Network Engineering Capstone Functionality Report Packet Tracer

Introduction

Provide a functionality report detailing the 10 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	Omar Sanchez
WGU Student ID	011060302
WGU Student Email	osanc52@wgu.edu

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 of medium size, with each site able to connect to the internet. The Main Office site is a 2-tier collapsed-core network containing one edge router, firewall, L3 switches, and access switches. The remote site similarly consists of one edge router and one firewall. However, it only contains one core router and one core switch. The two separate sites create an IPsec tunnel forming a site-to-site VPN established and managed by each firewall.

The Main Office site contains redundancy with two L3 switches configured as the core routers and distribution switches. An HSRP group actively manages the default gateway for each VLAN, with one router forwarding and another in standby. All IP services at the Main Office site serve both the Main and Remote Office sites. Devices at the Remote Office site must reach into the Main Office site over the VPN to reach them. Configured IP services include DHCP, DNS, NTP, Syslog, and AAA. A network controller provides a centralized network device management solution and provides network visibility.

Each network device uses OSPF internally to share routes. All external devices are configured with BGP for route sharing. The firewalls ensure that only acceptable connections are allowed access through stateful packet inspection. In this network, only internal network devices can establish a connection to external devices (webpages). External network devices are not allowed to access internal networks.

Main site internal networks:

Main-Edge-RT <-> Main-FW - 10.0.50.0/30

Main-FW <-> Main-Core/Distro-1 - 10.100.20.0/30

Main-FW <-> Main-Core/Distro-2 - 10.100.20.8/30

Main-Core/Distro-1 <-> Main-Core/Distro-2 - 10.100.20.16/30

Main site VLAN networks:

User: 172.16.11.0/26 - VLAN 400

Printer: 172.16.11.64/26 – VLAN 500

IP Services: 172.16.11.128/27 – VLAN 600

Guest: 172.16.11.160/27 – VLAN 900

Management: 172.16.11.192/28 – VLAN 80

Remote site internal networks:

Remote-Edge-RT <-> Remote-FW – 10.0.50.8/30

Remote-FW <-> Remote-Core/Distro – 10.200.20.0/30

Remote site VLAN networks:

User: 10.200.100.0/26 – VLAN 400

Printer: 10.200.100.64/26 – VLAN 500

IP Services: 10.200.100.128/27 – VLAN 600

Guest: 10.200.100.160/27 – VLAN 900

Management: 10.200.100.192/28 – VLAN 80

External Networks:

ISP RT <-> Main-Edge-RT <-> Remote-Edge-RT – 10.1.1.0/29 (All connected over a switch)

ISP RT <-> Trusted-Site – 10.3.3.0/30

ISP RT <-> Untrusted-Site – 10.8.8.0/29

Network Diagram or Segment

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

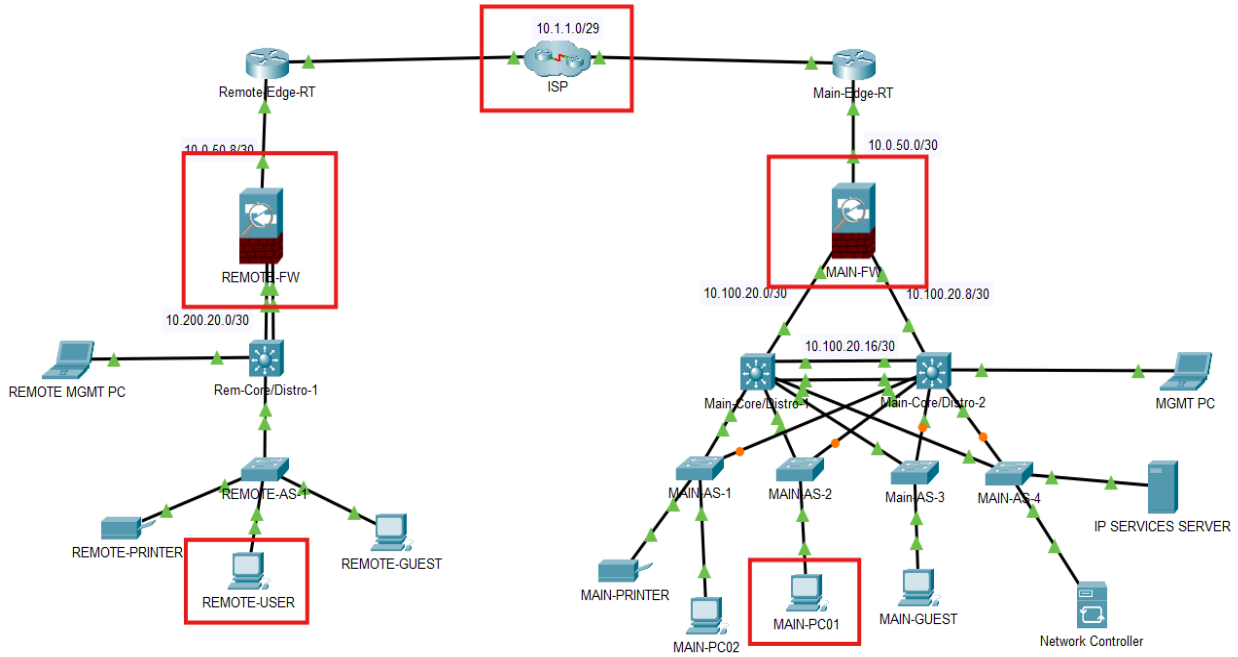


Figure 1- Network Overview

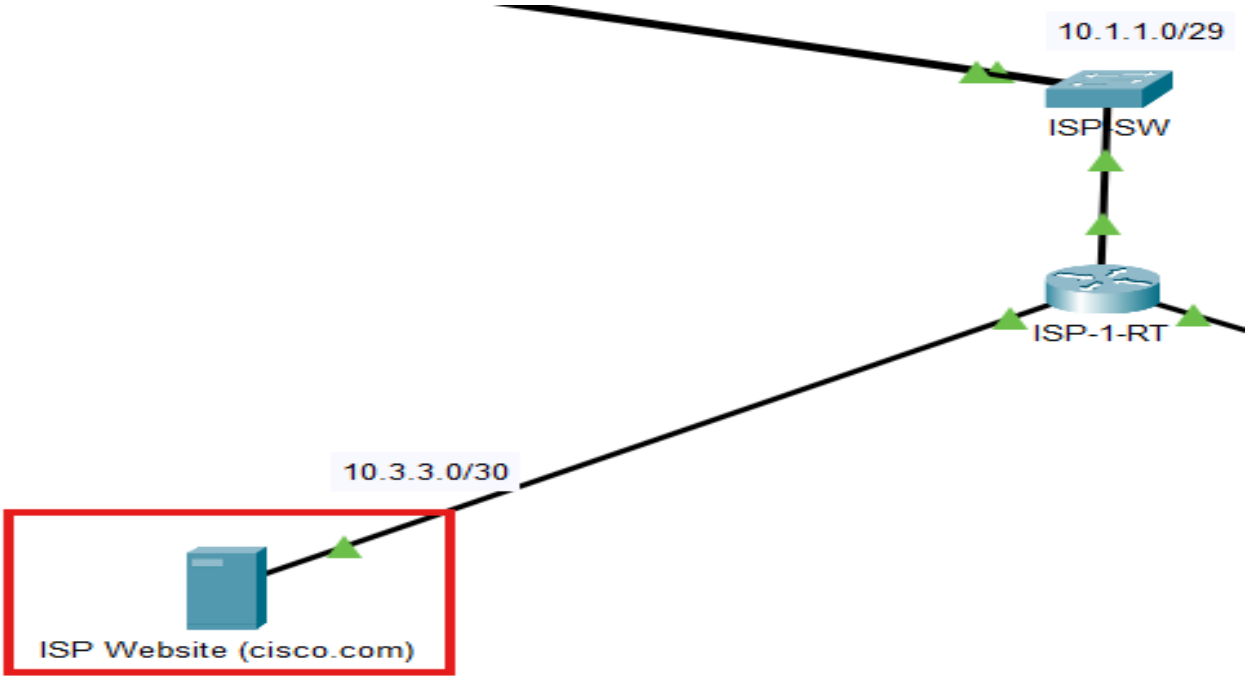


Figure 2- ISP Website (cisco.com)

Legend	
IP	Internet Protocol
RT	Router
AS	Access Switch
Main	Main Office
Remote	Remote Office
MGMT	Management
FW	Firewall
SW	Switch
REM	Remote
PC	Personal Computer
Distro	Distribution Switch
ISP	Internet Service Provider

Testing Method

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

This test will examine the device discovery and reachability throughout the network to show that the User VLAN network in the Main Office Site (172.16.11.0/26) and the Remote Office Site (10.200.100.0/26) can communicate with each other through ICMP messages and with the internet by accessing a website. The devices performing this reachability test are Remote-User-PC and Main-User-PC. The site-to-site VPN enables connectivity between each site. We will further test connectivity by accessing the same mock website (cisco.com), at network 10.3.3.0/30, from each site. This traffic will establish a session managed by the firewall and allow external traffic into the internal networks at each site.

We will send ICMP messages from the website to both assets to demonstrate a situation in which connectivity is limited/denied. This behavior, of an external device initiating a connection to a device within a network, is blocked by the stateful firewall (Main-FW and Remote-FW) at each site.

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.*

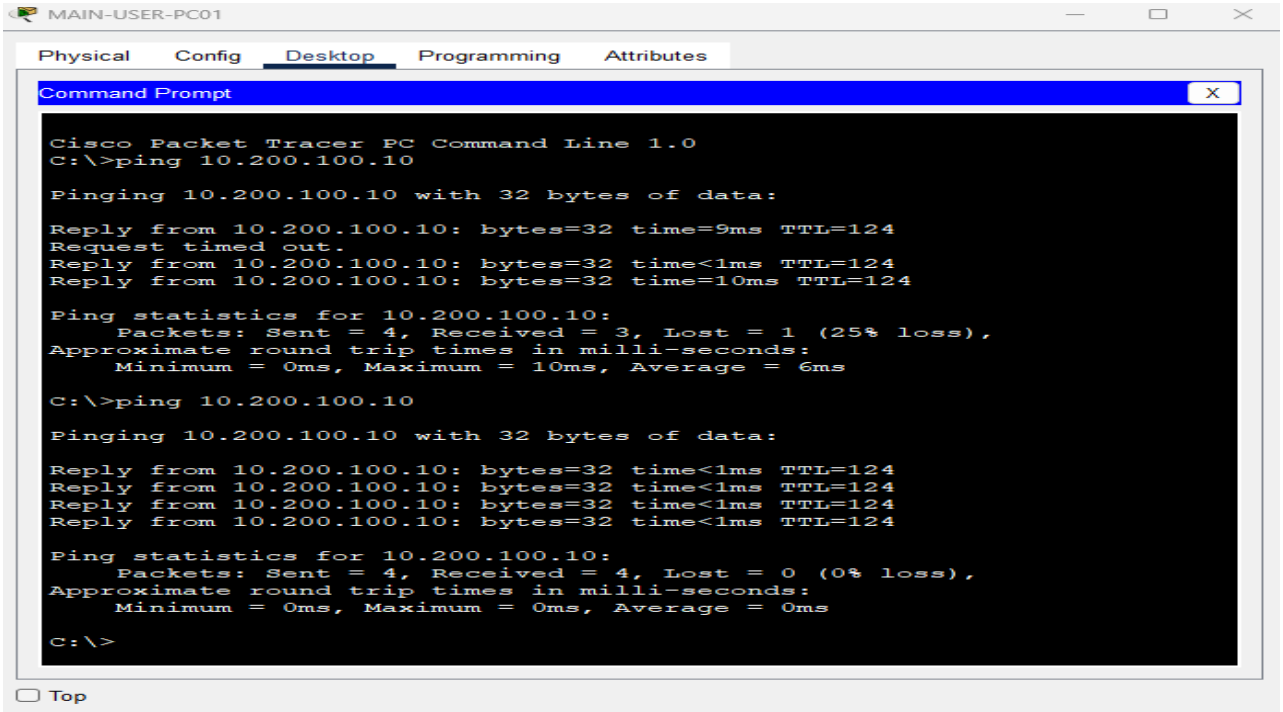
Main-USER-PC01 | IP: 172.16.11.10 (DHCP)

Remote-USER-PC | IP: 10.200.100.10 (DHCP)

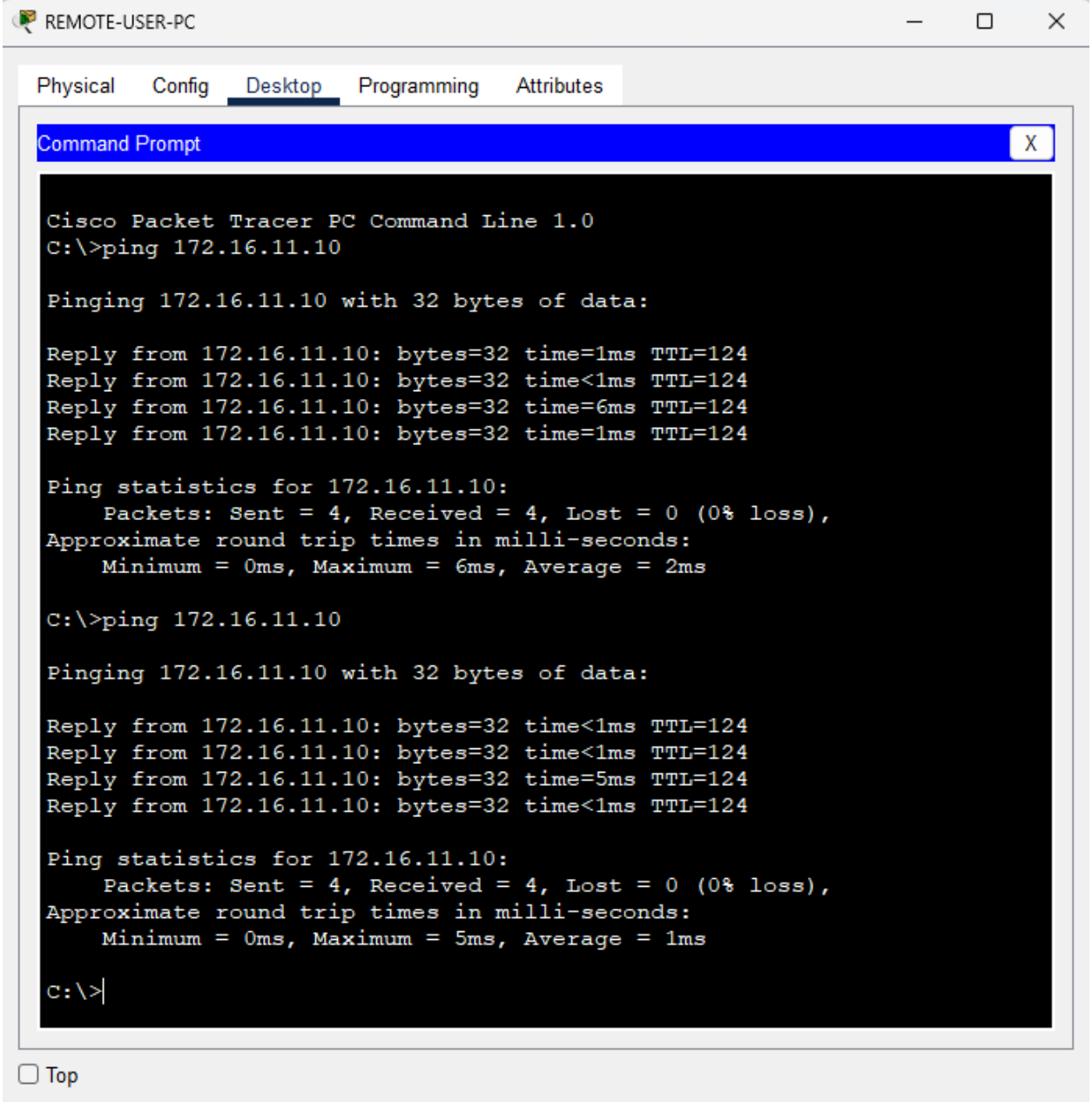
Website: Cisco.com | IP: 10.3.3.2 (Static)

Demonstrate Device Connectivity:

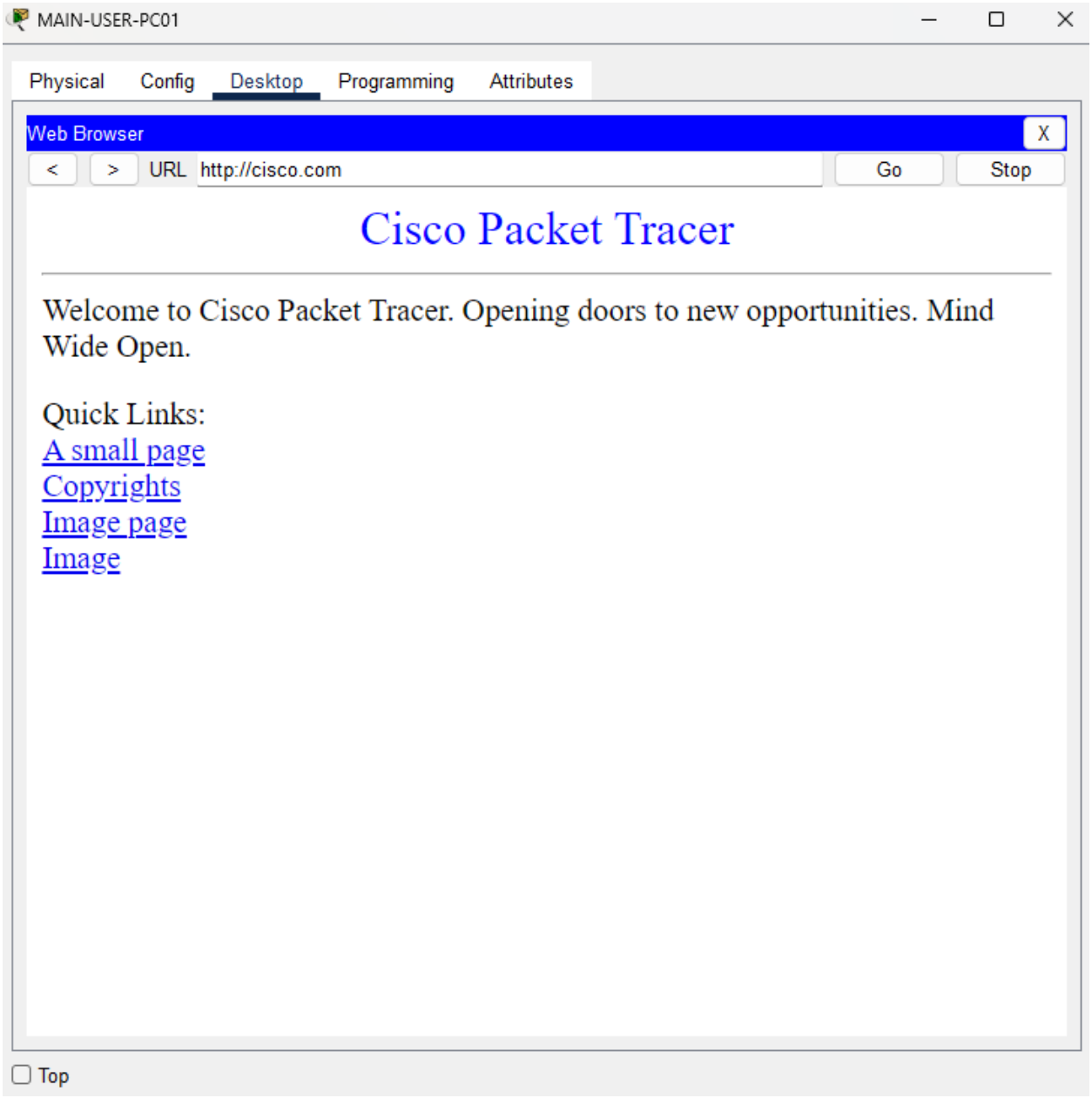
Step 1: From Main-USER-PC01, open the command prompt and ping Remote-USER-PC (10.200.100.10).



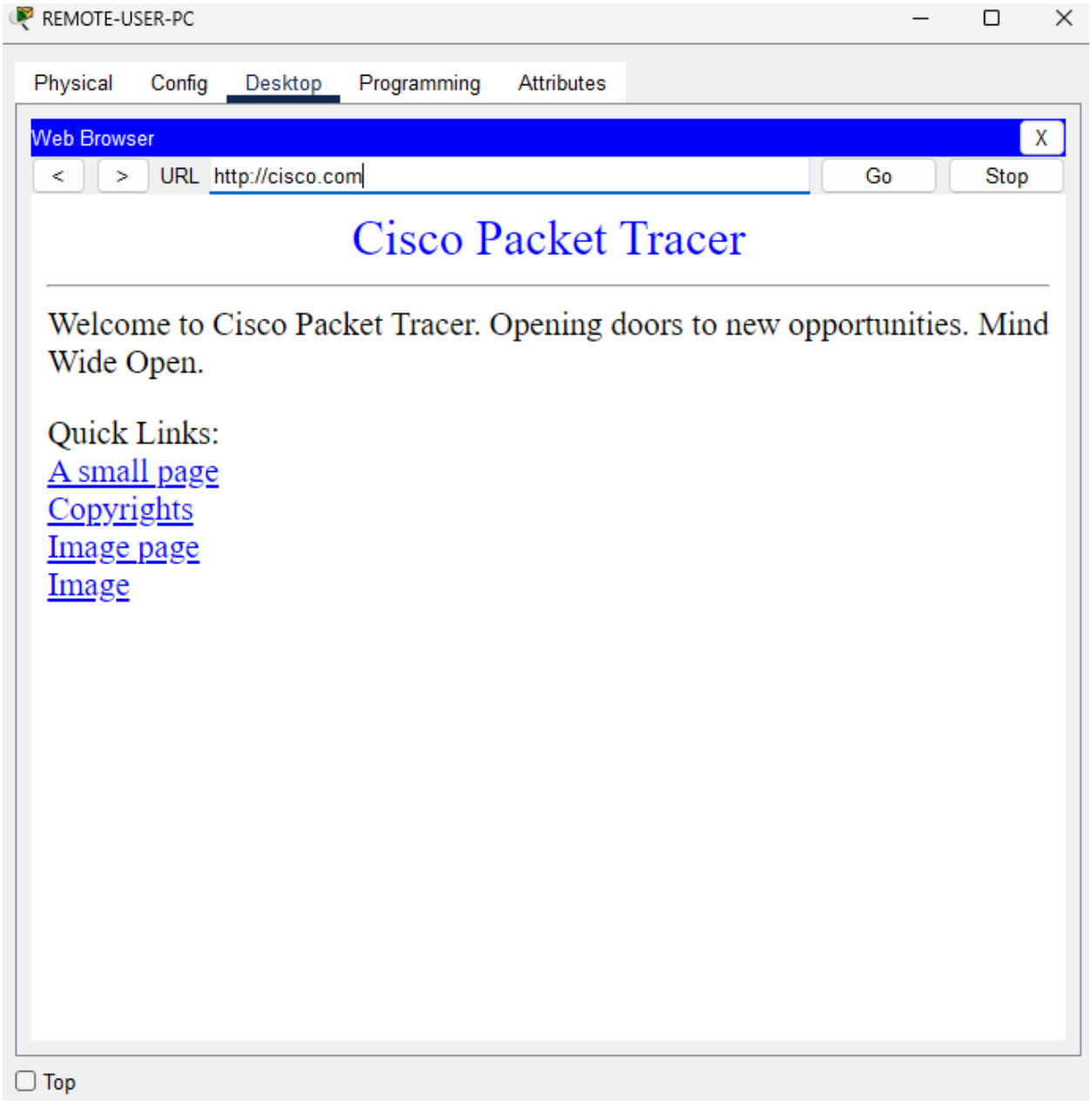
Step 2: From Remote-USER-PC, open the command prompt and pint Main-USER-PC01 (172.16.11.10).



Step 3: On Main-USER-PC01, open the web browser and in the address bar type cisco.com. The DNS server will handle IP address retrieval.



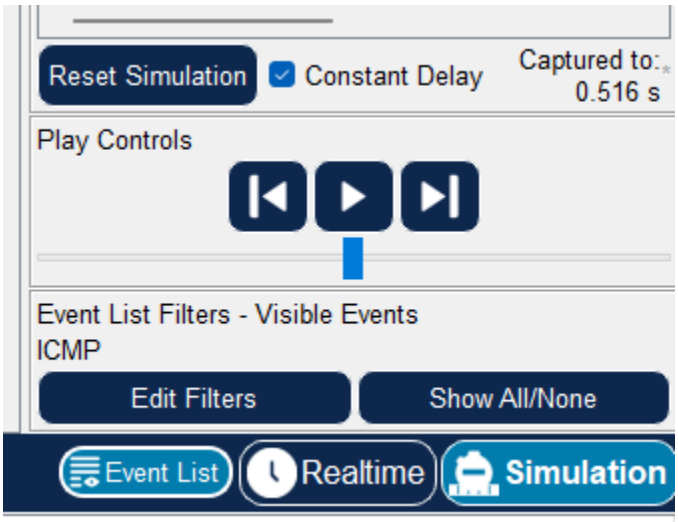
Step 4: On Remote-USER-PC, open a web browser and type cisco.com. The DNS server will handle IP address retrieval.



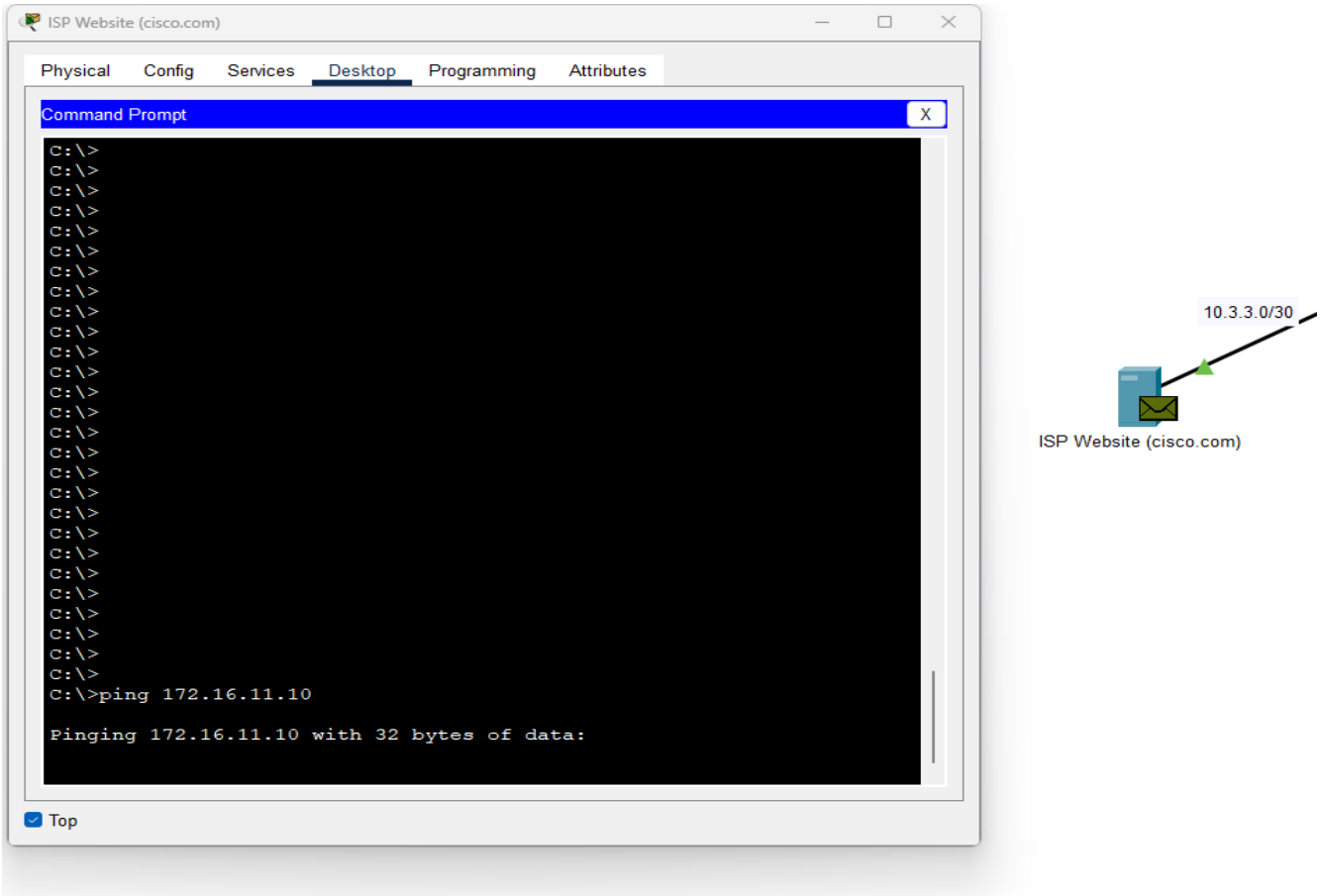
Demonstrate Limited\Denied Connectivity:

To show that Main-FW is blocking external requests and dropping the packets, we will ping from the website server and observe the path the packets follow.

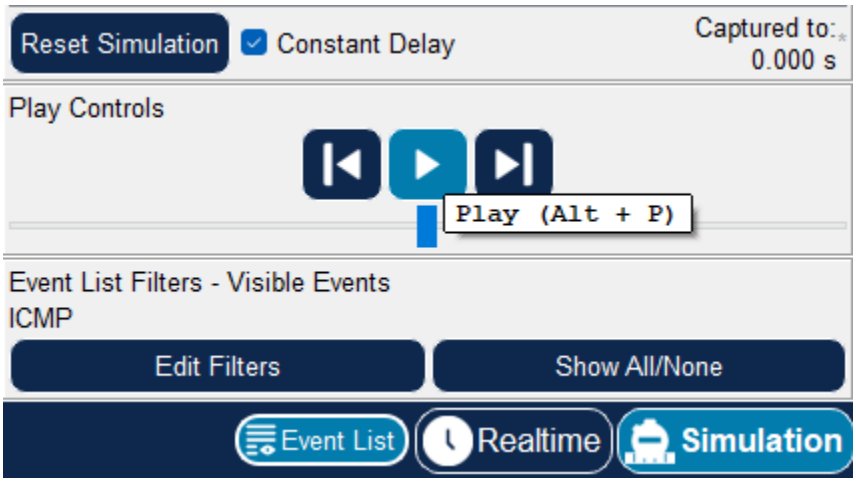
Step 1: Click on the Simulation button and update the Event List filters to ICMP only.



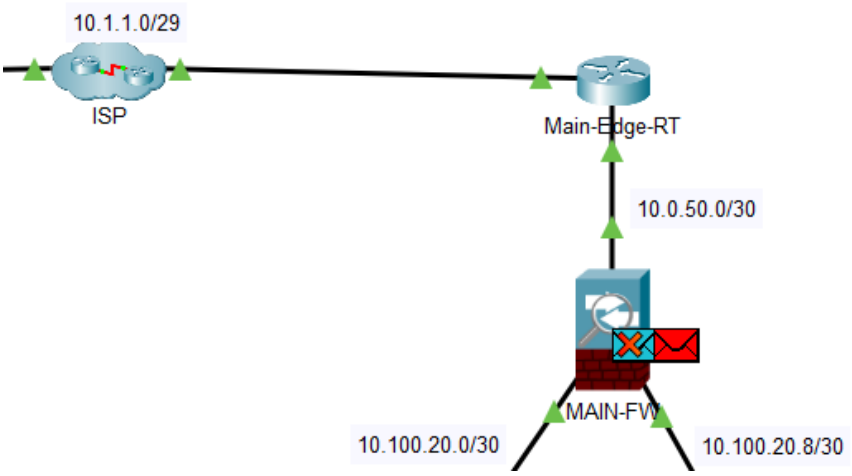
Step 2: Access ISP Website Server in the ISP Cluster. Open a command prompt and ping Main-USER-PC01 (172.16.11.10).



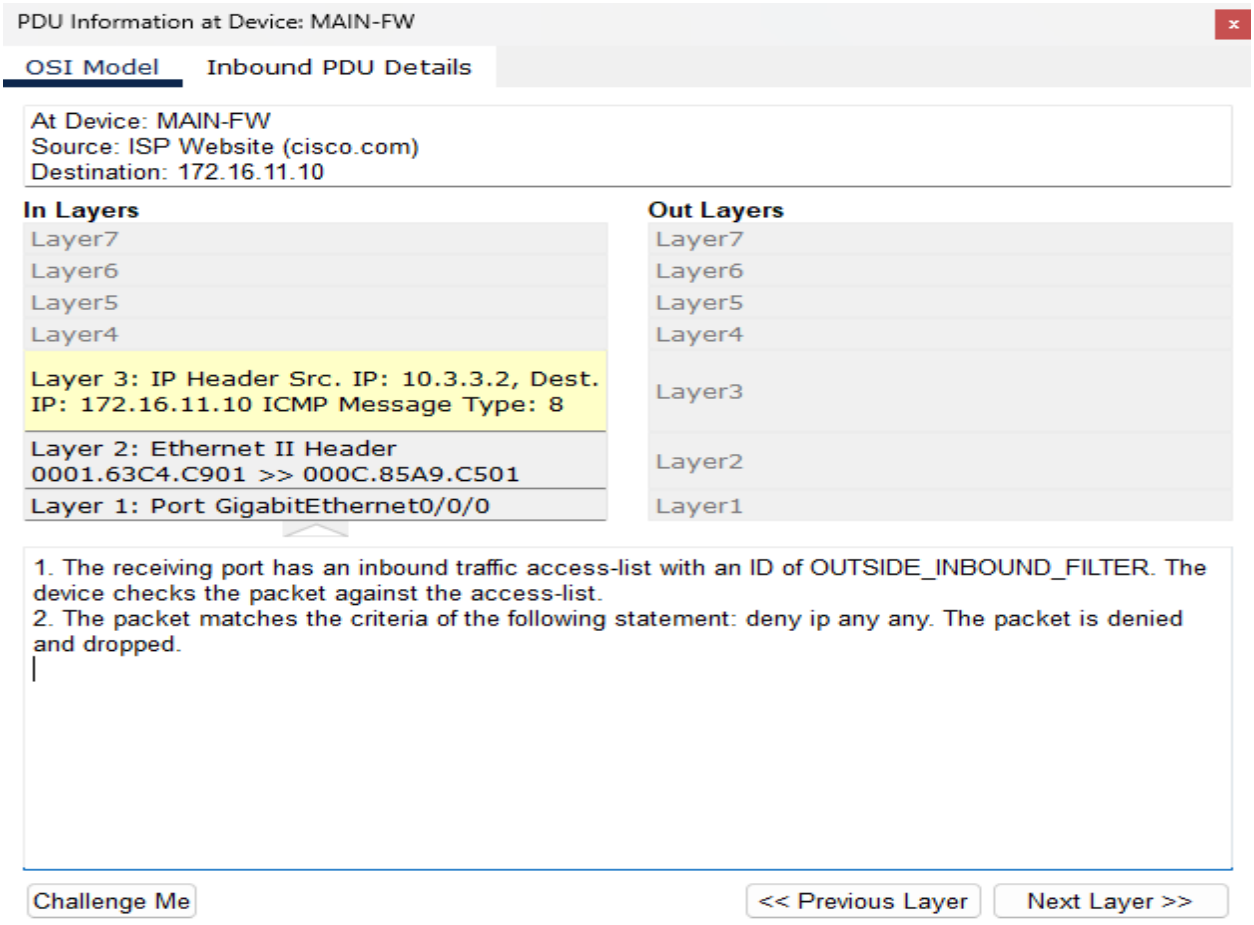
Step 3: Select “Play” in the simulation controls and watch the packet route.



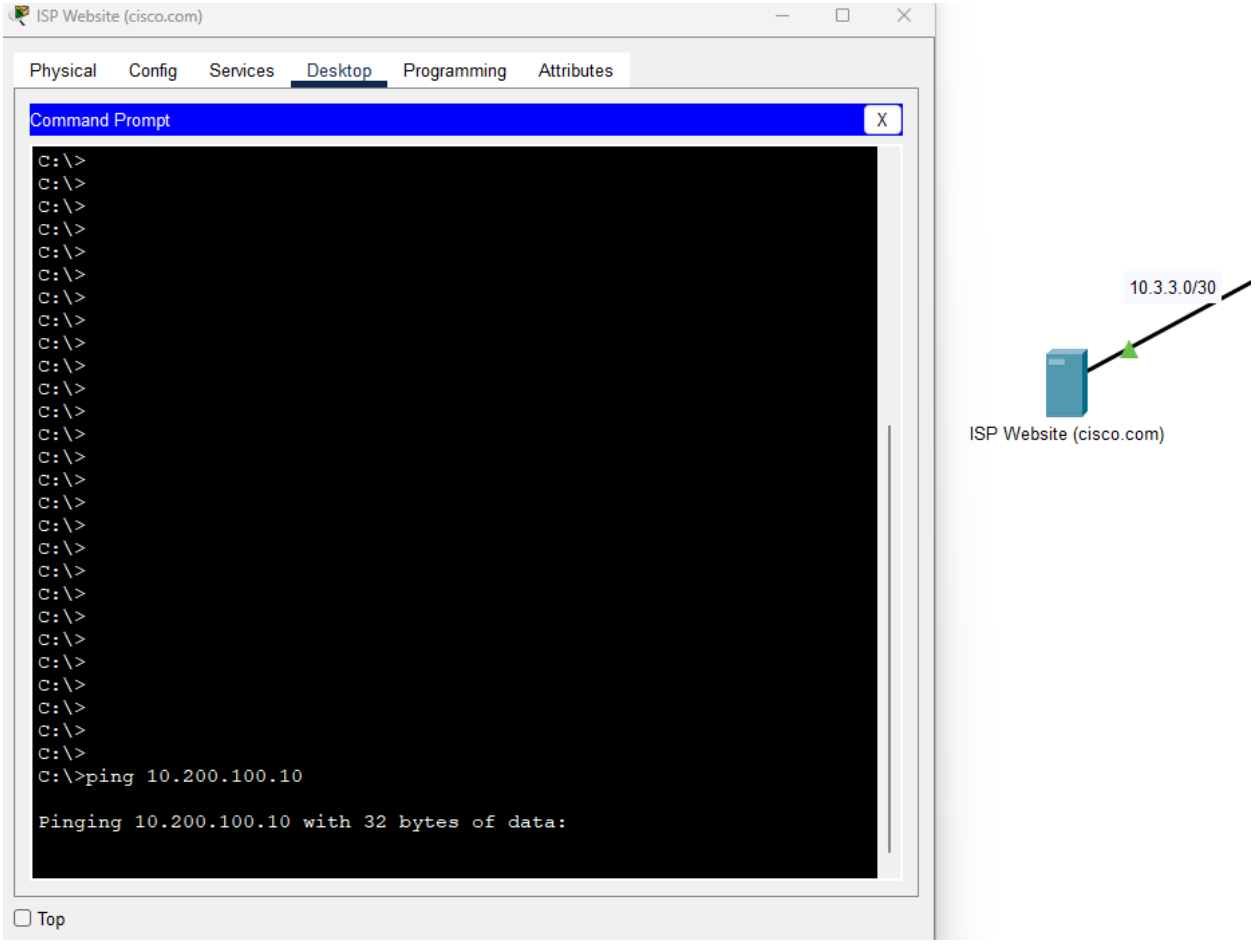
Step 4: When the packet reaches Main-FW, pause the simulation.



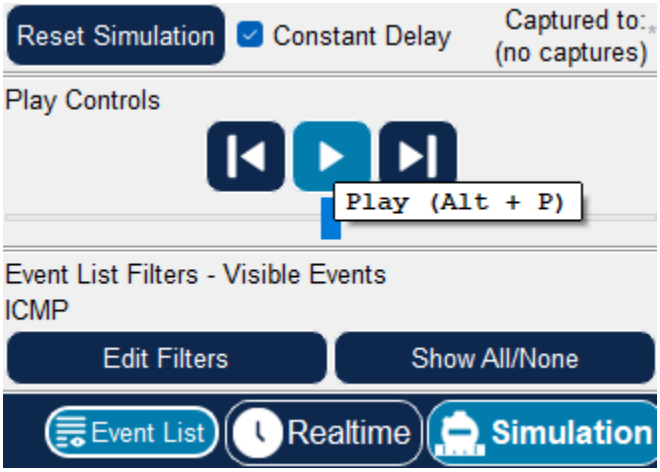
Step 5: Open the PDU Information screen. Last Device: Main-Edge-RT At Device: MAIN-FW. Under Layer 3, the description states that the firewall rule is being applied.



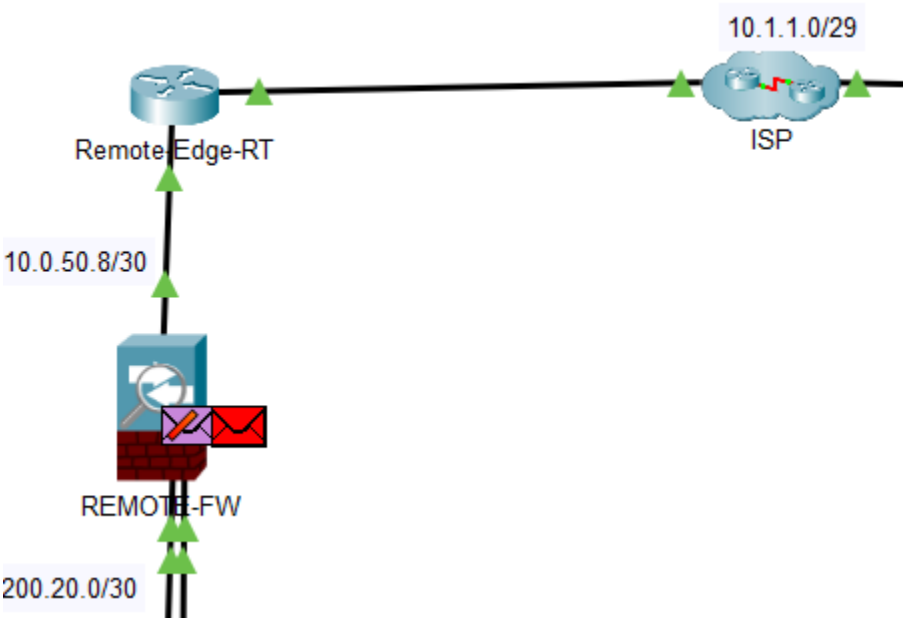
Step 6: Reset the simulation and access the ISP Website server. Open a command prompt and ping Remote-USER (10.200.100.10).



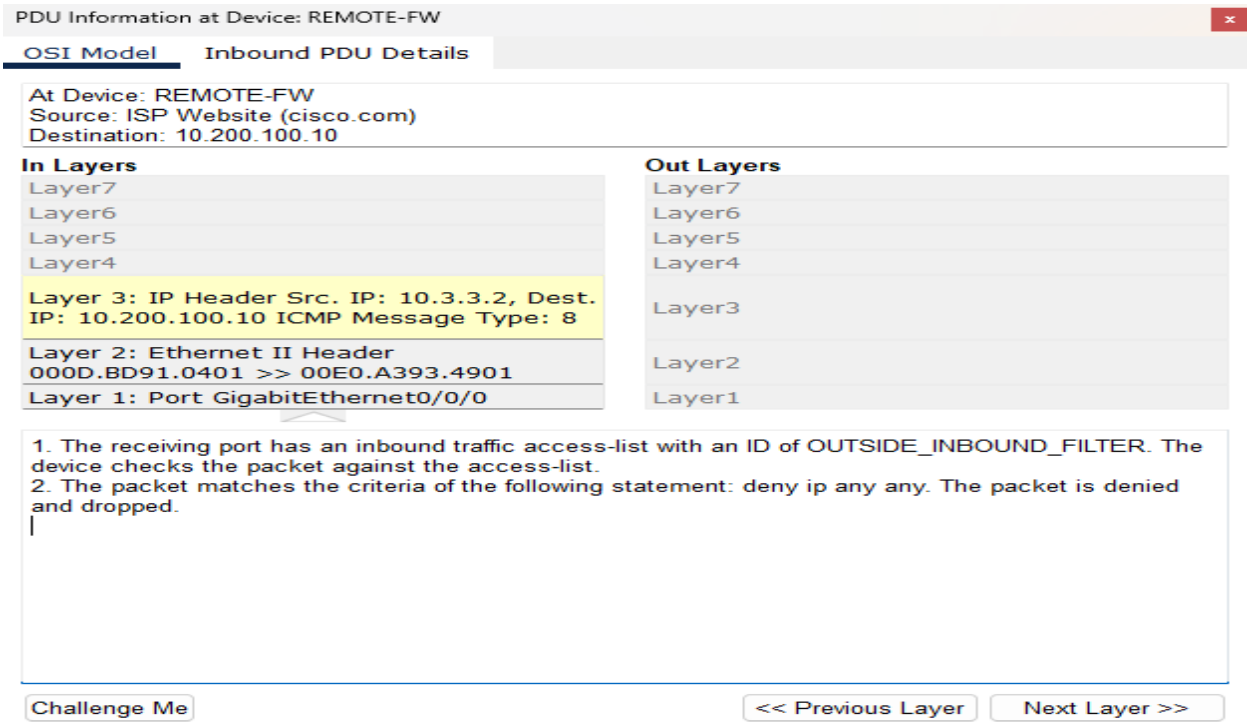
Step 7: Select "Play" in the simulation controls and watch the packet route.



Step 8: When the packet reaches Remote-FW, pause the simulation.



Step 9: Open the PDU Information screen. Last Device: Remote-Edge-RT At Device: Remote-FW. Under Layer 3, the description states that the firewall rule is being applied.



