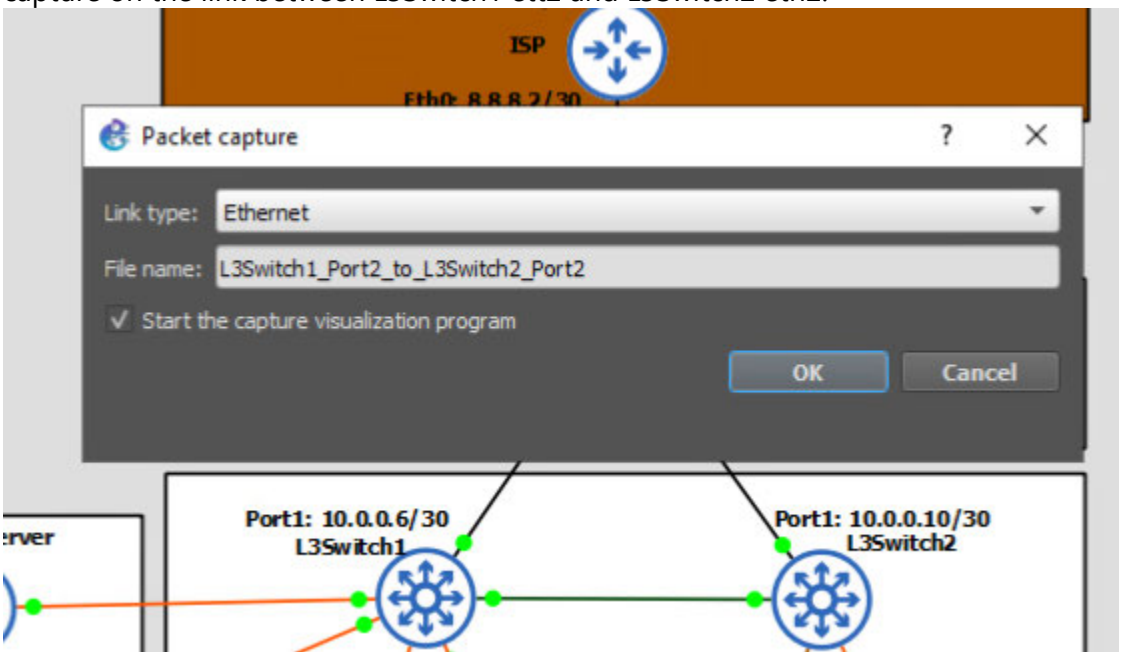
4. To verify that the network topology matches the output, hover over each connection in GNS3. It will detail which port is connected to each interface in the connection.



5. Port 2 is tagged with VLAN 40. We can verity this with “show ports tag 40”. Port 2 is connected to L3Switch2 which is why it is a tagged interface.

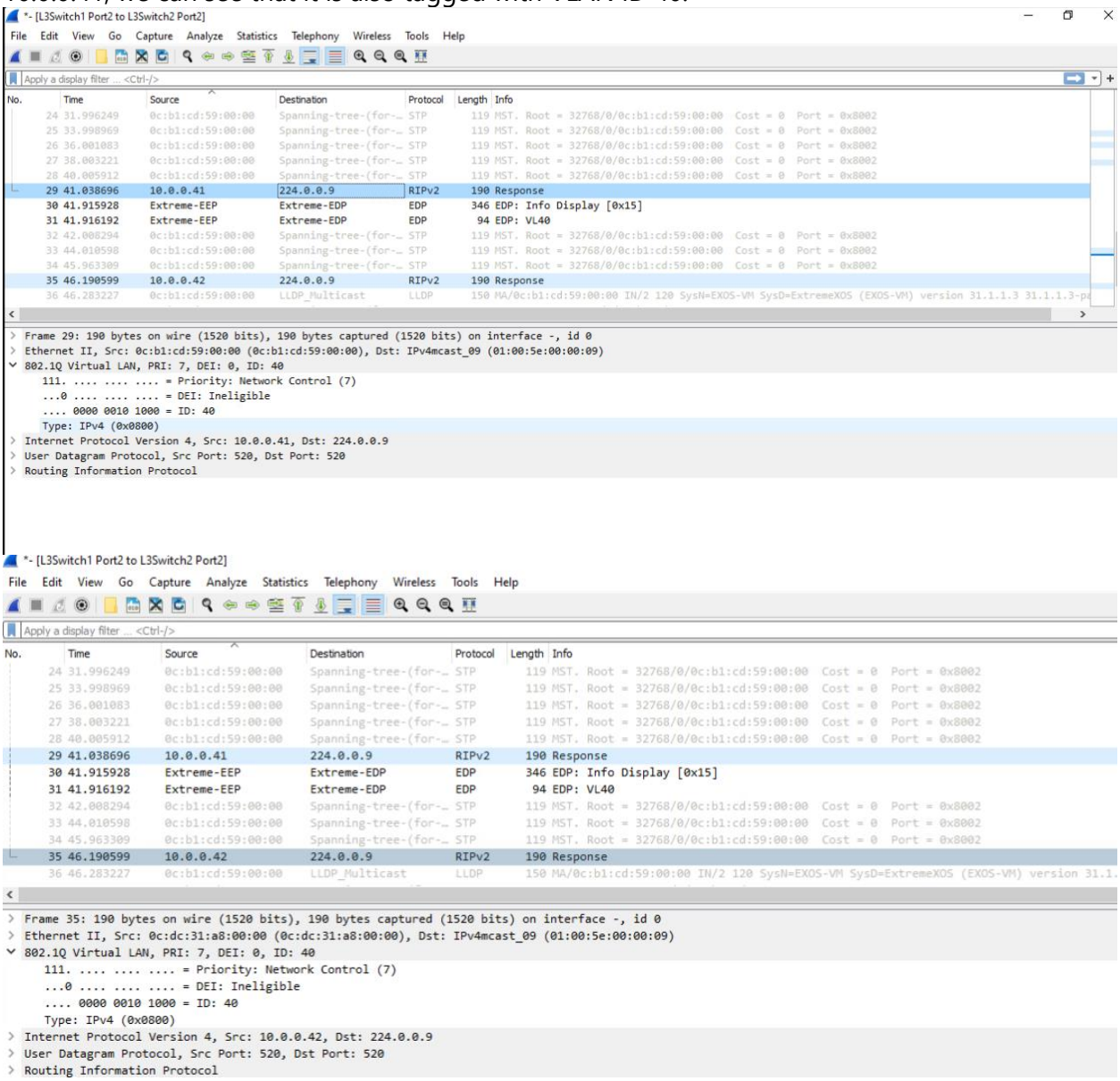


6. Repeat steps 1-5 for L3Switch2.
7. To verify that traffic is being tagged on port 2 of each interface, start a Wireshark packet capture on the link between L3Switch1 ett2 and L3Switch2 eth2.