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.*

The Main and Remote Office sites each contain their own Guest Vlan numbered 900. An ACL is applied to interface Vlan 900's gateway at the Main Office site. Since there are two L3 switches configured for HSRP, each device is configured with the ACL applied to it. The ACL allows DHCP traffic for hosts and permits connectivity to the DHCP/DNS server on the Inbound side of the interface at the L3 switches. The ACL then denies access to each internal and remote VLAN network with a permit statement at the end, allowing all other traffic to access the Internet (external) with the firewall's stateful inspection monitoring traffic. These traffic rules are also applied at the remote site and so, in function, mirror the main site guest network permissions

Main-Guest network: Vlan 900 – 172.16.11.160/27 Gateway 172.16.11.161

Remote-Guest network: Vlan 900 – 10.200.100.10/27 Gateway 10.200.100.161

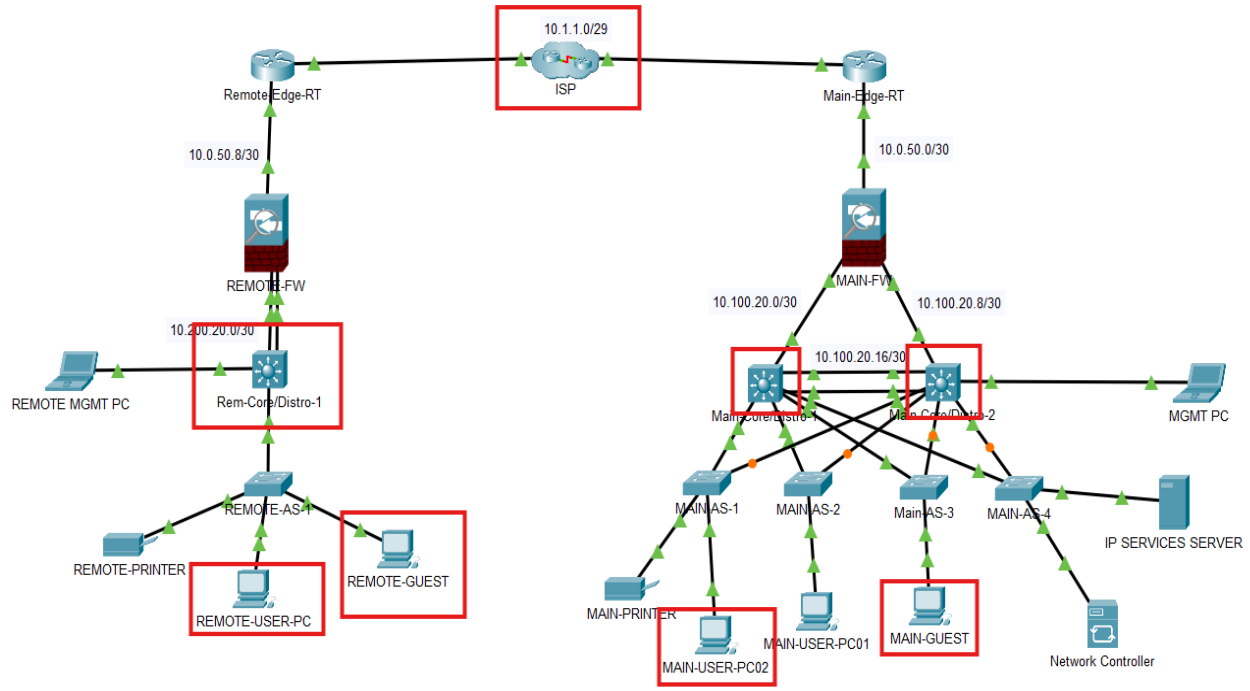
Mock Internet: cisco.com (10.3.3.2)

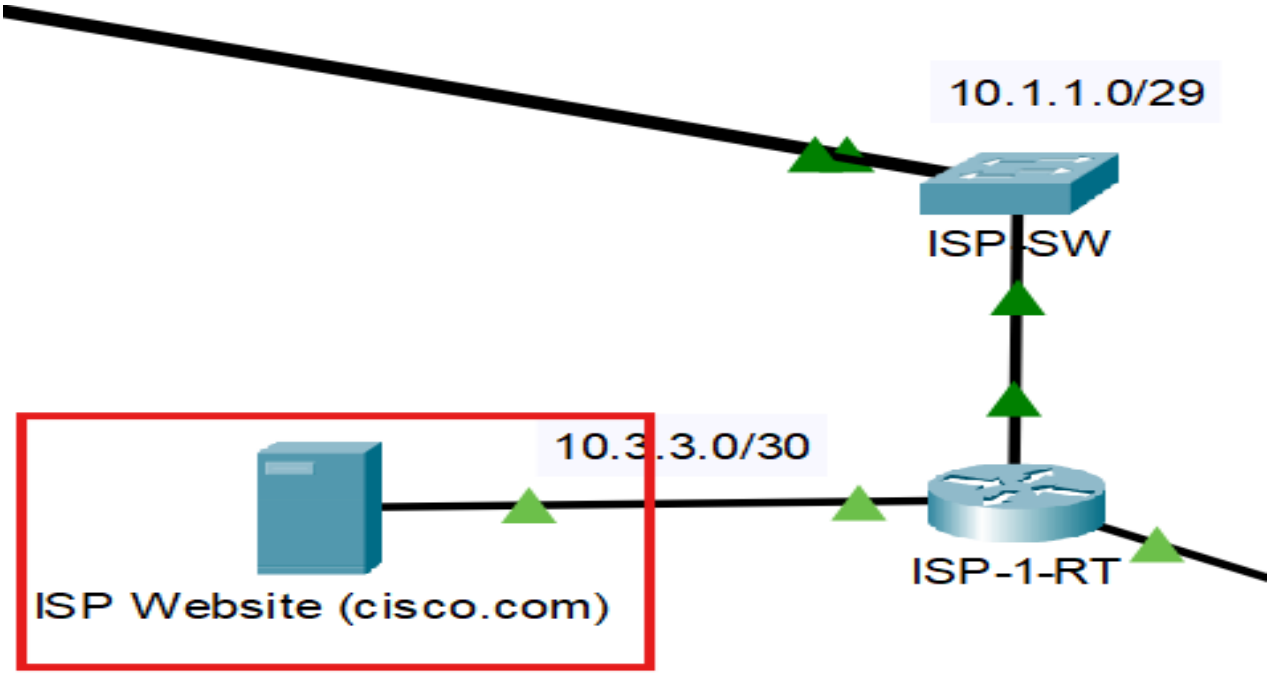
Main-User network: Vlan 400 – 172.16.11.0/26 Gateway 172.16.11.1

Remote-User network: Vlan 400 – 10.200.100.0/26 Gateway 10.200.100.1

Network Diagram or Segment

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





Legend	
IP	Internet Protocol
RT	Router
AS	Access Switch
Main	Main Office
Remote	Remote Office
MGMT	Management
FW	Firewall
SW	Switch
REM	Remote
PC	Personal Computer
Distro	Distribution Switch
ISP	Internet Service Provider

Testing Method

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

For this test, we will perform three key tasks for the guest networks at each site.

1. Show Internet access on the guest network.
2. Demonstrate no connectivity to devices in other VLAN networks internally and between office sites.
3. Temporarily remove the ACL, demonstrate that connectivity between networks and the remote site is allowed, and show the implemented ACLs' effectiveness.

We will perform all tasks at the Main Office site first and, once confirmed, repeat them at the Remote Office site.

Device IPs:

Main-Guest: 172.16.11.164/27

Main-User-PC01: 172.16.11.10/26

Remote-Guest: 10.200.100.165/27

Remote-User-PC: 10.200.100.10/26

Website: cisco.com – 10.3.3.2

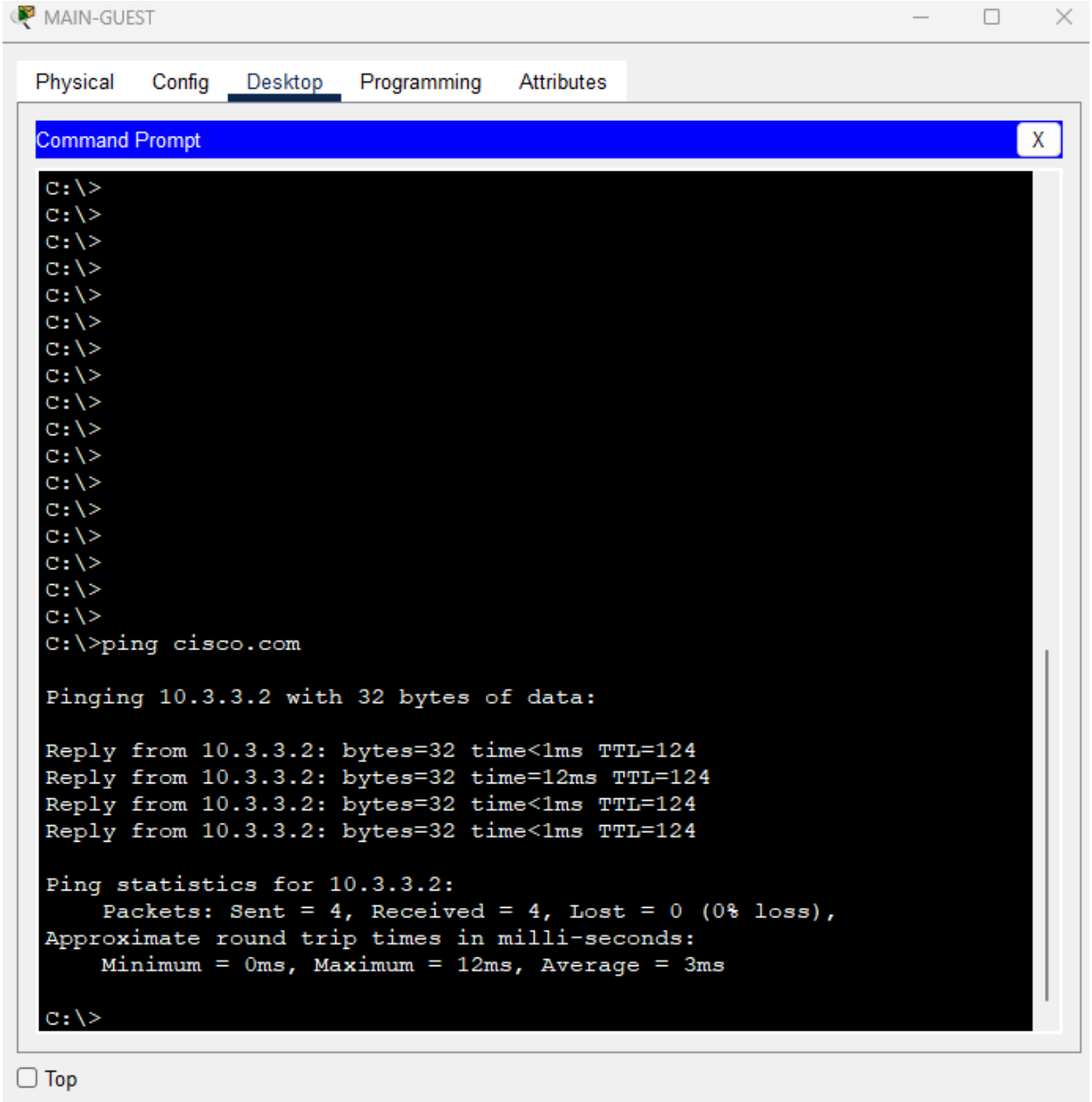
Note: Guest network devices still have access to DHCP and DNS services, so limited connectivity is allowed to the IP Services server.

Process List

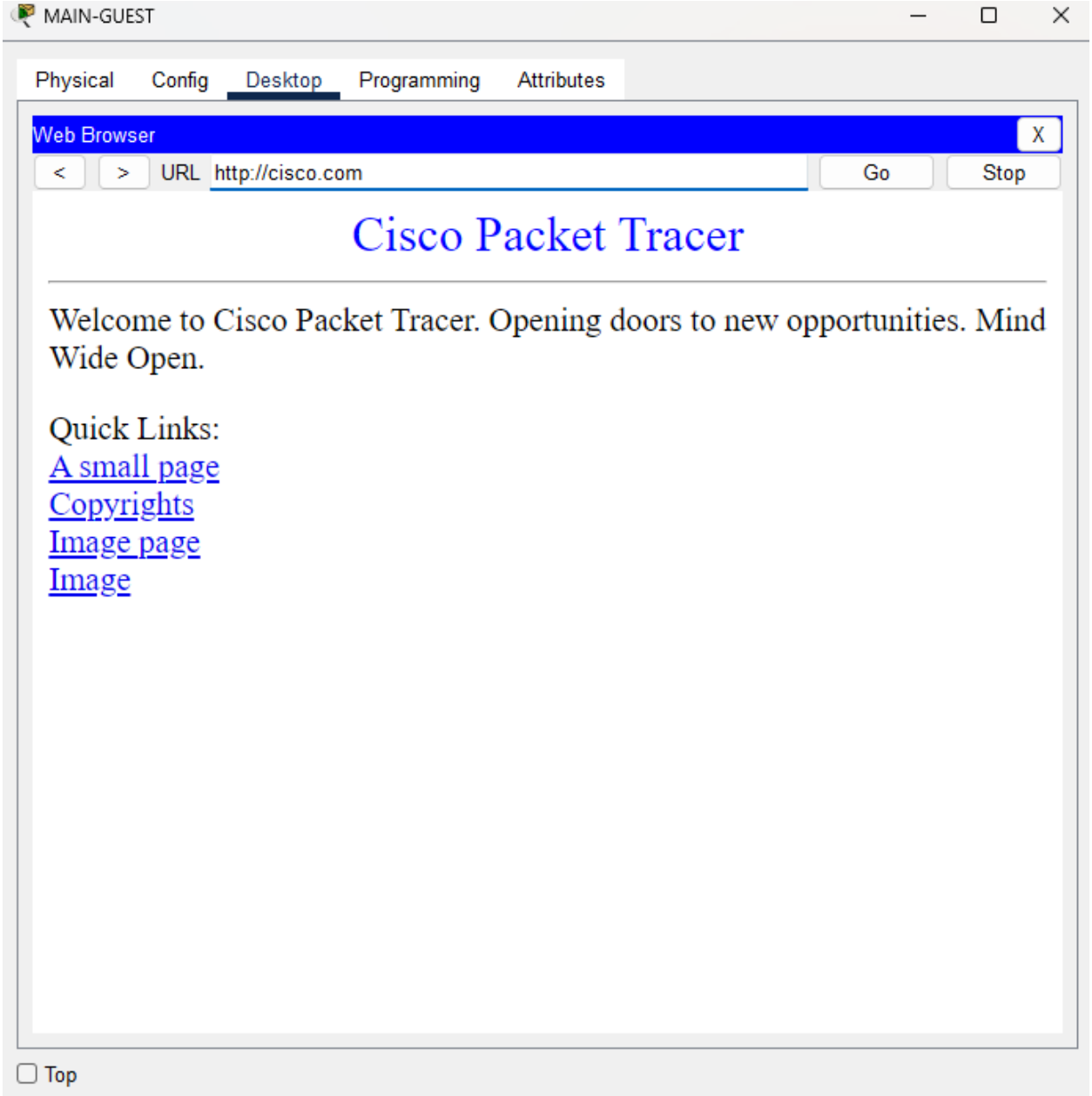
*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

Main Office Guest Network Internet Access

Step 1: Login to Main-Guest, open the command prompt, ping cisco.com (10.3.3.2).

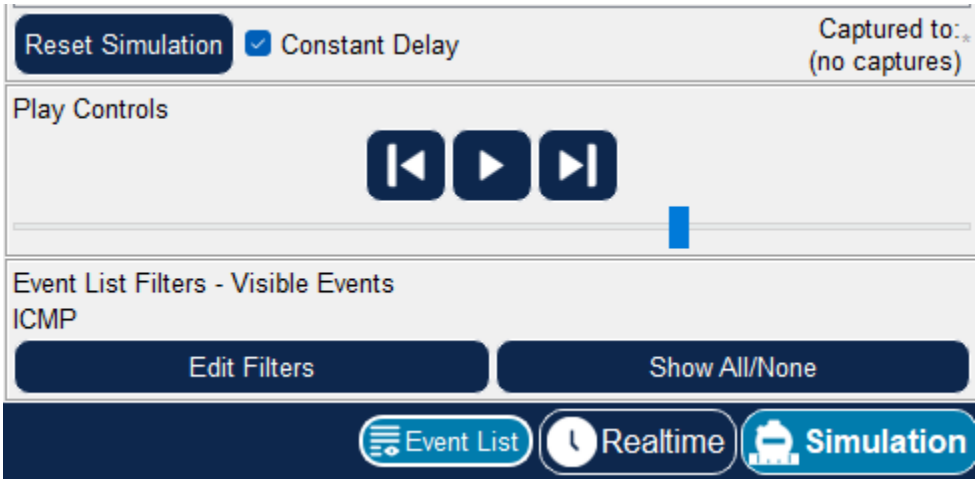


Step 2: On Main-Guest, open a web browser and access the website. (cisco.com: 10.3.3.2)

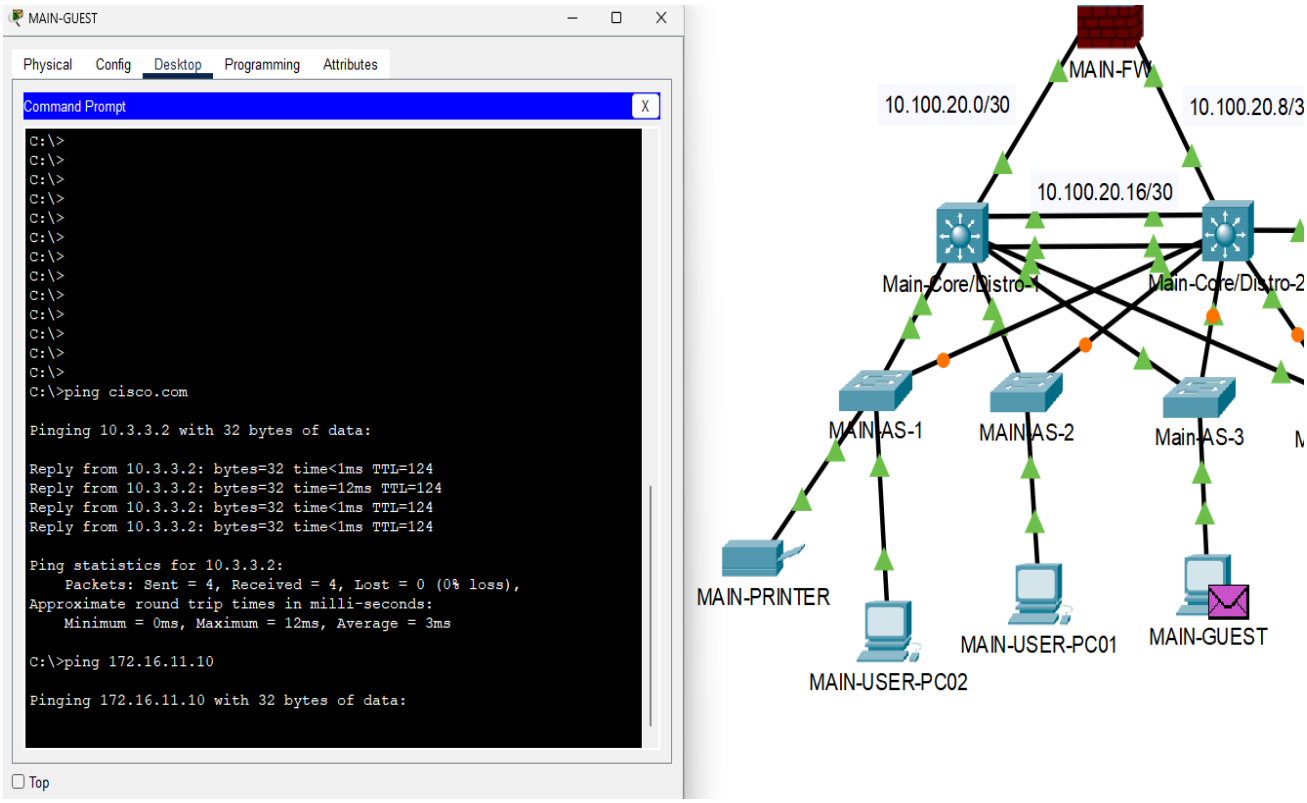


Main Guest Network No connectivity to Internal Networks

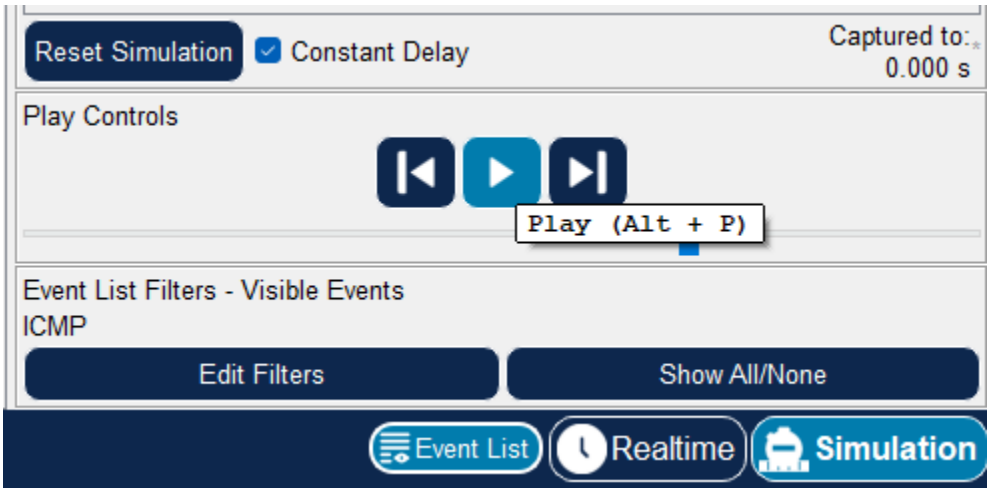
Step 3: Select simulation mode and filter for ICMP traffic.



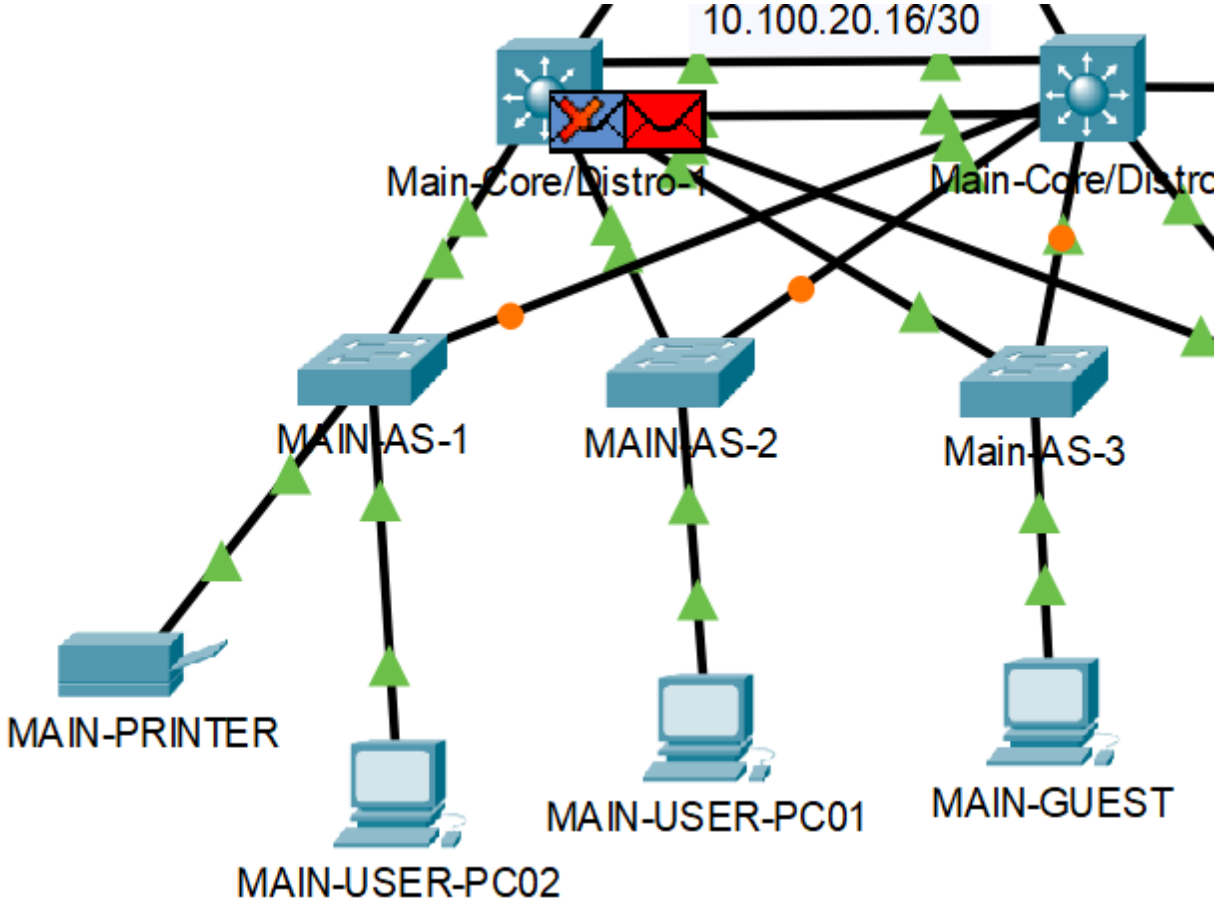
Step 4: On Main-Guest, open command prompt again and ping Main-User-PC01 (172.16.11.10).



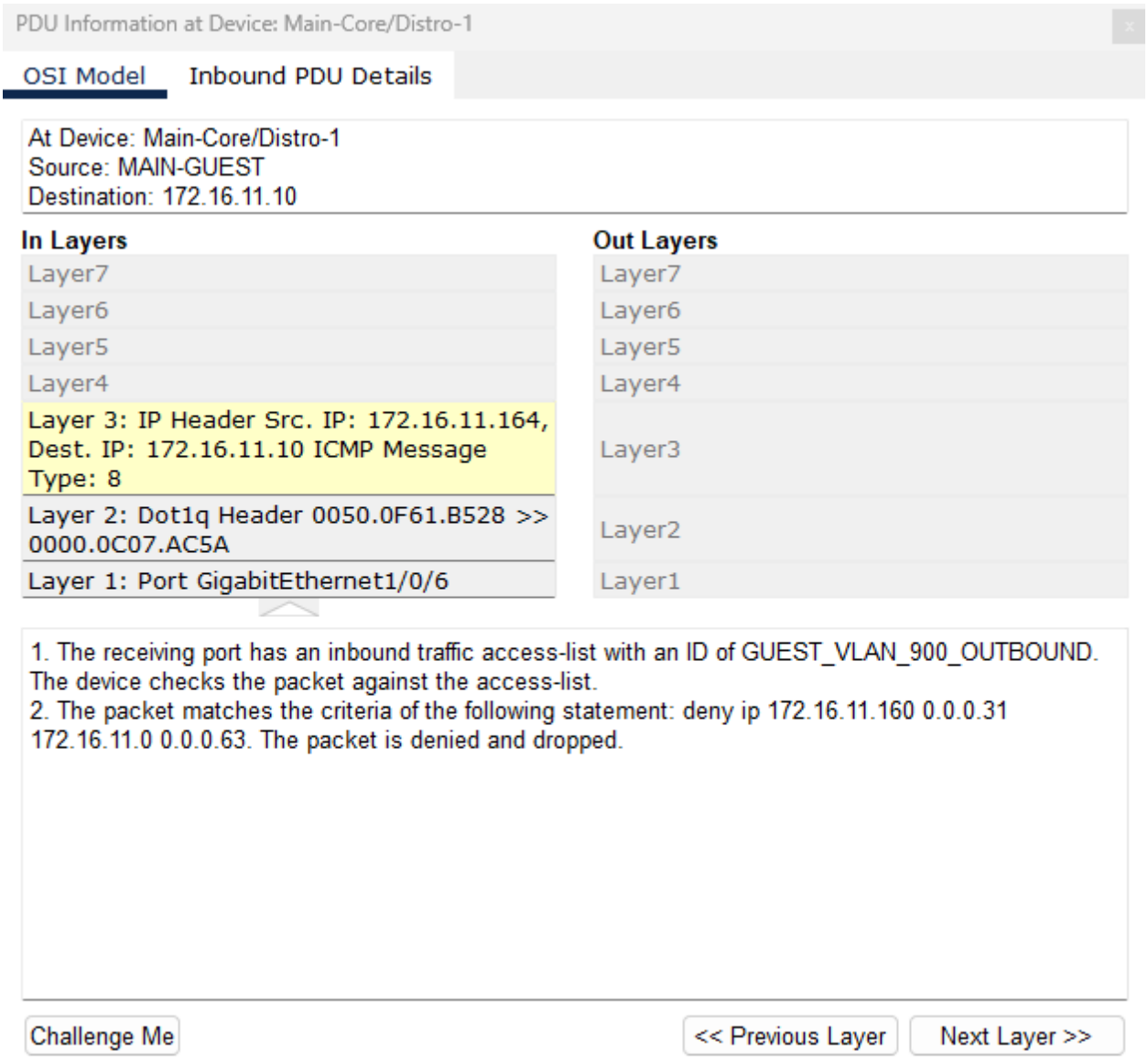
Step 5: Press play and watch the packet route.



Step 6: Press pause when packet reached Main-Core/Distro-1.



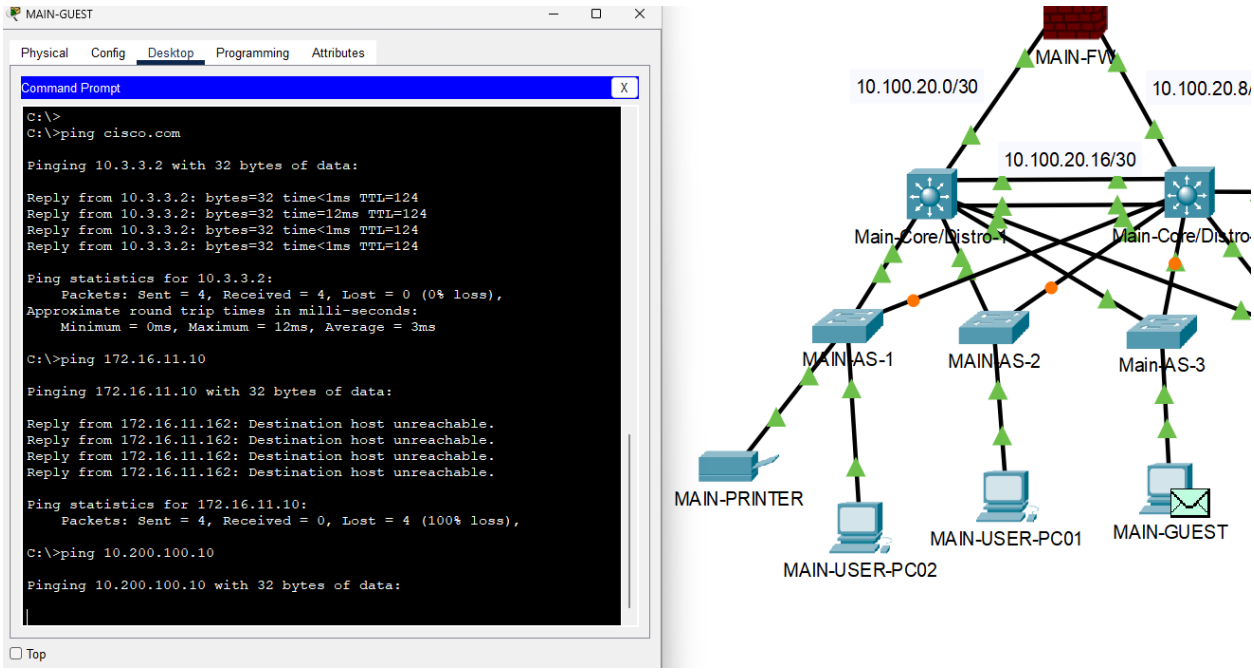
Step 7: Open PDU information. Last Device: Main-AS-3, At-Device: Main-Core/Distro-1. Switching to the layer 3 information panel, we can see the traffic being denied by the ACL rule.



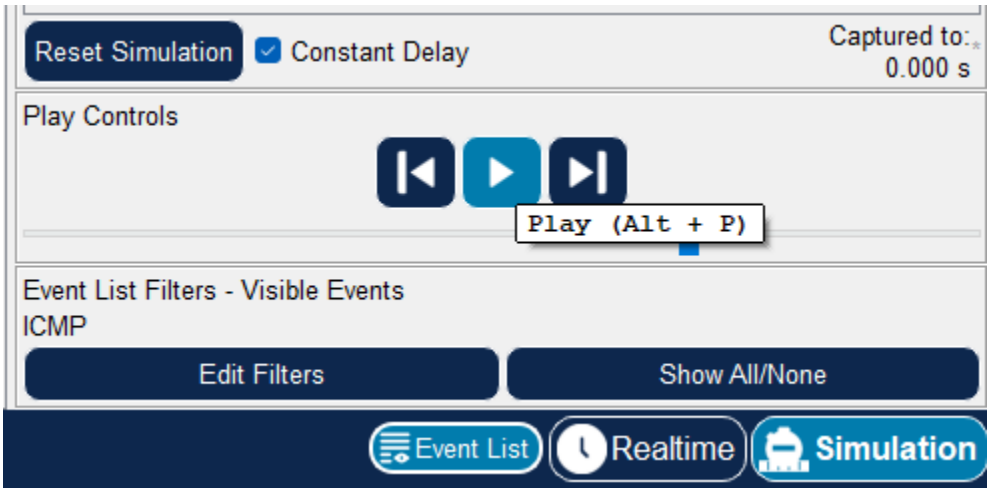
Main Guest Network No Access to Remote Network

Step 8: Select Realtime and let the ping complete, then return to simulation.

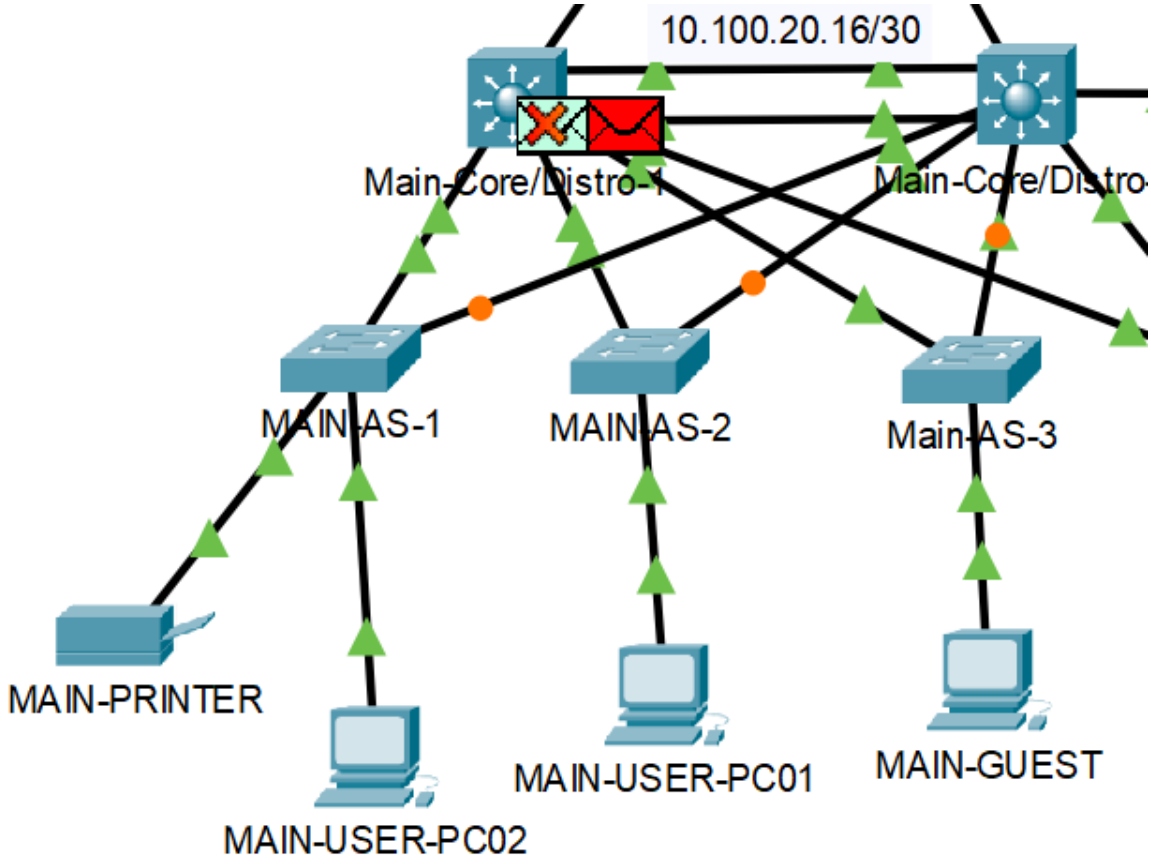
Step 9: On Main-Guest, open command prompt again and ping Remote-User (10.200.100.10).



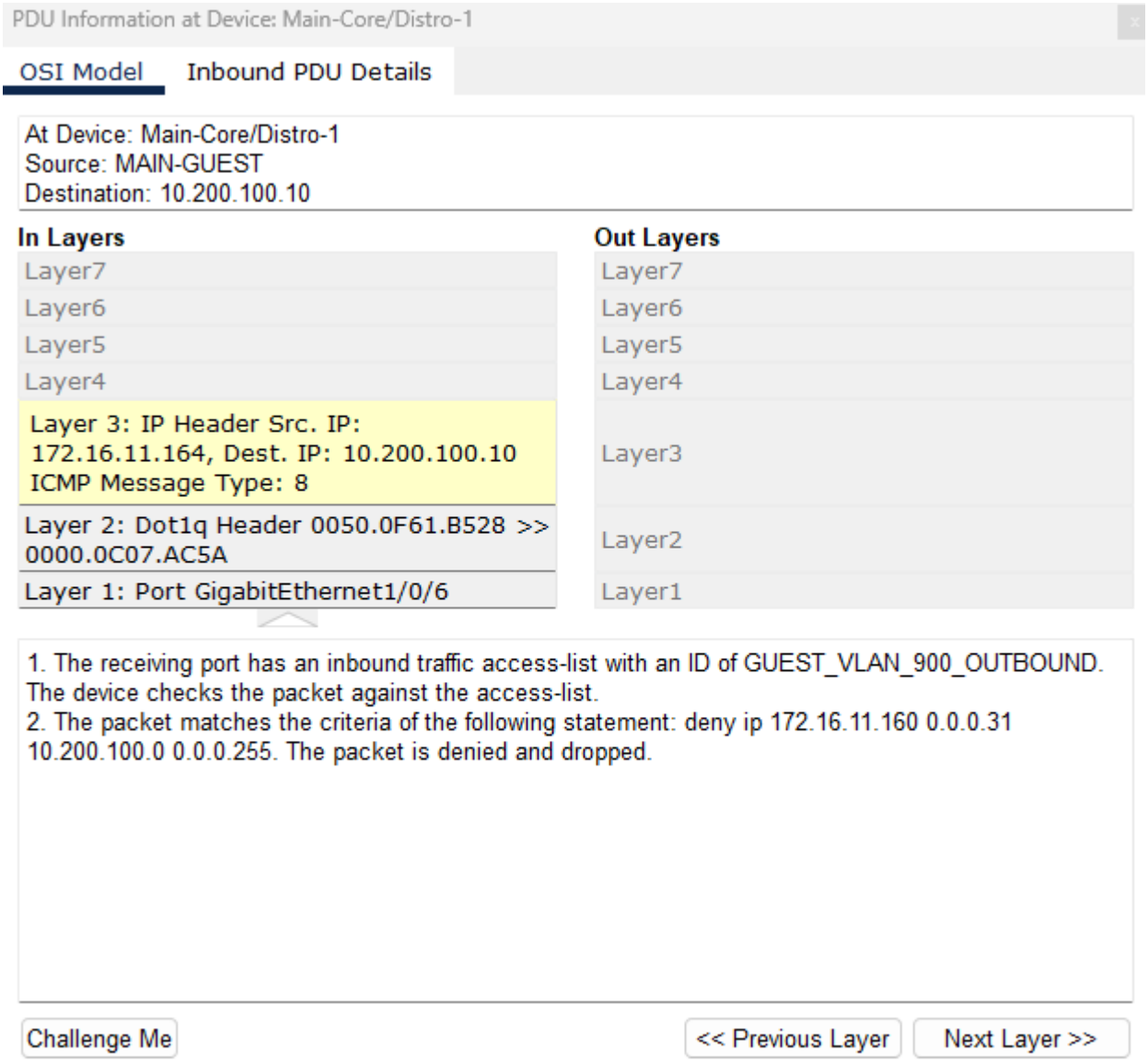
Step 10: Press play and watch the packet route.



Step 11: Press pause when packet reached Main-Core/Distro-1.



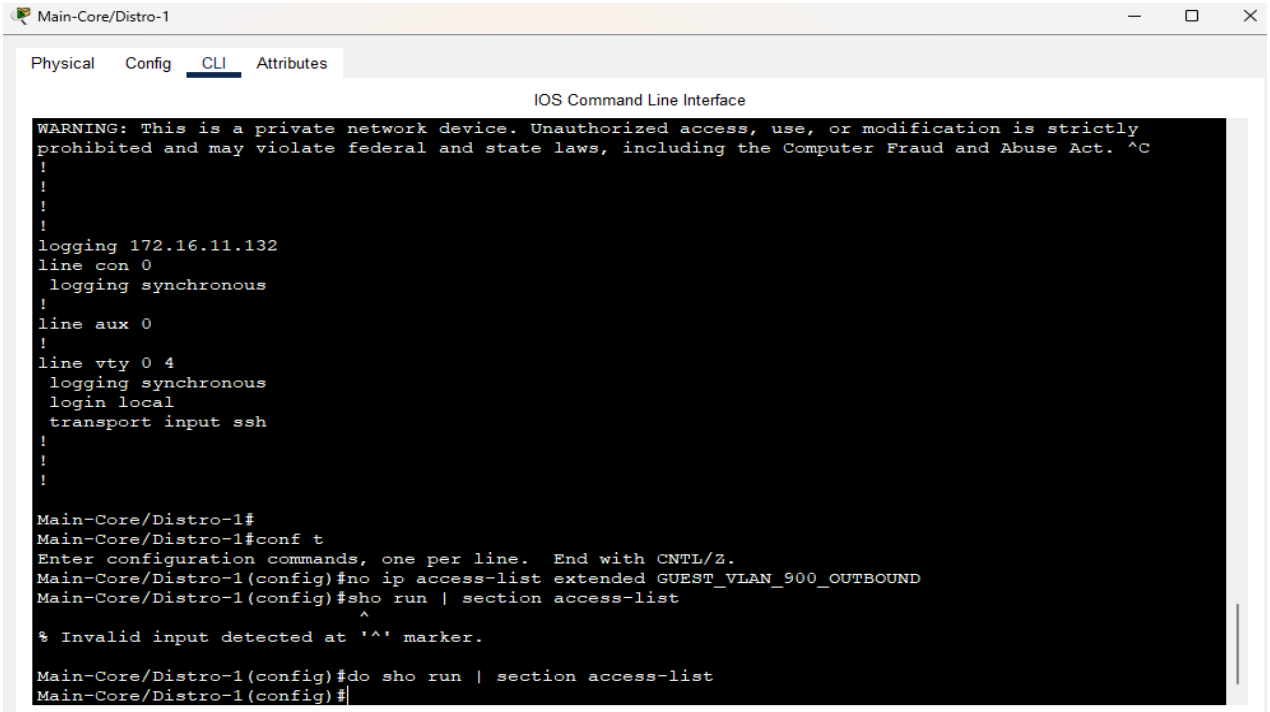
Step 12: Open PDU information. Last Device: Main-AS-3, At-Device: Main-Core/Distro-1. Switching to the layer 3 information panel, we can see the traffic being denied by the ACL rule.

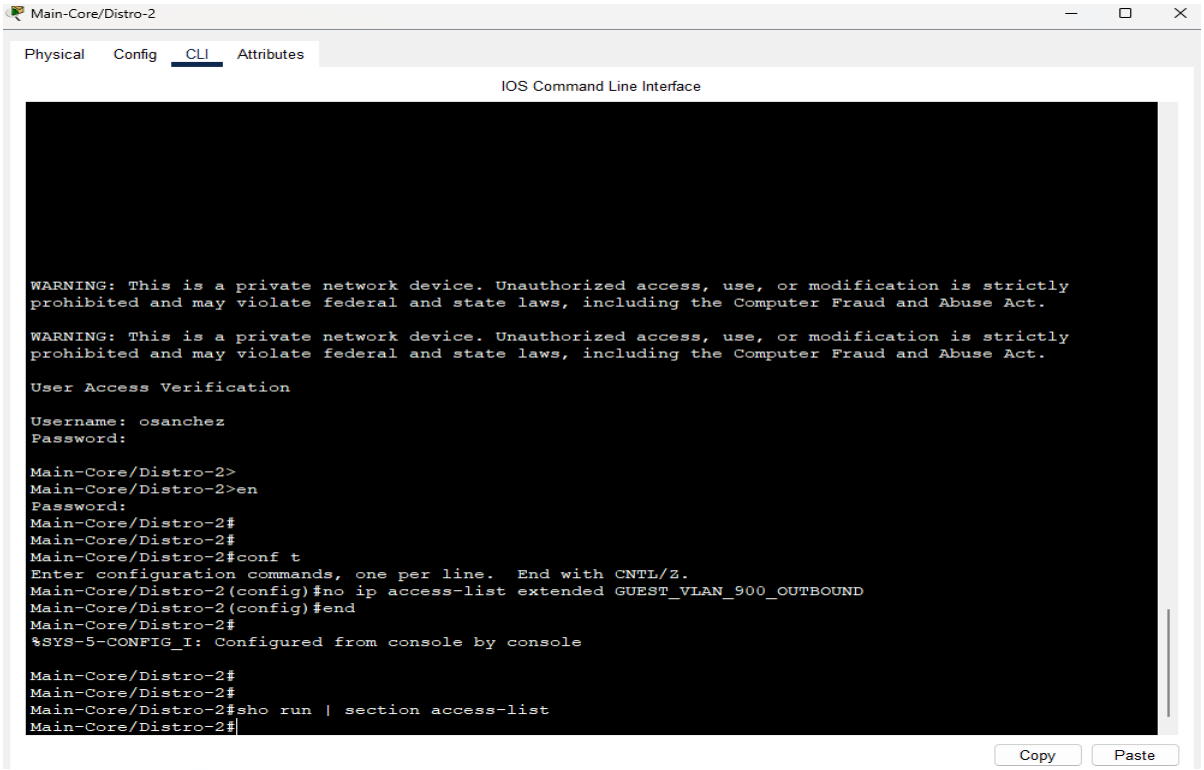


Temporarily Remove ACL. Further demonstration of ACL functionality.

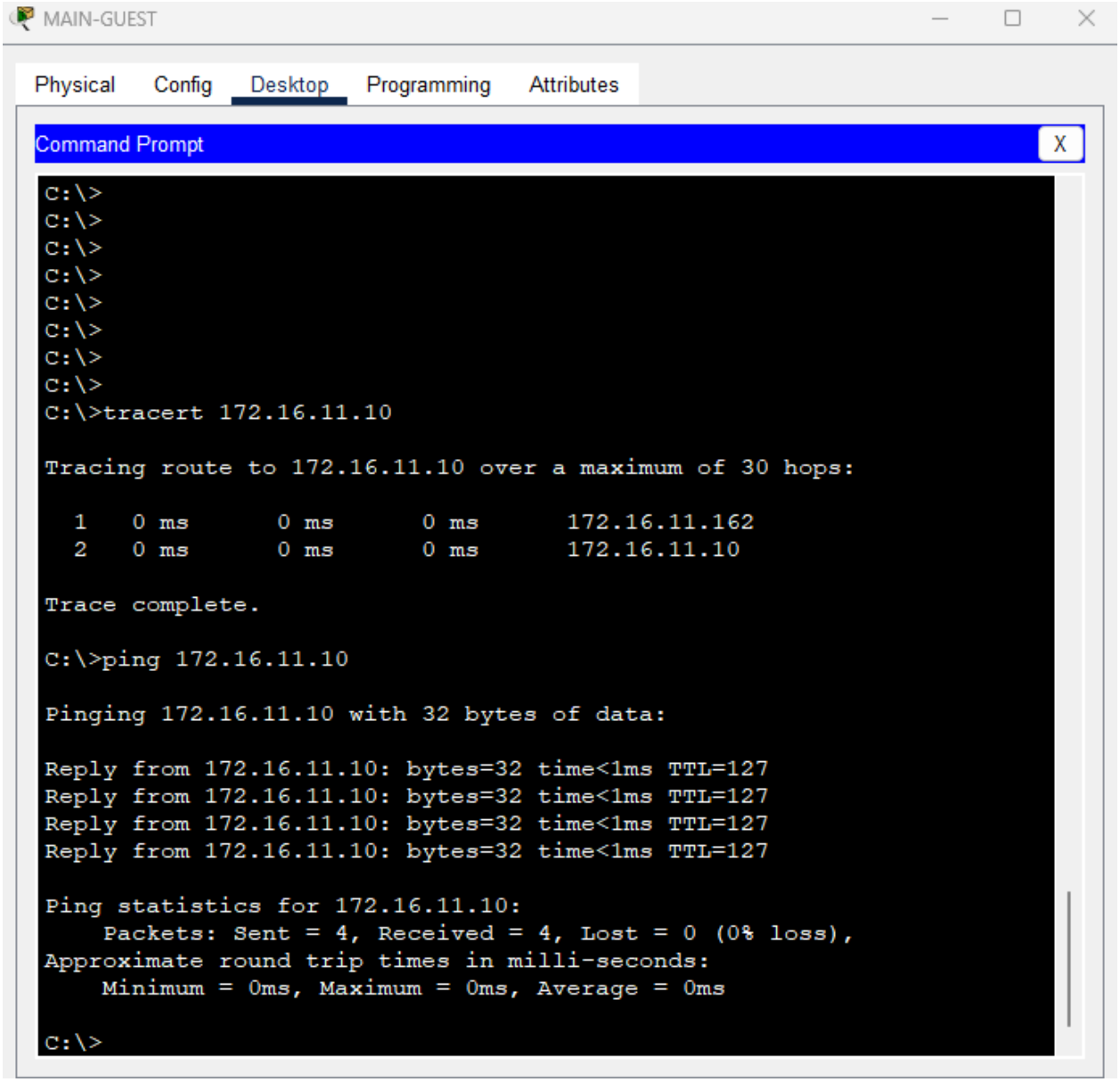
Step 13: Login to both Main-Core/Distro-1 and 2. Login and remove the ACL with the command:

<no ip access-list extended GUEST_VLAN_900_OUTBOUND>

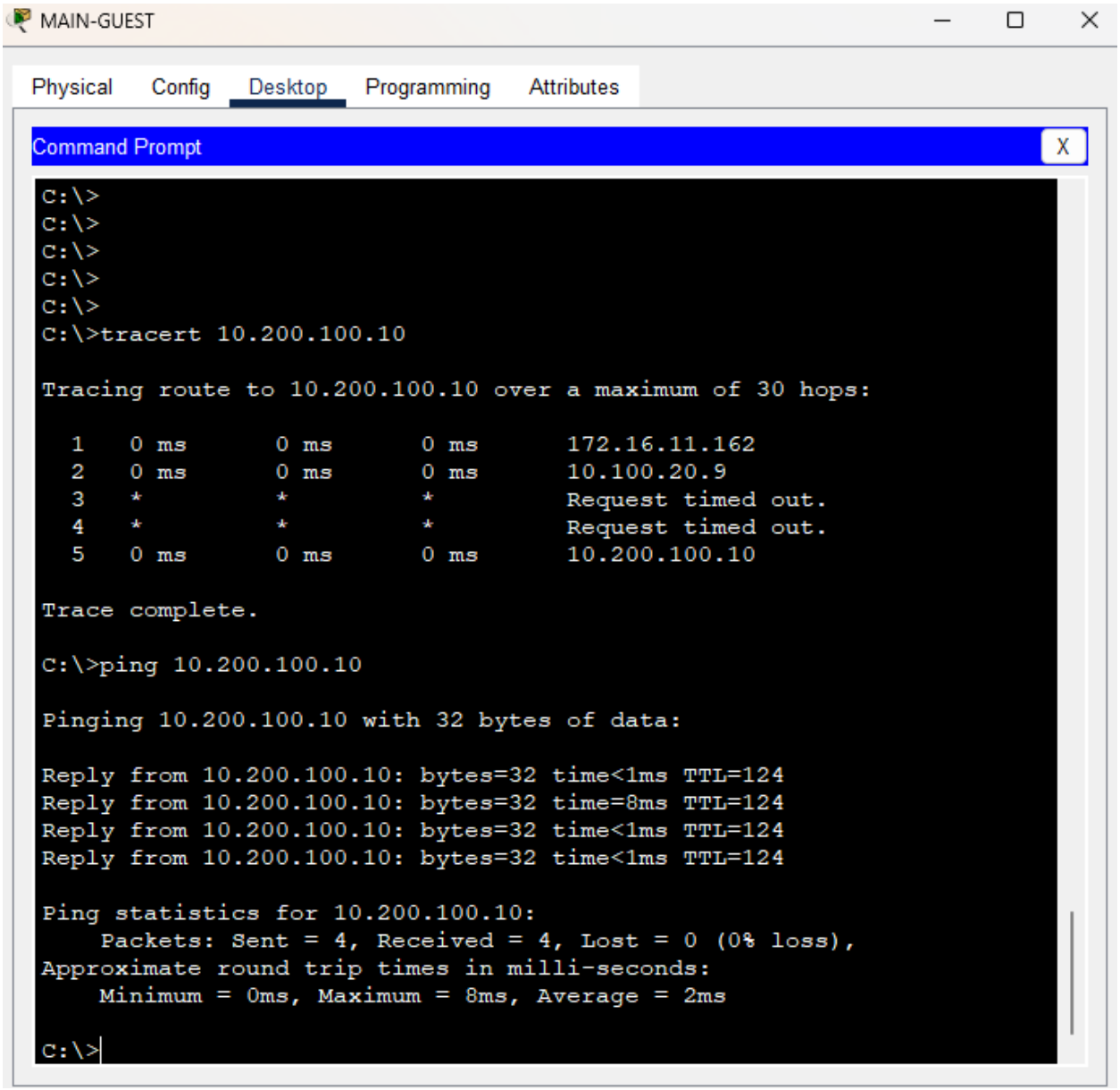




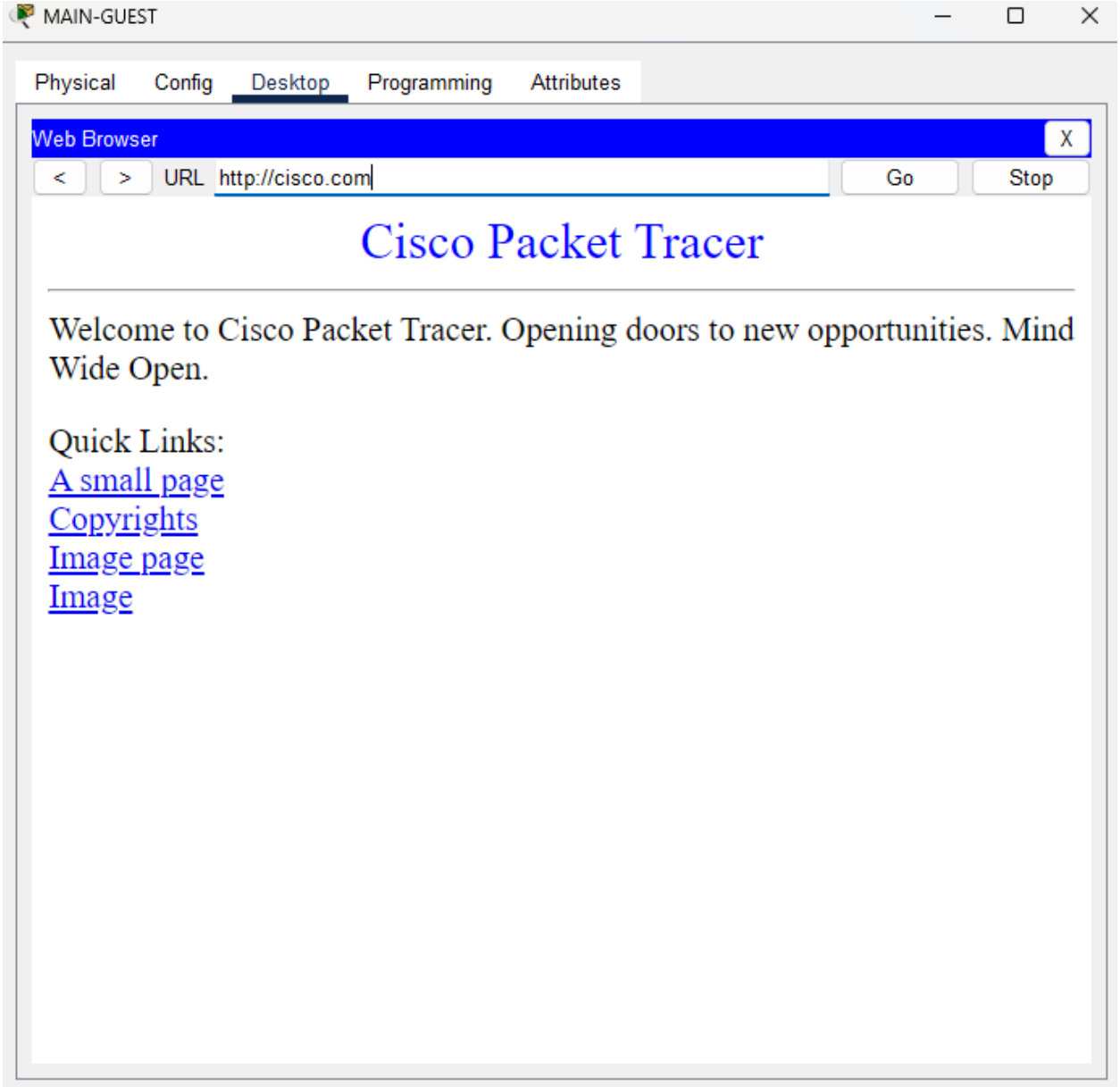
Step 14: On Main-Guest, open the command prompt to use “tracert” and “ping” commands to Main-User-PC01 (172.16.11.10).



Step 15: On Main-Guest open the command prompt to use “tracert” and “ping” commands to Remote-Main-PC (10.200.100.10).



Step 16: On Main-Guest, open the web browser and visit cisco.com (10.3.3.2).



Step 17: Re-apply the ACL on both L3 switches again to secure the guest network.

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

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 log into the 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.*

Functionally, this test will comprise logging into the device and showing the configuration where the banner message is stored in each device. Every device in the network must have a matching login banner displaying a warning message that describes the acceptable use policy (AUP). The warning message used is:

For devices that support banner login and banner motd:

banner login

Network Development Learning Center - Authorized Access Only.

Use of this system constitutes acceptance of AUP-NDLC-01. All activity may be monitored. Unauthorized access is strictly prohibited.

banner motd

WARNING: This is a private network device. Unauthorized access, use, or modification is strictly prohibited and may violate federal and state laws, including the Computer Fraud and Abuse Act.

For devices that only support banner motd:

banner motd

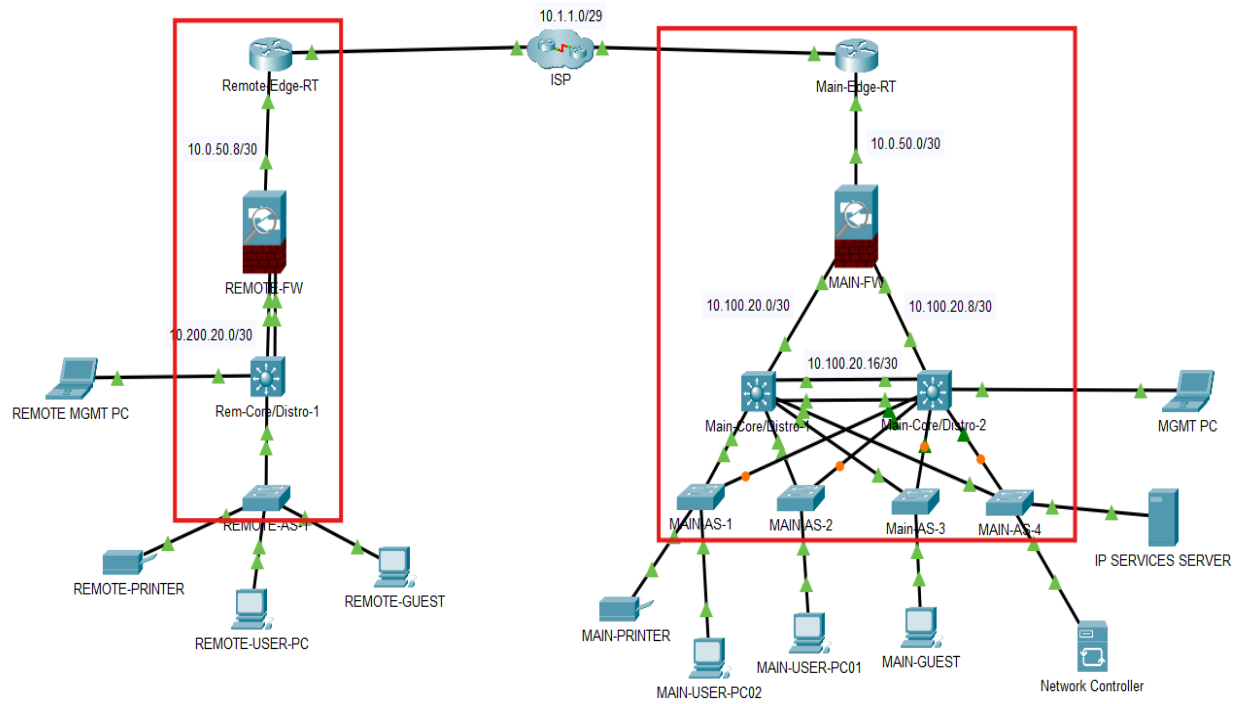
Network Development Learning Center - Authorized Access Only.

Use of this system constitutes acceptance of AUP-NDLC-01. All activity may be monitored. Unauthorized access is strictly prohibited.

Note: A character limit in Packet Tracer prevents an admin from writing a complete and all-encompassing message.

Network Diagram or Segment

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



Legend	
IP	Internet Protocol
RT	Router
AS	Access Switch
Main	Main Office
Remote	Remote Office
MGMT	Management
FW	Firewall
SW	Switch
REM	Remote
PC	Personal Computer
Distro	Distribution Switch
ISP	Internet Service Provider

Testing Method

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

This document demonstrates the behavior of logging into a device to show the banner message and its appearance. Each device will then be checked to verify that it has the correct banner message in the running configuration. The process for logging in will be the same throughout.

All device configurations will be shown and validated. The device used to demonstrate this example is Main-Core/Distro-1.

To verify the configuration, log in to a network device, enter privileged configuration mode, and run the following command:

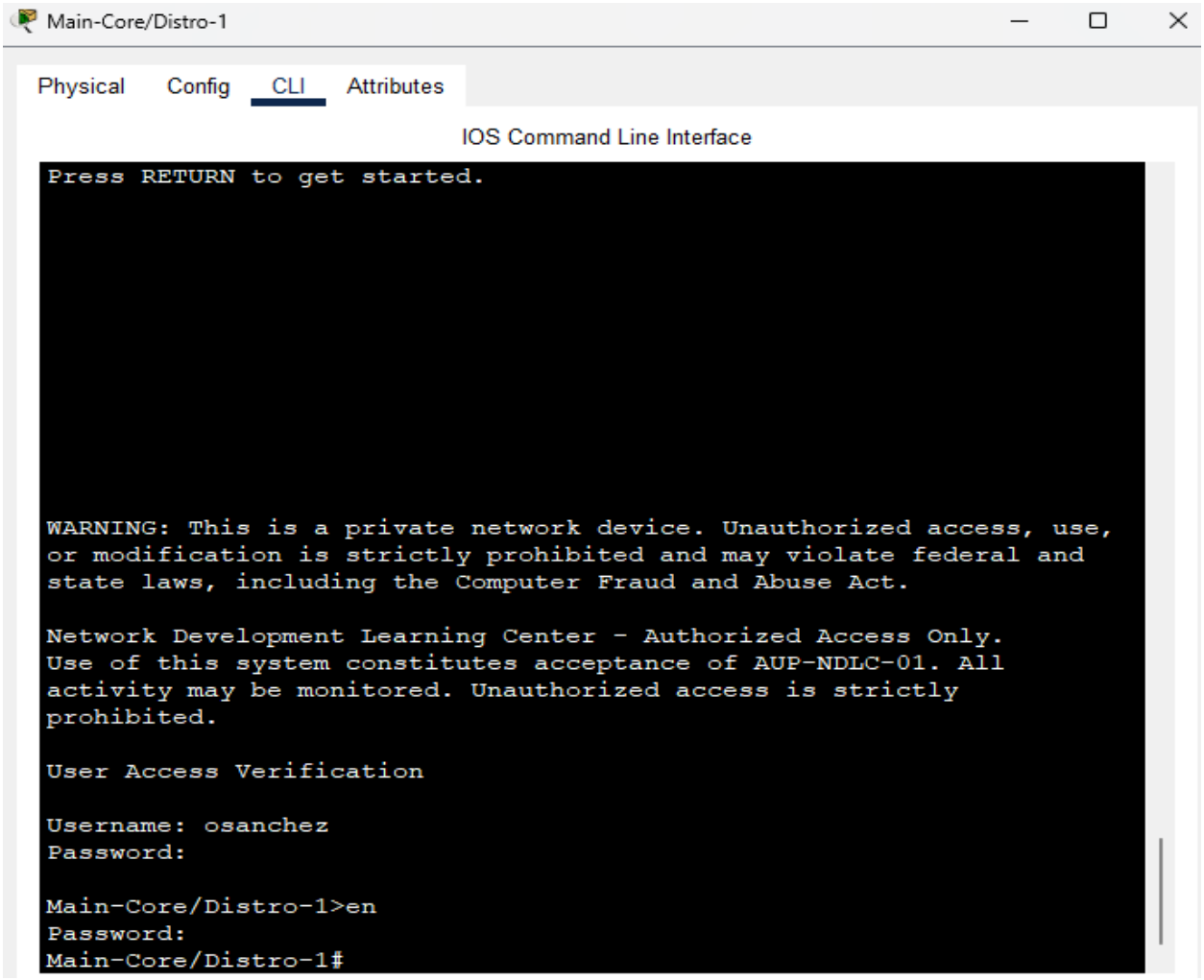
Example# show running-configuration | begin banner

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.*

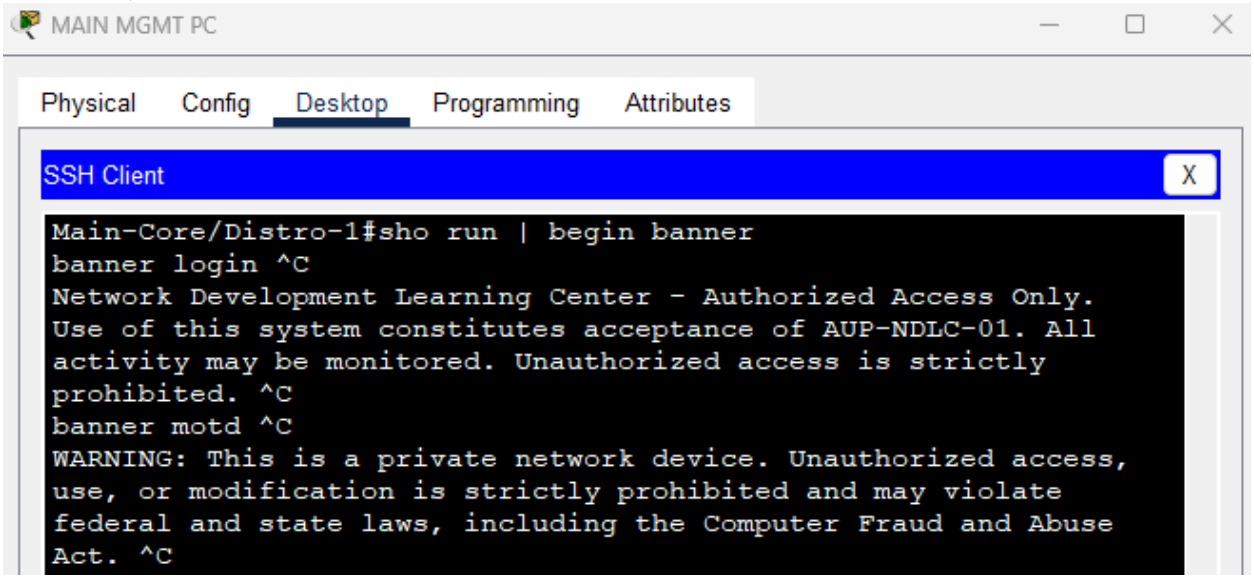
Login Behavior on Main-Core/Distro-1

Step 1: Access Main-Core/Distro-1 and visit its CLI.

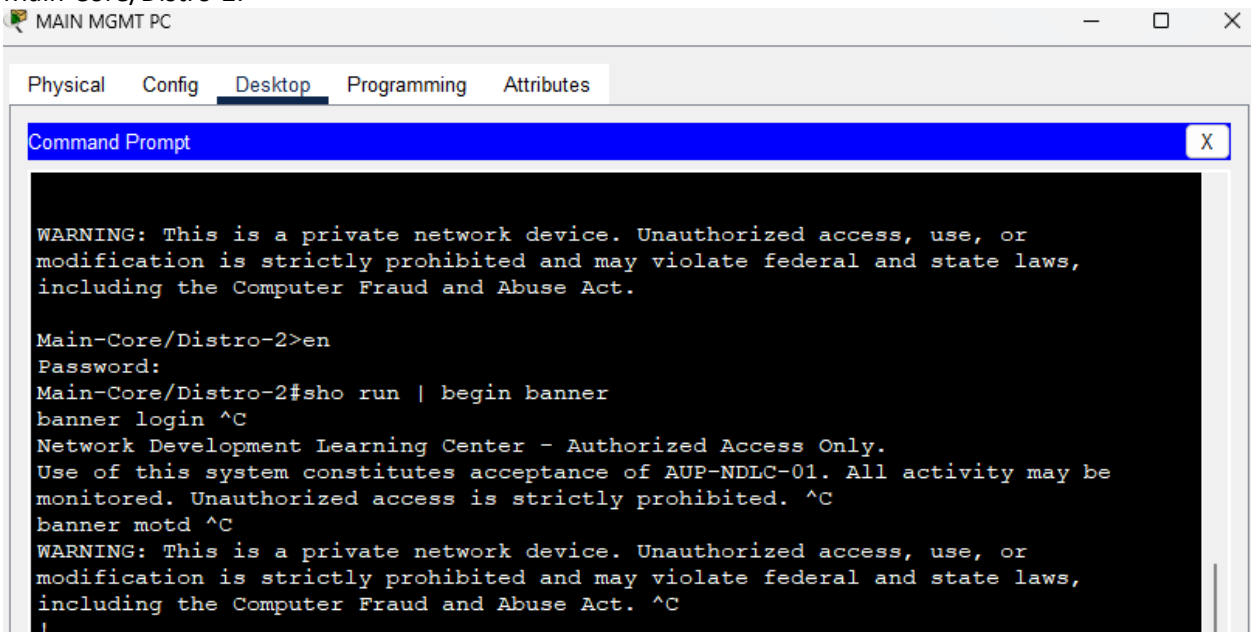


Show Banner Configurations

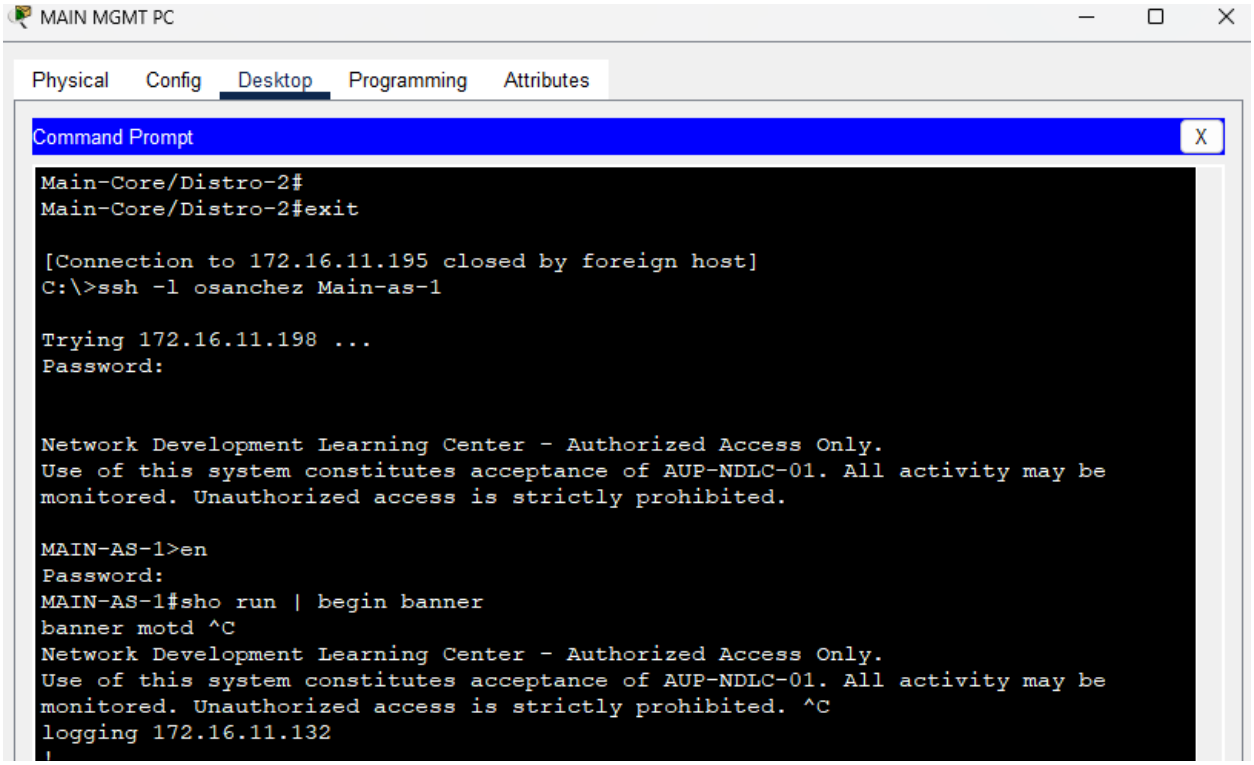
Main-Core/Distro-1:



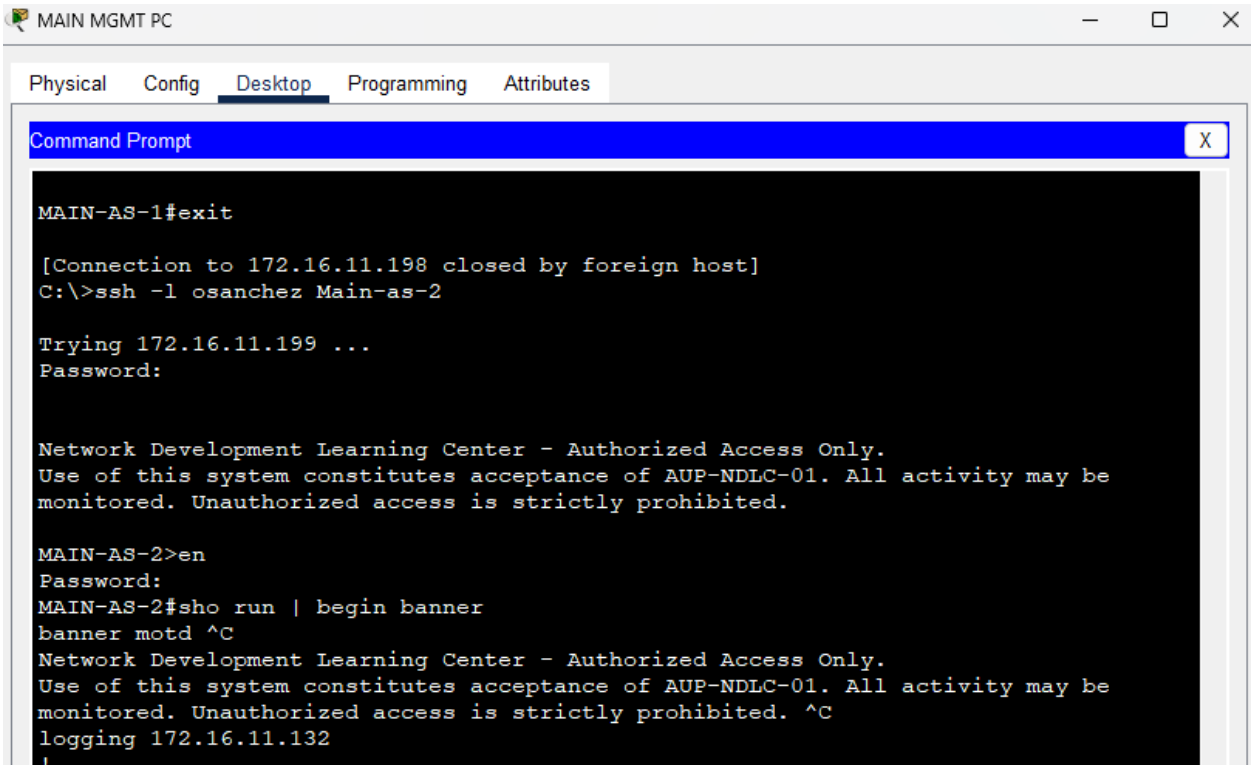
Main-Core/Distro-2:



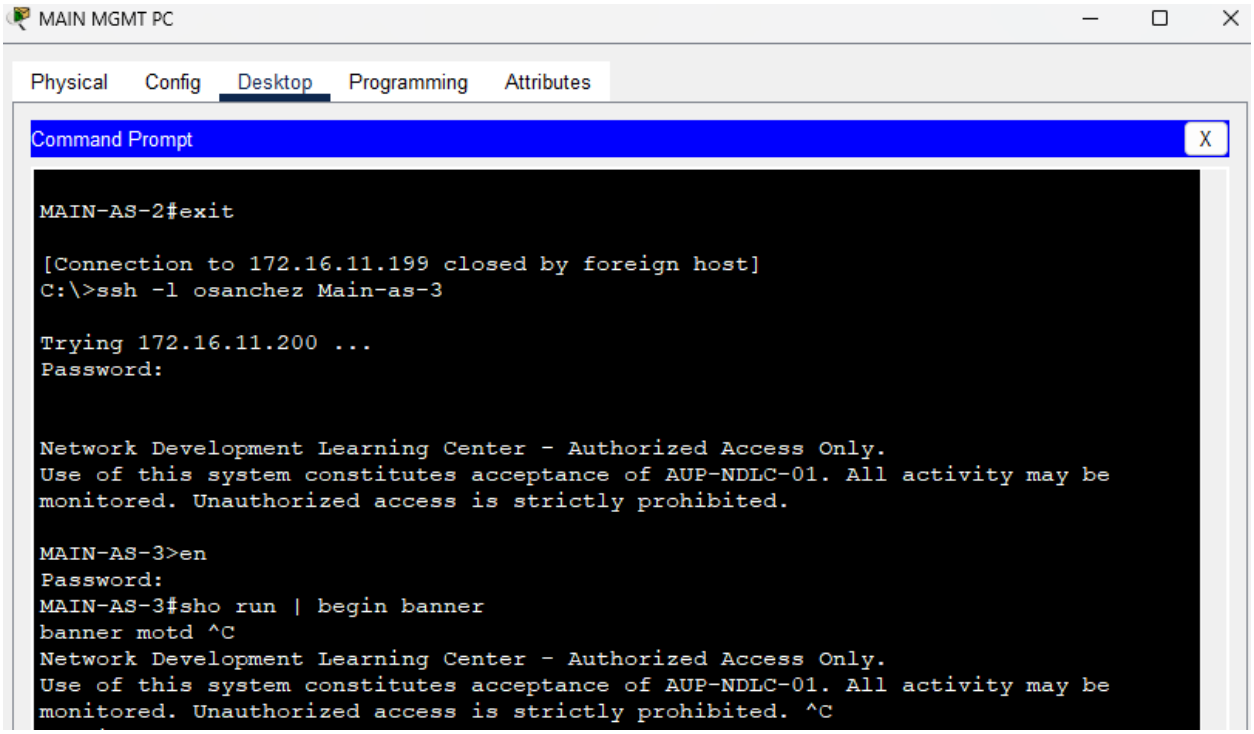
Main-AS-1:



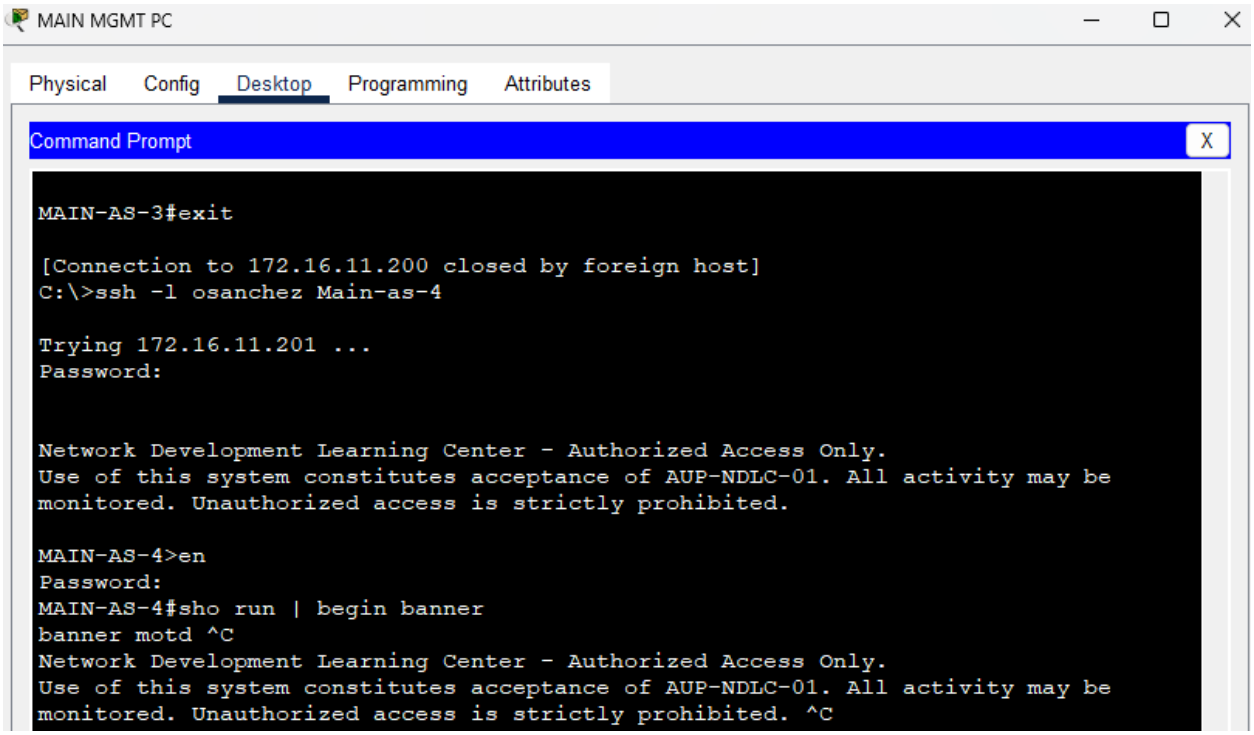
Main-AS-2:



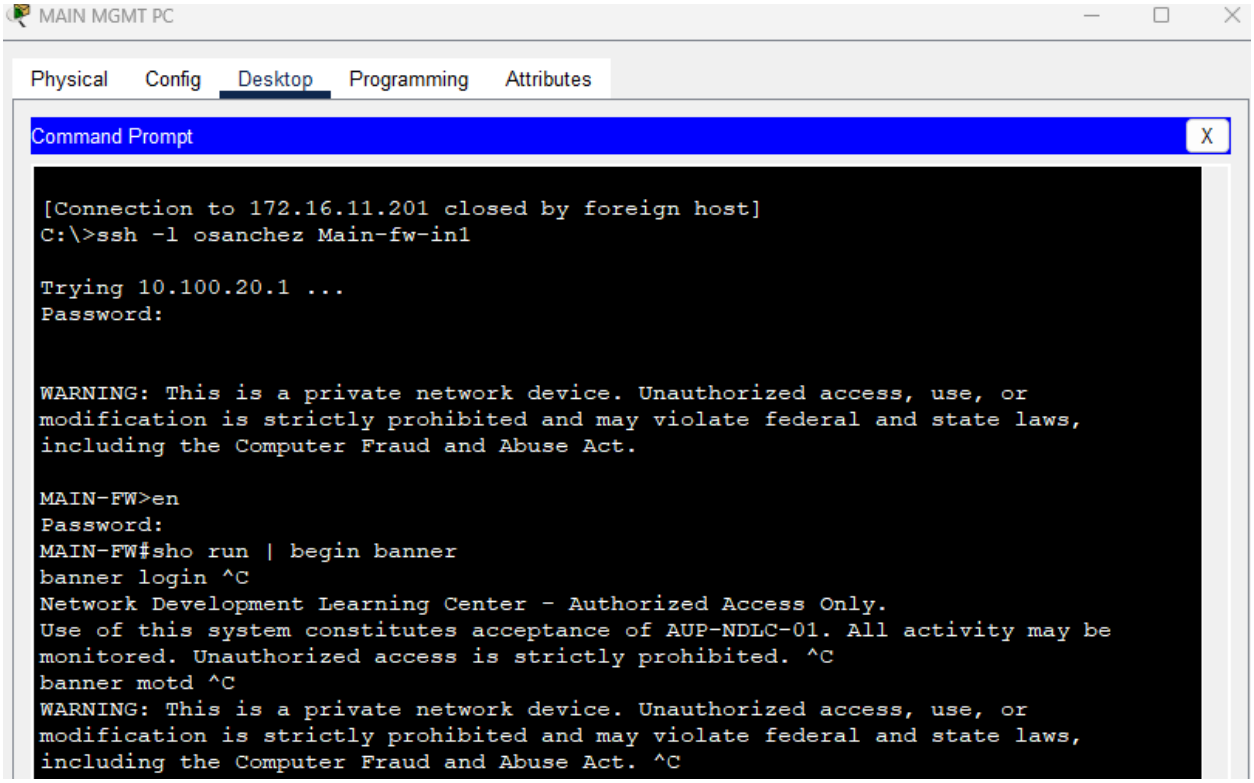
Main-AS-3:



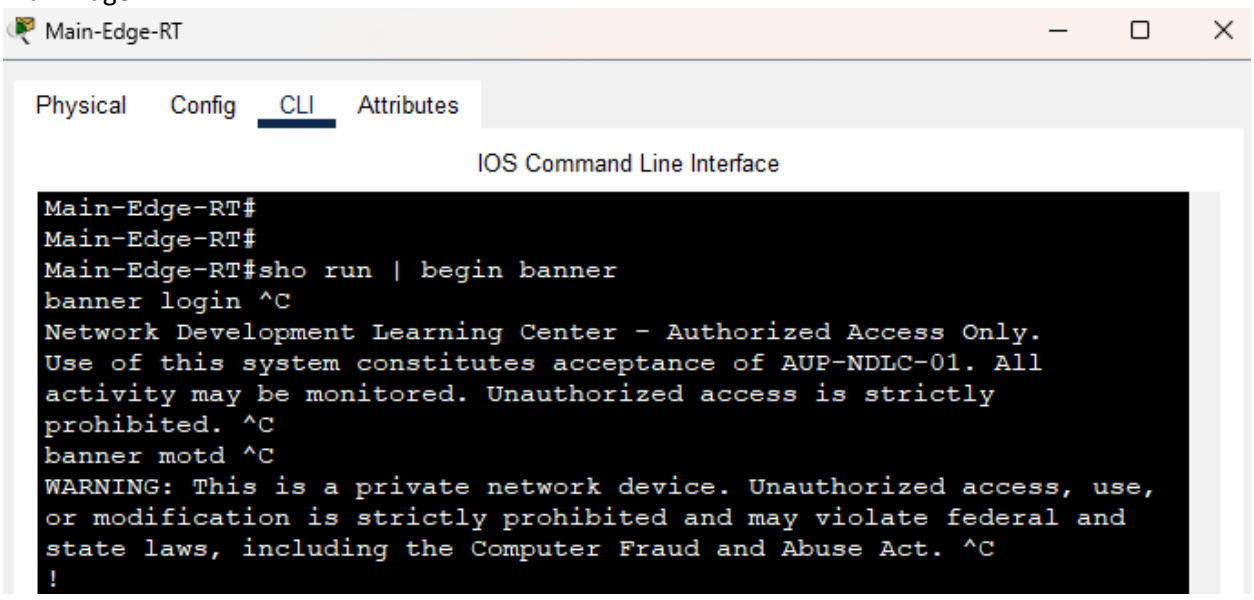
Main-AS-4:



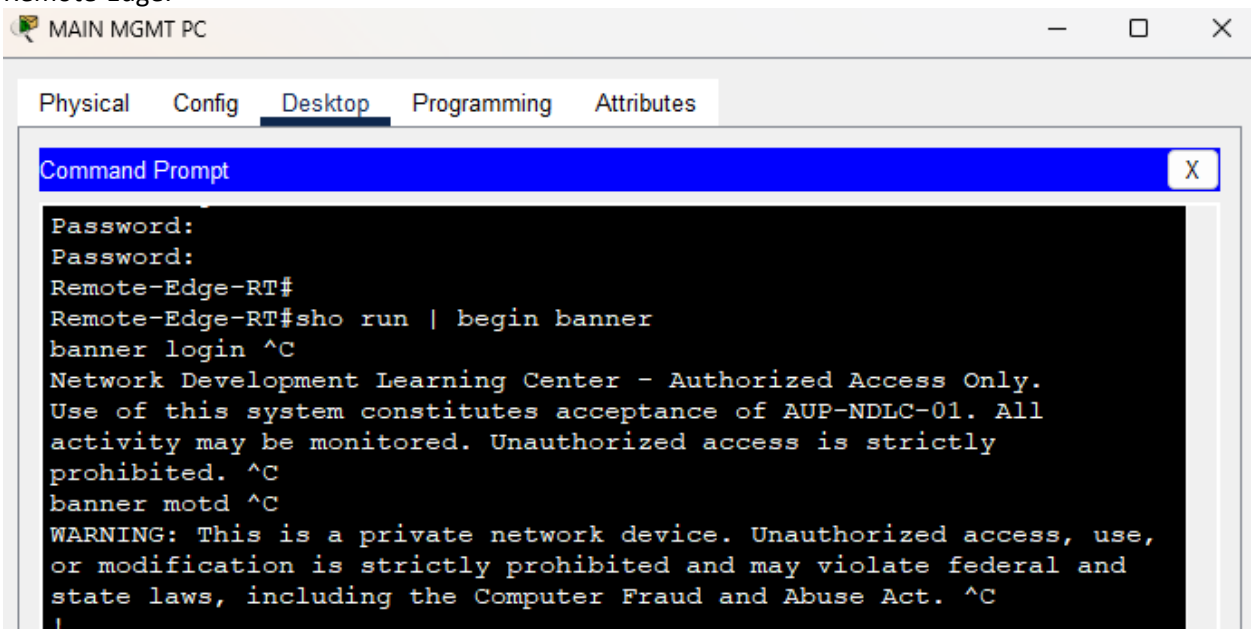
Main-FW:



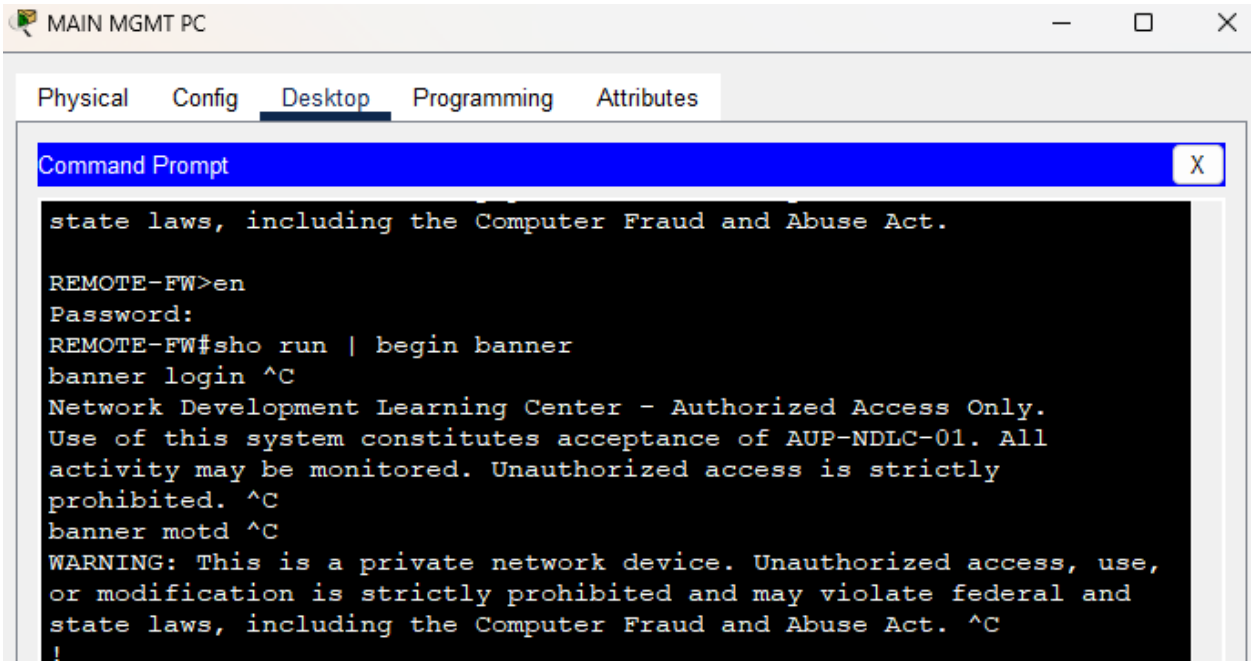
Main-Edge:



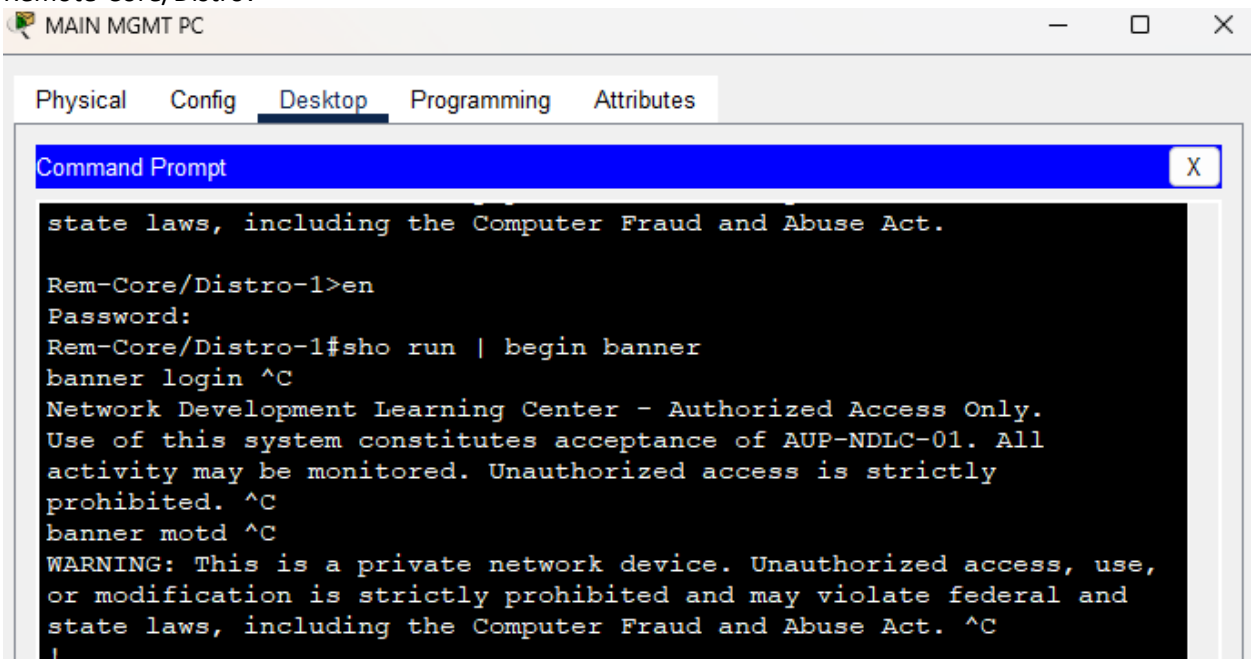
Remote-Edge:



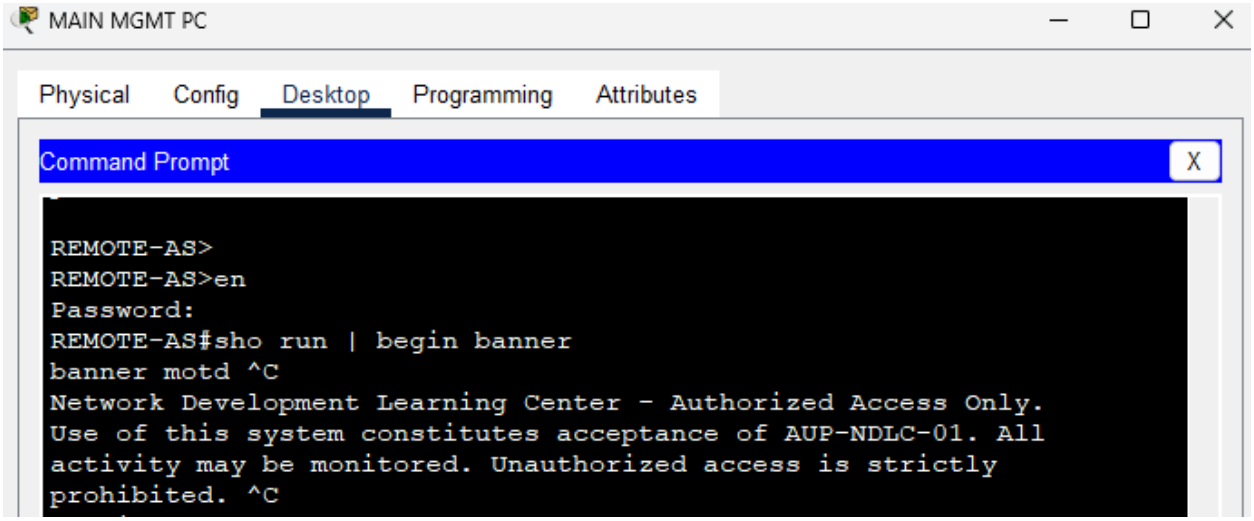
Remote-FW:



Remote-Core/Distro:



Remote-AS:



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.*

As part of the requirements of this network, User and Guest Vlan devices each utilize DHCP for client devices. This requirement applies to devices in the Main Office and the Remote Office. The IP Services Server provides DHCP leases to all devices based on the VLAN they are associated with. The Management, Services, and Printer VLAN networks each require a static network IP assignment for security reasons.

The VLAN interfaces are configured at each site's Core/Distro switches. At the Main Office site, each VLAN network is configured in an Active-Standby HSRP (Hot Standby Routing Protocol) status with Main-Core/Distro-1 acting as the primary/active gateway. This provides much-needed redundancy per the requirements listed. For the management network, each connected network equipment (e.g., routers, switches, firewalls) uses a static IP address that pertains to the VLAN 80 network.