8. By watching the packets, we can see that they are appropriately tagged. For example, L3Switch 1 and L3Switch2 are configured to broadcast routes with RIP. L3Switch2's VLAN 40 IP is 10.0.0.41. Looking at traffic from that source, we can see in the packet that there

is an 802.1q tag for VLAN ID 40. Likewise, if we look for L3Switch1's VLAN 40 IP address, 10.0.0.41, we can see that it is also tagged with VLAN ID 40.



Test Case #8: Basic or Advanced Networking

Custom Test Case

*Define a **custom test case** to be run within your network project aligned to your specific organizational need or opportunity identified in Task 1. The custom test case should be equivalent in scope and requirements to the predefined test cases and pertain to basic or advanced networking.*

"Your solution should have OSPF configured to get link state metrics to ensure that your connection to the critical service is fast and

stable. You should also enable logging for link state adjacency changes on the edge router."

Functionality

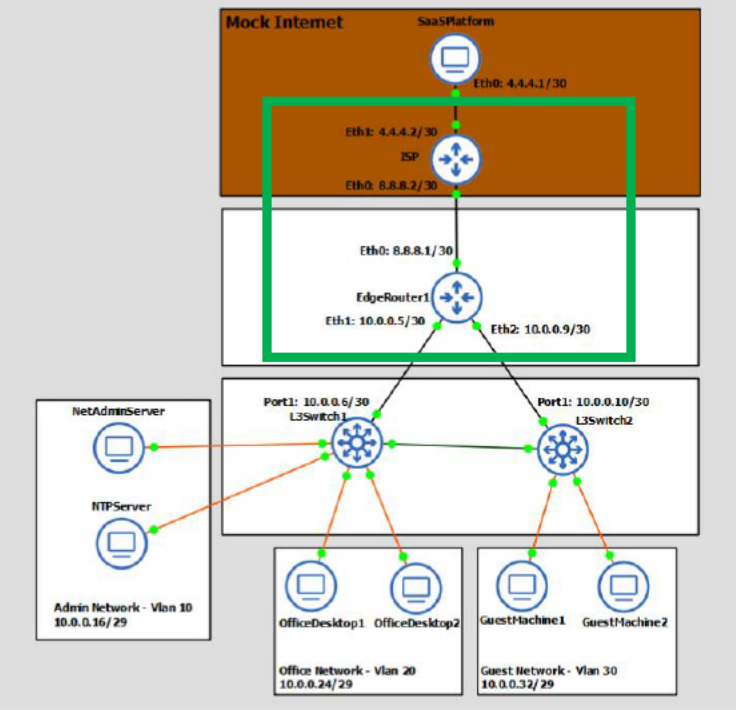
Describe the functionality of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.

EdgeRouter1 and ISP have OSPF configured and are neighbors. They are both in area 1. EdgeRouter1 advertises network 8.8.8.0/30 and ISP advertises network 4.4.4.0/30.

Network Diagram or Segment

Provide a network diagram or segment visualizing the topology and devices used in this test case.

Devices that are directly applicable to the testing method are enclosed in green boxes.



Legend

SaaS	Software as a Service
Eth*	Ethernet + port number
ISP	Internet Service Provider
L3	Layer 3
NetAdminServer	Network Administration Server
Admin	Administration
VLAN	Virtual Local Area Network

Testing Method

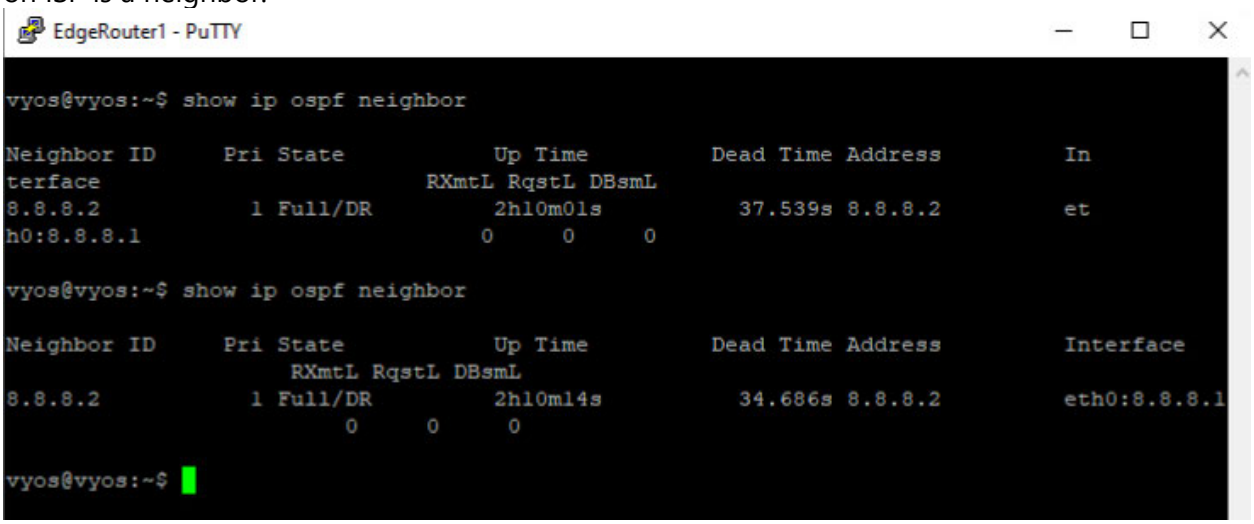
*Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.*

To verify the configuration, I will show that ISP and EdgeRouter1 are OSPF neighbors, and they each have the expected routes in their routing tables. I will also verify that the correct interfaces are configured. Lastly, I will take a packet capture on the link between ISP eth0 and EdgeRouter1 eth0 to verify that OSPF packets are being exchanged.