DHCP Server Vlan 600 (STATIC)

IP Address: 172.16.11.132

Main Office User Vlan Network – 400 (DHCP)

Network: 172.16.11.0/26, Gateway IP: 172.16.11.1/26

Main Office Printer Vlan Network - 500 (STATIC)

Network: 172.16.11.64/26, Gateway IP: 172.16.11.65/26

Main Office Services Vlan Network – 600 (STATIC)

Network: 172.16.11.128/27, Gateway IP: 172.16.11.129/27

Main Office Guest Vlan Network – 900 (DHCP)

Network: 172.16.11.160/27, Gateway IP: 172.16.11.161/27

Main Office Management Vlan Network – 80 (STATIC)

Network: 172.16.11.192/28, Gateway IP: 172.16.11.193/28

Remote Office User Vlan Network – 400 (DHCP)

Network: 10.200.100.0/26, Gateway IP: 10.200.100.1/26

Remote Office Printer Vlan Network – 500 (STATIC)

Network: 10.200.100.64/26, Gateway IP: 10.200.100.65/26

Remote Office Services Vlan Network – 600 (STATIC)

Network: 10.200.100.128/27, Gateway IP: 10.200.100.129/27

Remote Office Guest Vlan Network – 900 (DHCP)

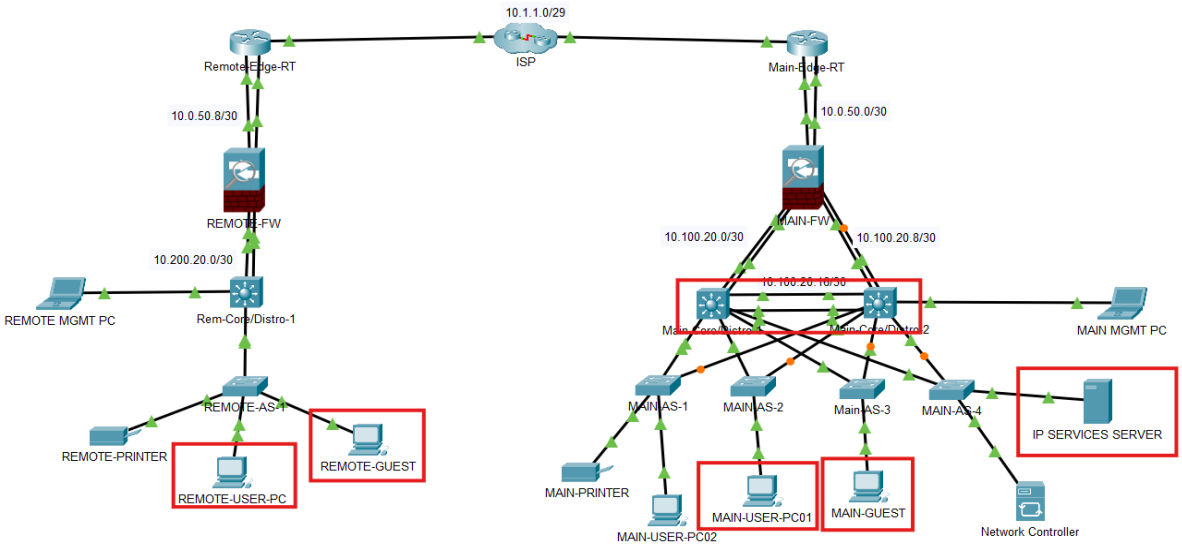
Network: 10.200.100.160/27, Gateway IP: 10.200.100.161/27

Remote Office Management Vlan Network – 80 (STATIC)

Network: 10.200.100.192/27, Gateway IP: 10.200.100.193/27

Network Diagram or Segment

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



Legend	
IP	Internet Protocol
RT	Router
AS	Access Switch
Main	Main Office
Remote	Remote Office
MGMT	Management
FW	Firewall
SW	Switch
REM	Remote
PC	Personal Computer
Distro	Distribution Switch
ISP	Internet Service Provider

Testing Method

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

This test will be three simple phases. First, we will test various devices across the Main and Remote Office networks for DHCP services. We will log in to the following four devices and request a new IP address from the IP Services Server (DHCP Server). This test will prove that the DHCP request is working.

Testing Devices:

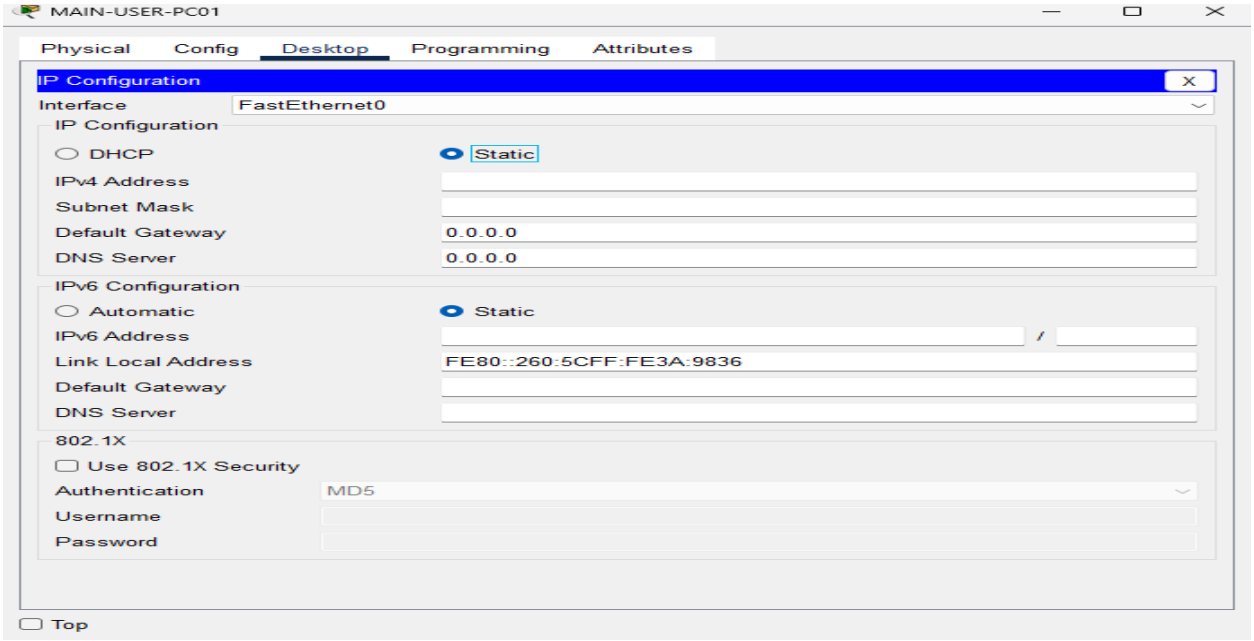
MAIN-USER-PC01, MAIN-GUEST, REMOTE-USER-PC, REMOTE-GUEST-PC

Next, we will run a DHCP request from the Remote Office network and evaluate the packet path as it travels across the VPN tunnel to the DHCP Server, and the request is complete. Lastly, we will see the configuration for the User and Guest network gateways, showing the IP Helper address, thus verifying that only the Guest and User networks utilize DHCP for connectivity.

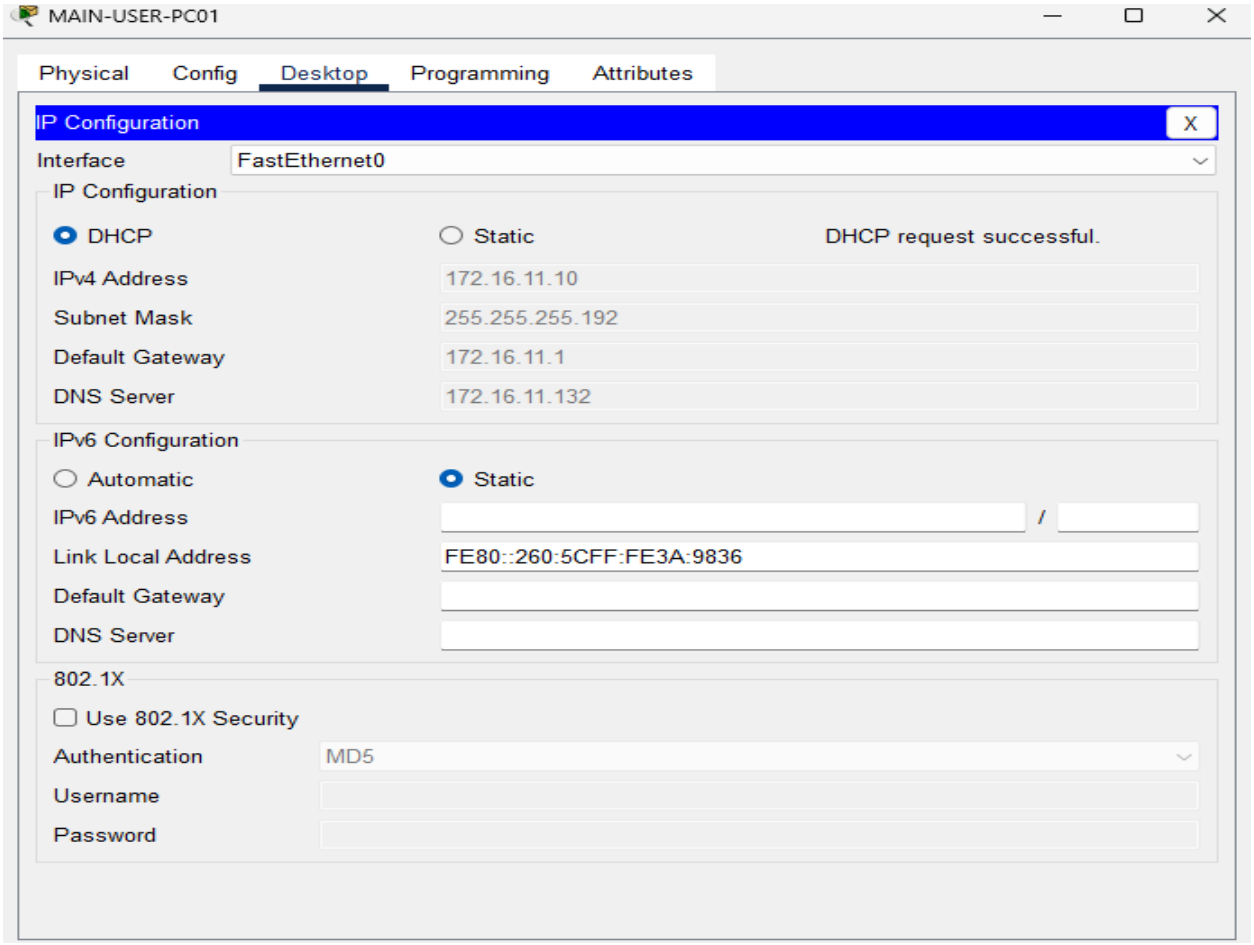
Process List

*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.*

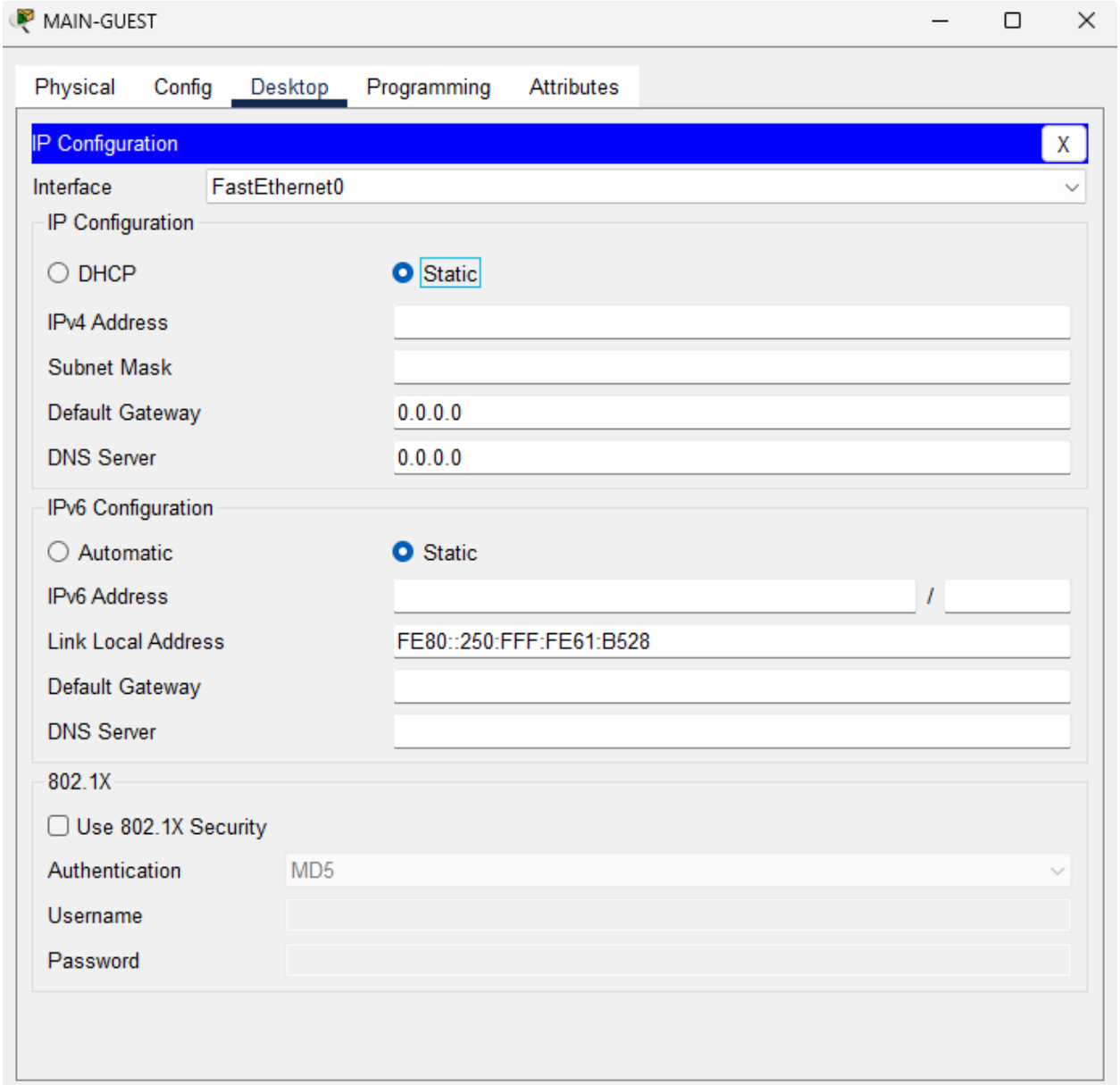
Step 1: On MAIN-USER-PC01, open the Desktop and enter IP Configuration, click the Static radio button.



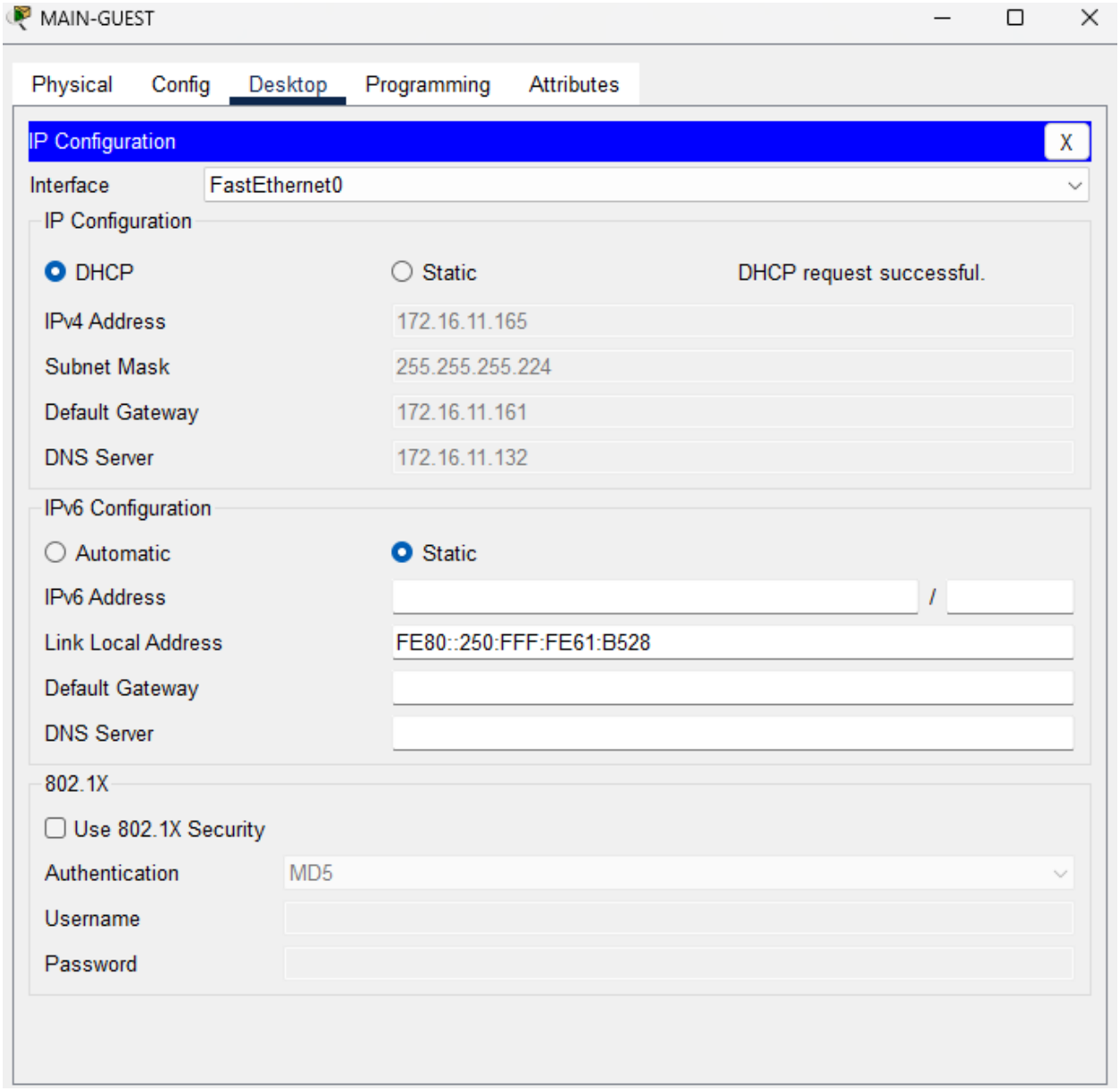
Step 2: Select the DHCP radio button and verify the IP address is part of Vlan 400.



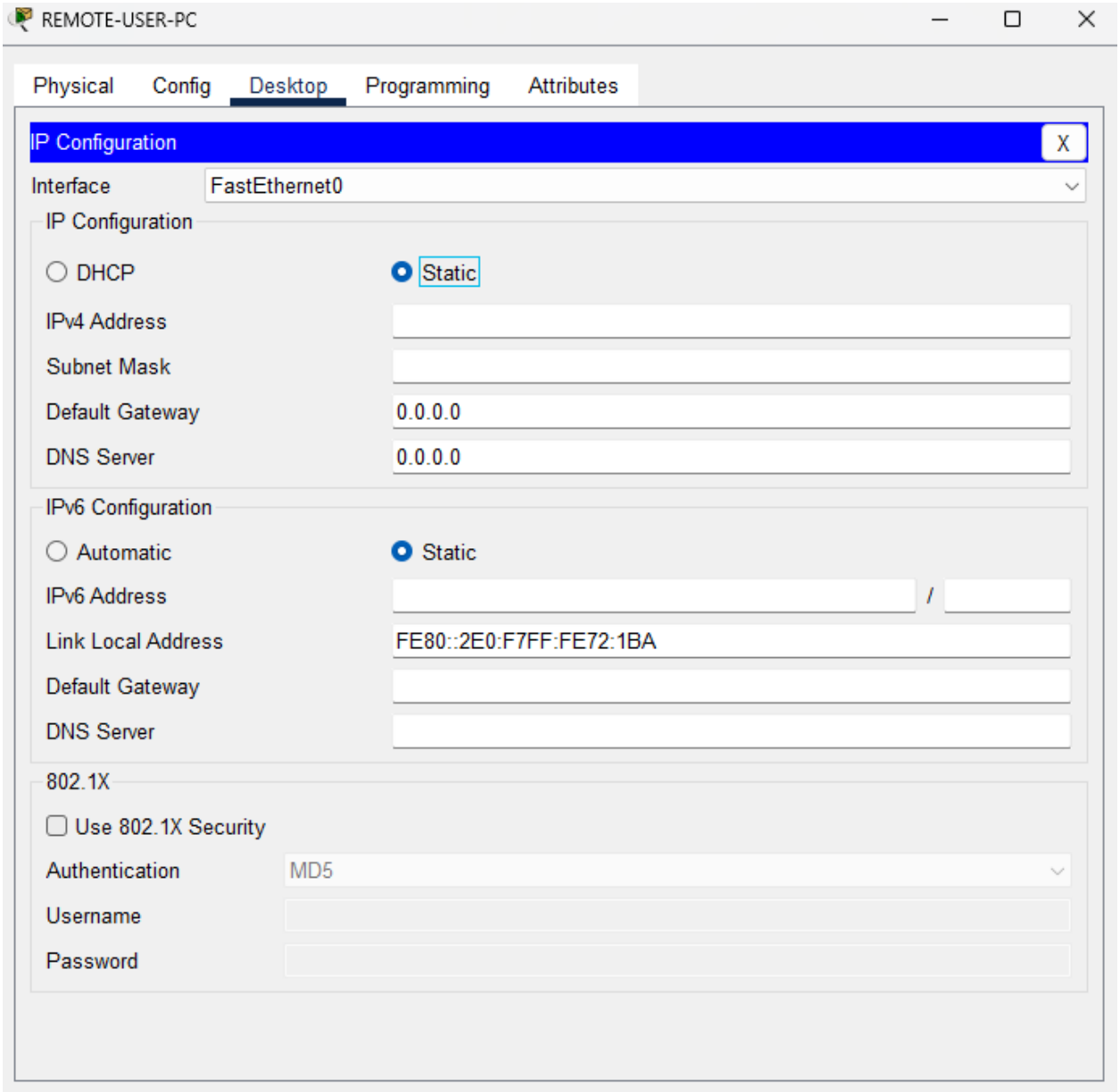
Step 3: On MAIN-GUEST, open the Desktop and enter IP Configuration, click the Static radio button.



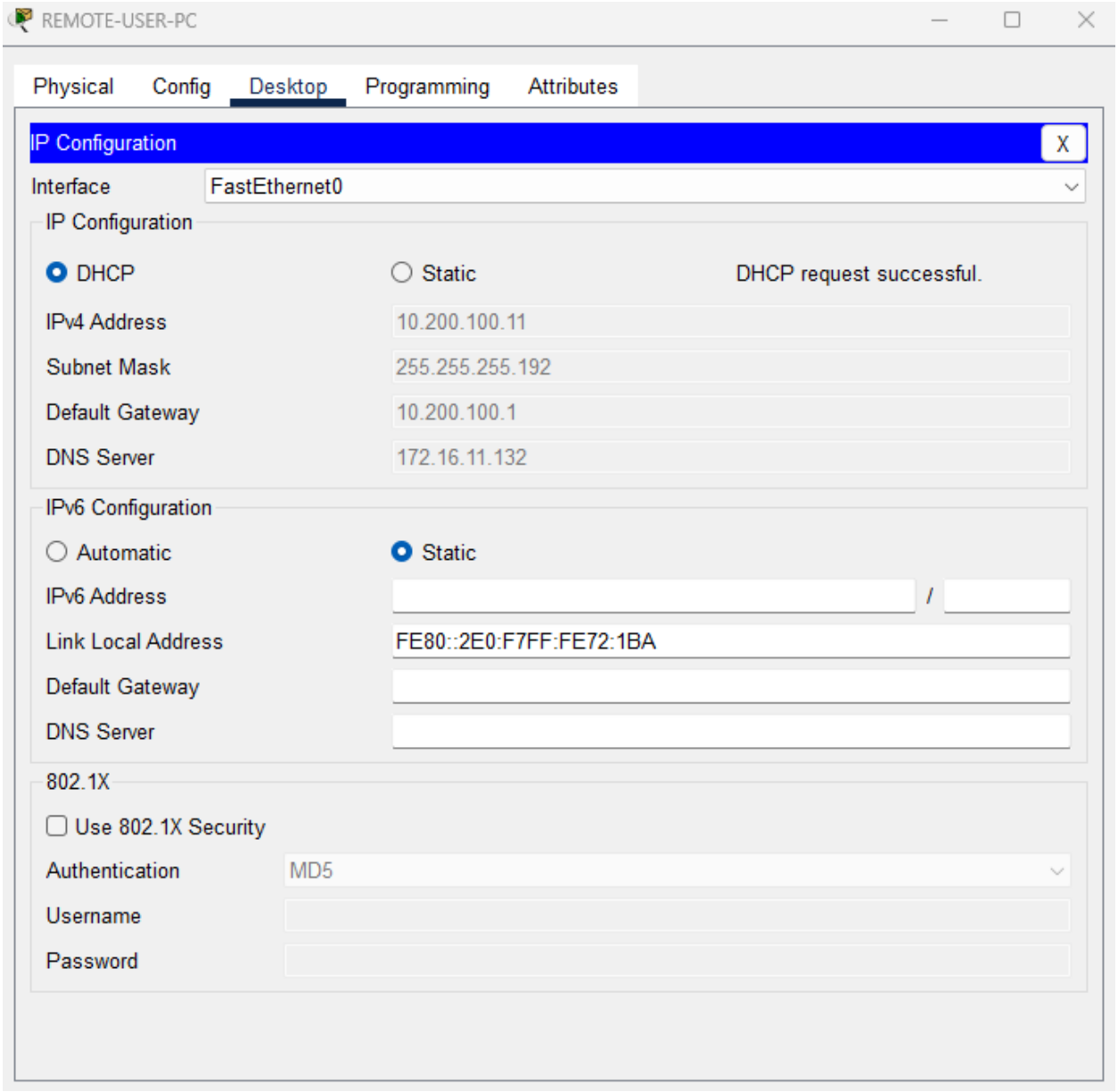
Step 4: Select the DHCP radio button and verify the IP address is part of Vlan 900.



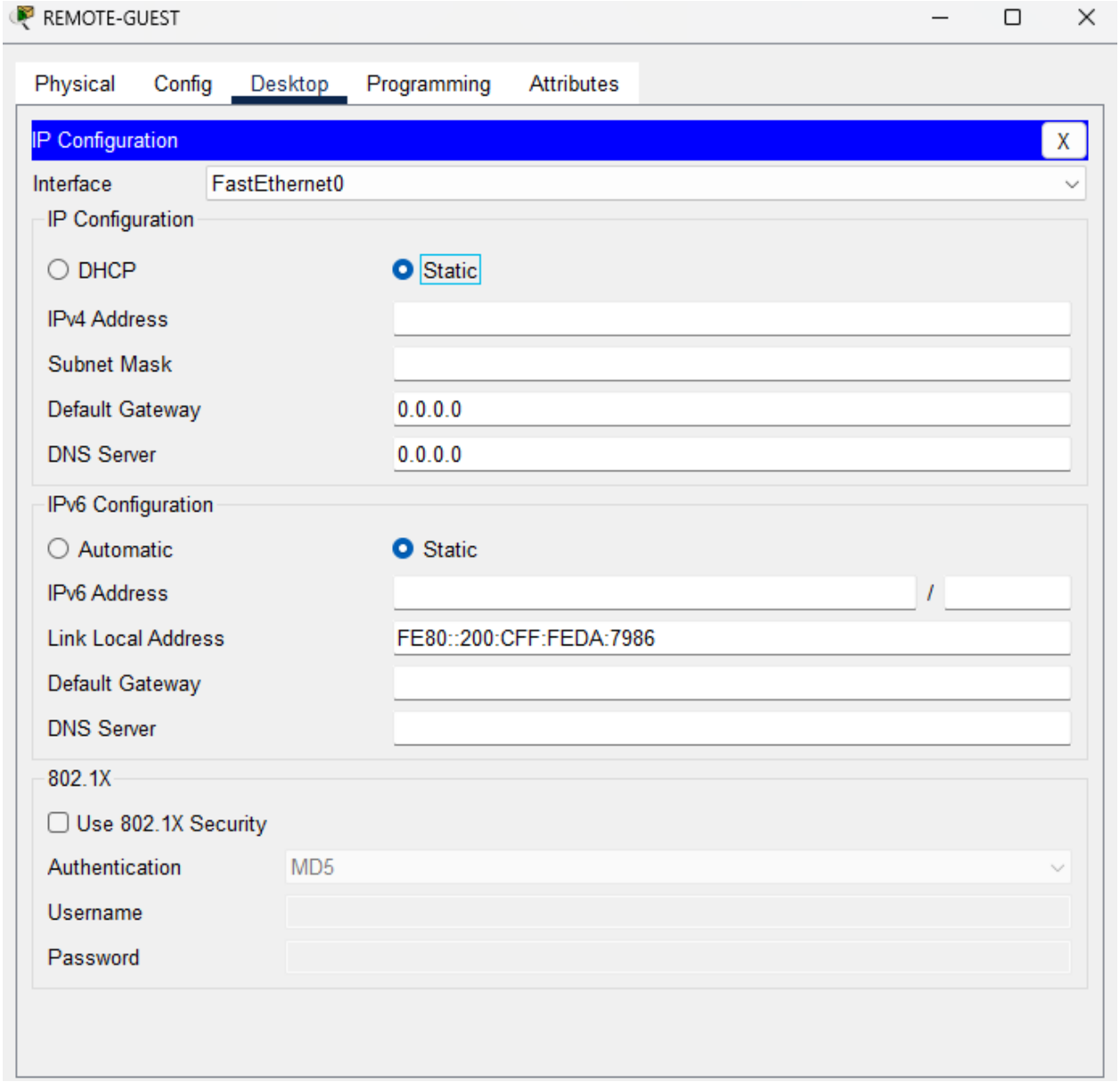
Step 5: On REMOTE-USER-PC, open the Desktop and enter IP Configuration, click the Static radio button.



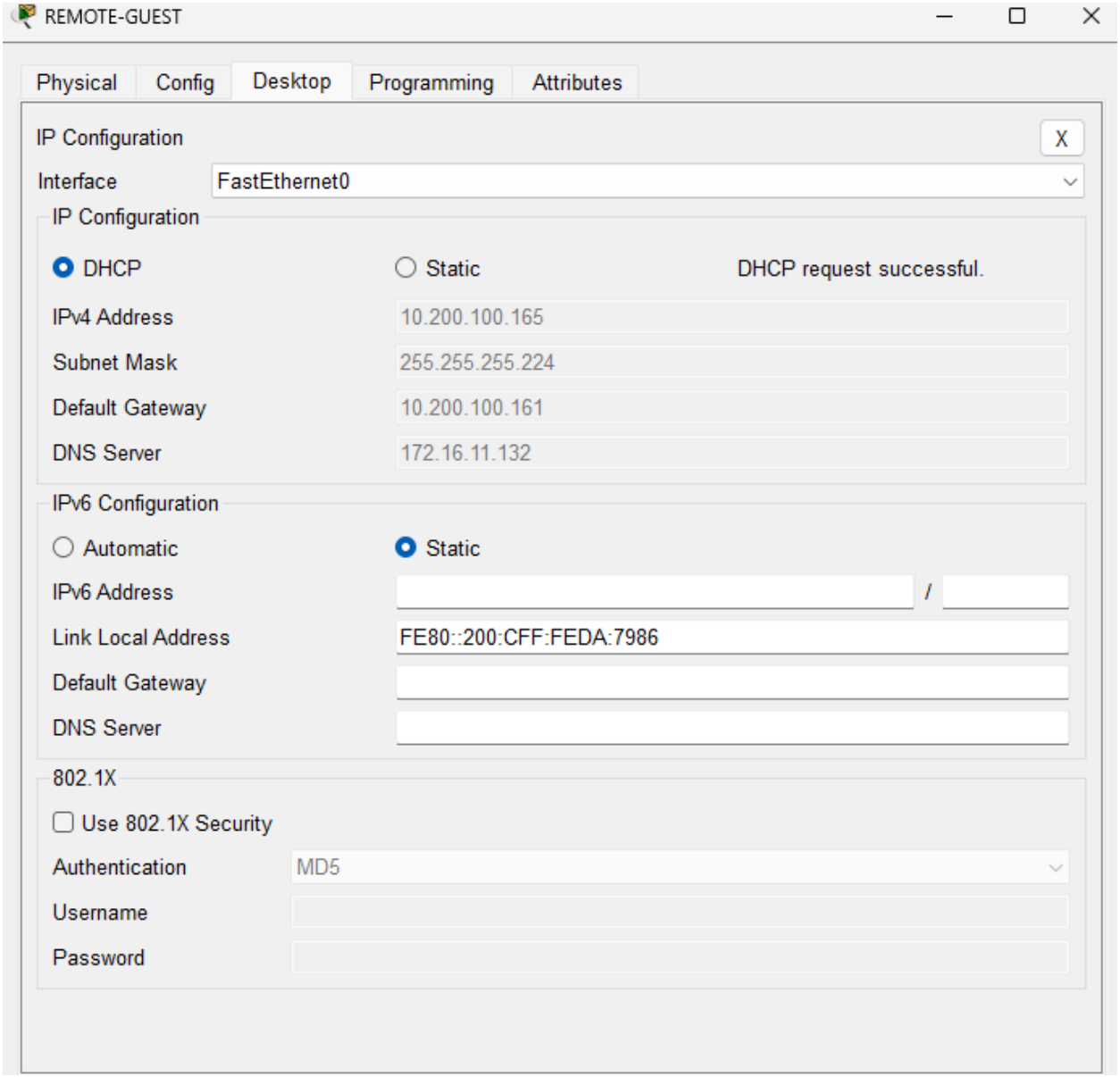
Step 6: Select the DHCP radio button and verify the IP address is part of Vlan 400.



Step 7: On REMOTE-MAIN, open the Desktop and enter IP Configuration, click the Static radio button.

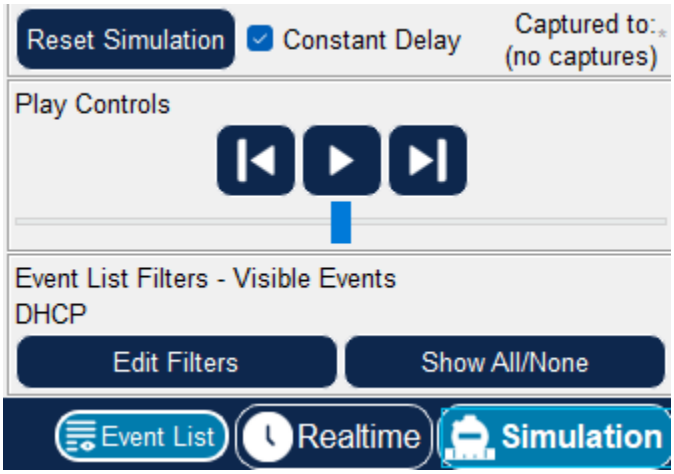


Step 8: Select the DHCP radio button and verify the IP address is part of Vlan 900.

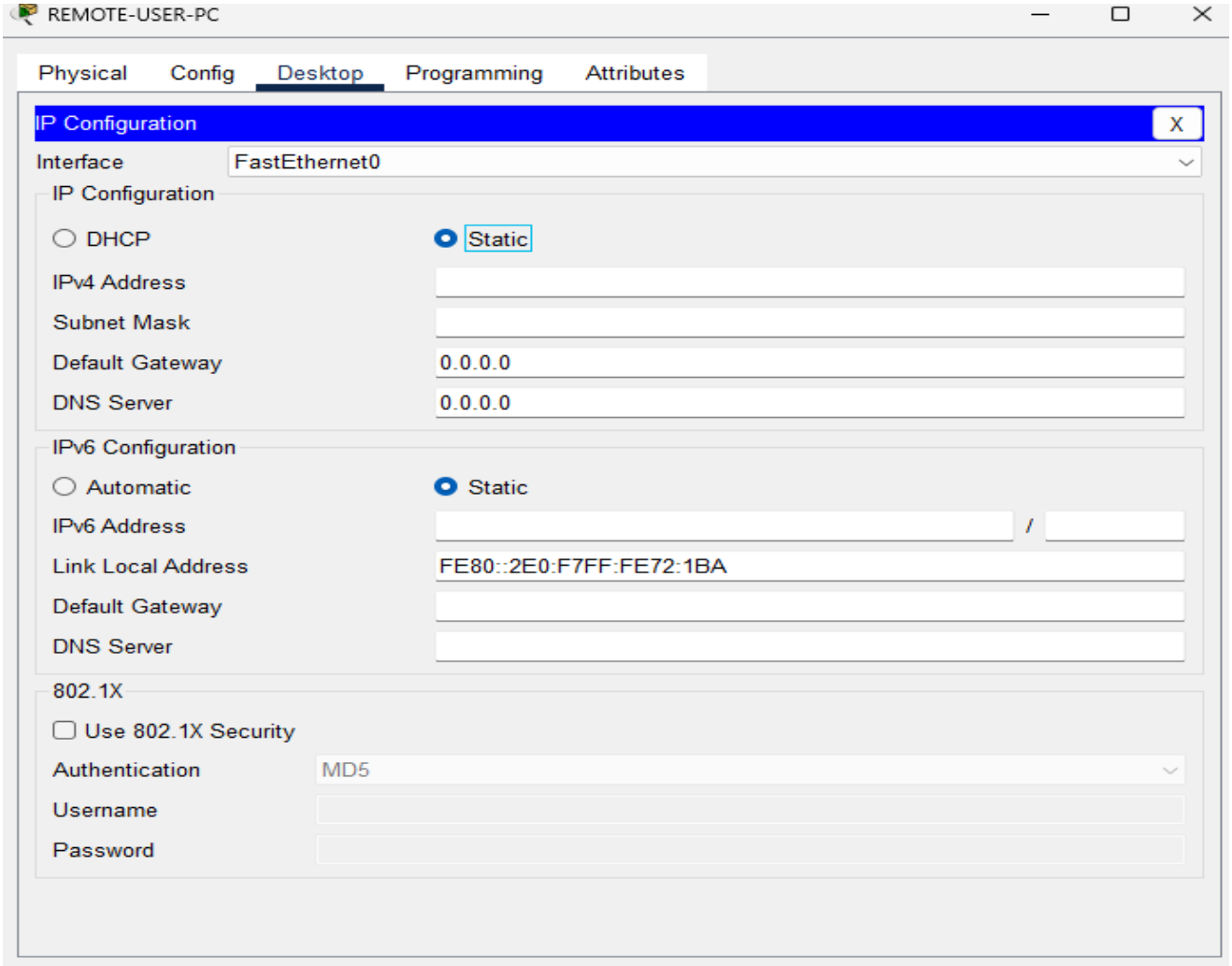


Examine DHCP Request (Simulation)

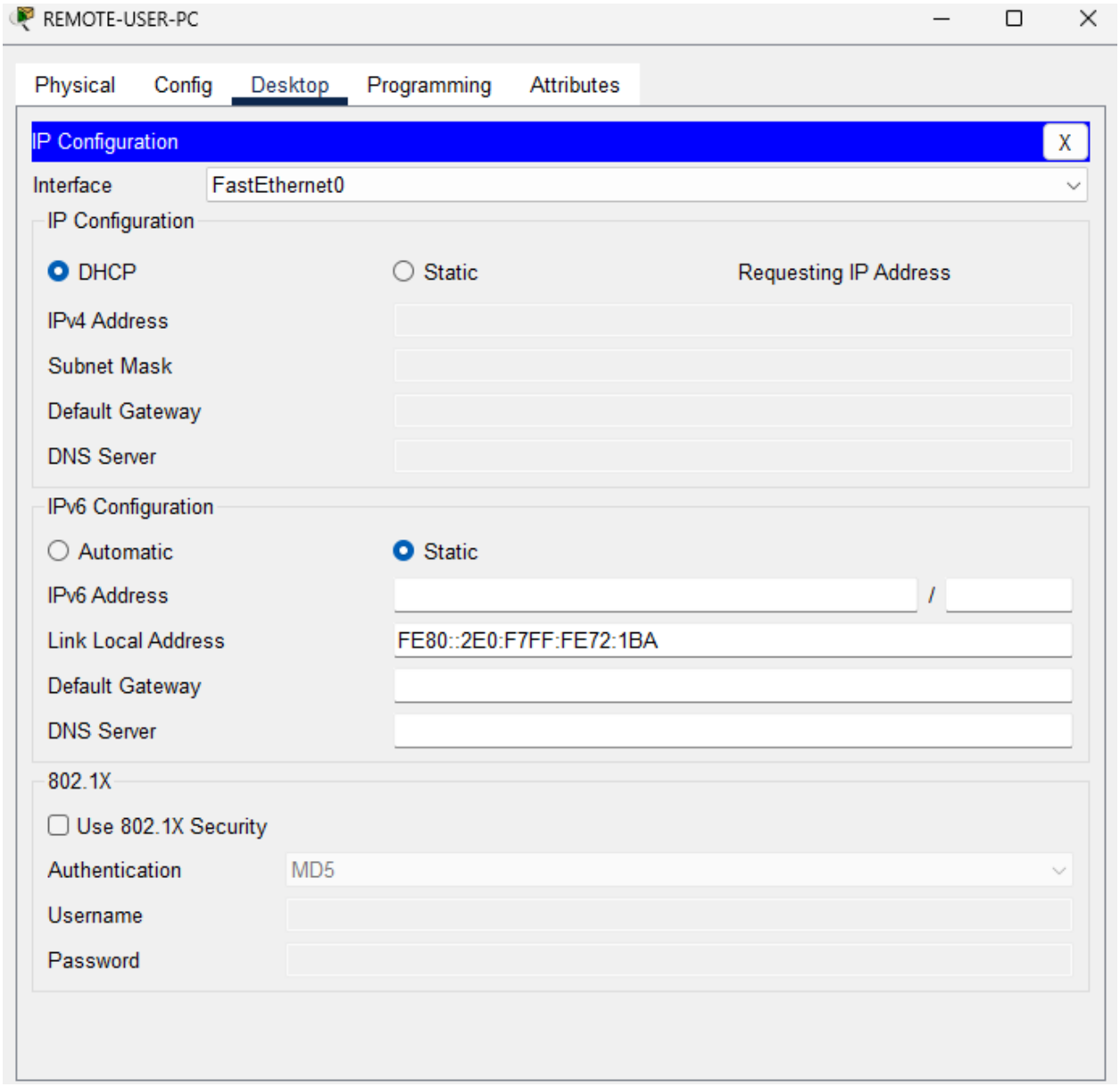
Step 9: Select Simulation and filter for DHCP.



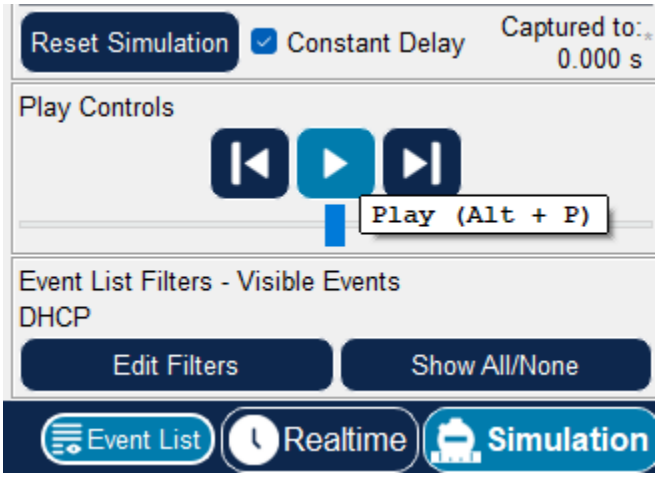
Step 10: On Remote-USER-PC, go to desktop, select IP Configuration and select the Static radio button.



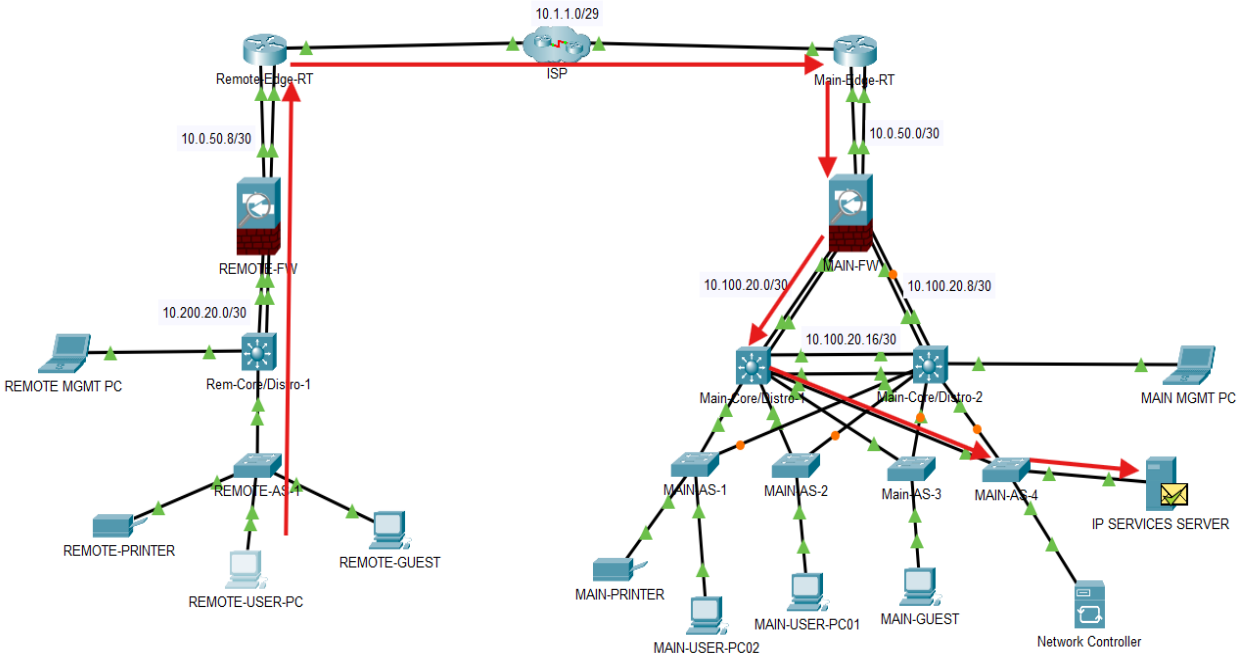
Step 11: Now select, DHCP radio button.



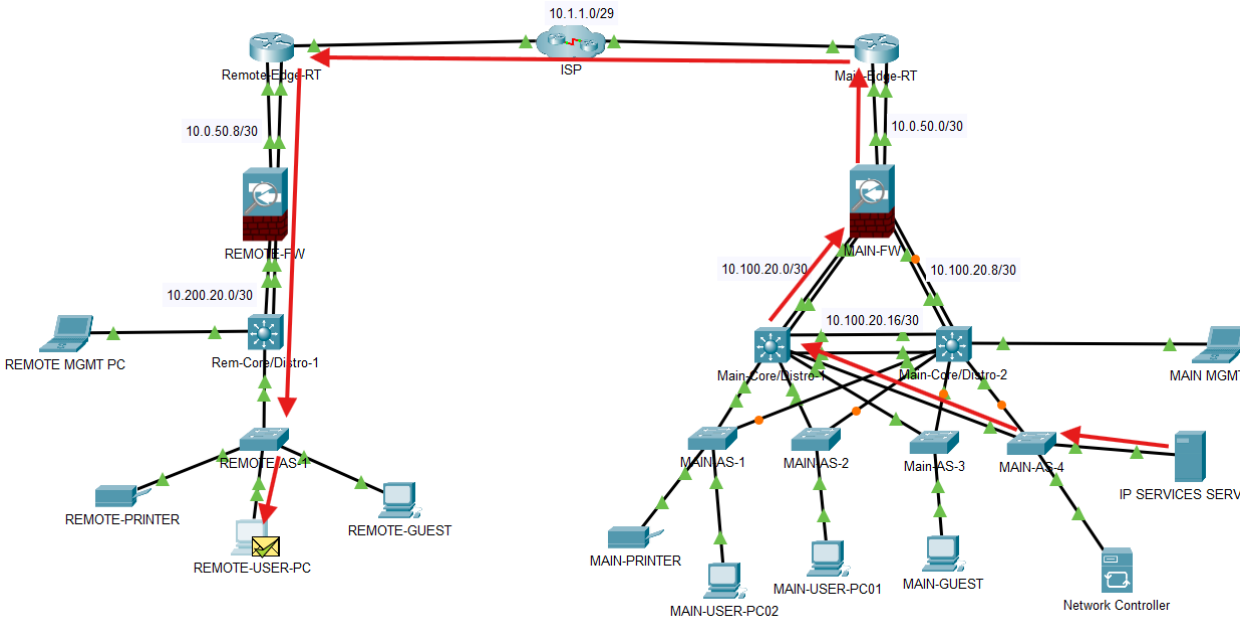
Step 12: Press Play on the simulation control panel.