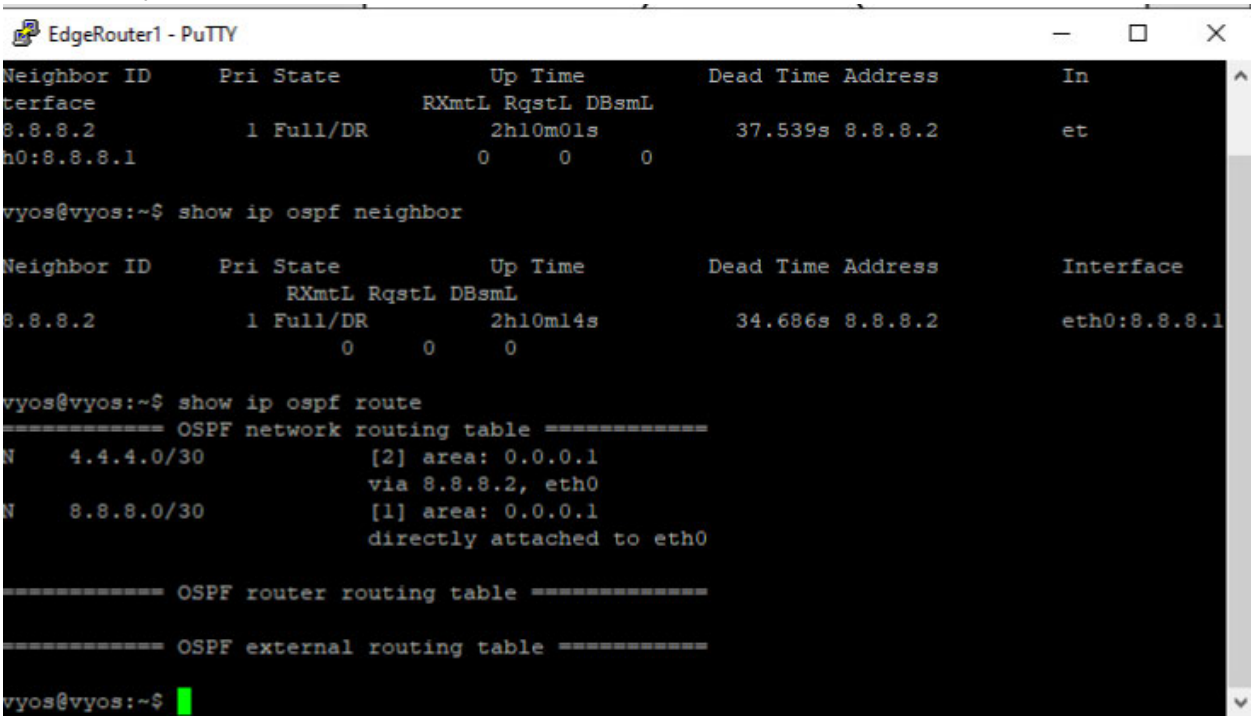
Process List

*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

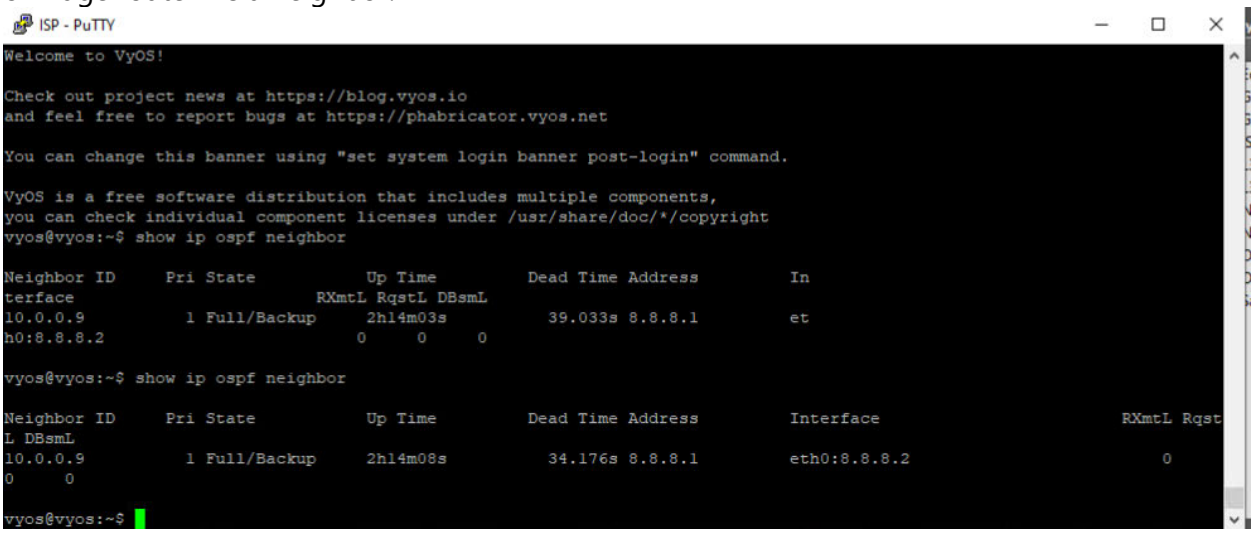
1. Login to EdgeRouter1.
2. Run "show ip ospf neighbor". This will show that the directly connected 8.8.8.2 interface on ISP is a neighbor.



3. Run "show ip ospf route" to verify that ISP is broadcasting the 4.4.4.0/30 network. We see that 4.4.4.0/30 is an OSPF route via ISP 8.8.8.2.

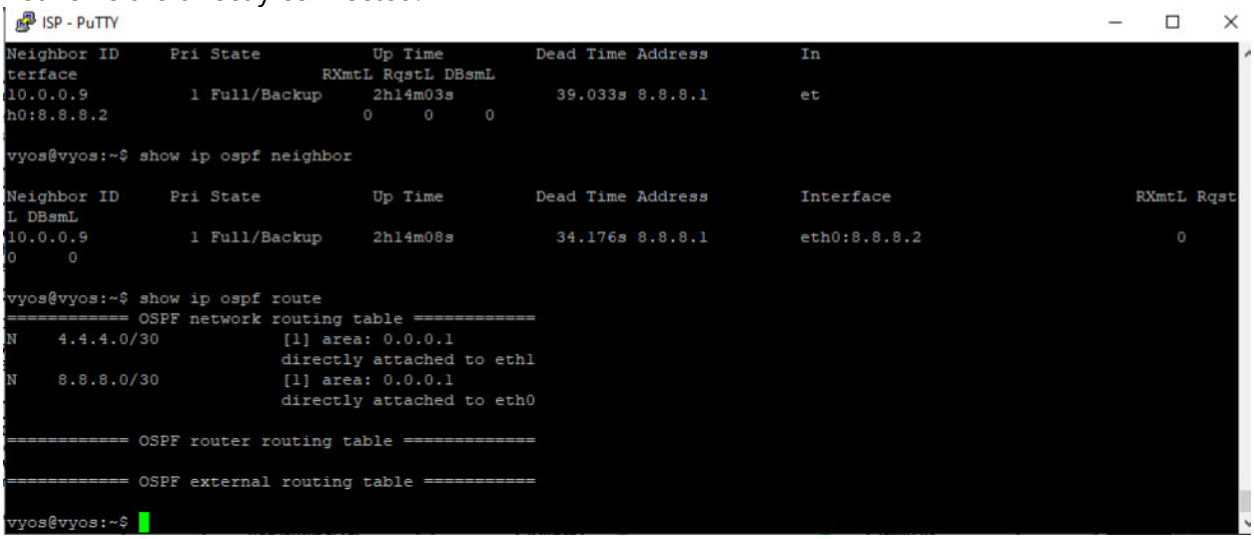


4. Login to ISP.
5. Run "show ip ospf neighbor". This will show that the directly connected 8.8.8.1 interface on EdgeRouter1 is a neighbor.