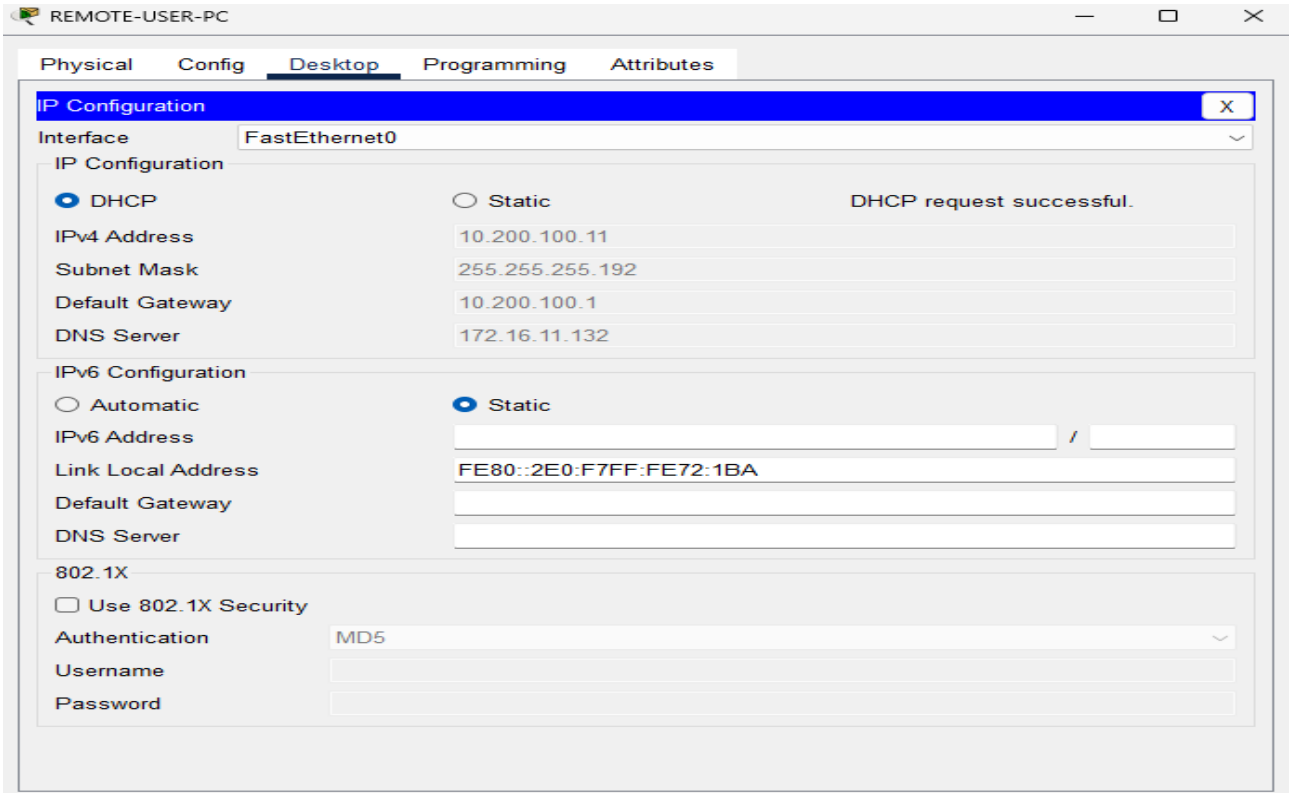
Step 13: Observe as the request travels from the remote site, through the VPN tunnel and reaches the IP Services Server (DHCP Server).



Step 14: Observe as the requested payload travels back to the remote site to the requesting device.



Step 15: On REMOTE-USER-PC, you should see the interface configured with an IP address in the Remote User Vlan network (10.200.100.0/26).

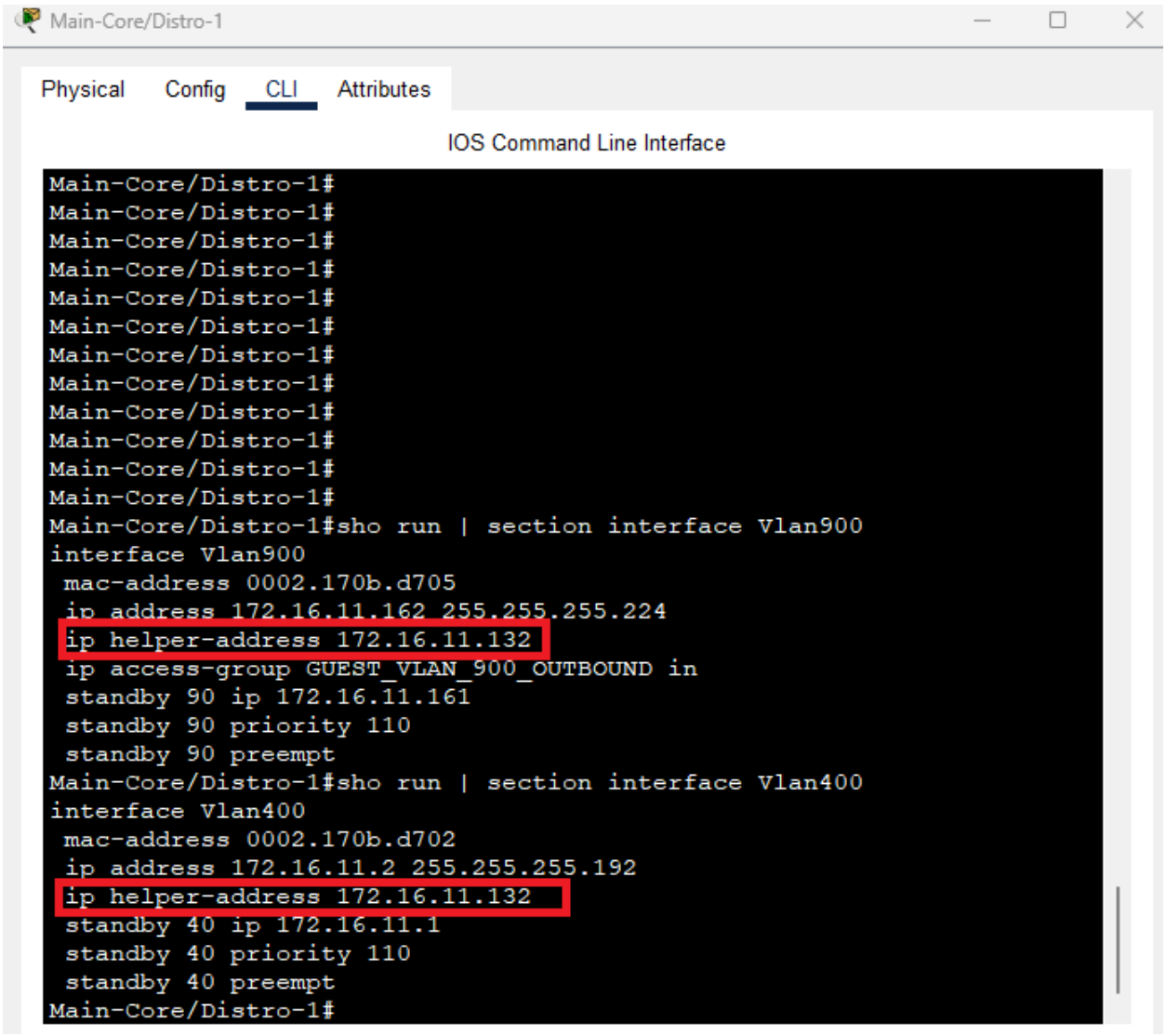


Review of the IP Helper Address

Step 16: Click Realtime to exit simulation and access Main-Core/Distro-1. Login and run the commands:

show run | section interface Vlan900

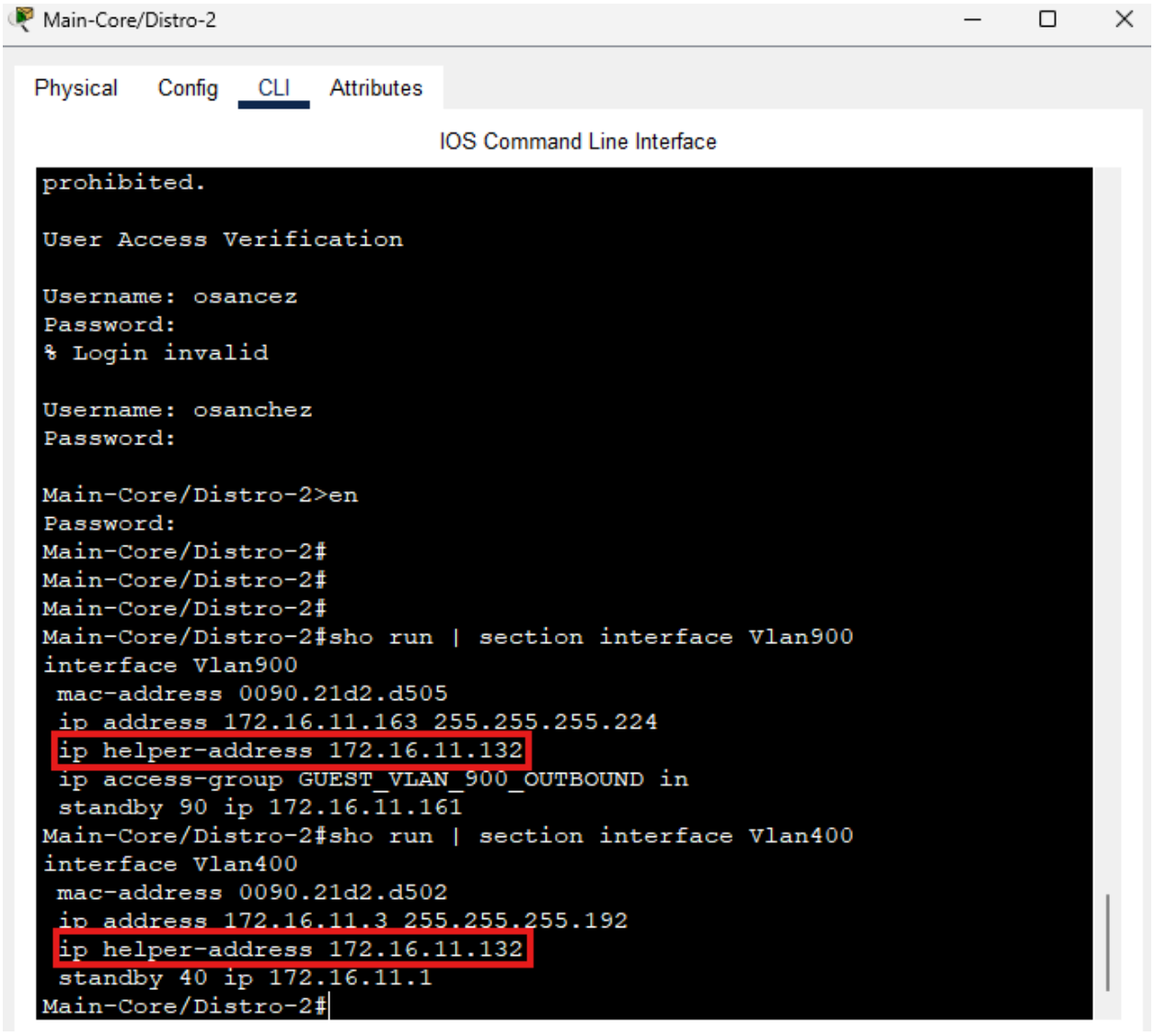
show run | section interface Vlan400



Step 17: Click Realtime to exit simulation and access Main-Core/Distro-2. Login and run the commands:

show run | section interface Vlan900

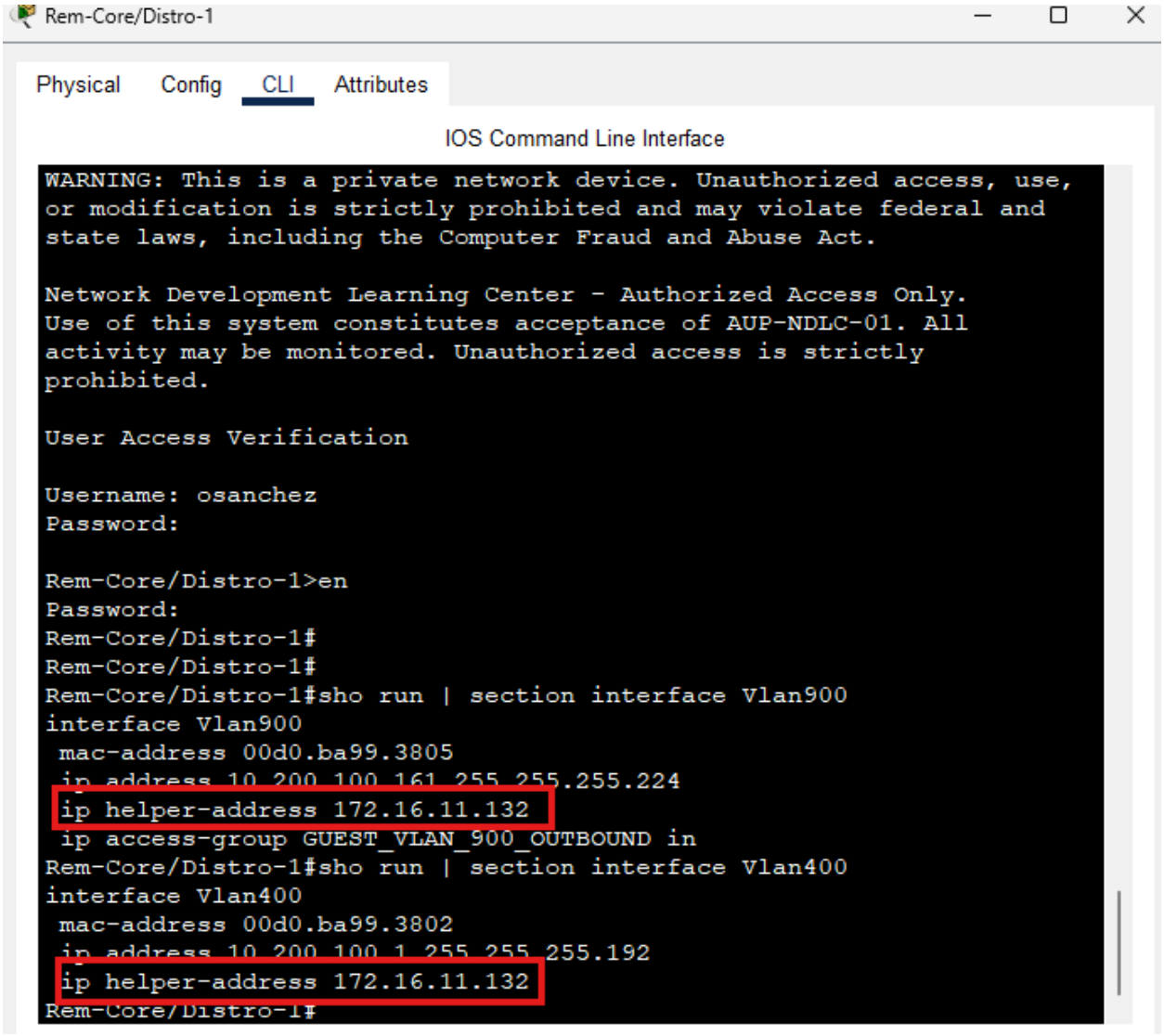
show run | section interface Vlan400



Step 18: Click Realtime to exit simulation and access Remote-Core/Distro-1. Login and run the commands:

show run | section interface Vlan900

show run | section interface Vlan400



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.*

Both the Main and Remote Office sites use switches with the spanning-tree protocol configured. However, the Main Office site is the only one of the two sites vulnerable to broadcast loops because of the many switch connections. In this network, Main-Core/Distro-1 is the primary (root) switch for each VLAN network, and Main-Core/Distro-2 is the secondary switch for each VLAN network. Each access switch is connected to each L3 switch via a trunk port. Lastly, each Core/Distro switch is connected to MAIN-FW through an access port via Vlan 80 (Management Vlan) for admin access and manageability. MAIN-FW also contains a connection to MAIN-EDGE via switchport modules physically added to them and a link via Vlan 80.

Main-Core/Distro-1 G1/0/4 <-> Main-AS-1 F0/1 – Trunk interface

Main-Core/Distro-1 G1/0/5 <-> Main-AS-2 F0/1 – Trunk interface

Main-Core/Distro-1 G1/0/6 <-> Main-AS-3 F0/1 – Trunk interface

Main-Core/Distro-1 G1/0/7 <-> Main-AS-4 F0/1 – Trunk interface

Main-Core/Distro-2 G1/0/4 <-> Main-AS-1 F0/2 – Trunk interface

Main-Core/Distro-2 G1/0/5 <-> Main-AS-2 F0/2 – Trunk interface

Main-Core/Distro-2 G1/0/6 <-> Main-AS-3 F0/2 – Trunk interface

Main-Core/Distro-2 G1/0/7 <-> Main-AS-4 F0/2 – Trunk interface

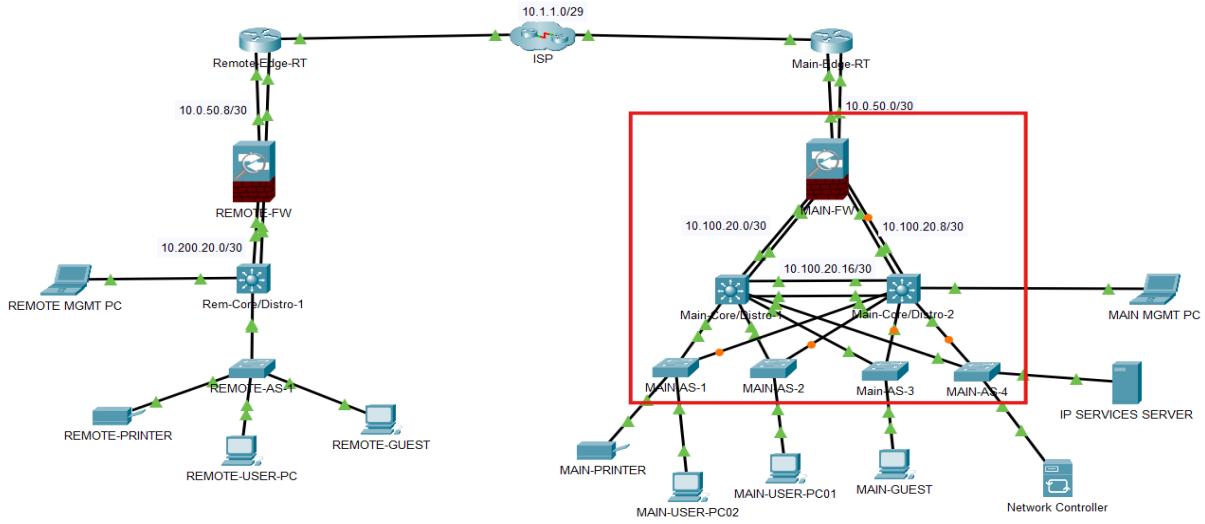
Main-Core-Distro-1 G1/0/23 <-> Main-FW G0/1/0 – Access Interface

Main-Core-Distro-2 G1/0/23 <-> Main-FW G0/1/1 – Access Interface

Main-FW G0/1/2 <-> Main-Edge G0/1/0 - Access Interface

Network Diagram or Segment

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



Legend	
IP	Internet Protocol
RT	Router
AS	Access Switch
Main	Main Office
Remote	Remote Office
MGMT	Management
FW	Firewall
SW	Switch
REM	Remote
PC	Personal Computer
Distro	Distribution Switch
ISP	Internet Service Provider

Testing Method

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

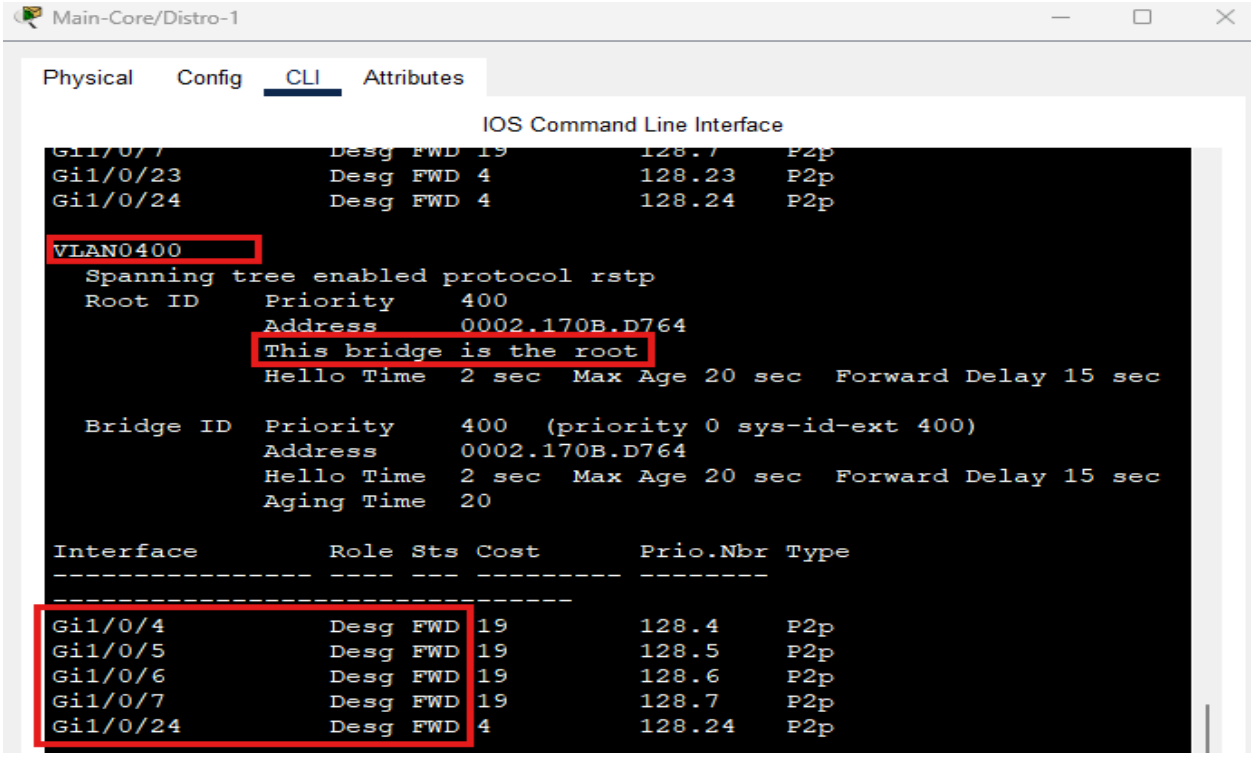
Spanning-tree protocol is configured on every switch throughout the network. The primary (root) switch is Main-Core/Distro-1, and the secondary is Main-Core/Distro-2. We will review STP status on Main-Core/Distro-1 to demonstrate that the “root bridge” for each VLAN is Main-Core/Edge-1. Afterwards, we will review the STP status on one of the MAIN-AS switches and identify the root bridge per Vlan from its perspective. Ultimately, we will disable each trunk port on the Main-Core/Distro-1, review Main-

Core/Distro-2 acting as the new root bridge, and review STP on the same MAIN-AS to see the update from its perspective.

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.*

Step 1: Login to Main-Core/Distro-1 and issue the command *show spanning-tree active* and observe the STP information for each VLAN.



Main-Core/Distro-1

Physical Config CLI Attributes

IOS Command Line Interface

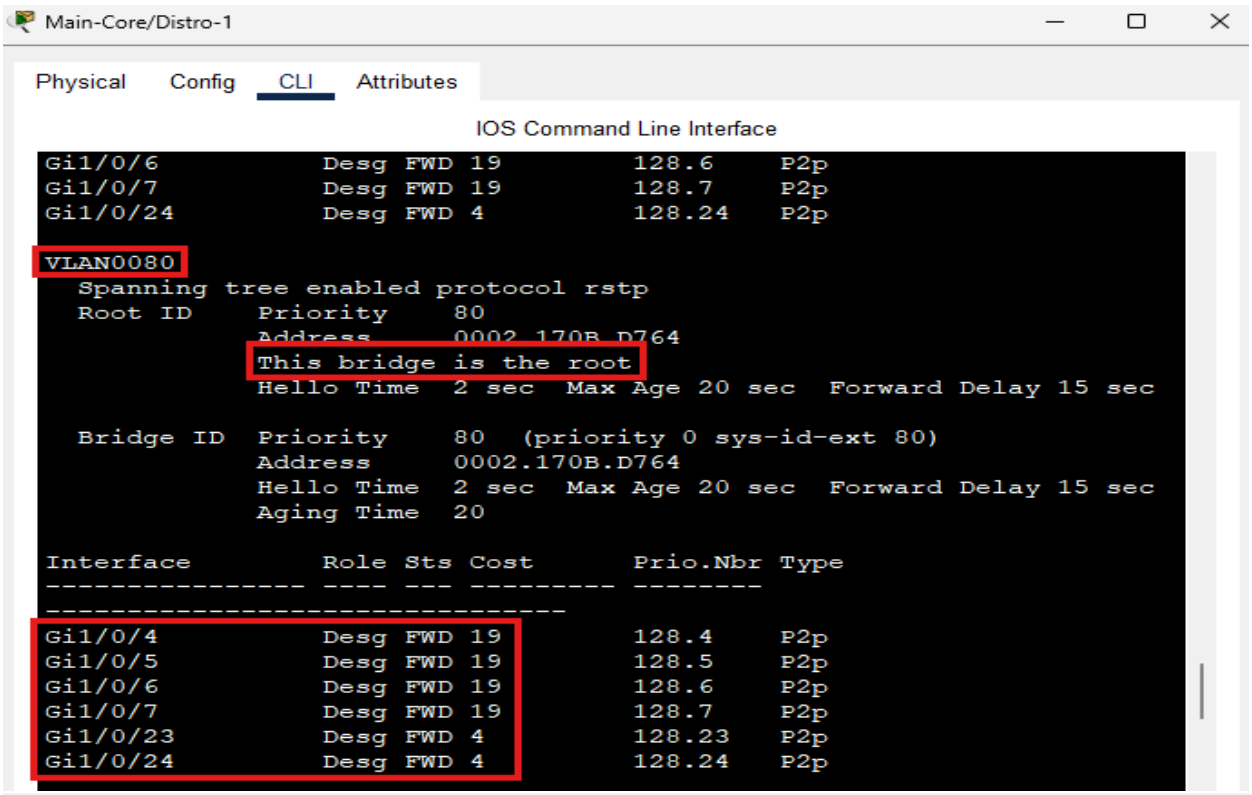
```
Gi1/0/7          Desg FWD 19        128.7    P2p
Gi1/0/24         Desg FWD 4         128.24   P2p

VLAN0500
  Spanning tree enabled protocol rstp
  Root ID     Priority    500
              Address     0002.170B.D764
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    500  (priority 0 sys-id-ext 500)
              Address     0002.170B.D764
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Gi1/0/4          Desg FWD 19        128.4    P2p
Gi1/0/5          Desg FWD 19        128.5    P2p
Gi1/0/6          Desg FWD 19        128.6    P2p
Gi1/0/7          Desg FWD 19        128.7    P2p
Gi1/0/24         Desg FWD 4         128.24   P2p
```

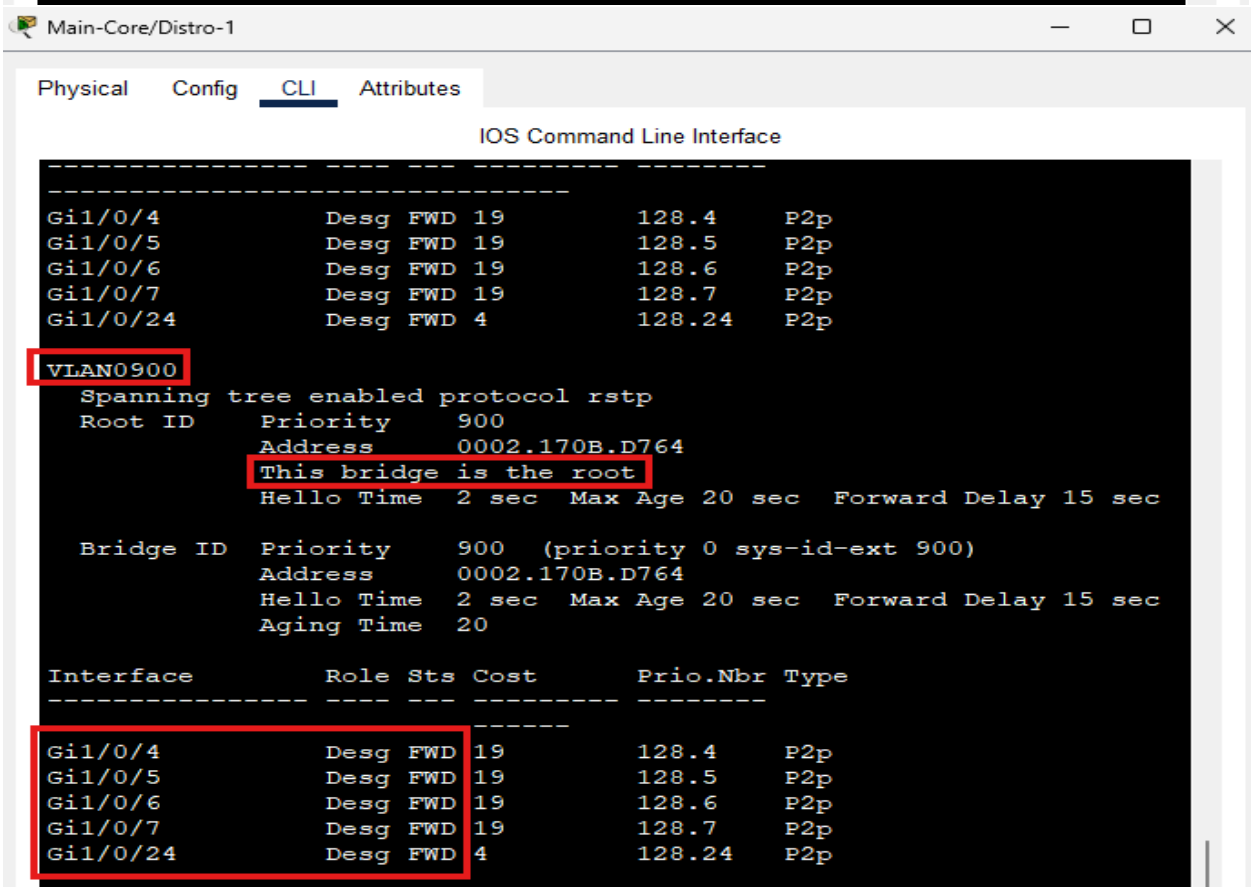
Main-Core/Distro-1

Physical Config CLI Attributes

IOS Command Line Interface

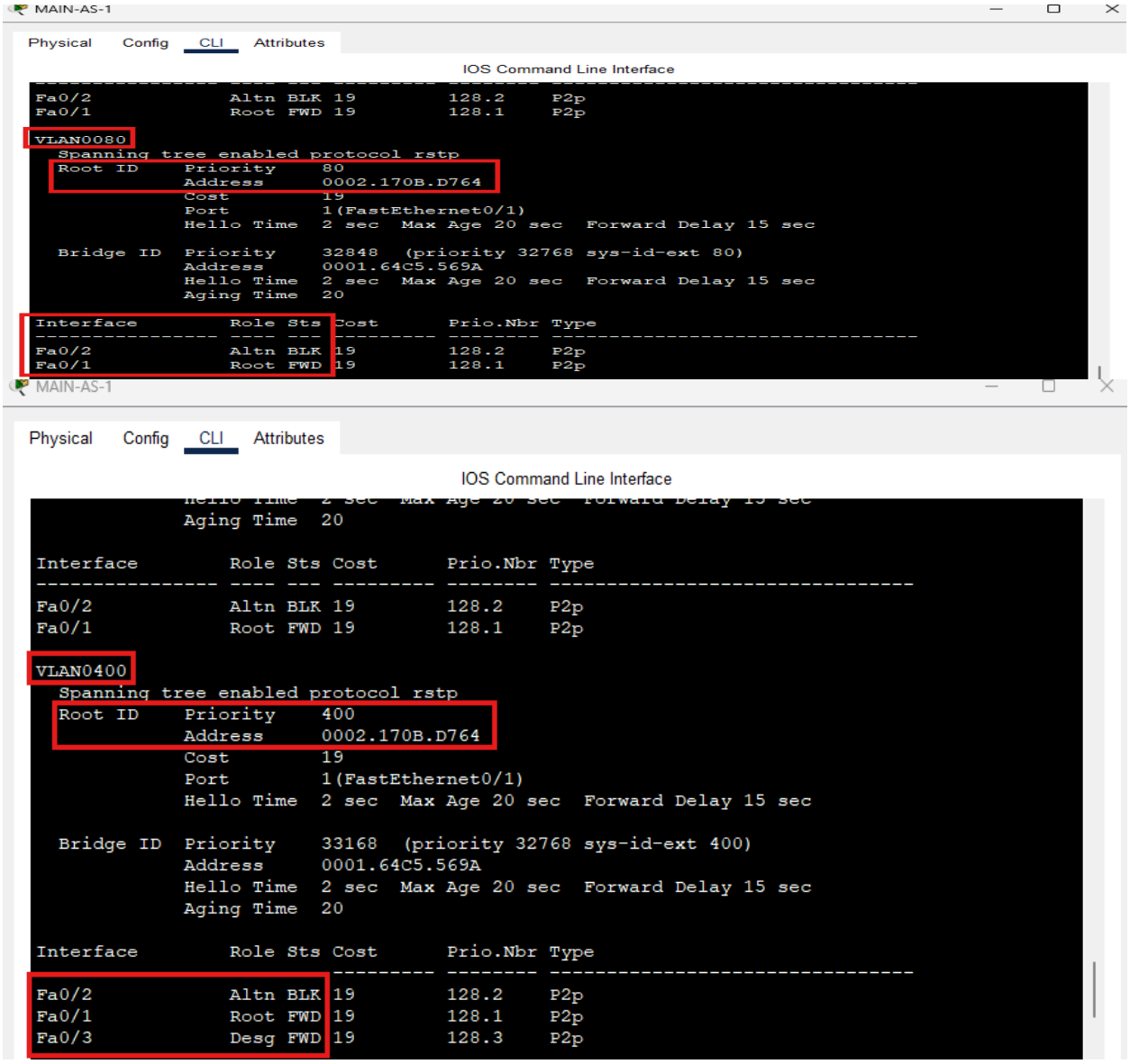
```
Gi1/0/7          Desg FWD 19        128.7    P2p
Gi1/0/24         Desg FWD 4         128.24   P2p

VLAN0600
  Spanning tree enabled protocol rstp
  Root ID     Priority    600
              Address     0002.170B.D764
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    600  (priority 0 sys-id-ext 600)
              Address     0002.170B.D764
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Gi1/0/4          Desg FWD 19        128.4    P2p
Gi1/0/5          Desg FWD 19        128.5    P2p
Gi1/0/6          Desg FWD 19        128.6    P2p
Gi1/0/7          Desg FWD 19        128.7    P2p
Gi1/0/24         Desg FWD 4         128.24   P2p
```


Main-Core/Distro-1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Gi1/0/6 Desg FWD 19 128.6 P2p
Gi1/0/7 Desg FWD 19 128.7 P2p
Gi1/0/24 Desg FWD 4 128.24 P2p
VLAN0080
Spanning tree enabled protocol rstp
Root ID Priority 80
Address 0002.170B.D764
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 80 (priority 0 sys-id-ext 80)
Address 0002.170B.D764
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
Gi1/0/4 Desg FWD 19 128.4 P2p
Gi1/0/5 Desg FWD 19 128.5 P2p
Gi1/0/6 Desg FWD 19 128.6 P2p
Gi1/0/7 Desg FWD 19 128.7 P2p
Gi1/0/23 Desg FWD 4 128.23 P2p
Gi1/0/24 Desg FWD 4 128.24 P2p


Main-Core/Distro-1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Gi1/0/4 Desg FWD 19 128.4 P2p
Gi1/0/5 Desg FWD 19 128.5 P2p
Gi1/0/6 Desg FWD 19 128.6 P2p
Gi1/0/7 Desg FWD 19 128.7 P2p
Gi1/0/24 Desg FWD 4 128.24 P2p
VLAN0900
Spanning tree enabled protocol rstp
Root ID Priority 900
Address 0002.170B.D764
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 900 (priority 0 sys-id-ext 900)
Address 0002.170B.D764
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
Gi1/0/4 Desg FWD 19 128.4 P2p
Gi1/0/5 Desg FWD 19 128.5 P2p
Gi1/0/6 Desg FWD 19 128.6 P2p
Gi1/0/7 Desg FWD 19 128.7 P2p
Gi1/0/24 Desg FWD 4 128.24 P2p

Step 2: Login to any of the access switches. In this case MAIN-AS-1 will be the test subject. Run the command *show spanning-tree active* and review the Root ID. If the Root ID address at MAIN-AS-1 matches Main-Core/Distro-1's MAC, then we can definitively state the Main-Core/Distro-1 is acting as the root.

Main-Core/Distro-1 MAC Address: 0002.170B.D764



MAIN-AS-1

Physical Config CLI Attributes

IOS Command Line Interface

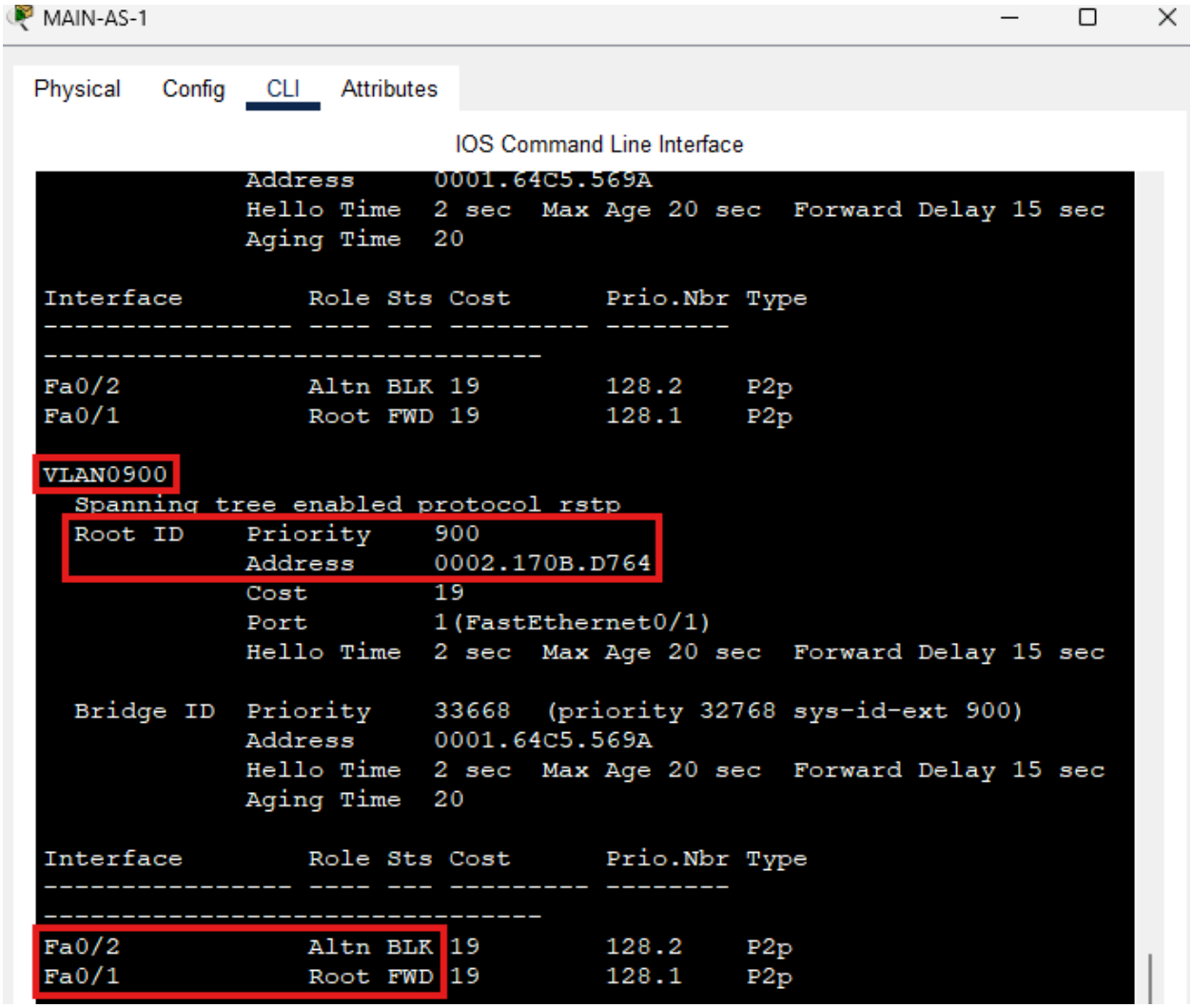
```
Fa0/3            Desg FWD 19        128.3    P2p

VLAN0500
  Spanning tree enabled protocol rstp
  Root ID     Priority    500
              Address     0002.170B.D764
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    33268  (priority 32768 sys-id-ext 500)
              Address     0001.64C5.569A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/1            Root FWD 19        128.1    P2p
Fa0/24           Desg FWD 19        128.24   P2p
```

MAIN-AS-1

Physical Config CLI Attributes

IOS Command Line Interface

```
Fa0/1            Root FWD 19        128.1    P2p
Fa0/24           Desg FWD 19        128.24   P2p

VLAN0600
  Spanning tree enabled protocol rstp
  Root ID     Priority    600
              Address     0002.170B.D764
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    33368  (priority 32768 sys-id-ext 600)
              Address     0001.64C5.569A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/1            Root FWD 19        128.1    P2p
```



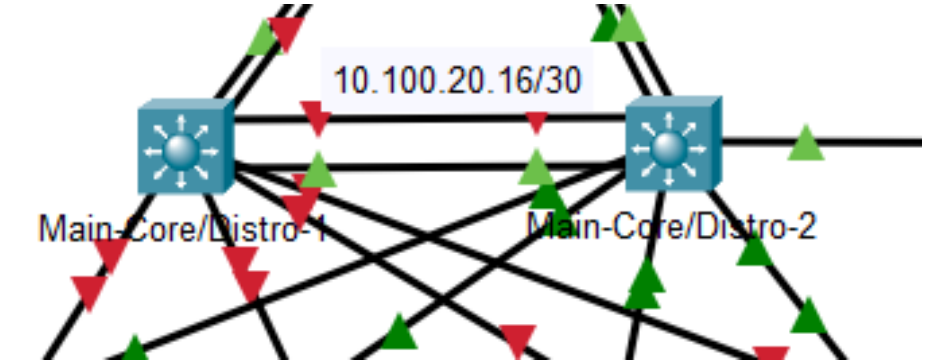
Step 3: Disable all trunk and Vlan ports on Main-Core/Distro-1.

Main-Core/Distro-1

Physical Config CLI Attributes

IOS Command Line Interface

```
Main-Core/Distro-1#
Main-Core/Distro-1#sho int status
Port      Name               Status       Vlan       Duplex  Speed Type
Gig1/0/1                     connected    routed     auto    auto  10/100BaseTX
Gig1/0/2                     notconnect   80         auto    auto  10/100BaseTX
Gig1/0/3                     connected    routed     auto    auto  10/100BaseTX
Gig1/0/4  MAIN-AS-1          disabled trunk       auto    auto  10/100BaseTX
Gig1/0/5  MAIN-AS-2          disabled trunk       auto    auto  10/100BaseTX
Gig1/0/6  MAIN-AS-3          disabled trunk       auto    auto  10/100BaseTX
Gig1/0/7  MAIN-AS-4          disabled trunk       auto    auto  10/100BaseTX
Gig1/0/8                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/9                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/10                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/11                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/12                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/13                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/14                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/15                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/16                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/17                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/18                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/19                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/20                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/21                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/22                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/23 Main-FW            disabled 80          auto    auto  10/100BaseTX
Gig1/0/24 Main-Core/Distro-2 disabled trunk       auto    auto  10/100BaseTX
Gig1/1/1                     notconnect   1          auto    auto  10/100BaseTX
Gig1/1/2                     notconnect   1          auto    auto  10/100BaseTX
Gig1/1/3                     notconnect   1          auto    auto  10/100BaseTX
```



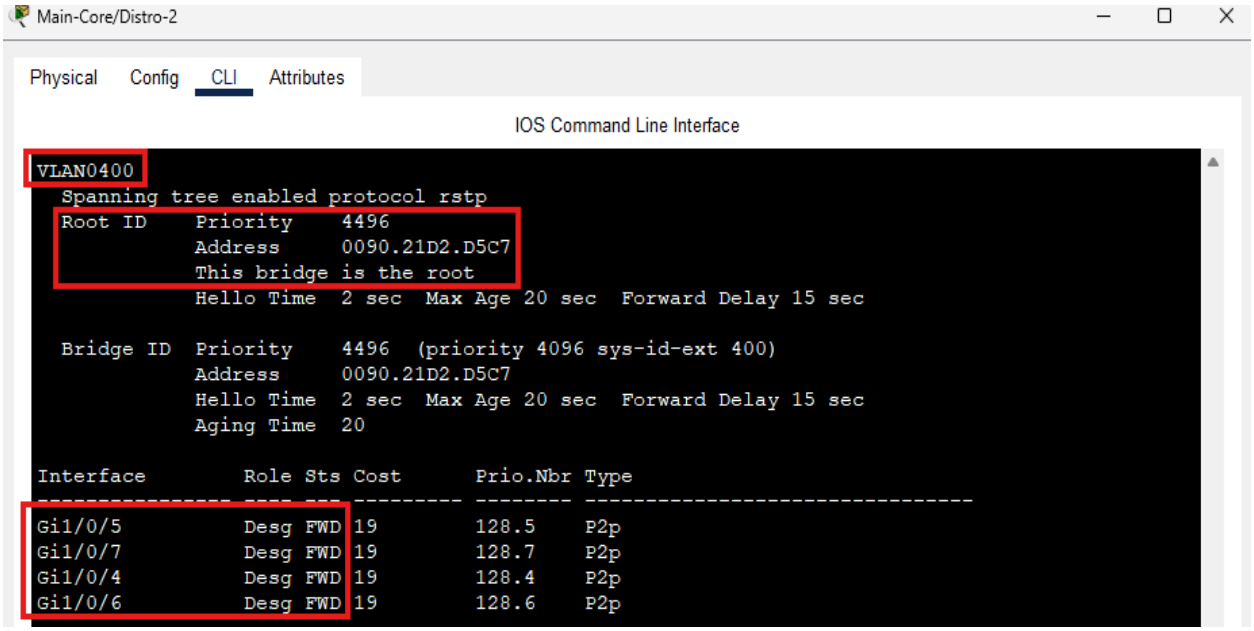
Step 4: Login to Main-Core/Distro-2, run the command *show spanning-tree active* and review STP configuration.