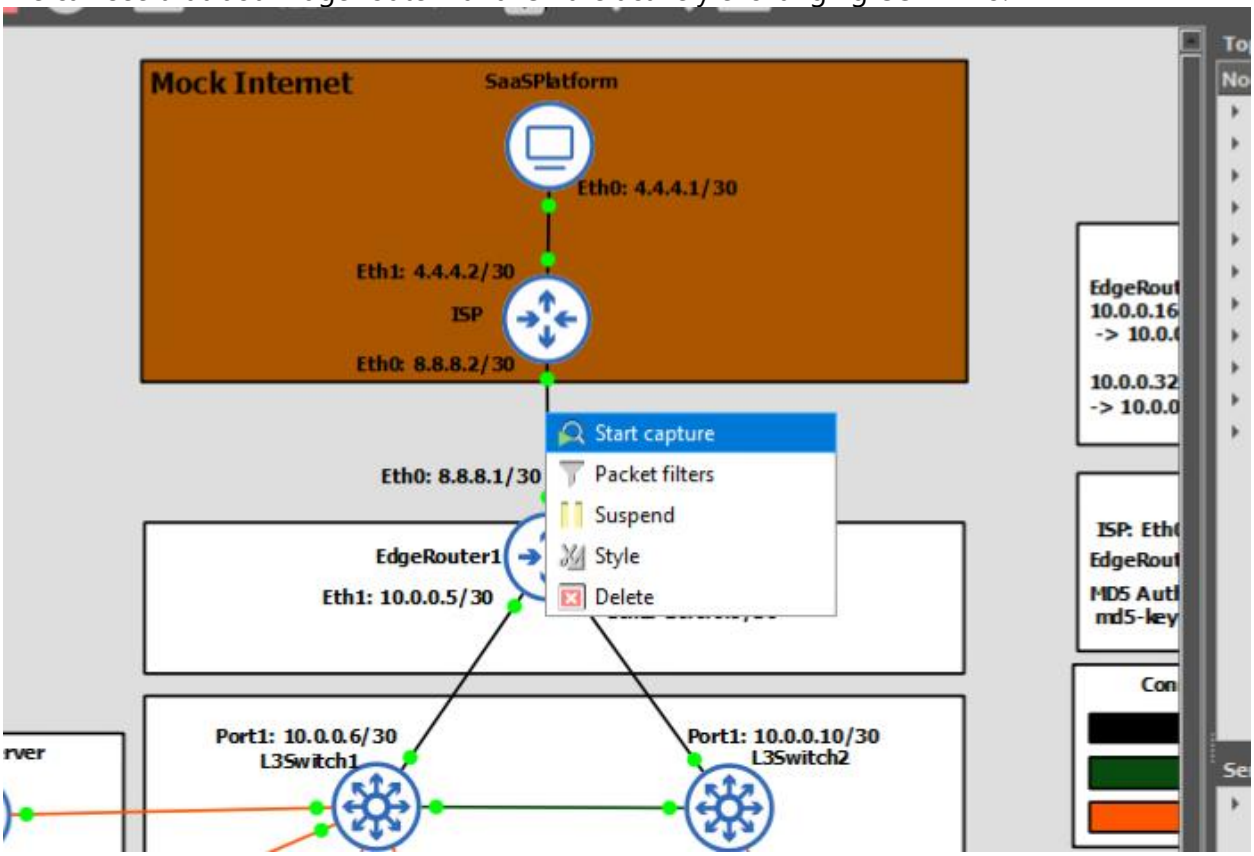


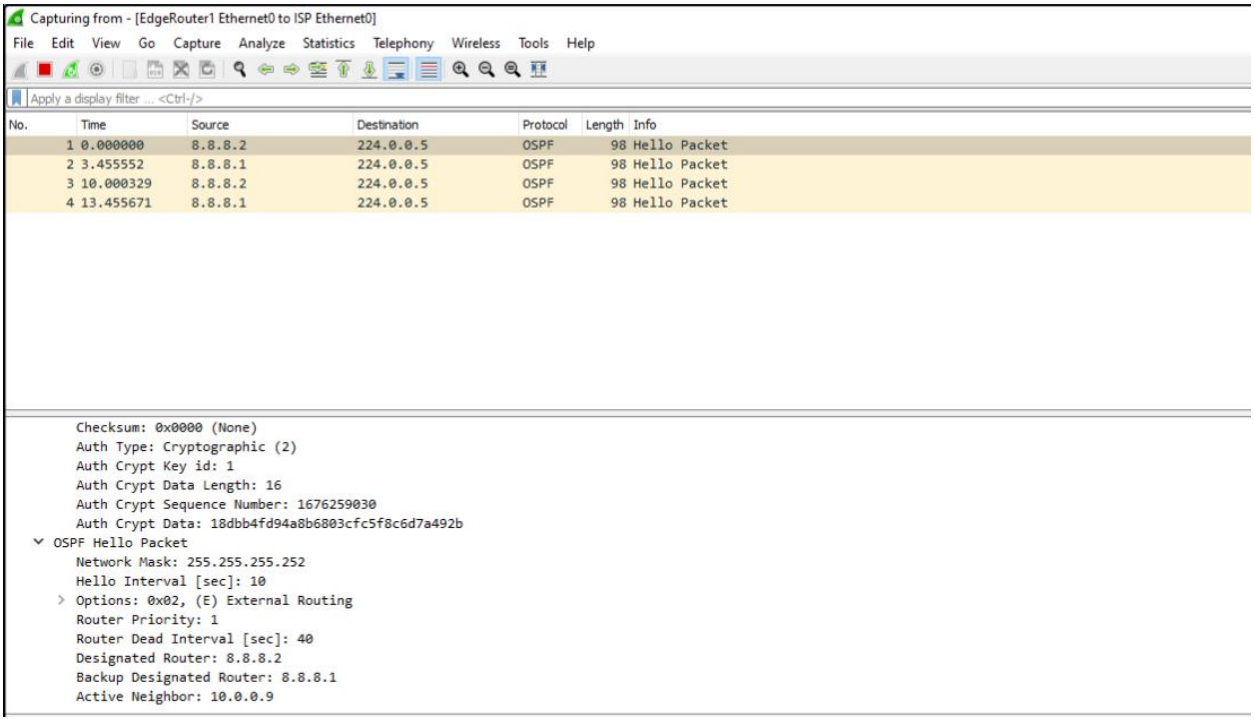
6. ISP is already aware of the 8.8.8.0/30 and 4.4.4.0/30 networks so it does not need to receive any routes from 8.8.8.1. We can see from running "show ip ospf route" that both

networks are directly connected.



7. Start a Wireshark packet capture on the link between EdgeRouter1 eth0 and ISP eth0. We can see that both EdgeRouter1 and ISP are actively exchanging OSPF info.