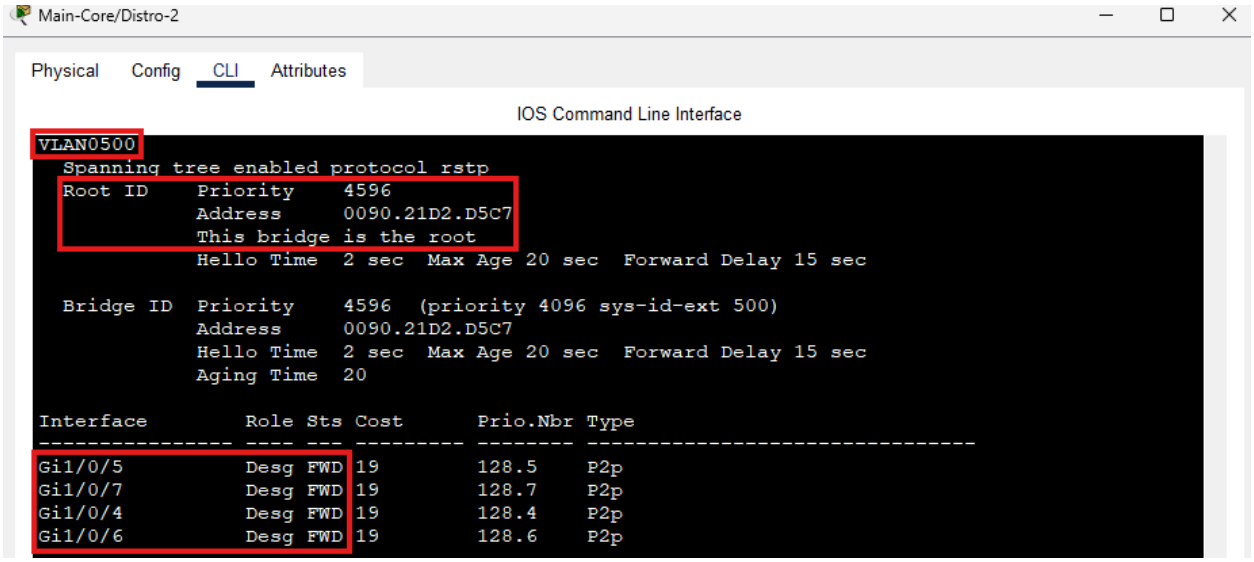
Main-Core/Distro-2

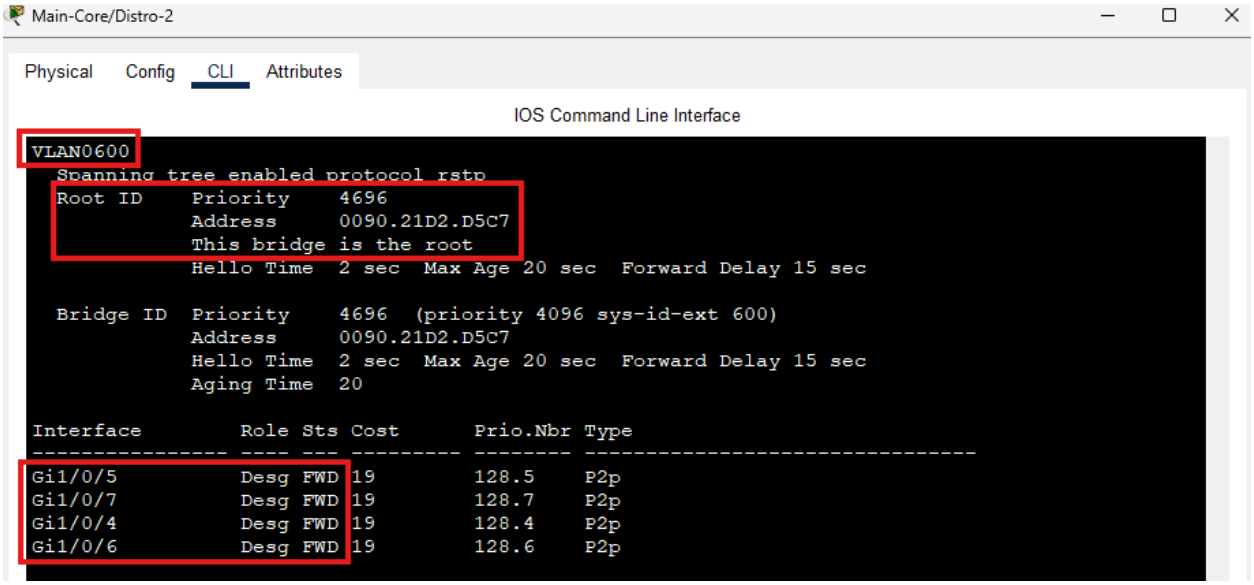
Physical Config CLI Attributes

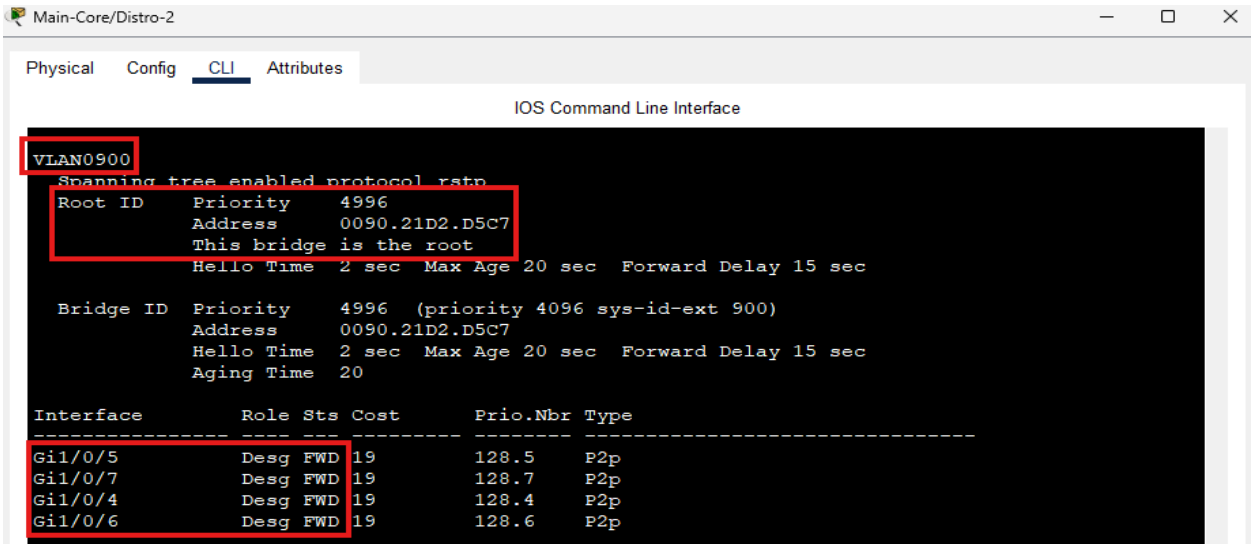
IOS Command Line Interface

```
Gi1/0/4          Desg FWD 19        128.4    P2p
Gi1/0/6          Desg FWD 19        128.6    P2p

VLAN0080
  Spanning tree enabled protocol rstp
  Root ID     Priority    4176
              Address     0090.21D2.D5C7
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4176  (priority 4096 sys-id-ext 80)
              Address     0090.21D2.D5C7
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/5          Desg FWD 19        128.5    P2p
Gi1/0/7          Desg FWD 19        128.7    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Gi1/0/8          Desg FWD 19        128.8    P2p
Gi1/0/6          Desg FWD 19        128.6    P2p
Gi1/0/23         Desg FWD 4         128.23   P2p
```


Main-Core/Distro-2
Physical
Config
CLI
Attributes
IOS Command Line Interface
VLAN0400
Spanning tree enabled protocol rstp
Root ID Priority 4496
Address 0090.21D2.D5C7
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 4496 (priority 4096 sys-id-ext 400)
Address 0090.21D2.D5C7
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
Gi1/0/5 Desg FWD 19 128.5 P2p
Gi1/0/7 Desg FWD 19 128.7 P2p
Gi1/0/4 Desg FWD 19 128.4 P2p
Gi1/0/6 Desg FWD 19 128.6 P2p

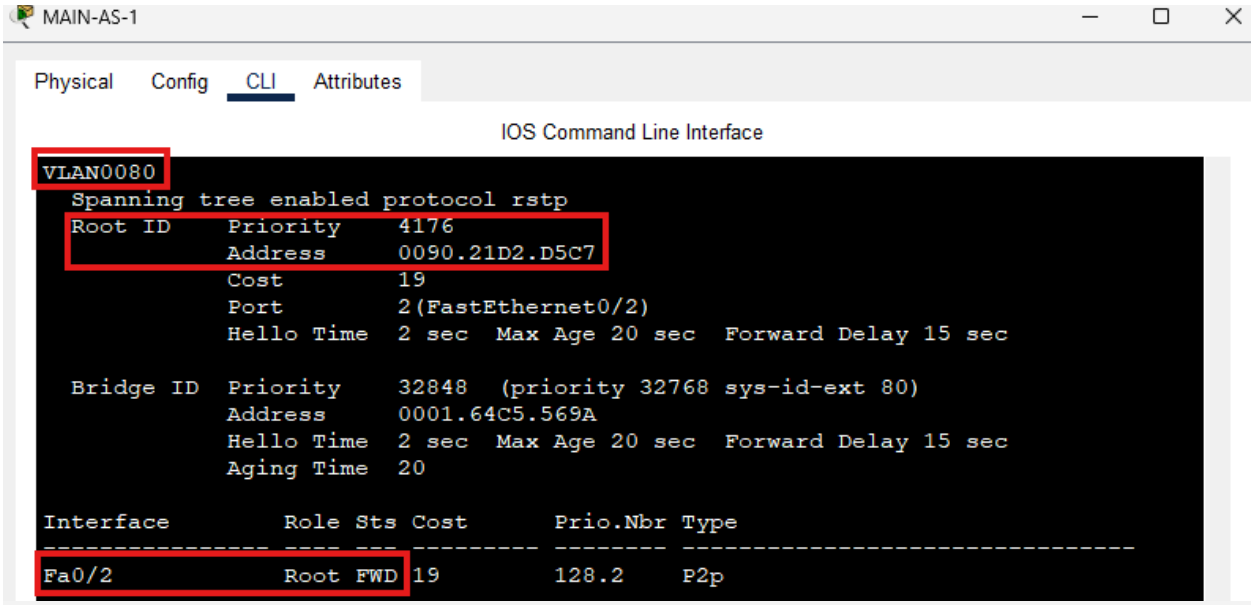

Main-Core/Distro-2
Physical
Config
CLI
Attributes
IOS Command Line Interface
VLAN0500
Spanning tree enabled protocol rstp
Root ID Priority 4596
Address 0090.21D2.D5C7
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 4596 (priority 4096 sys-id-ext 500)
Address 0090.21D2.D5C7
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
Gi1/0/5 Desg FWD 19 128.5 P2p
Gi1/0/7 Desg FWD 19 128.7 P2p
Gi1/0/4 Desg FWD 19 128.4 P2p
Gi1/0/6 Desg FWD 19 128.6 P2p

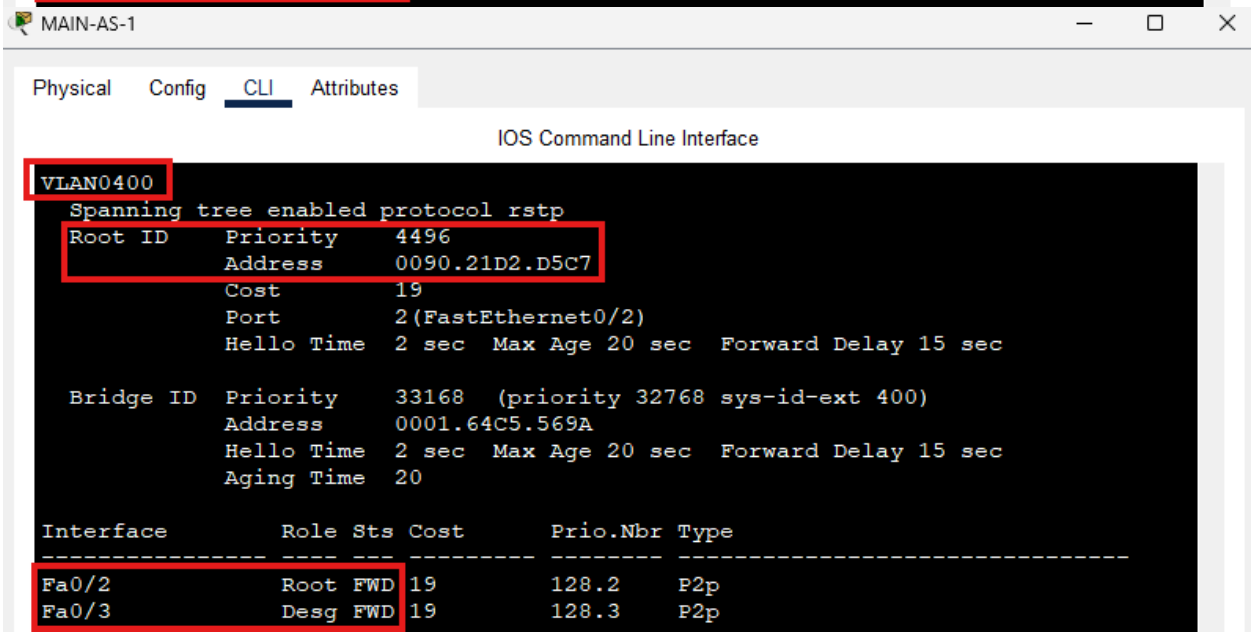

Main-Core/Distro-2
Physical
Config
CLI
Attributes
IOS Command Line Interface
VLAN0600
Spanning tree enabled protocol rstp
Root ID Priority 4696
Address 0090.21D2.D5C7
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 4696 (priority 4096 sys-id-ext 600)
Address 0090.21D2.D5C7
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
Gi1/0/5 Desg FWD 19 128.5 P2p
Gi1/0/7 Desg FWD 19 128.7 P2p
Gi1/0/4 Desg FWD 19 128.4 P2p
Gi1/0/6 Desg FWD 19 128.6 P2p


Main-Core/Distro-2
Physical
Config
CLI
Attributes
IOS Command Line Interface
VLAN0900
Spanning tree enabled protocol rstp
Root ID Priority 4996
Address 0090.21D2.D5C7
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 4996 (priority 4096 sys-id-ext 900)
Address 0090.21D2.D5C7
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
Gi1/0/5 Desg FWD 19 128.5 P2p
Gi1/0/7 Desg FWD 19 128.7 P2p
Gi1/0/4 Desg FWD 19 128.4 P2p
Gi1/0/6 Desg FWD 19 128.6 P2p

Step 5: Login to MAIN-AS-1 and run the command *show spanning-tree active* and review the Root ID. If the Root ID address at MAIN-AS-1 matches Main-Core/Distro-2's MAC, then we can definitively state the Main-Core/Distro-2 is acting as the root and STP is functioning correctly.

Main-Core/Distro-2 MAC Address: 0090.21D2.D5C7





MAIN-AS-1

Physical Config CLI Attributes

IOS Command Line Interface

```
VLAN0500
  Spanning tree enabled protocol rstp
  Root ID     Priority    4596
              Address     0090.21D2.D5C7
              Cost        19
              Port        2(FastEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    33268  (priority 32768 sys-id-ext 500)
              Address     0001.64C5.569A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/24           Desg FWD 19        128.24   P2p
```

MAIN-AS-1

Physical Config CLI Attributes

IOS Command Line Interface

```
VLAN0600
  Spanning tree enabled protocol rstp
  Root ID     Priority    4696
              Address     0090.21D2.D5C7
              Cost        19
              Port        2(FastEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    33368  (priority 32768 sys-id-ext 600)
              Address     0001.64C5.569A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
```

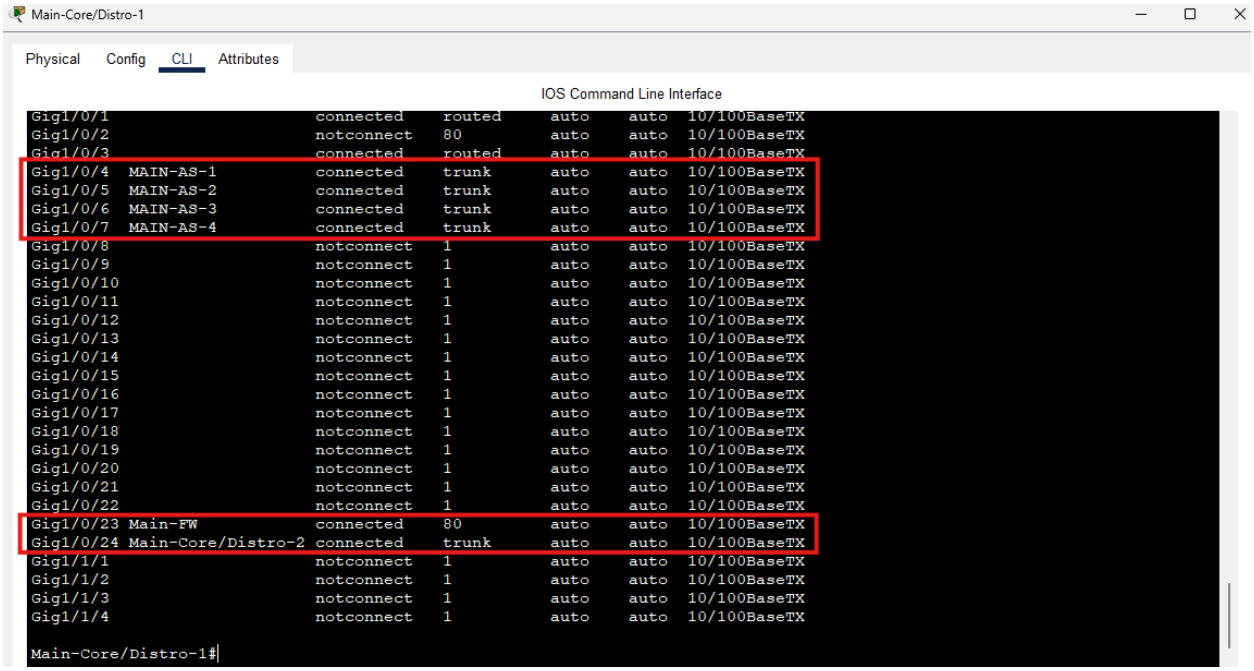
MAIN-AS-1

Physical Config CLI Attributes

IOS Command Line Interface

```
VLAN0900
  Spanning tree enabled protocol rstp
  Root ID     Priority    4996
              Address     0090.21D2.D5C7
              Cost        19
              Port        2(FastEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    33668  (priority 32768 sys-id-ext 900)
              Address     0001.64C5.569A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
```

Step 6: Login to Main-Core/Distro-1 and enable the down ports to restore full services.



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.

***NOTE:** Packet Tracer's limited logging capabilities can sometimes pose a challenge when trying to simulate a real-world scenario for capturing unwanted traffic and generating system logs. Below are some alternative solutions to satisfying the test case.

1. **Use an External Syslog Server:**

- **Set up a simple syslog server:** You can use a Linux machine or a virtual machine to do this.
- **Configure your Packet Tracer devices:** Tell your devices to send their logs to this external server.
- **Analyze logs:** This gives you more flexibility to analyze logs and troubleshoot issues.
- **Document your work.**

2. **Focus on ACLs and Verification:**

Even though Packet Tracer might not log ACL violations directly, you can still:

- **Configure ACLs:** Set up rules to block unwanted traffic.
- **Verify the ACLs:** Use Packet Tracer's packet capture or simulation tools to check if the ACLs are working as expected.
- **Document your work:** Explain your ACL configuration and the verification process.

Items to be included in the documentation:

- Clearly document the limitations of Packet Tracer's logging capabilities.
- Explain the alternative method used to assess unwanted traffic detection.
- Emphasize your understanding of the desired logging behavior and how you would implement it in a real-world scenario.

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.*

Packet Tracer has limitations with logging ACL violations to a syslog server; however, there are ways to verify that ACLs are correctly blocking unpermitted network connections. Also, logging system notifications are possible in Packet Tracer. These are not ACL-specific but function similarly to how a real-world scenario can play out.

The Network Development Learning Center network does support, and internal syslog functionality exists on the IP Services server. The server readily receives logs and stores them internally. An admin can

then go to a specific timestamp and review the log for action. This same server also acts as the network's NTP server.

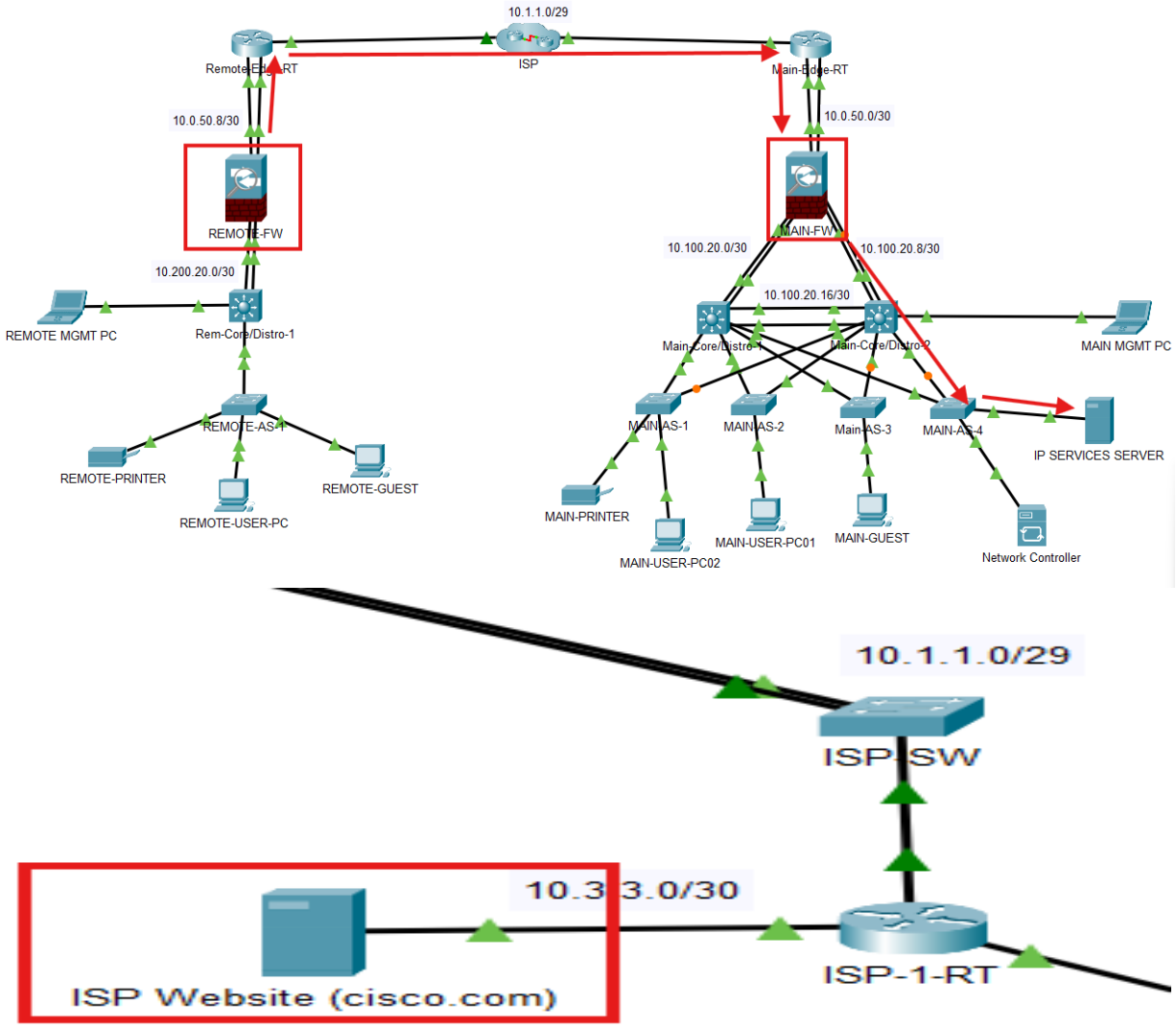
IP Services Server (Syslog Server): 172.16.11.132/27

Main-FW: 172.16.11.203/28

Remote-FW: 10.200.100.196/28

Network Diagram or Segment

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



Legend	
IP	Internet Protocol
RT	Router
AS	Access Switch
Main	Main Office
Remote	Remote Office
MGMT	Management
FW	Firewall
SW	Switch
REM	Remote
PC	Personal Computer
Distro	Distribution Switch
ISP	Internet Service Provider

Testing Method

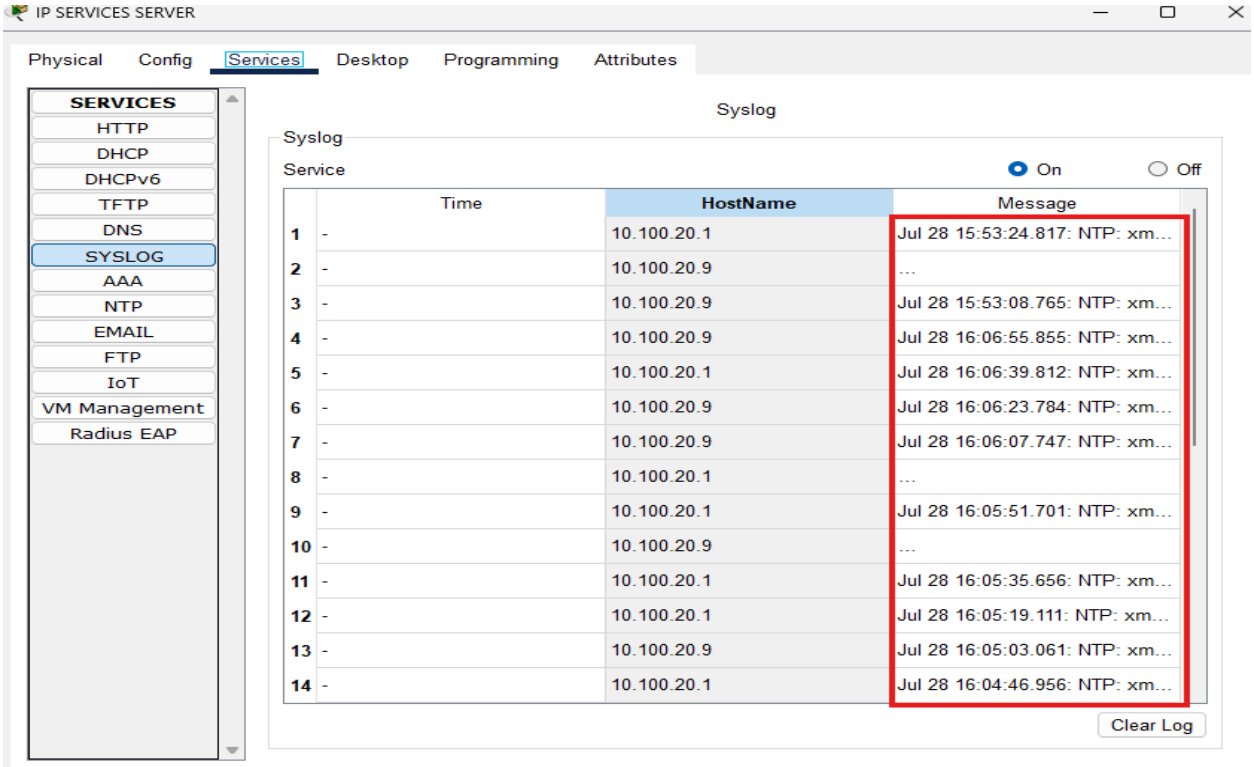
*Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.*

This test will attempt to circumvent the logging limitations found in Packet Tracer as they pertain to specific ACL actions. Main-FW and REMOTE-FW are each configured to send logs to the Syslog server 172.16.11.132. We will review the logs currently stored in that server as an example. Then we will send traffic from an exterior network device to the Remote Office site and review the PDU as it reaches the respective firewall. Here, the firewall ACL will prevent unsolicited traffic from entering the networks, and thus, by examining the PDU, we can derive information that would usually be sent to the syslog server, as it captures unwanted traffic.

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.*

Step 1: On the IP Services server, go to the Services tab, and select Syslog to review the logs.



Example Logs for clarity:

- Jul 28 16:05:51.701: NTP: xmit packet to 172.16.11.132
- Jul 28 15:54:45.165: NTP: xmit packet to 172.16.11.132

These logs capture the key information needed by an administrator for review and to take company action as required.

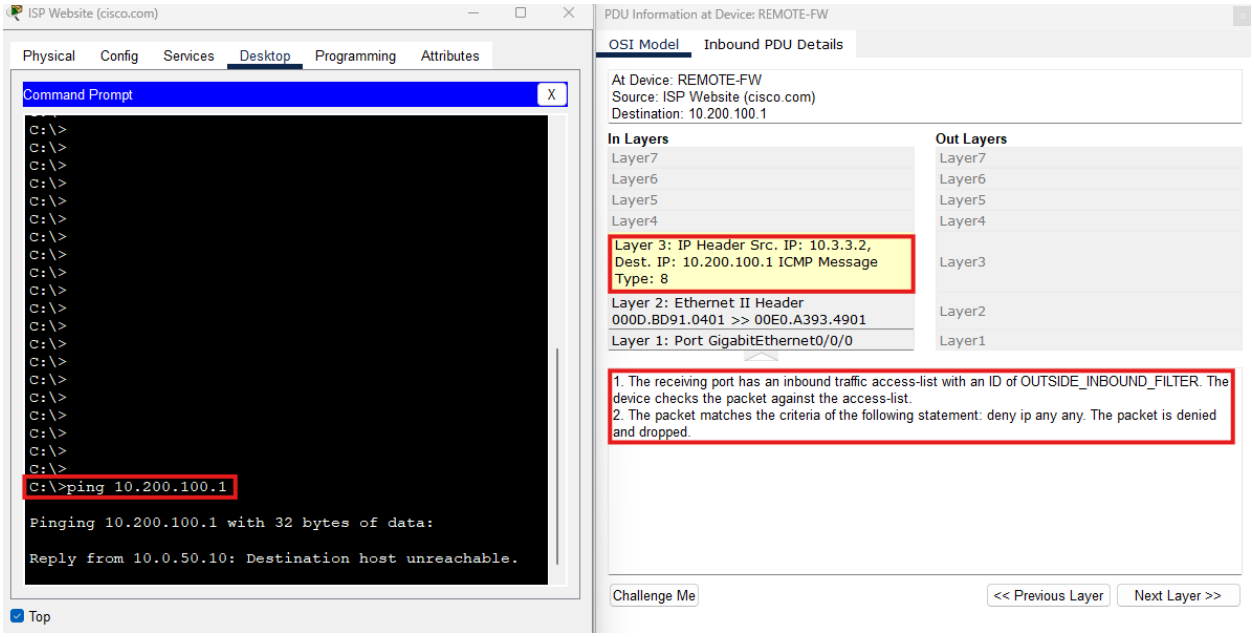
1. Time and Date
2. Protocol
3. Hostname
4. Destination IP address

A traditional ACL log would contain even further information pertaining to the specific action taken by the firewall after detecting an unsolicited request.

1. Access List Number

2. Source IP Address
3. Permit/Deny Status
4. Packet Count

Step 2: Enter simulation mode and filter for ICMP traffic. On ISP website server (cisco.com), go to desktop, ping 10.200.100.1 (User Vlan GW), press PLAY. Pause the simulation when the packet reaches the Remote-FW. Open the packet PDU and examine the description.



If ACL violation logging was supported in Packet Tracer, then at this step the Remote-FW would flag and log this packet and then send the log to the syslog server. For this specific packet we can expect that syslog to look like:

Jul 28 16:05:00 ICMP: DENY packet from 10.3.3.2 to 10.200.100.1 : ACL OUTSIDE_INBOUND_FILTER : 3

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.*

Network Development Learning Center has five main subnets per site: User Vlan, Printer Vlan, Service Vlan, Guest Vlan, and Management Vlan. The network scheme at the Main Office site uses VLSM on 172.16.11.0/24 to segment each VLAN subnet.

Main Office:

Vlan 400 – User – 172.16.11.0/26

Vlan 500 – Printer – 172.16.11.64/26

Vlan 600 – Services – 172.16.11.128/27

Vlan 900 – Guest – 172.16.11.160/27

Vlan 80 – Management – 172.16.11.192/28

The Remote Office site also has five subnets: user VLAN, printer VLAN, service VLAN, guest VLAN, and management VLAN. However, we created a separate network per VLAN for the Remote Office VLANs through VLSM subnetting on the 10.200.100.0/24 network.

Remote Office:

Vlan 400 – User – 10.200.100.0/26

Vlan 500 – Printer – 10.200.100.64/26

Vlan 600 – Services – 10.200.100.128/27

Vlan 900 – Guest – 10.200.100.160/27

Vlan 80 – Management – 10.200.100.192/28

The gateway for each VLAN is applied at the Core/Distro switches. At the Main Office site, HSRP is configured on Main-Core/Distro-1 and Main-Core/Distro-2, with Main-Core/Distro-1 acting as the "active router' and Main-Core/Distro-2 acting as the "standby router". Since there is only one L3 switch located at the Remote Office, the SVI for each VLAN is configured as the gateway interface.

Main Office:

VLAN	Main-Core/Distro-1	Main-Core/Distro-2	Virtual IP
400	172.16.11.2	172.16.11.3	172.16.11.1
500	172.16.11.66	172.16.11.67	172.16.11.65
600	172.16.11.130	172.16.11.131	172.16.11.129
900	172.16.11.162	172.16.11.163	172.16.11.161
80	172.16.11.194	172.16.11.195	172.16.11.193

Remote Office:

VLAN	Remote-Core/Distro-1
400	10.200.100.1
500	10.200.100.65
600	10.200.100.129
900	10.200.100.161
80	10.200.100.193

Each Core/Distro router has a trunk port that connects to at least one access switch.

Main-Core/Distro-1 G1/0/4 <-> Main-AS-1 F0/1 – Trunk interface

Main-Core/Distro-1 G1/0/5 <-> Main-AS-2 F0/1 – Trunk interface

Main-Core/Distro-1 G1/0/6 <-> Main-AS-3 F0/1 – Trunk interface

Main-Core/Distro-1 G1/0/7 <-> Main-AS-4 F0/1 – Trunk interface

Main-Core/Distro-2 G1/0/4 <-> Main-AS-1 F0/2 – Trunk interface

Main-Core/Distro-2 G1/0/5 <-> Main-AS-2 F0/2 – Trunk interface

Main-Core/Distro-2 G1/0/6 <-> Main-AS-3 F0/2 – Trunk interface

Main-Core/Distro-2 G1/0/7 <-> Main-AS-4 F0/2 – Trunk interface

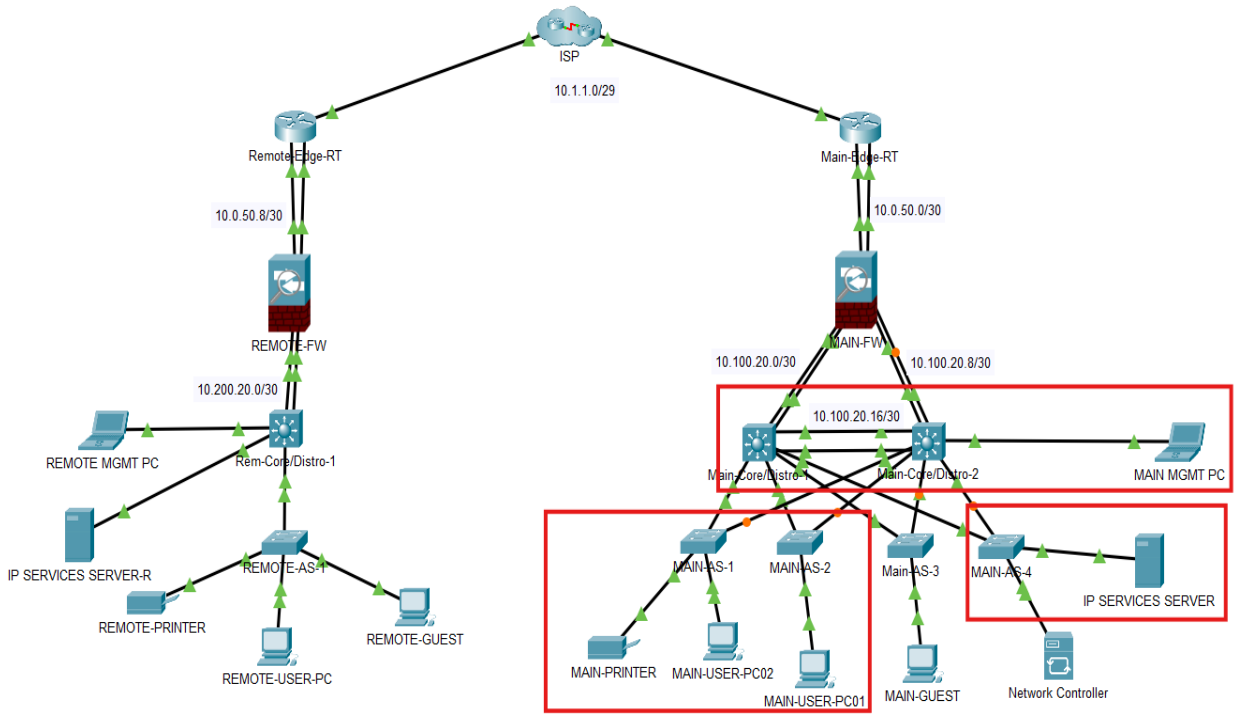
Remote-Core/Distro-1 G1/0/2 <-> Remote-AS F0/1 – Trunk interface

All VLAN traffic, at each site, is forwarded to and processed by the Core/Distro switches. In the case of the Main Office, Main-Core/Distro-1 will process all traffic forwarded. In case of a device failure at Main-

Core/Distro-1, Main-Core/Distro-2 will act as the primary. Access switches contain two trunk ports (one per core/distro switch), leaving everything else as an access port, allowing a specific VLAN to be configured per client interface.

Network Diagram or Segment

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



Legend	
IP	Internet Protocol
RT	Router
AS	Access Switch
Main	Main Office
Remote	Remote Office
MGMT	Management
FW	Firewall
SW	Switch
REM	Remote
PC	Personal Computer
Distro	Distribution Switch
ISP	Internet Service Provider

Testing Method

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

This test will simply demonstrate connectivity between devices across different switches and VLANs. The device will demonstrate connectivity between the following devices:

MAIN-USER-PC02 | Vlan 400 | MAIN-AS-1 <-> MAIN-USER-PC01 | Vlan 400 | MAIN-AS-2
MAIN-USER-PC02 | Vlan 400 | MAIN-AS-1 <-> MAIN-MGMT-PC | Vlan 80 | Main-Core/Distro-2

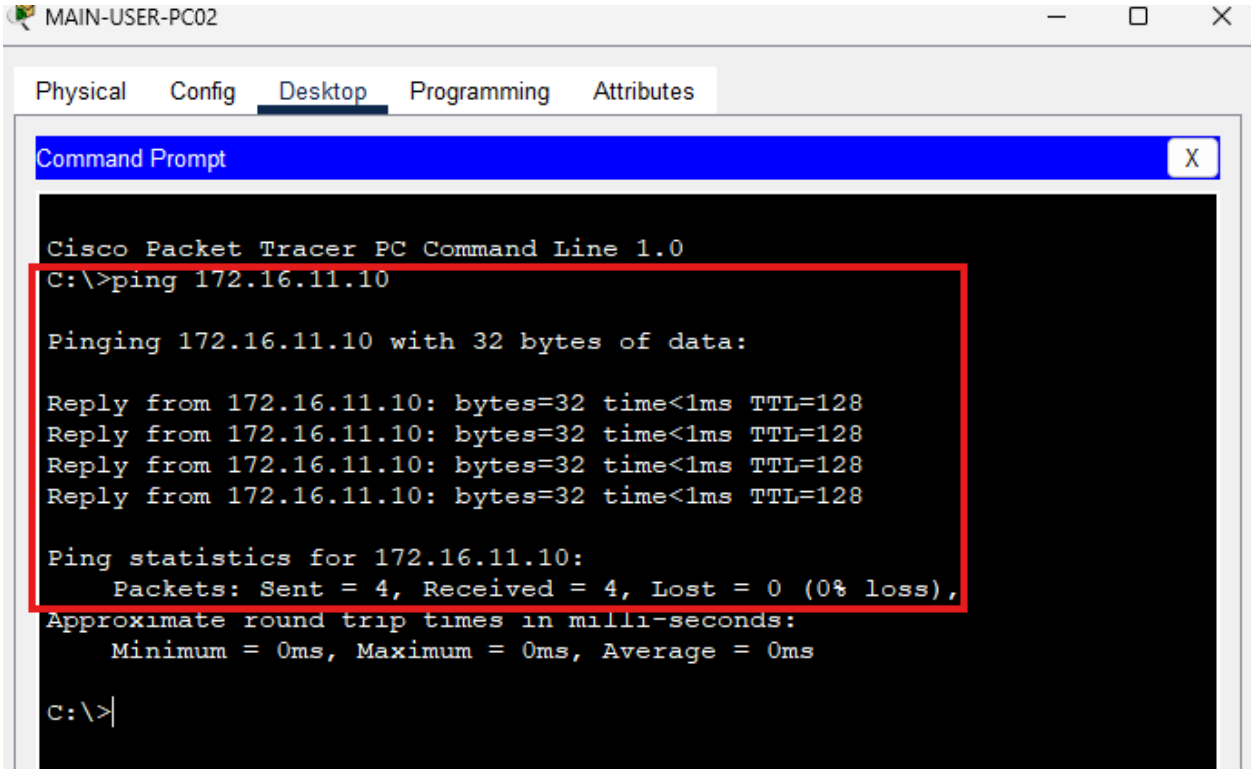
At the end of each demonstration of connectivity, we will explore the interfaces that made this connectivity possible.

Process List

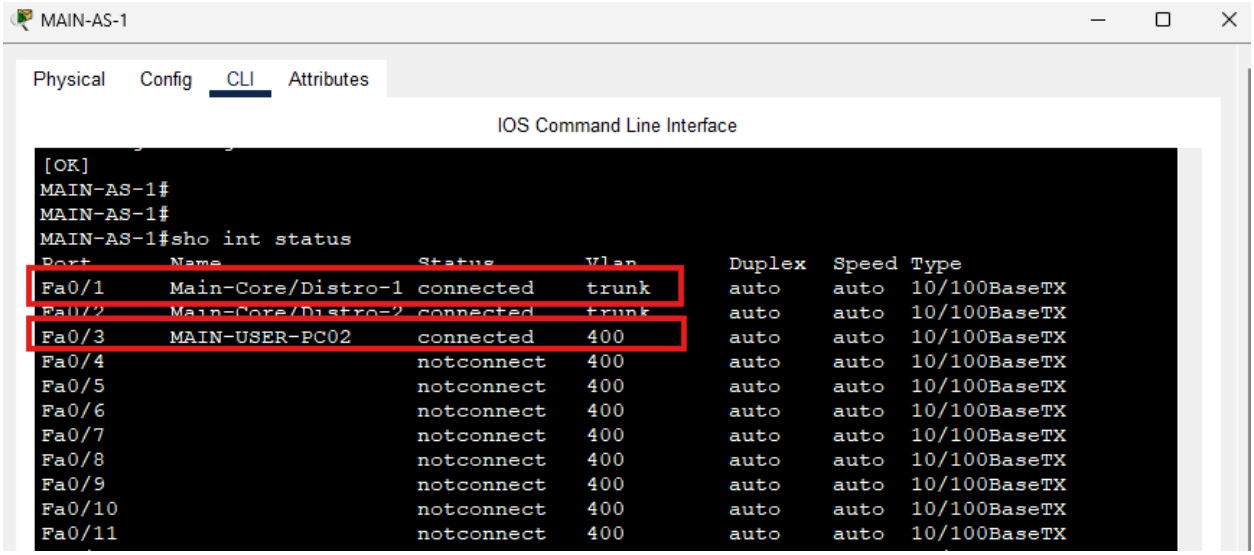
*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

Step 1: On MAIN-USER-PC02, go to desktop, open the command prompt and ping 172.16.11.10 (MAIN-

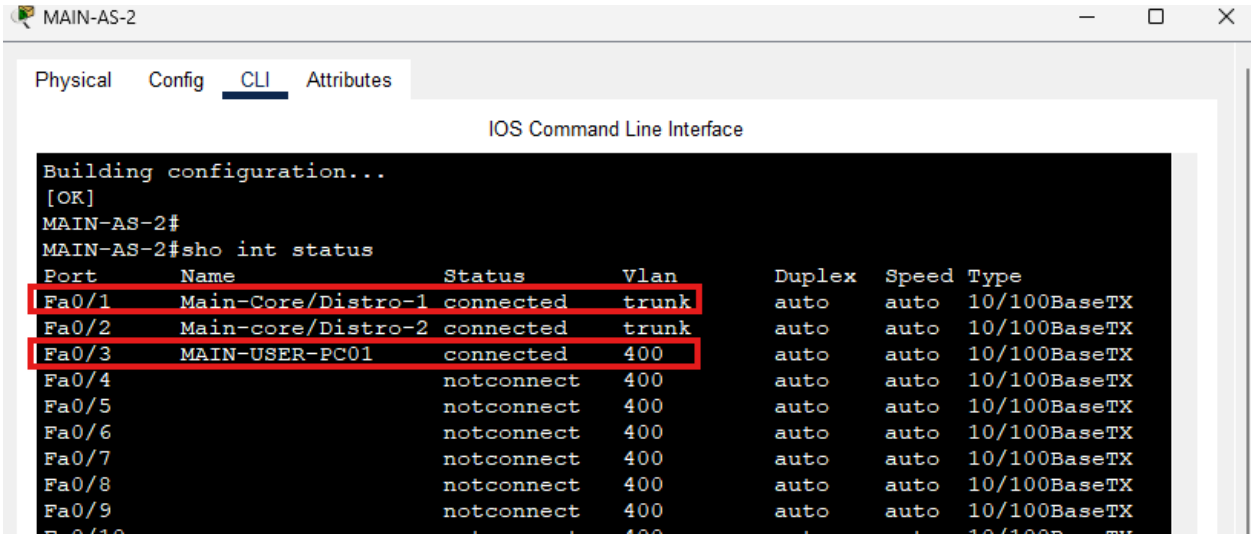
USER-PC01).



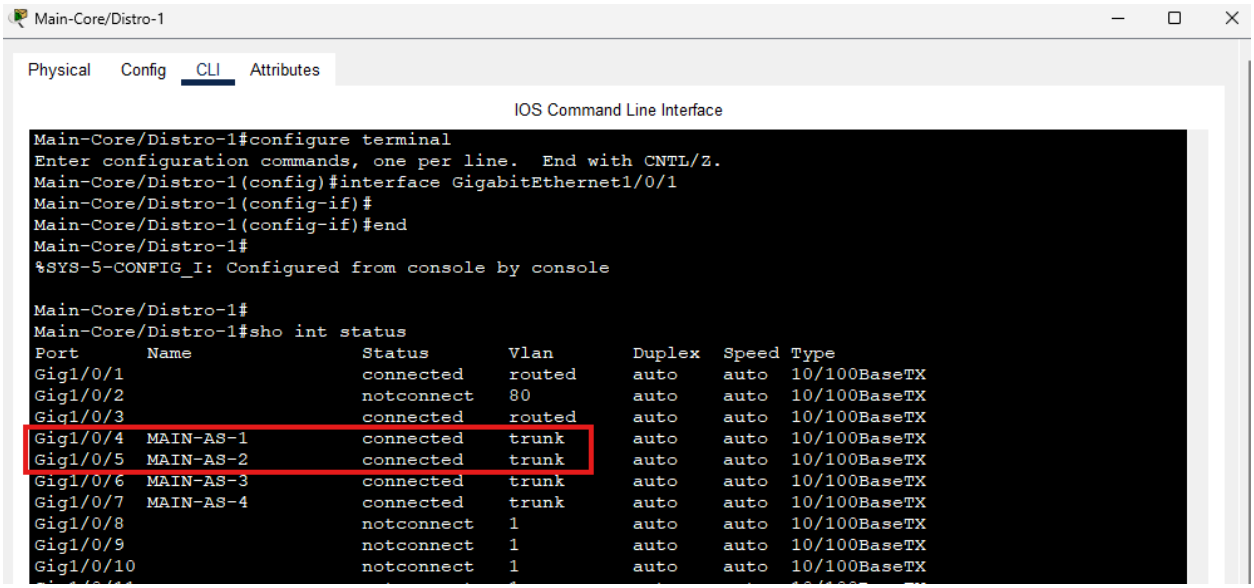
Step 2: On MAIN-AS-1, login and run the command *show interface status* to see the interface and Vlan for MAIN-USER-PC02.