Test Case #9: Network Automation

Custom Test Case

*Define a **custom test case** to be run within your network project aligned to your specific organizational need or opportunity identified in Task 1. The custom test case should be equivalent in scope and requirements to the predefined test cases and pertain to network automation.*

"To save backups of network device configurations, a script should be configured on a server to retrieve the full network device configuration for each network device and store it on the server executing the script"

Functionality

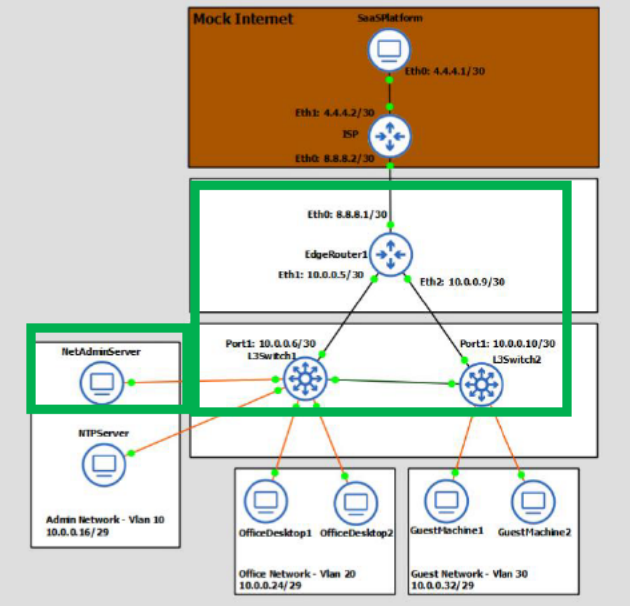
*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

NetAdminServer has a script located at "/home/student/NetAutomation/backup.py". The script uses netmiko to login to EdgeRouter1, L3Switch1 and L3Switch2 via SSH, show the full device configurations, and copy it to a folder located at "/home/student/NetAutomation/Backups" using the backup file name configured in the script.

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*

Devices that are directly applicable to the testing method are enclosed in green boxes.



Legend

SaaS	Software as a Service
Eth*	Ethernet + port number
ISP	Internet Service Provider
L3	Layer 3
NetAdminServer	Network Administration Server
Admin	Administration
VLAN	Virtual Local Area Network

Testing Method

*Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.*

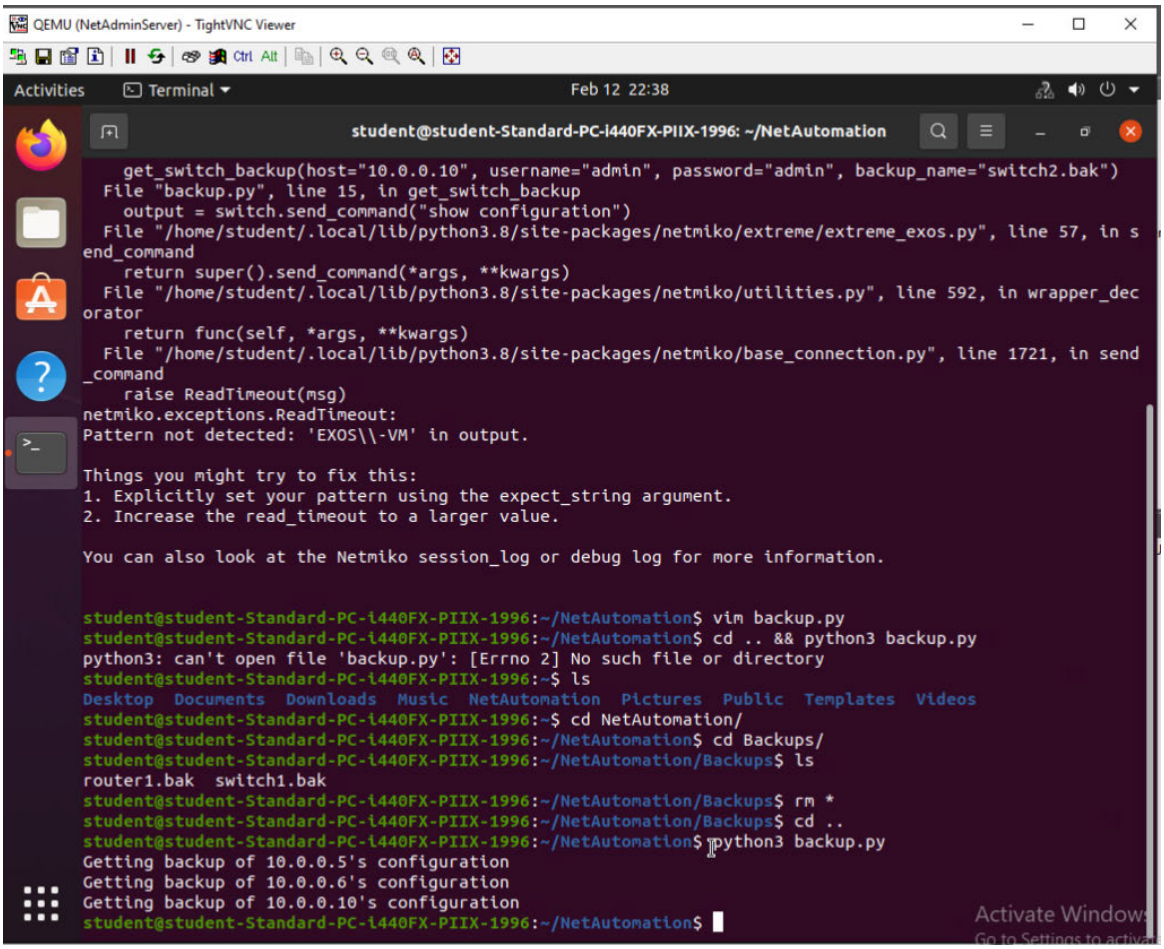
To verify the functionality of the script, I will remove any existing backups in the folder, execute the script, view the backups stored in the folder, and verify that they match the configurations on the network devices.

Process List

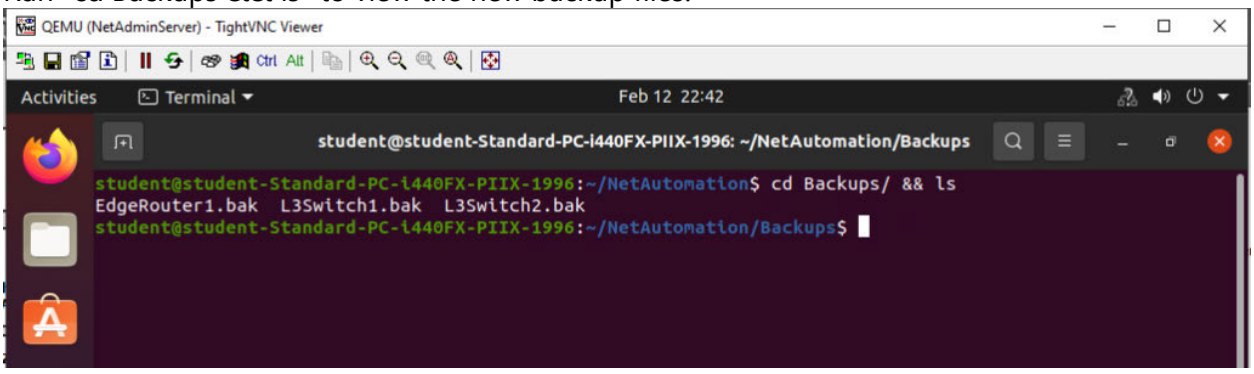
*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

1. Login to NetAdminServer.
2. Open a terminal and run "cd /home/student/NetAutomation/Backups"
3. Run "rm -f *" to remove all previous backups for testing.

4. Run "cd .. && python3 backup.py" to execute the script to get backups. If it errors, re-run the script with "python3 backup.py" since your current working directory will be where it is located now.

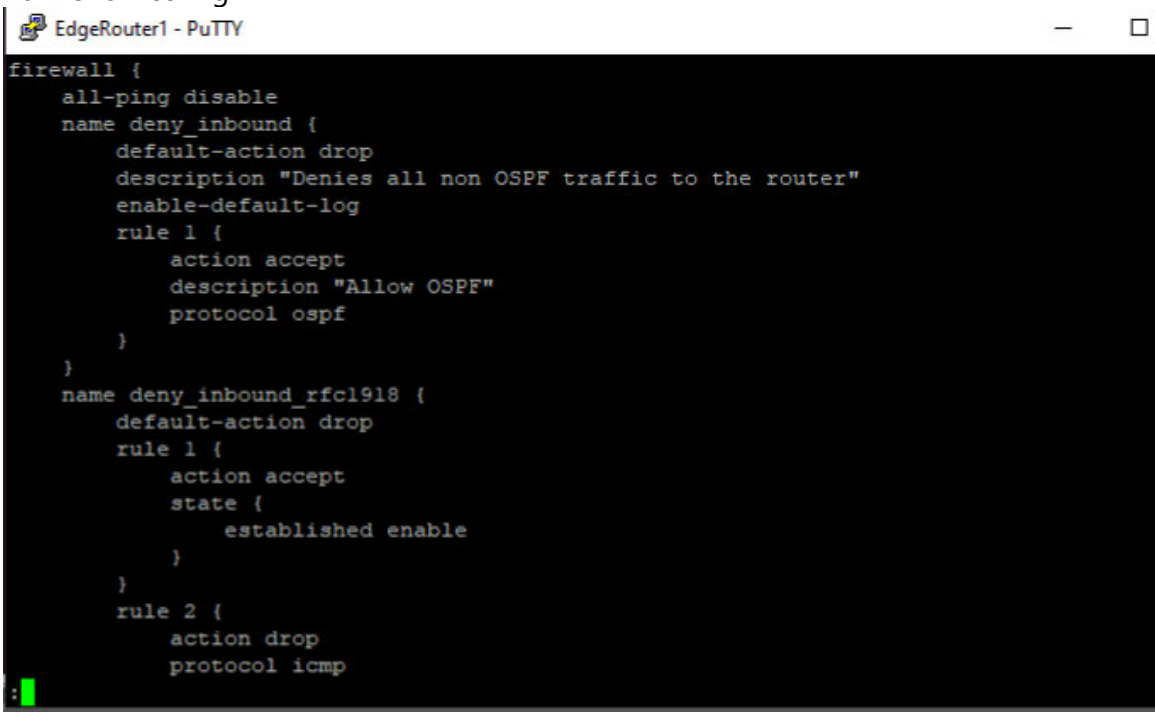


5. Run "cd Backups && ls" to view the new backup files.

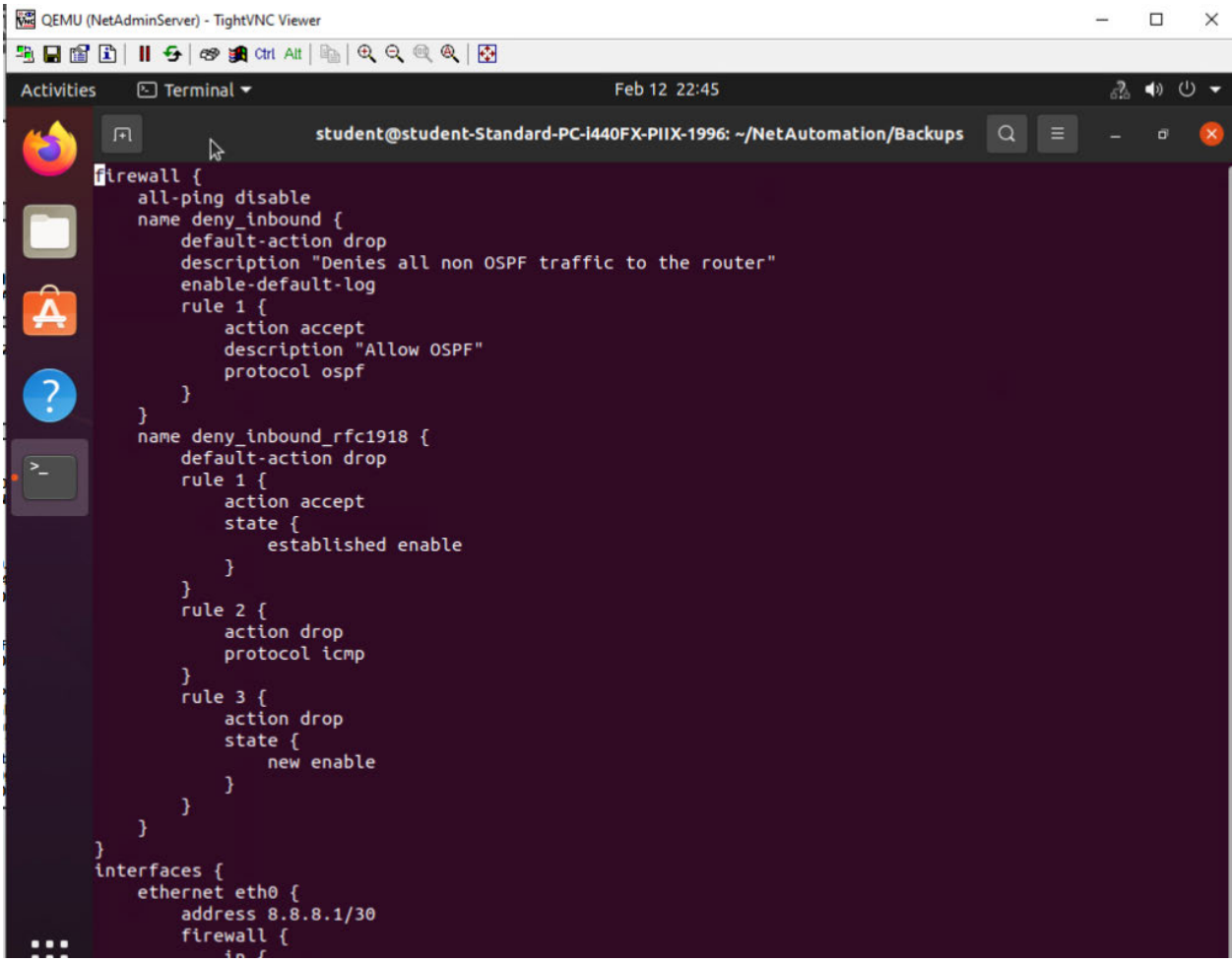


6. For each file, Login to the respective network device and run "show config" on the network device. Compare the output of the "show config" with the backup taken on the NetAdminServer by opening the respective ".bak" text file in your favorite text editor and checking for any discrepancies.
    a. Example:
        i. Login to EdgeRouter1.

ii. Run "show config"



iii. On NetAdminServer, open EdgeRouter1.bak with vim "vim EdgeRouter1.bak". We can initially see that these outputs are identical, and can conduct a manual review if needed.