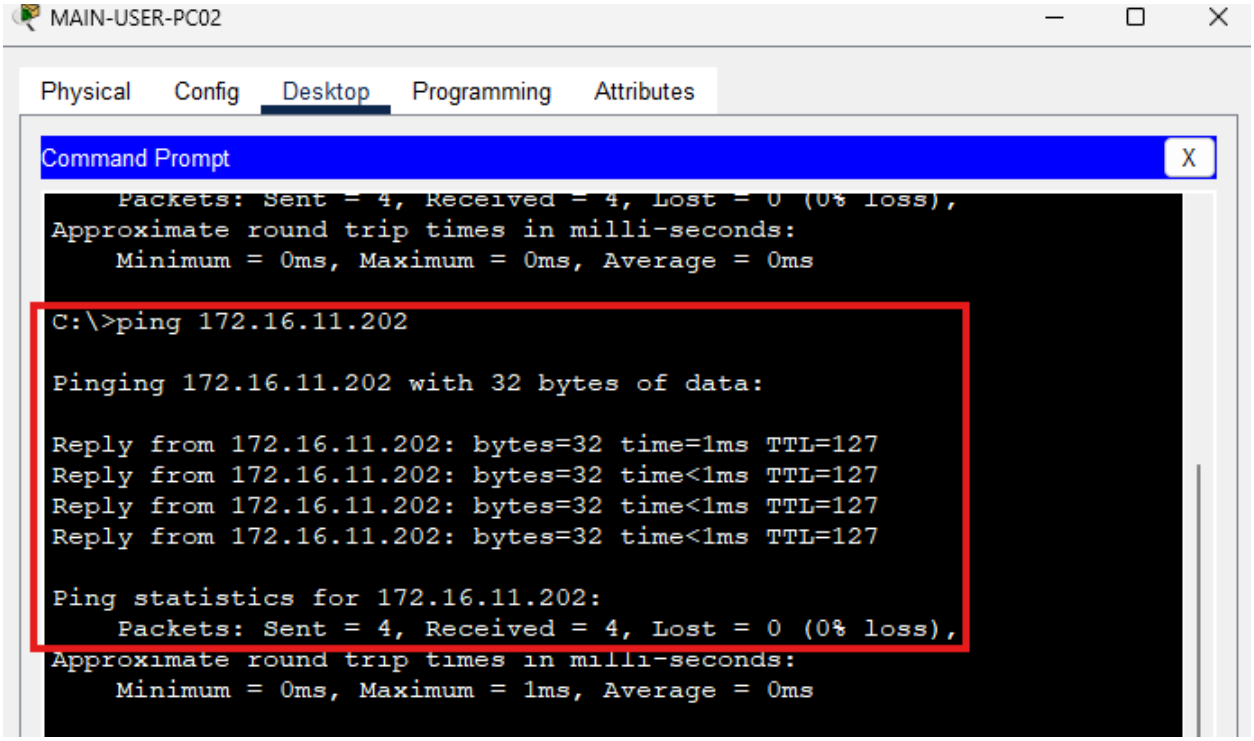
Step 3: On MAIN-AS-2, login and run the command *show interface status* to see the interface and VLAN for MAIN-USER-PC01.



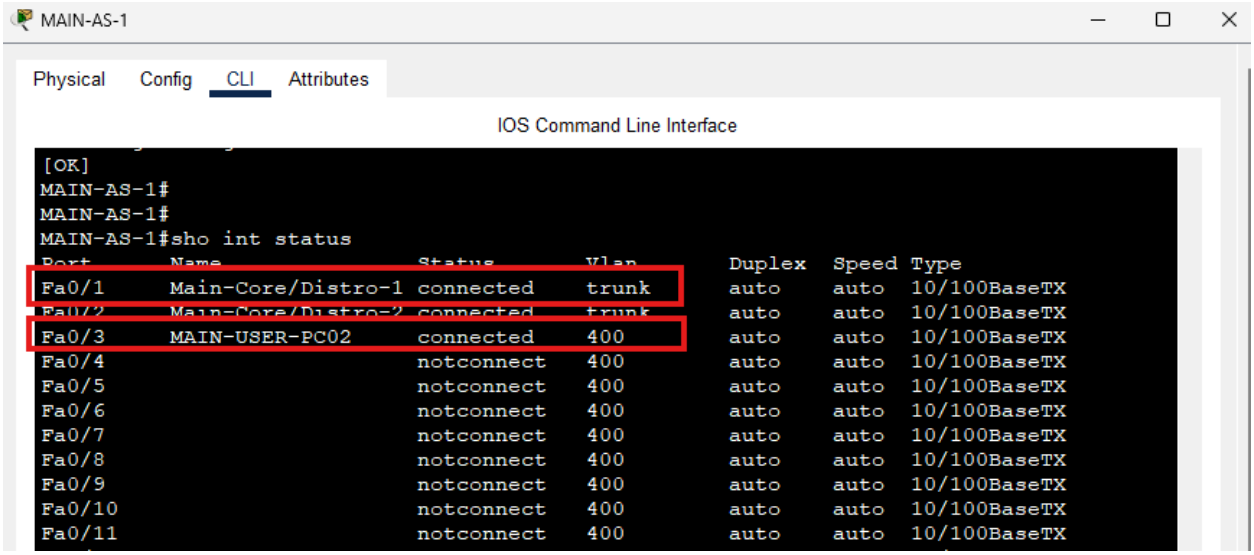
Step 4: On Main-core/Distro-1, login and run the command *show interface status* to see the trunk interfaces for each switch.



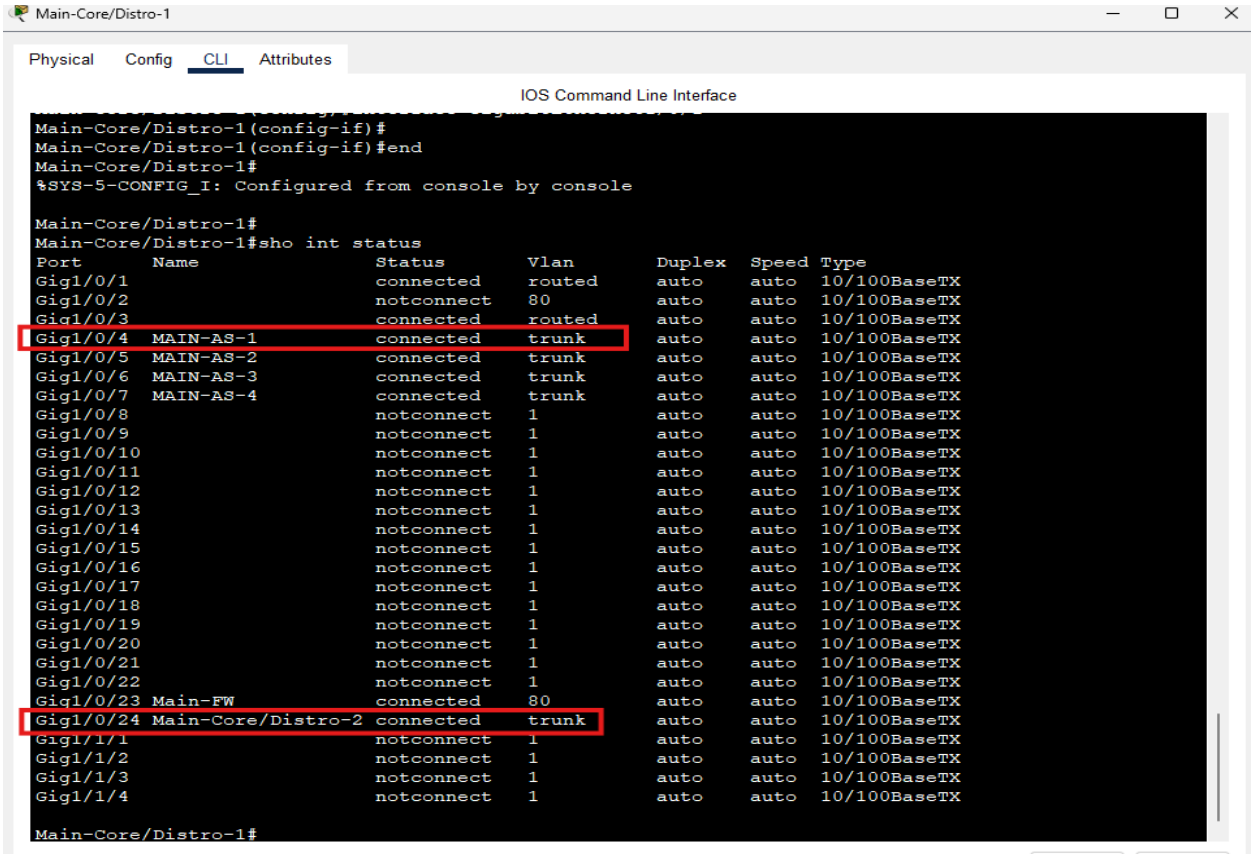
Step 5: On MAIN-USER-PC02, go to desktop, open the command prompt and ping 172.16.11.202 (MAIN-MGMT-PC).



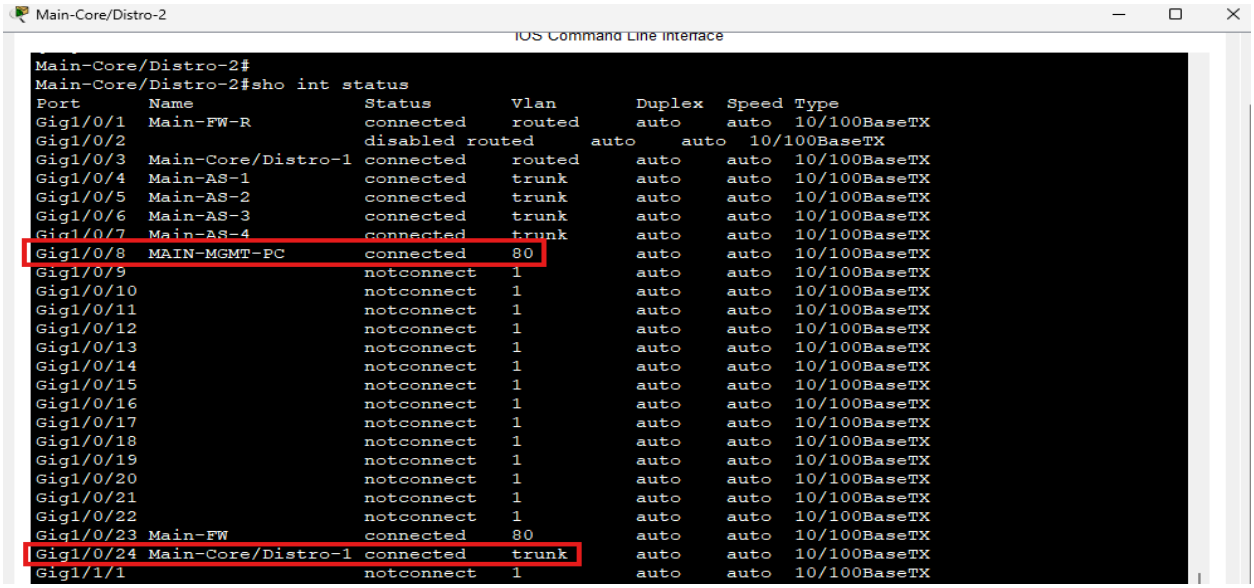
Step 6: On MAIN-AS-1, login and run the command *show interface status* to see the interface and Vlan for MAIN-USER-PC02.



Step 7: On Main-Core/Distro-1, login and run the command *show interface status* to see the interface for Main-AS-1 and Main-Core/Distro-2.



Step 8: On Main-Core/Distro-2, login and run the command *show interface status* to see the interface for MAIN-MGMT-PC.



Test Case #8: Advanced Network Routing

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.*

Configure OSPF and BGP. Establish adjacency and neighborship between devices and ensure all Layer 3 devices are advertising and are updating their routing tables.

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 configured with OSPF for internal network routing at the Main Office site and the Remote Office site. Each device falls under OSPF area 0 for this network. OSPF is not shared with external network devices or interfaces.

Main Office OSPF configured devices:

- Main-Edge-RT (Inside Interface)
- Main-FW
- Main-Core/Distro-1
- Main-Core/Distro-2

Remote Office OSPF configured Devices:

- Remote-Edge-RT
- Remote-FW
- Remote-Core/Distro-1

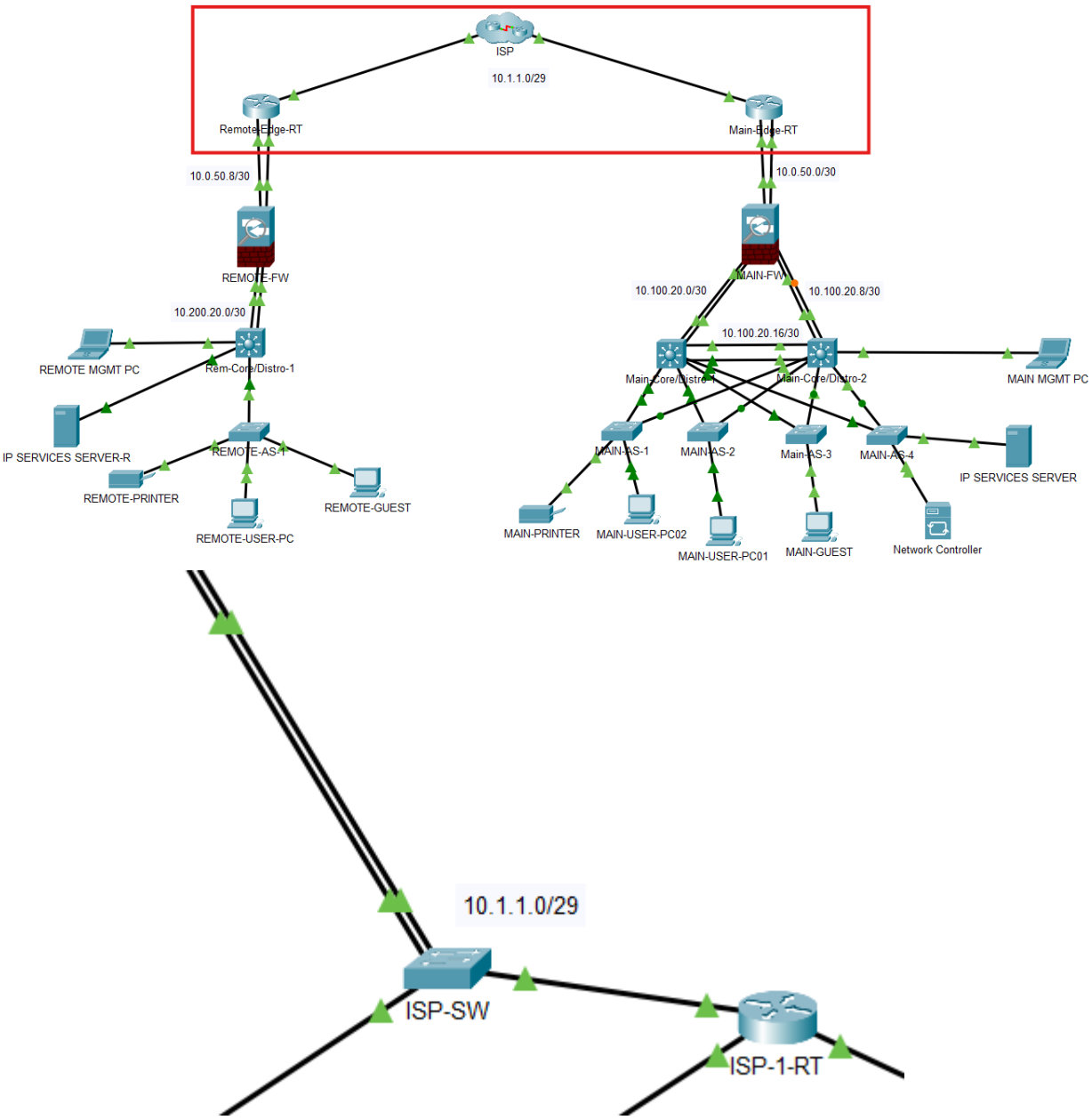
The Mock ISP is configured with BGP for neighborship between the Edge Routers and the ISP router itself. The ISP is part of AS 40000, the Main-Edge RT is part of AS 41000, and the Remote-Edge is part of AS 42000.

ISP BGP configured devices:

- ISP RT: 10.1.1.1/29
- Main-Edge: 10.1.1.2/29 (Outside Interface)
- Remote-Edge: 10.1.1.3/29 (Outside Interface)

Network Diagram or Segment

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



Legend	
IP	Internet Protocol
RT	Router
AS	Access Switch
Main	Main Office
Remote	Remote Office
MGMT	Management
FW	Firewall
SW	Switch
REM	Remote
PC	Personal Computer
Distro	Distribution Switch
ISP	Internet Service Provider

Testing Method

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

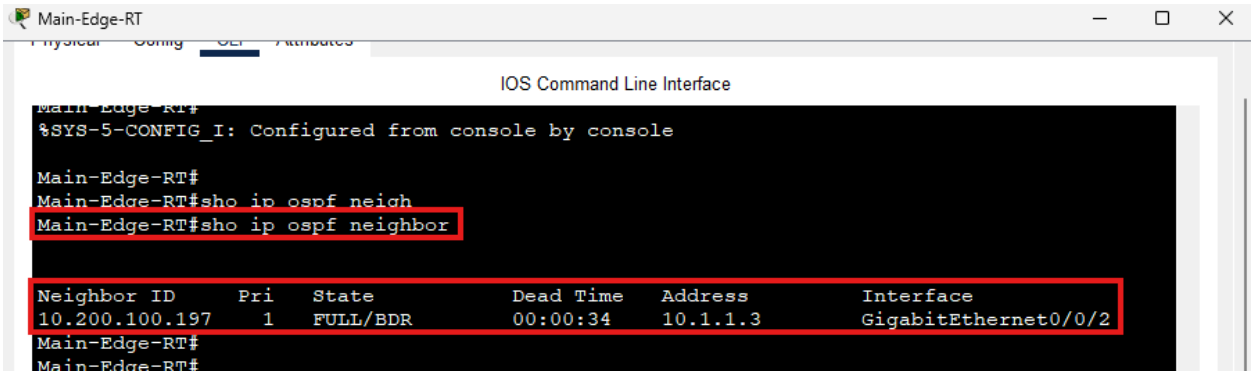
To verify the configuration of OSPF, we will see OSPF neighborship between network devices inside both the Main Office site and the Remote site. Then we will see the routing table inside each site's firewalls. The significance here is that most internal networks are not configured on firewalls and require link-state advertisements to learn the necessary routes. Lastly, we will clear the routing table information and reset an interface in the remote firewall to observe adjacency behavior, confirming that OSPF is configured and learning routes.

To verify the BGP configuration, we will visit the ISP-RT and check the current neighborship status. Lastly, we will clear the BGP database from the ISP-RT and observe as it establishes neighbor adjacency and learns routes.

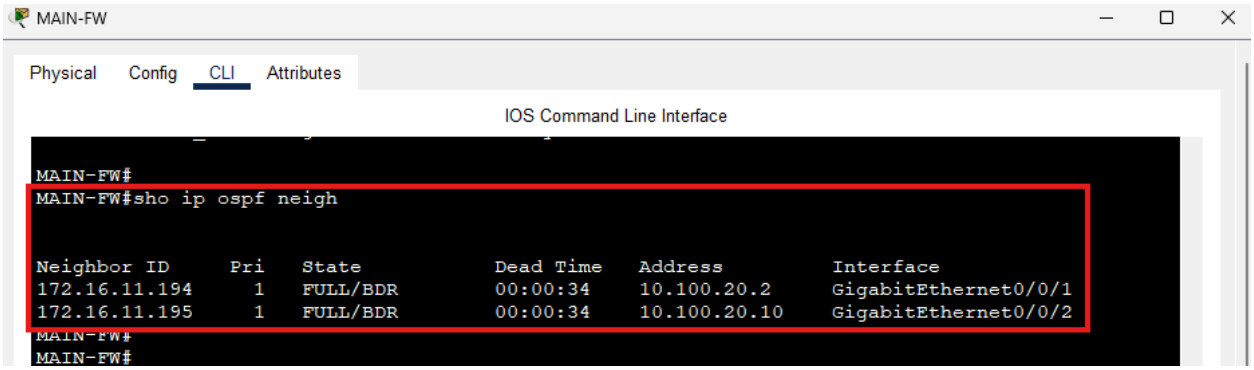
Process List

*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.*

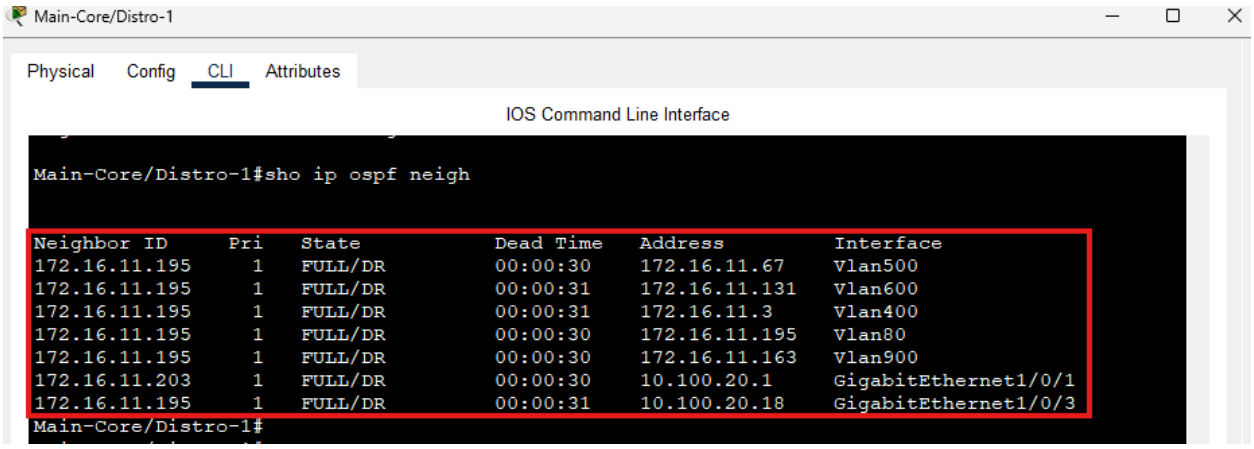
Step 1: Login to Main-Edge-RT, run the command *show ip ospf neighbor*. Here we can see the current neighbor being the inside interface G0/0/2.



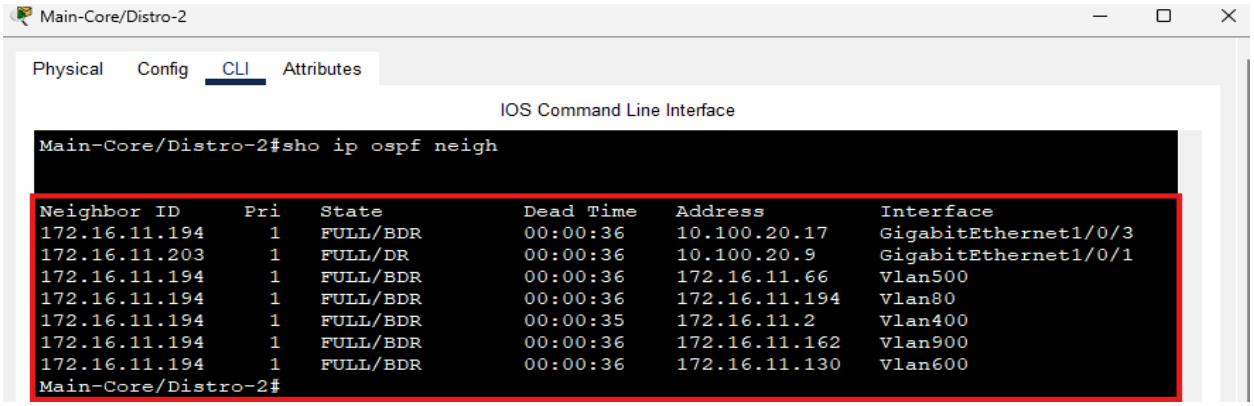
Step 2: Login to Main-FW, run the command ***show ip ospf neighbor***. Here we can see any ospf neighbors.



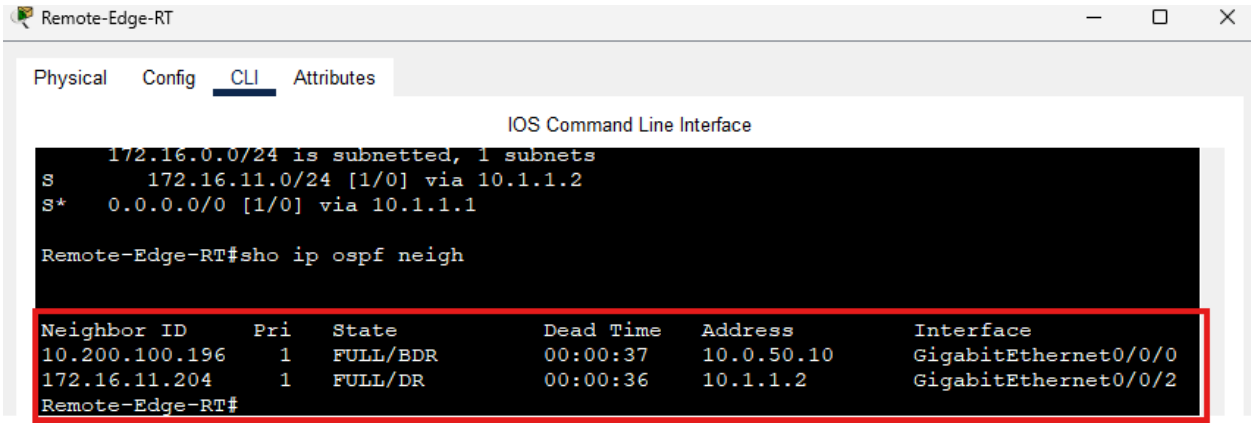
Step 3: Login to Main-Core/Distro-1, run the command ***show ip ospf neighbor***. Here we can see any ospf neighbors.



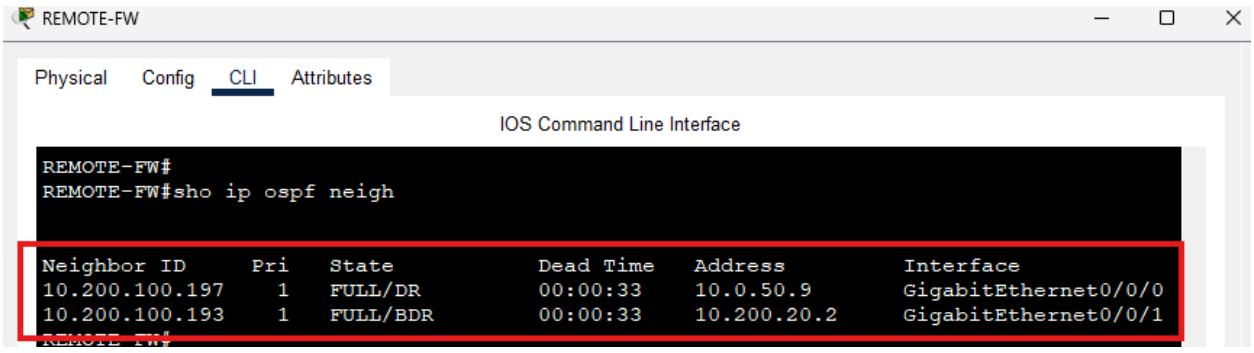
Step 4: Login to Main-Core/Distro-2, run the command ***show ip ospf neighbor***. Here we can see any ospf neighbors.



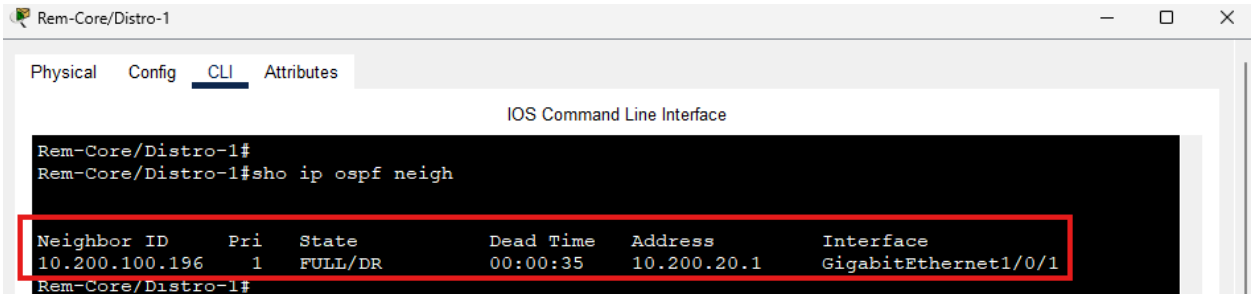
Step 5: Login to Remote-Edge-RT, run the command ***show ip ospf neighbor***. Here we can see any ospf neighbors.



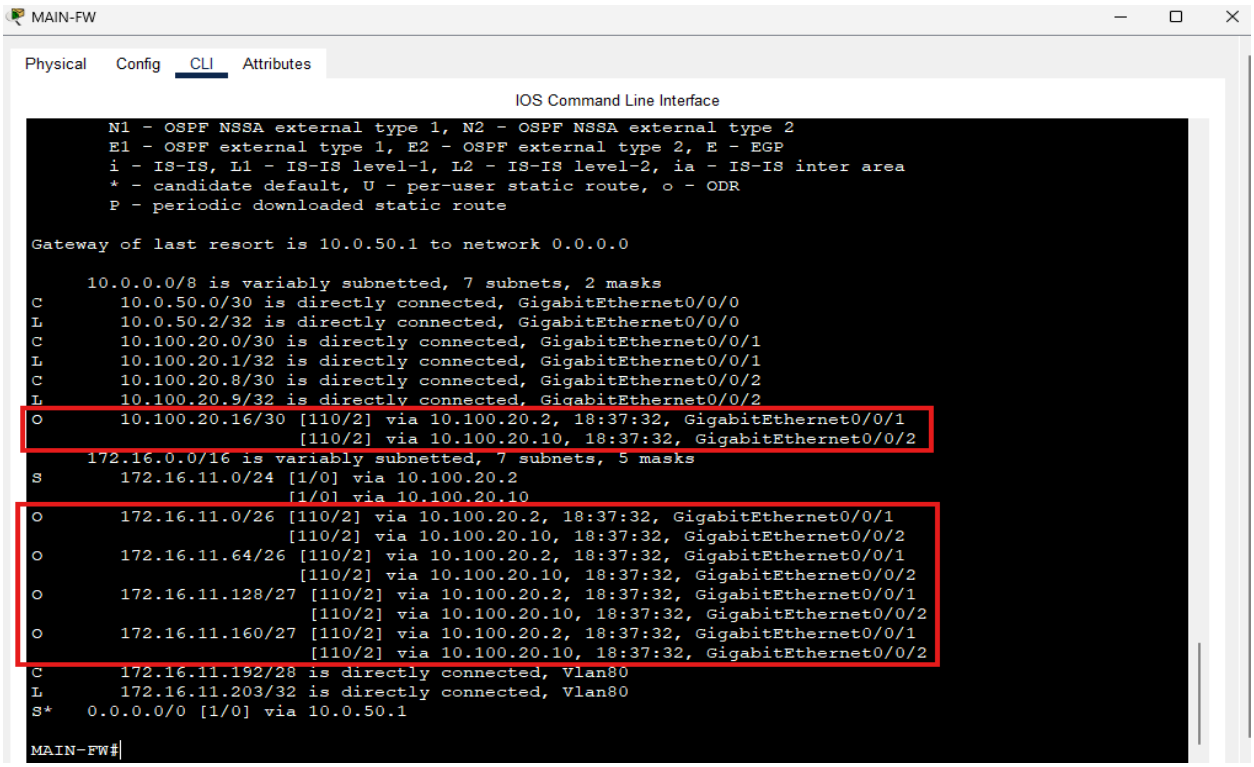
Step 6: Login to Remote-FW, run the command ***show ip ospf neighbor***. Here we can see any ospf neighbors.



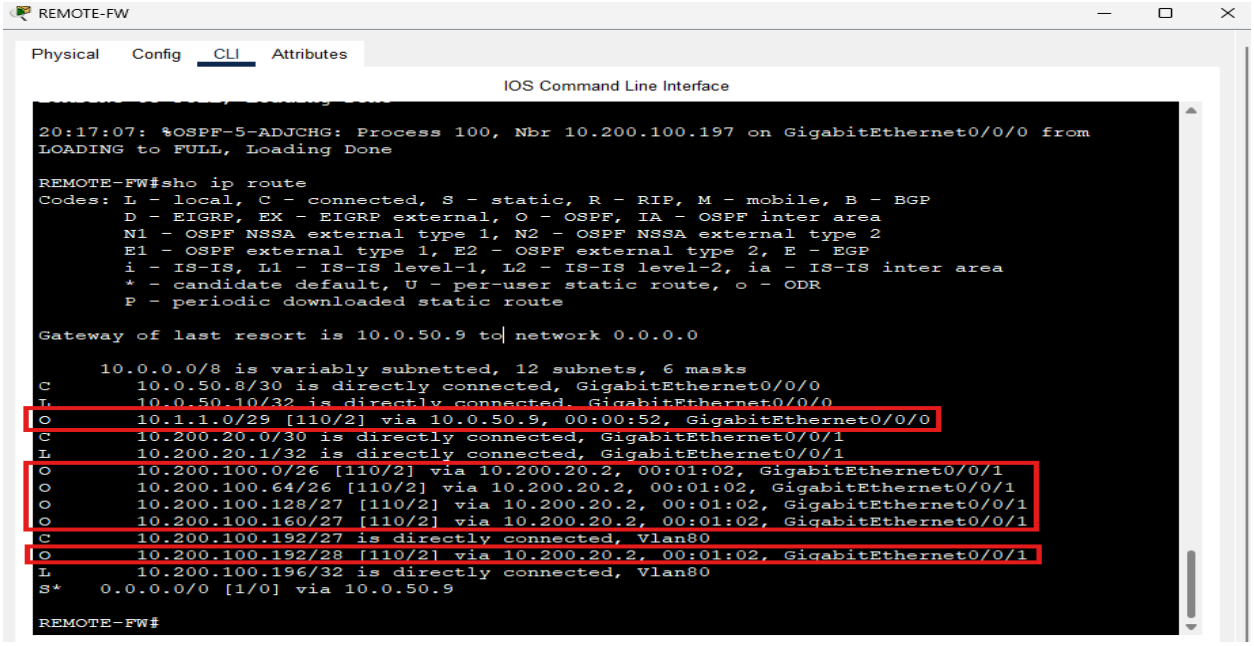
Step 7: Login to Remote-Core/Distro-1, run the command ***show ip ospf neighbor***. Here we can see any ospf neighbors.



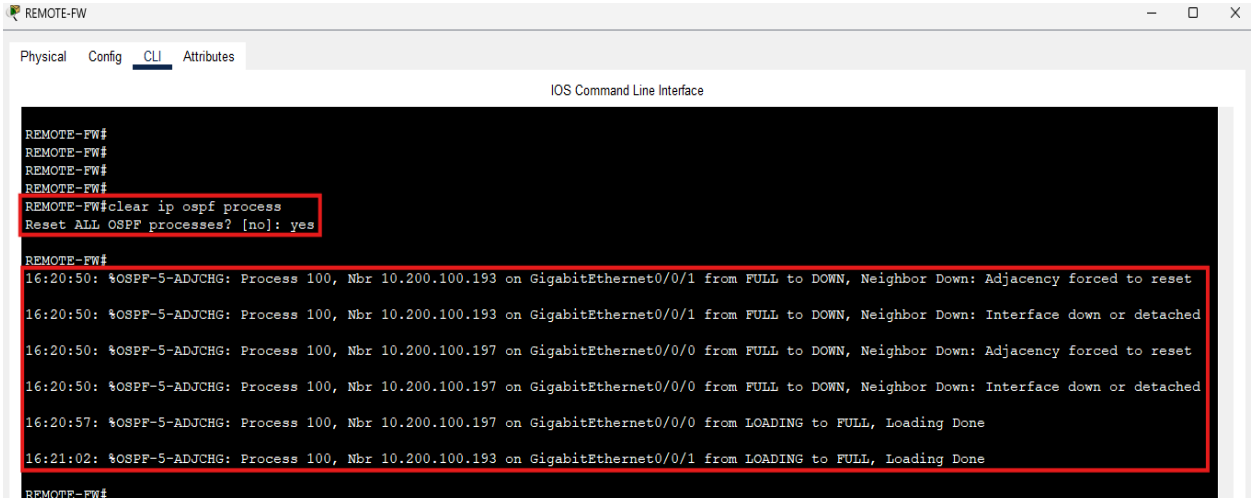
Step 8: Return to the Main-FW, login, and run the command ***show ip route***. This will display the routing table, and we can see the routes learned over OSPF.



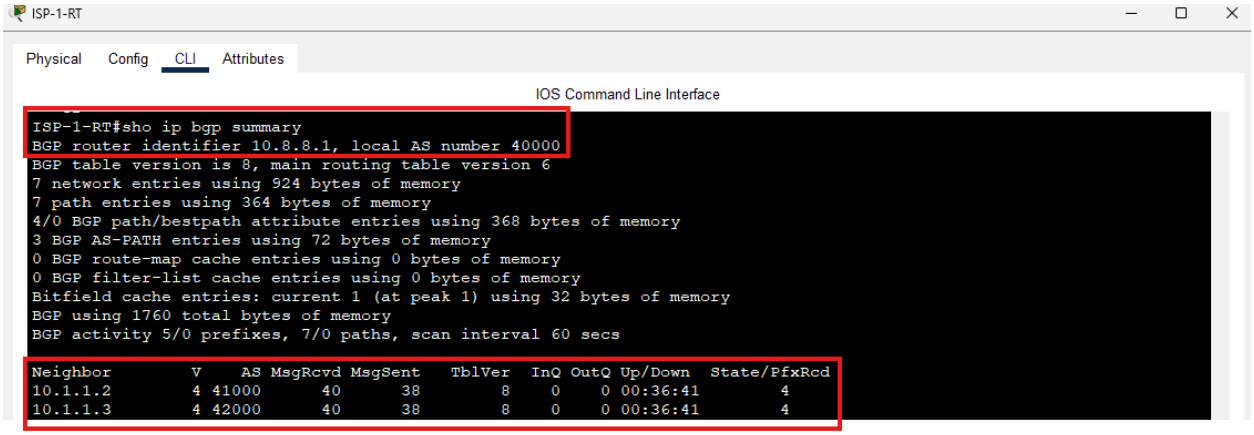
Step 9: On Remote-FW, login, and run the command ***show ip route***. This will display the routing table, and we can see the routes learned over OSPF.



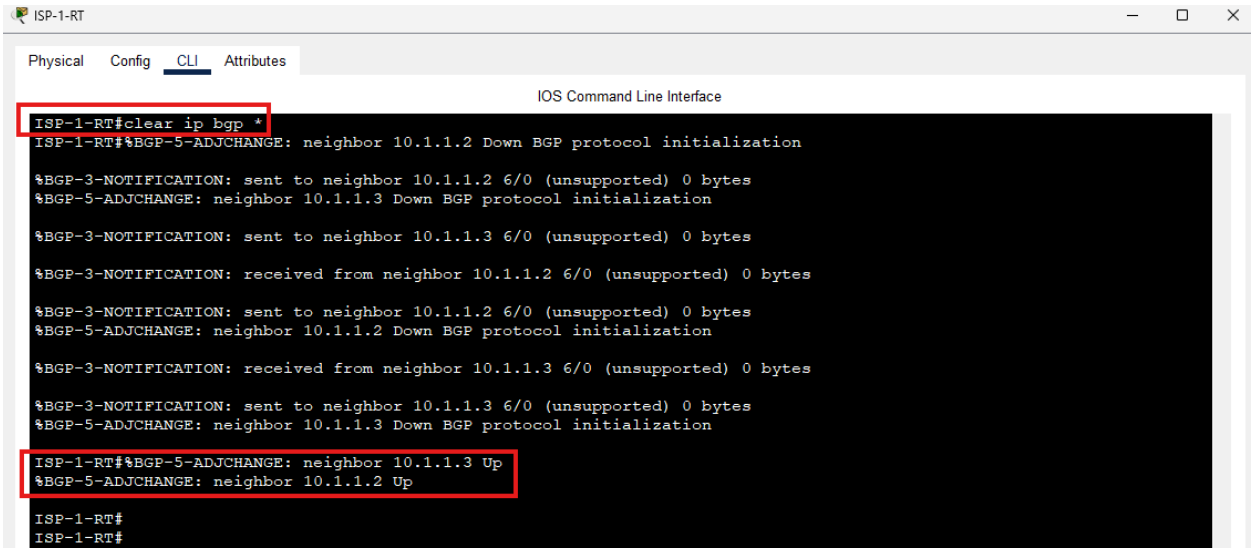
Step 10: Login to Remote-FW. Run the command ***clear ip ospf process*** *-> yes.* This will restart OSPF on the firewall and re-initialize neighbor adjacency.



Step 11: Login to ISP-RT, run the command ***show ip bgp summary***. This will display neighborship status and the number of learned prefixes, demonstrating adjacency and route learning.



Step 12: On ISP-RT, run the command ***clear ip bgp ** to reset bgp on the router and wait 30 – 60 seconds for adjacency to establish.



Test Case #9: IPSec Site-to-Site VPN

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 IPSec.*

Implement IPSec Site-to-Site VPN. Verify the tunnel is established and devices from the remote site can access resources from the Main site, and vice versa. Ensure the traffic is fully encrypted until it arrives at the destination site.

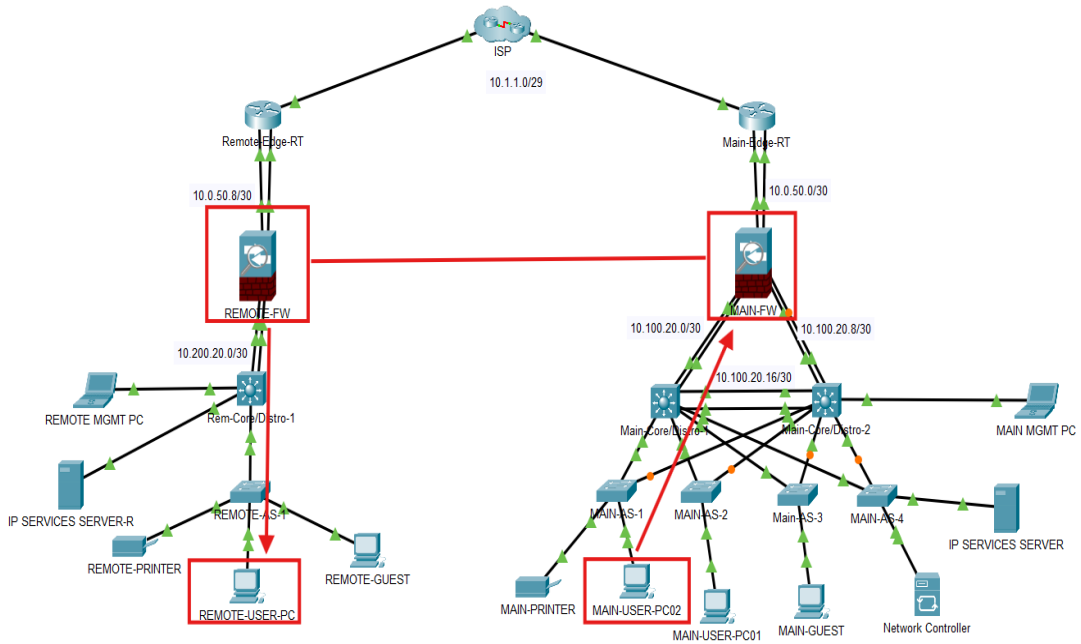
Functionality

*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 Main and Remote Office sites communicate over an IPSec site-to-site VPN. VPN communication originates at each site from the firewalls. This configuration allows all traffic with a destination IP address of the opposite site to be encrypted while traversing the public network. For example, when a device in the Main Office sends traffic to a device in the Remote Office, traffic will travel over the network tunnel established between Main-FW and Remote-FW.

Network Diagram or Segment

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



Legend	
IP	Internet Protocol
RT	Router
AS	Access Switch
Main	Main Office
Remote	Remote Office
MGMT	Management
FW	Firewall
SW	Switch
REM	Remote
PC	Personal Computer
Distro	Distribution Switch
ISP	Internet Service Provider

Testing Method

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

Simulation mode in Packet Tracer will be used to test the IPSec VPN functionality used in the network.

We will review the IPSec SA status at each firewall. After verifying that the tunnel is established, we will use MAIN-USER-PC02 to send ICMP messages to REMOTE-USER-PC and examine the traffic PDU before it enters the VPN, while it is traversing the tunnel, and after it exits, verifying that the traffic is protected.

MAIN-USER-PC02 IP Address: 172.16.11.11/26

REMOTE-USER-PC IP Address: 10.200.100.10/26

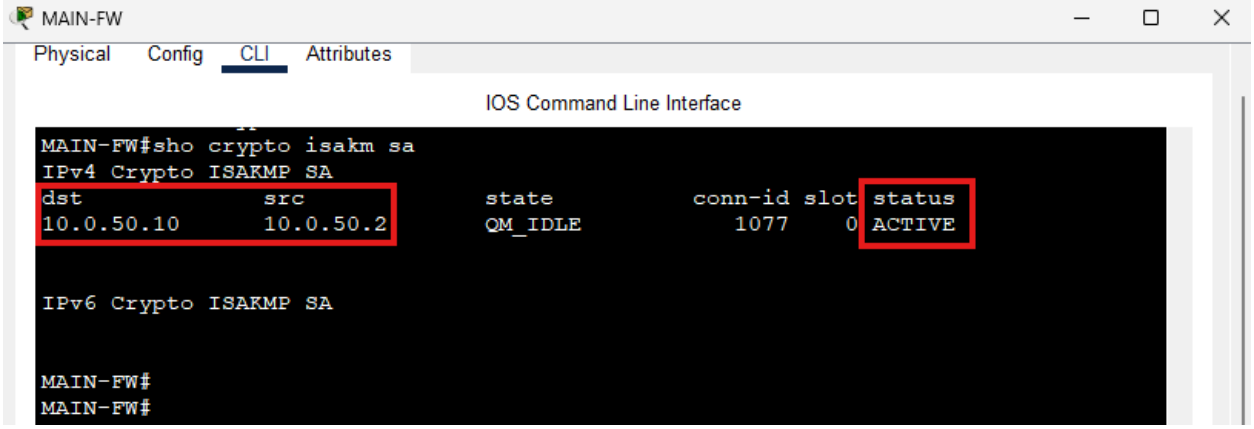
Main-FW: Outbound Interface IP: 10.0.50.2/30

Remote-FW: Outbound Interface IP: 10.0.50.10/30

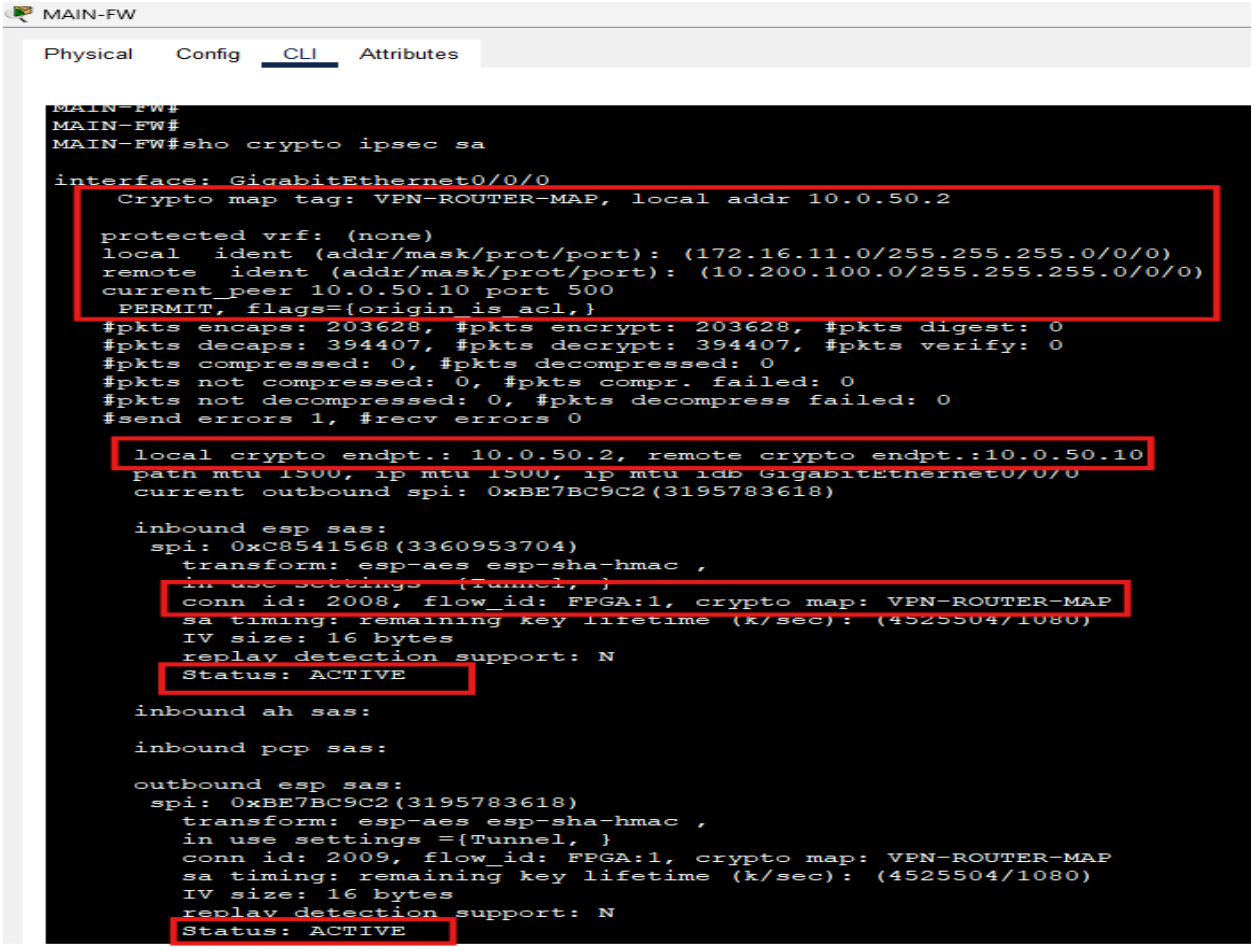
Process List

*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.*

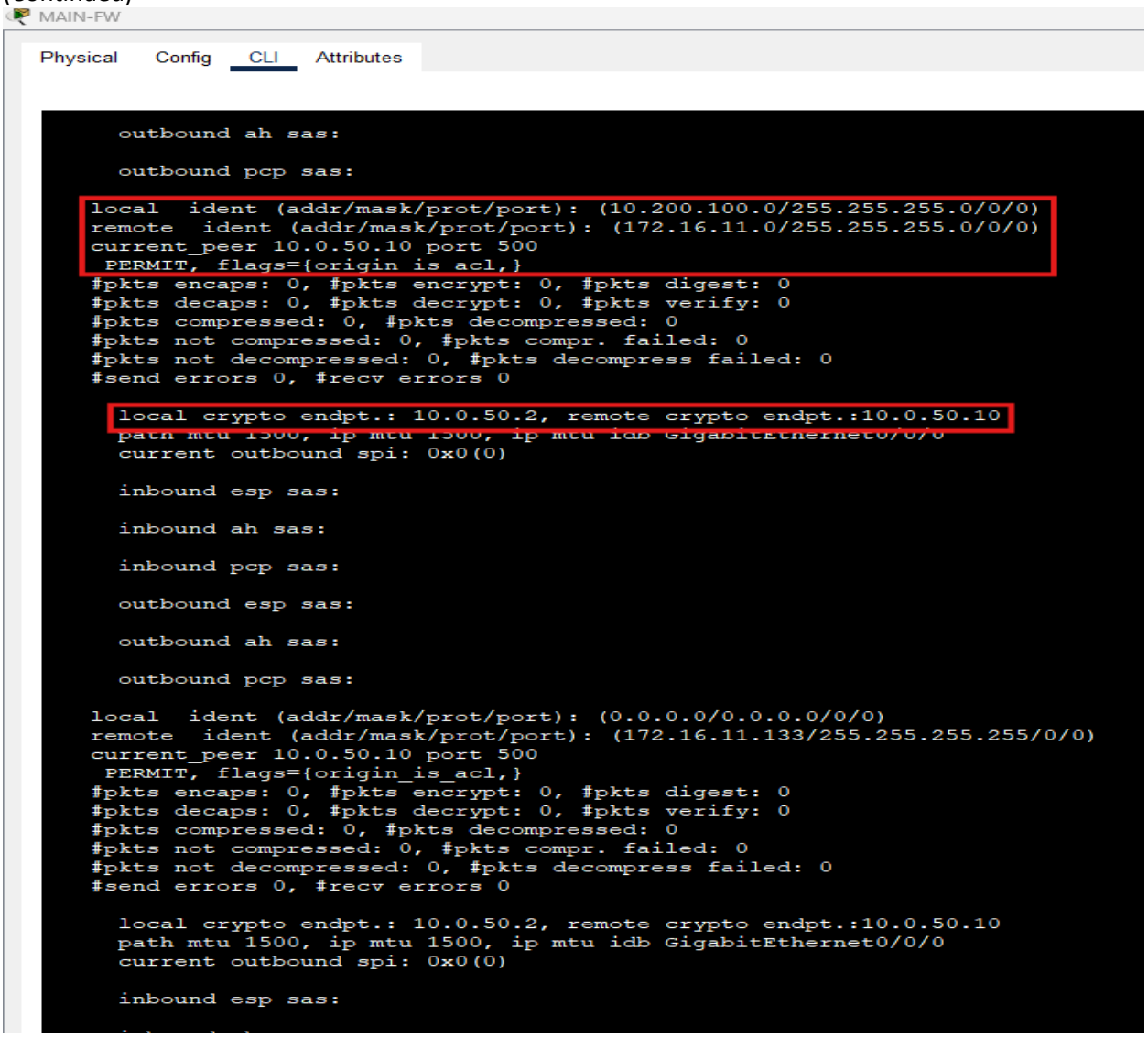
Step 1: Login to Main-FW and run the commands ***show crypto isakmp sa*** to see the status of the tunnel.