Test Case #10: Network Security

Custom Test Case

*Define a **custom test case** to be run within your network project aligned to your specific organizational need or opportunity identified in Task 1. The custom test case should be equivalent in scope and requirements to the predefined test cases and pertain to network security.*

"Configure MD5 OSPF authentication to ensure that only authorized users will receive routes to the SaaS and company network."

Functionality

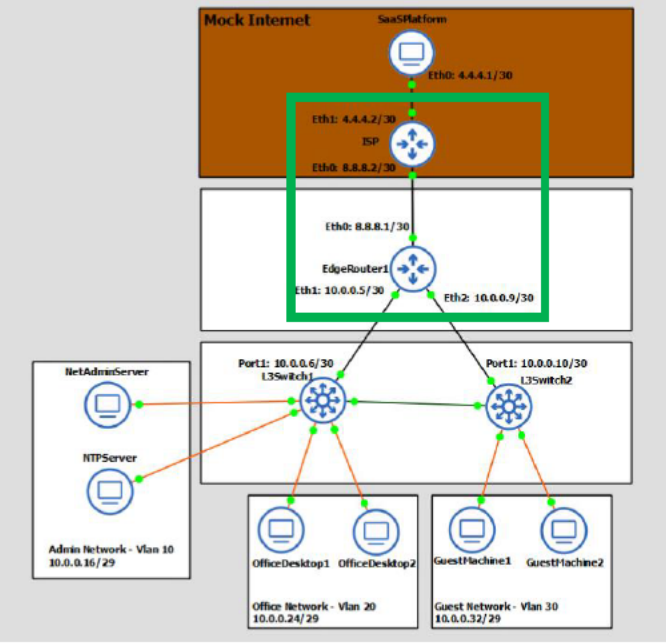
*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

As discussed, both EdgeRouter1 and ISP have OSPF configured to advertise and receive routes. MD5 authentication has been configured on ISP eth0 and EdgeRouter1 eth0 using key-id1 1 with the md5-key "secretkey1""

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*

Devices that are directly applicable to the testing method are enclosed in green boxes.



Legend

SaaS	Software as a Service
Eth*	Ethernet + port number
ISP	Internet Service Provider
L3	Layer 3
NetAdminServer	Network Administration Server
Admin	Administration
VLAN	Virtual Local Area Network

Testing Method

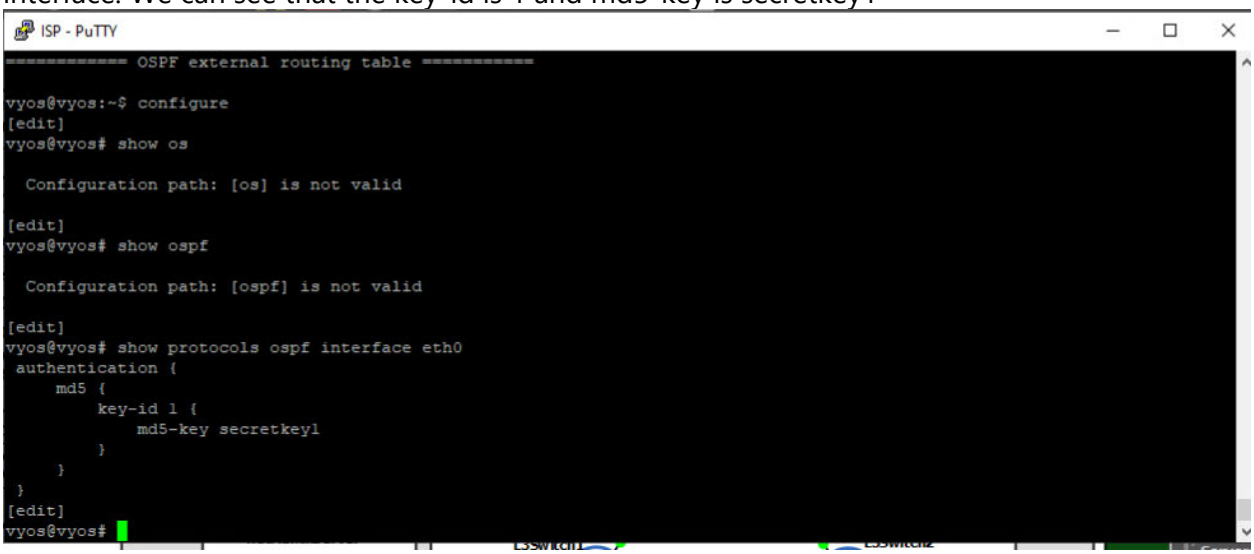
*Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.*

To verify the configuration, I will show the interface OSPF configuration, and inspect the OSPF packets on the link between EdgeRouter1 eth0 and ISP eth0 to verify that authentication parameters are contained in the packets.

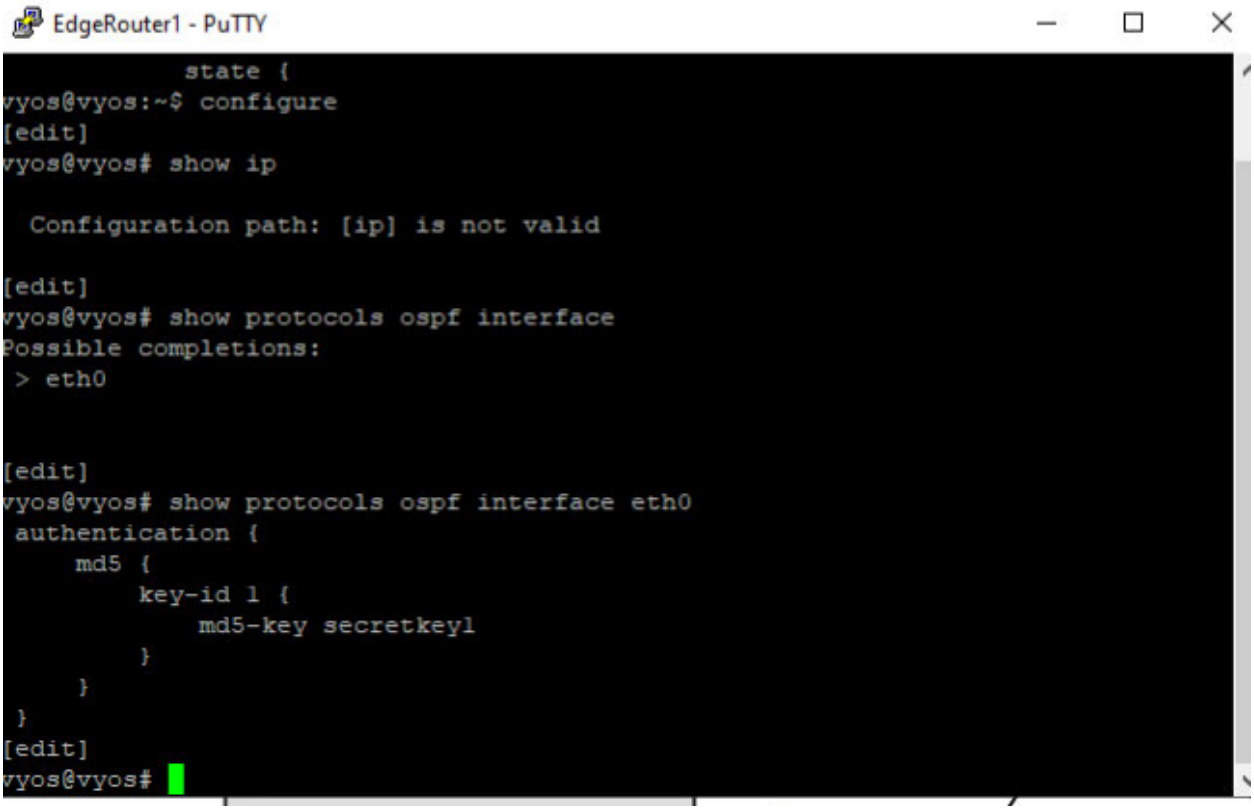
Process List

*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

1. Login to ISP.
2. Run "config" to enter configuration mode.
3. Run "show protocols ospf interface eth0" to view the MD5 authentication settings for the interface. We can see that the key-id is 1 and md5-key is secretkey1

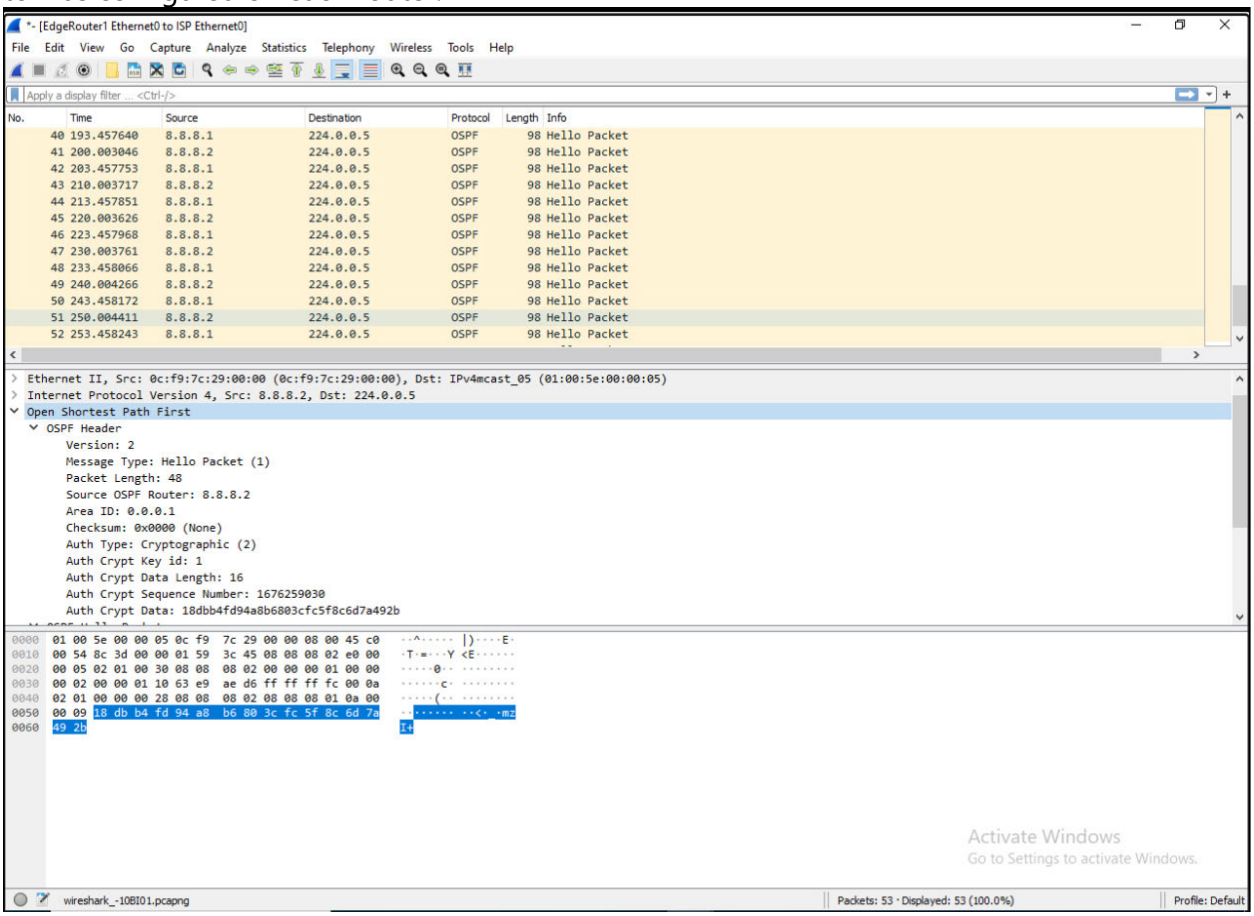


4. Login to EdgeRouter1.
5. Run "config" to enter configuration mode"
6. Run "show protocols ospf interface eth0" to view the MD5 authentication settings for the interface. We can see that the key-id is 1 and md5-key is secretkey1



7. Take a Wireshark packet capture to inspect the OSPF packets being exchanged. As we can see in the packet, Auth Type field is Cryptographic, the Auth Crypt Key id field is set

to 1 as configured on each router.



Network Troubleshooting

Discuss how you analyzed the network to identify, troubleshoot, and resolve issues during development or when ensuring functionality of the test cases.

During the development of the network, there were various types of issues I encountered. Fortunately, GNS3 and the software on network devices and endpoints made troubleshooting possible. Sometimes restarting GNS3 and the VDI resolved issues as well. The most helpful troubleshooting method was inspecting packets through Wireshark. Wireshark allowed me to view both IP packet headers, and detailed information about most protocols. This was helpful in troubleshooting both network service, routing, and switching issues.

On network devices, I most commonly used traceroute, ping and "show" commands. I utilized traceroute to view that the appropriate path was being taken for IR routing, ping to verify basic connectivity, and "show" commands to view configurations on each network device. I also referenced the relevant network device documentation to gain an understanding of their features.

On endpoints, I used several commands. On Ubuntu desktops, I used “dhclient” to release DHCP releases and get new ones. I also used “nmtui” to configure network interfaces on the host. On Windows, I used “ipconfig” to view IP address information, and manage host DHCP leases.

References

Charles, K. (2018, July 22). *Warning banner sample for systems and network devices*. SecurityOrb.com | The Information Security, Digitial Privacy & Internet Safety Website... Retrieved February 12, 2023, from https://securityorb.com/general-security/warning-banner-sample-for-systems-and-network-devices/