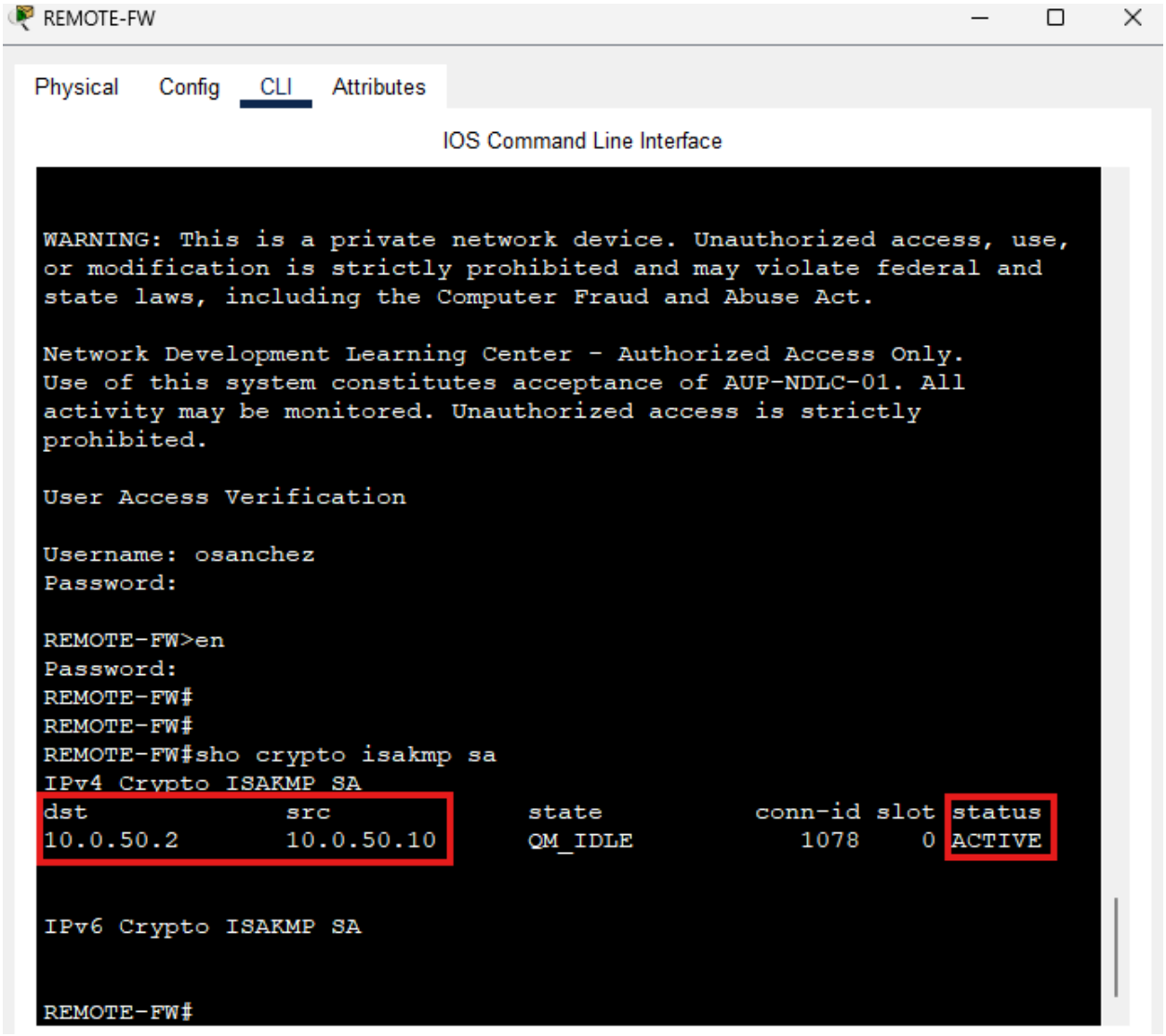
Step 2: Still on Main-FW, run the command ***show crypto ipsec sa*** to observe the security associations.



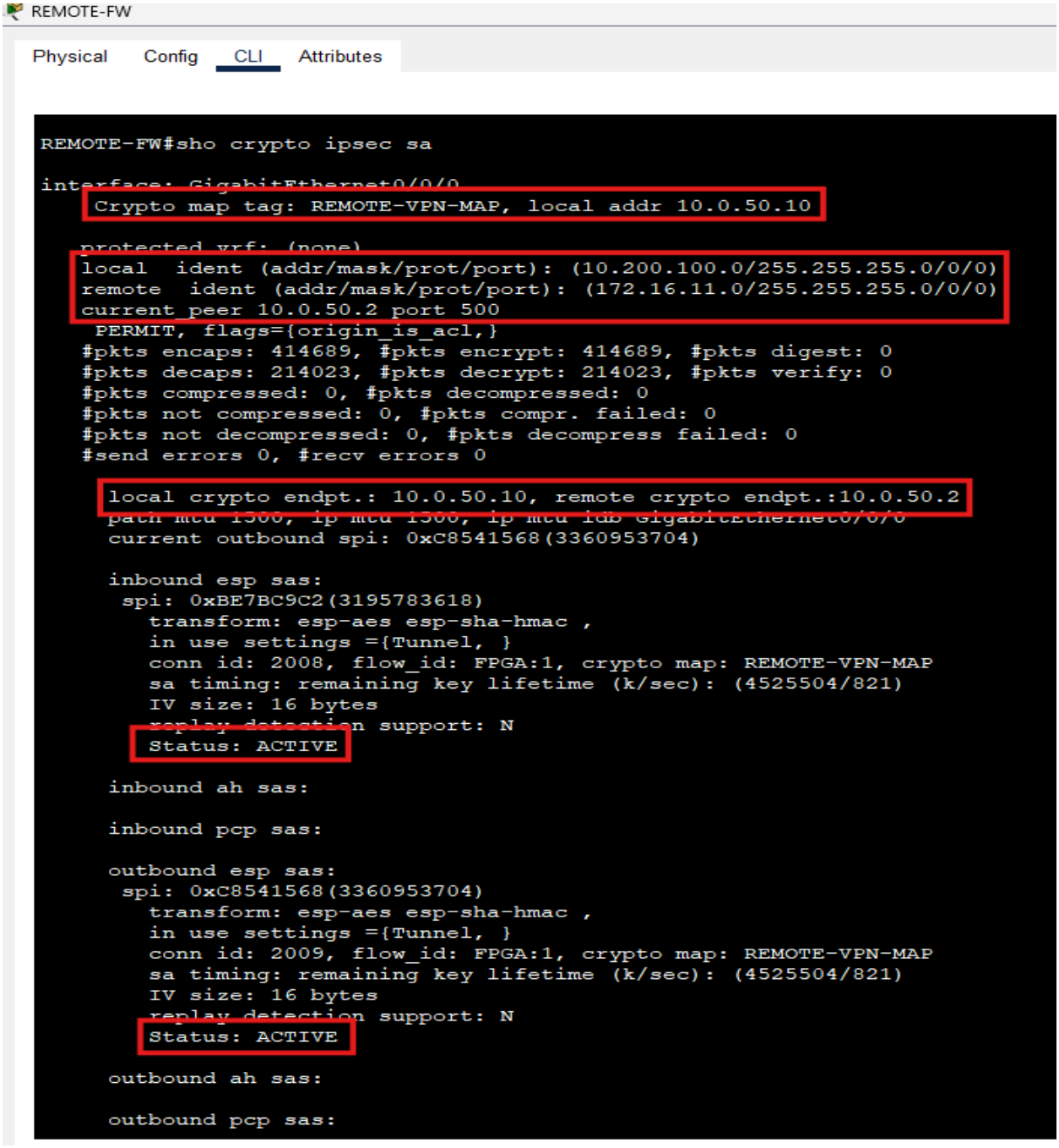
(Continued)

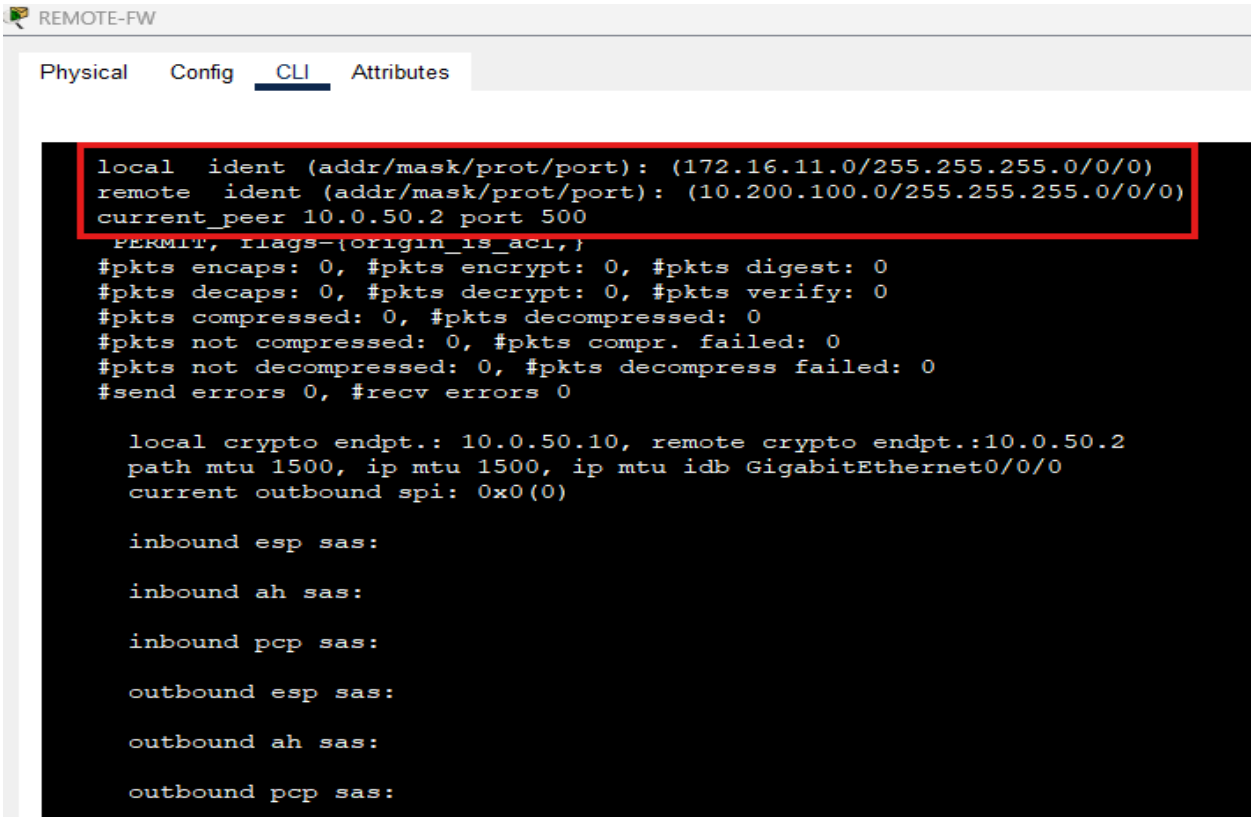

MAIN-FW
Physical
Config
CLI
Attributes
outbound ah sas:
outbound pcp sas:
local ident (addr/mask/prot/port): (10.200.100.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.11.0/255.255.255.0/0/0)
current_peer 10.0.50.10 port 500
PERMIT, flags={origin is acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 10.0.50.2, remote crypto endpt.:10.0.50.10
current outbound spi: 0x0(0)
inbound esp sas:
inbound ah sas:
inbound pcp sas:
outbound esp sas:
outbound ah sas:
outbound pcp sas:
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.11.133/255.255.255.255/0/0)
current_peer 10.0.50.10 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 10.0.50.2, remote crypto endpt.:10.0.50.10
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
current outbound spi: 0x0(0)
inbound esp sas:

Step 3: Login to Remote-FW and run the commands *show crypto isakmp sa* to see the status of the tunnel.

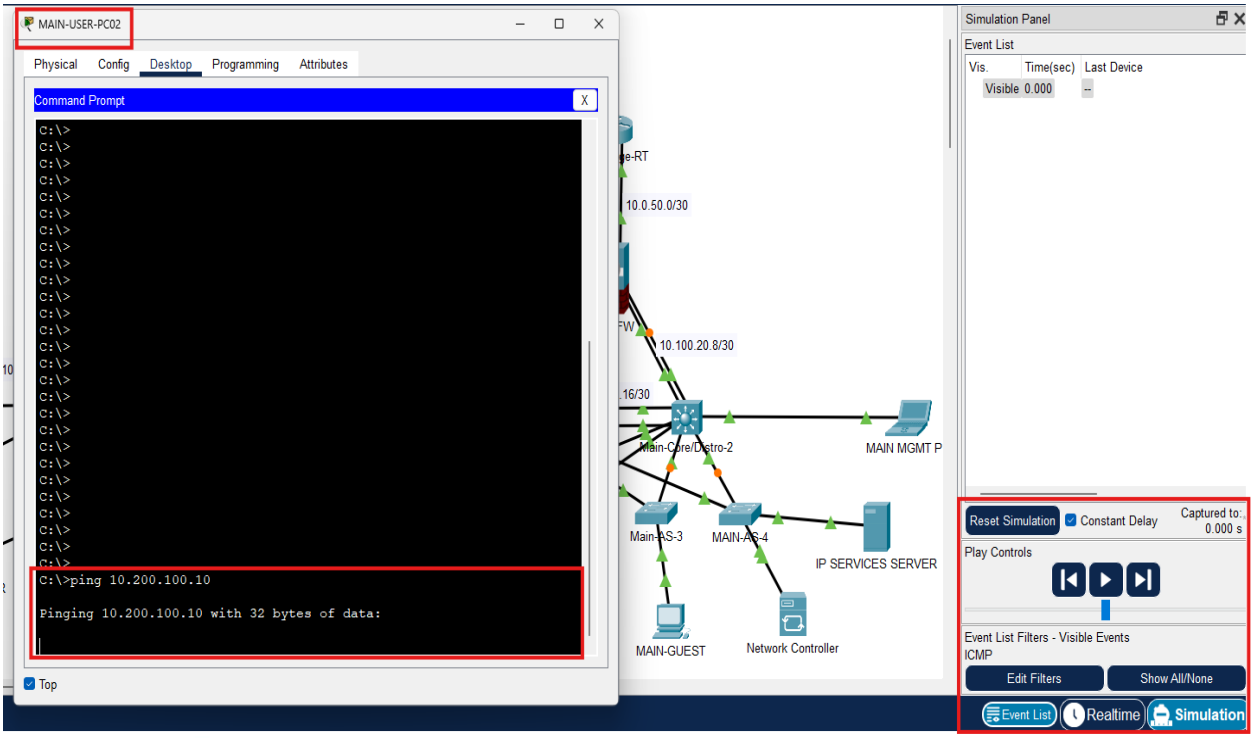


Step 4: Still on Remote-FW, run the command *show crypto ipsec sa* to observe the security associations.

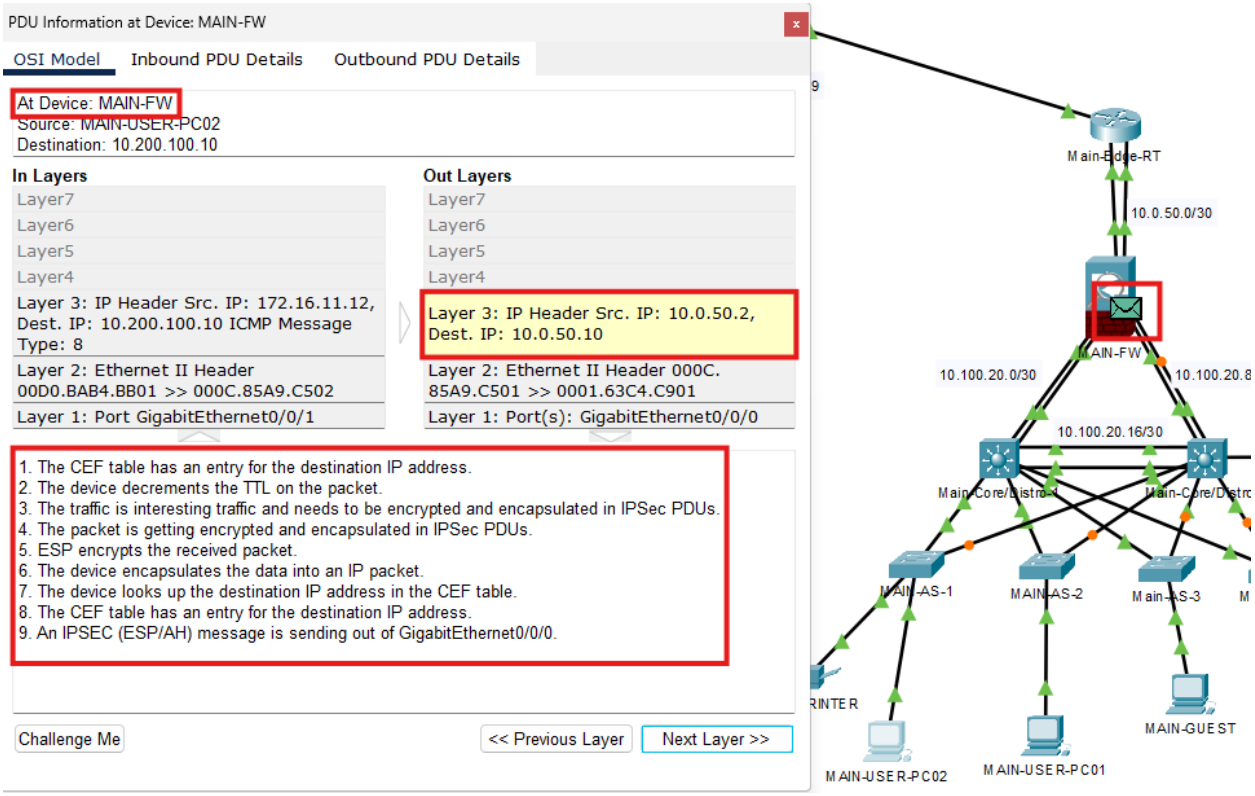




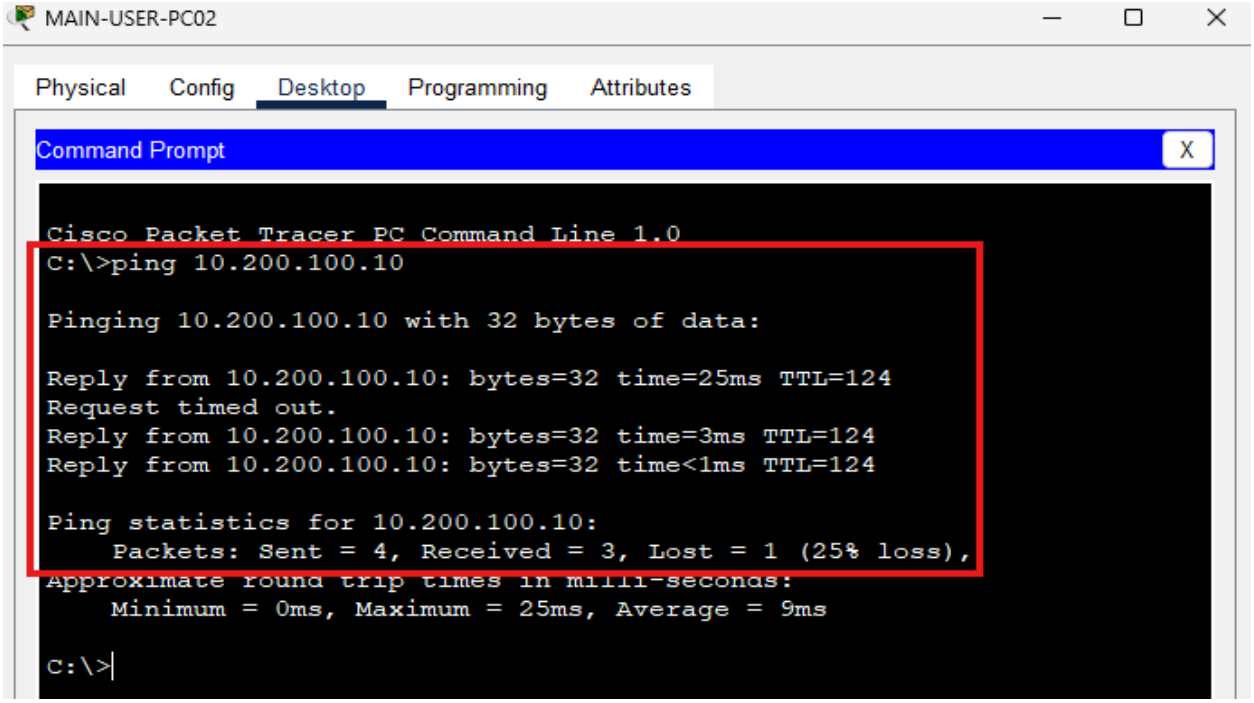
Step 5: Enter simulation mode and filter for ICMP traffic. On MAIN-USER-PC02, go to desktop and open a command prompt. Ping REMOTE-USER-PC (10.200.100.10).



Step 6: Press play and observe as the packet traverses the network. When it reaches Main-FW pause the simulation. Open the PDU information panel. **Last Device: Main-Core/Distro-1, At Device: MAIN-FW**. Click “Next Layer” until the focus is on Out Layers, Layer 3 for a description of what occurs when the packet enters the firewall tunnel.



Step 7: Return to Realtime to exit Simulation mode and watch as MAIN-USER-PC02 completes its ping action.



Test Case #10: Network Security, AAA and 802.1x

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.*

Implement NAC through 802.1x. Verify that unverified devices are not allowed access to any resources, ensure alerts are sent to the syslog server and ports get shut down.

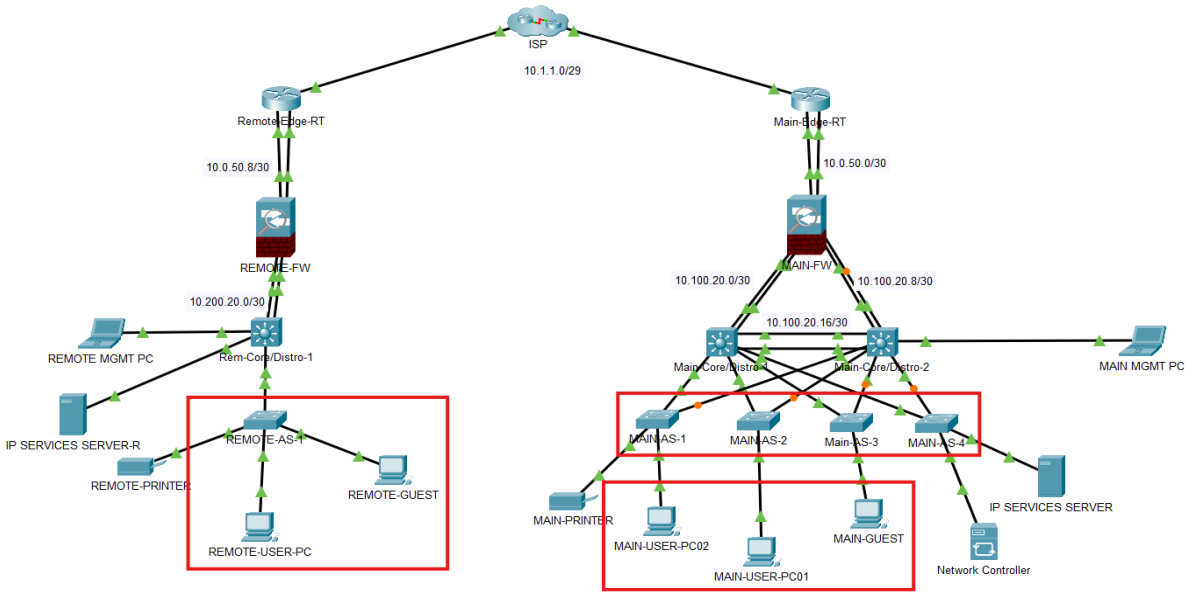
Functionality

*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.*

Network access controls (NAC) are a defense-in-depth methodology that prevents unauthorized network access through a centralized authentication server. This network implements dot1x for user and device authentication and network access at the network's perimeter. Configured on each access switch, a user must have an account to log in to the network and utilize network resources.

Network Diagram or Segment

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



Legend	
IP	Internet Protocol
RT	Router
AS	Access Switch
Main	Main Office
Remote	Remote Office
MGMT	Management
FW	Firewall
SW	Switch
REM	Remote
PC	Personal Computer
Distro	Distribution Switch
ISP	Internet Service Provider

Testing Method

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

Since unauthorized users cannot connect their devices to the network, we will test this functionality by connecting a rogue pc to MAIN-AS-2. We will observe that it does not authenticate and never establishes a connection to the network. Next, we will disconnect MAIN-USER-PC01 from the network and remove the current account from the device. We move on to connecting the device to the network again, input user credentials, and observe that over time, it is authorized and gains access to the network.

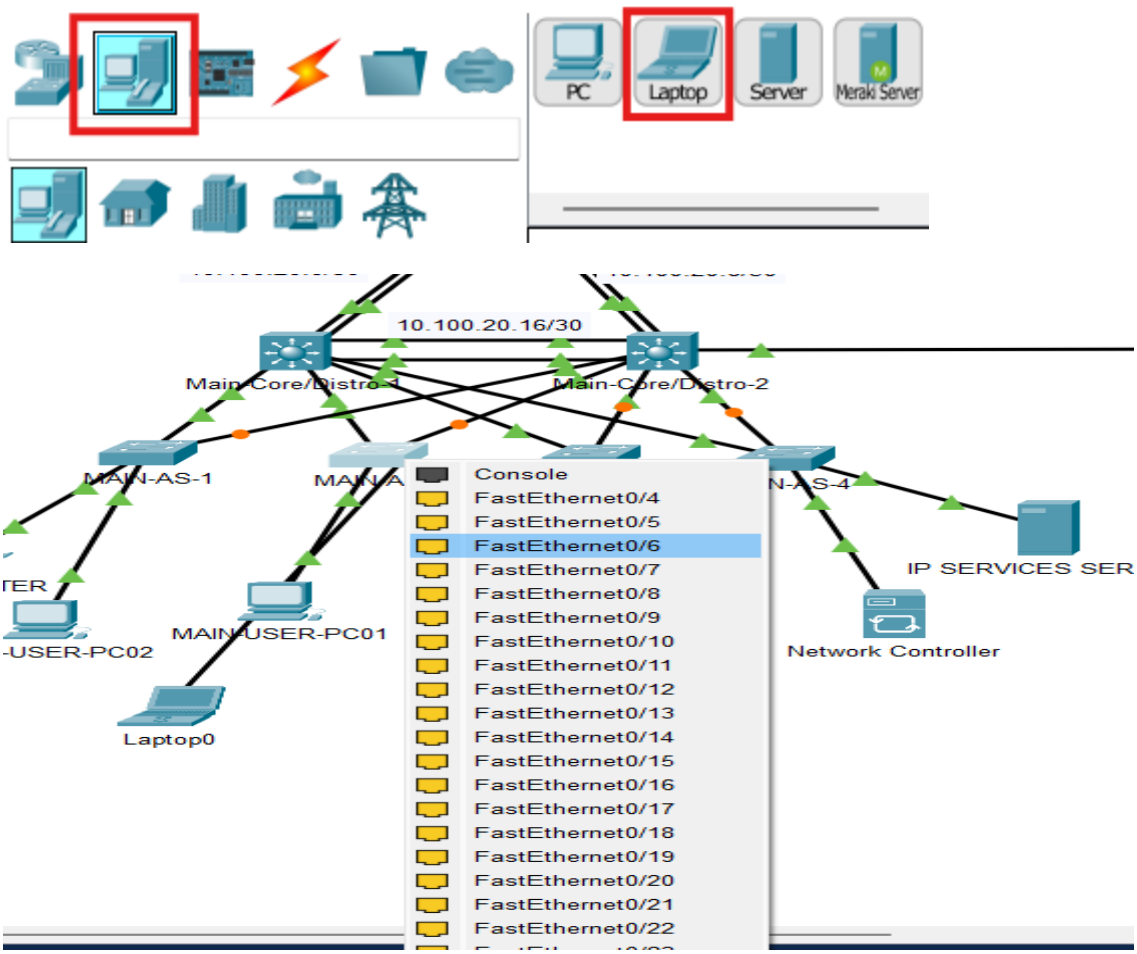
Note: Packet Tracer does not have full support for dot1x show commands. This prevents us from observing the authentication tables on access switches. To validate authentication, we must utilize the "link lights" feature of Packet Tracer as we witness it changing from amber to green.

Process List

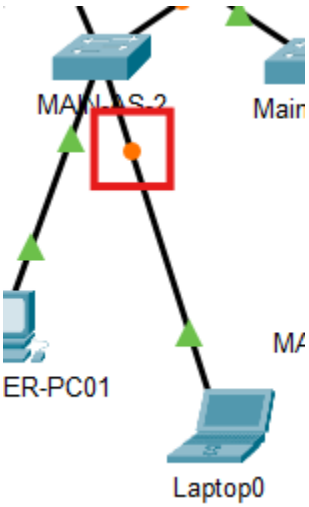
*Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.*

Step 1: From the device list, select [End Devices] to drag and drop a laptop into the network area.

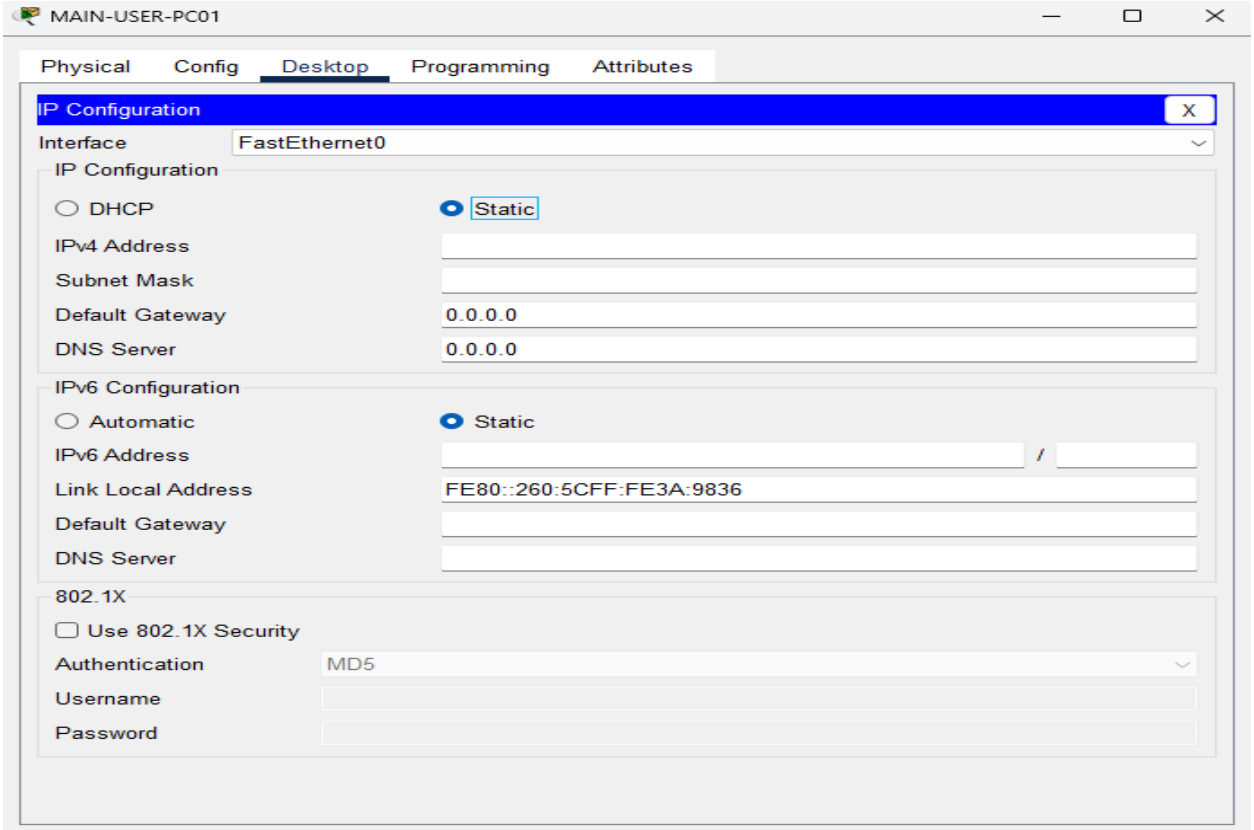
Connect the laptop to switchport Fast Ethernet 0/6 on switch MAIN-AS-2.



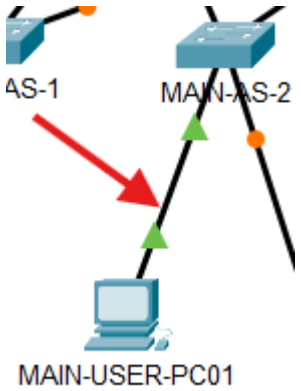
Step 2: Wait 2-5 minutes, observing the link-lights. The amber light will not change to green because the device is not authenticated with the Radius server.

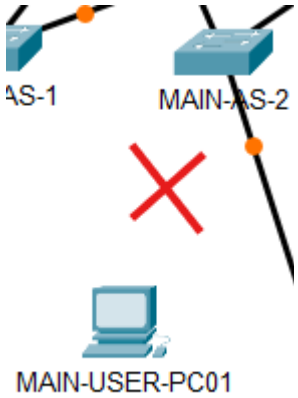


Step 3: On MAIN-USER-PC01, go to Desktop, and IP Configuration. Press the “Static” radio button and uncheck the “Use 802.1X Security” checkbox.

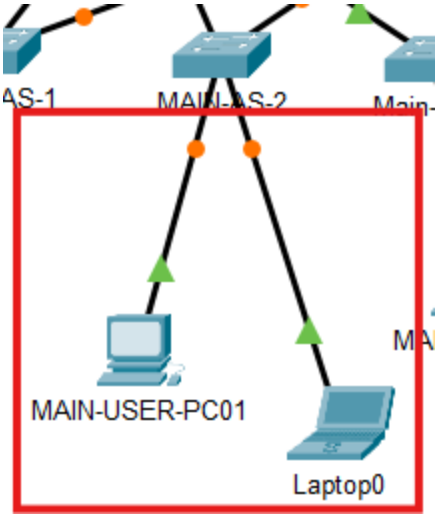


Step 4: Next delete/disconnect the cable between MAIN-USER-PC01 and MAIN-AS-2.





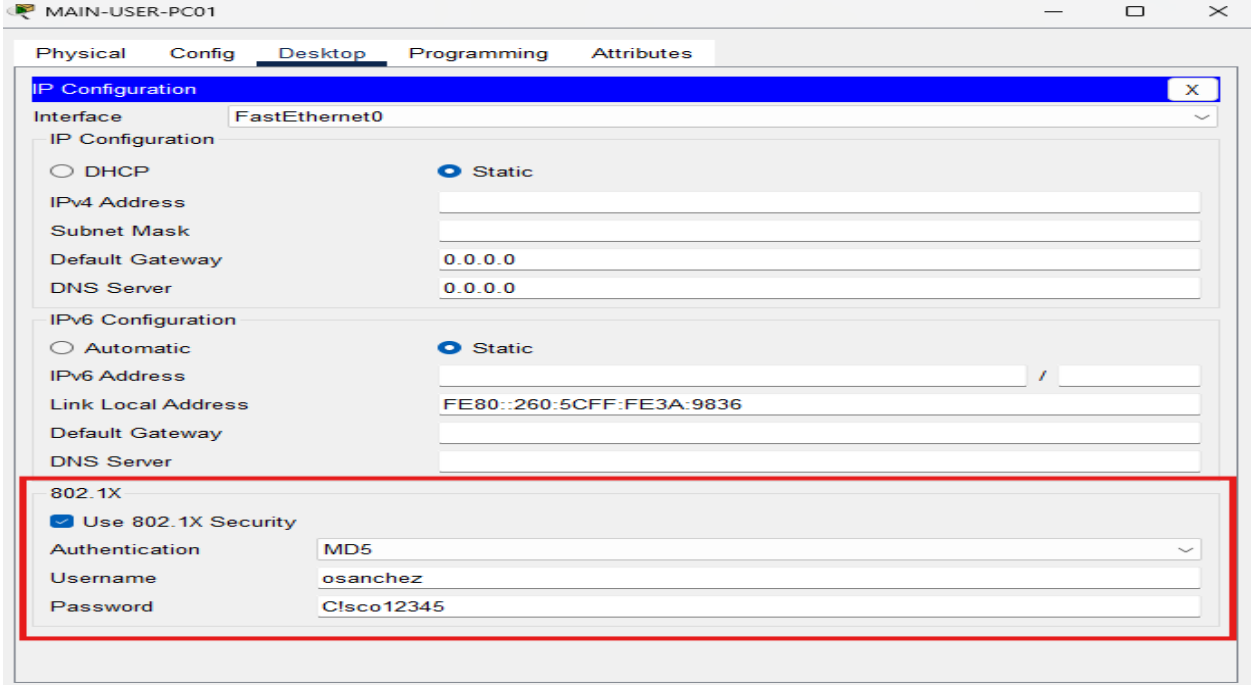
Step 5: Reconnect MAIN-USER-PC01 to MAIN-AS-2 port Fast Ethernet 0/3. Both devices should have amber lights as they are not authenticating.



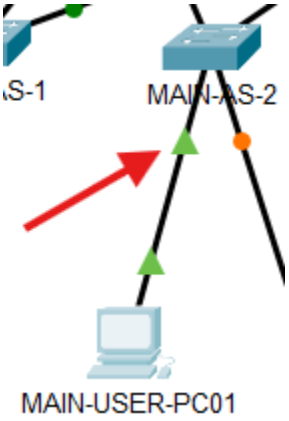
Step 6: On MAIN-USER-PC01, go to Desktop and IP Configuration. Check the “Use 802.1X Security” checkbox. Enter the following credentials.

User: osanchez

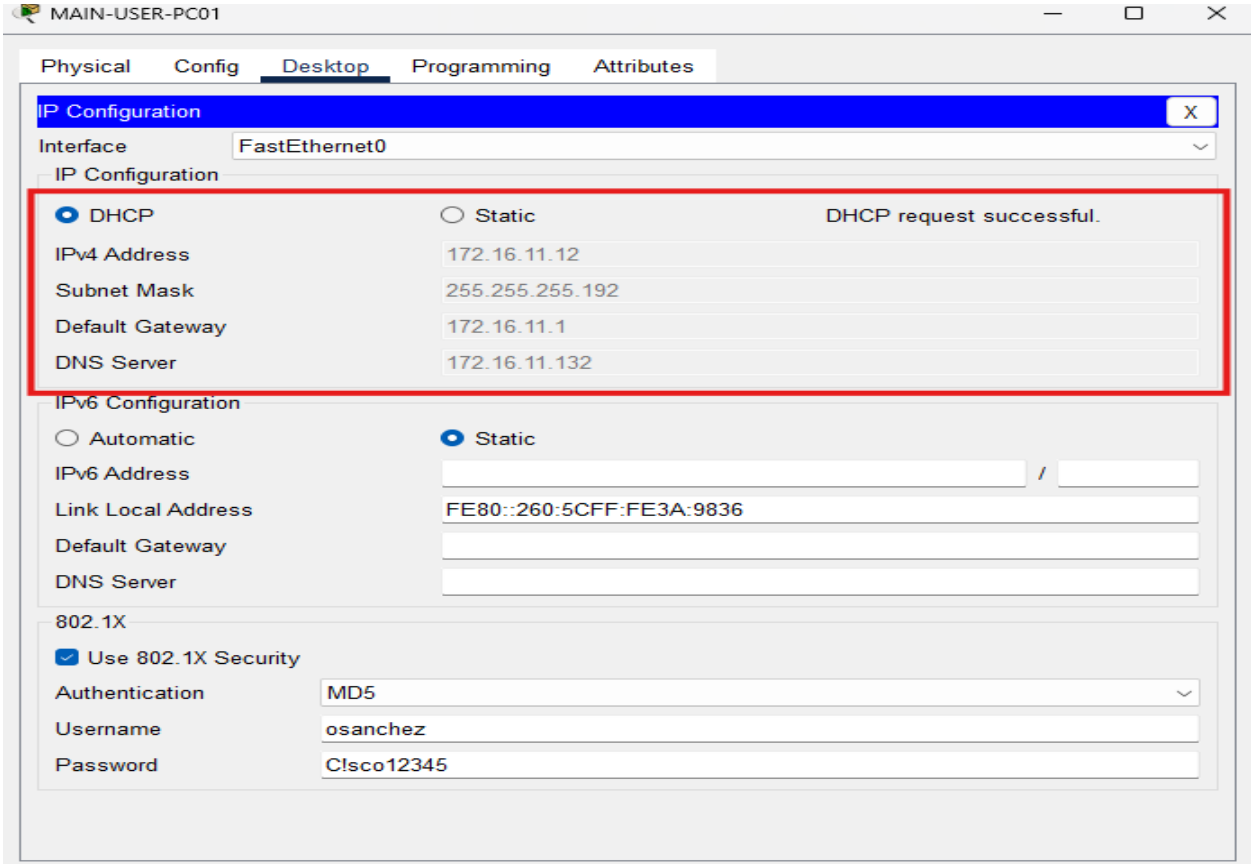
Password: C!sco12345



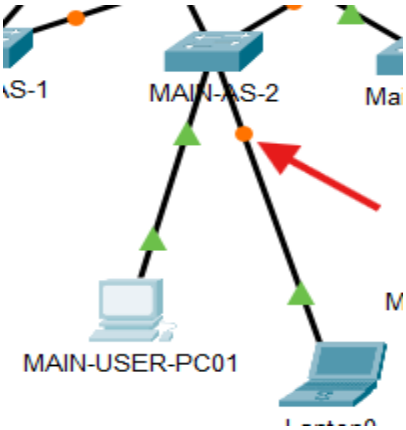
Step 7: Wait 2-5 minutes and observe the amber link-light. It will change to green, meaning the device authenticates and is now able to access network services.



Step 8: To confirm that MAIN-USER-PC01 can access network services, select the DHCP radio button and confirm the device gains an IP address.



Step 9: Through this process notice that our rogue device still has amber link-lights. It does not have network access.



Network Troubleshooting

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

Developing this medium-sized two-tier collapsed core architecture came with many challenges and issues that needed to be overcome. My approach was to begin with non-complicated tasks requiring minimal commands to ensure functionality while achieving connectivity between network devices. This approach allowed for fluid and continuous work with little slowdowns or bugginess with the Packet Tracer software.

Since the network is developed within Packet Tracer, I was limited to utilizing tools within the software. The sophisticated network simulator supports many features, allowing troubleshooting and network analysis. Key tools I used were ping and traceroute. These tools demonstrated connectivity to devices and routers at each hop, respectively. A major surprise to me was the simulation tool, which lets you look under the hood and better understand what is happening to the packet at each step along its path. All the network devices support various useful “show” commands, which are also critical to ensuring the functionality of technologies.

I encountered a few issues early on with ASA firewalls within Packet Tracer. ASA firewalls in Packet Tracer do not support standard show commands, such as show ip ospf, or other traffic monitoring and debugging commands. This lack of support caused issues when troubleshooting device routing tables and traffic behaviors. The ASA firewall would also change OSPF configuration on every reboot and require admin reconfiguration on every restart. It also lacks support for BGP. My initial plan was to deploy the firewall as the primary edge device for this network. However, BGP is not a feature supported by ASA firewalls in Packet Tracer, so I pivoted to placing the firewall behind an edge router. This change allowed me to configure BGP, but I still encountered issues with troubleshooting VPN and OSPF traffic routing. Ultimately, I replaced the ASA firewall device with a Cisco ISR-4331 router that

supports many security features while giving me access to many great troubleshooting features required to implement OSPF and VPN technologies correctly.

Another interesting problem I continued to experience was ACL statements at each firewall and each core/distro device. At first, the implementation was straightforward, and I was confident this would not pose issues. However, things became complicated as I started implementing stateful packet inspection. This grouping of ACL statements created issues with the VPN connecting, specific VLAN traffic was triggering a deny statement when it should be permitted, and at other times, traffic that should be denied was permitted into the network. ACL issues also created problems with OSPF and BGP advertisement sharing with neighbors and prevented adjacencies. To resolve all these little bugs, I used the simulation tool heavily to visually inspect the traffic flow and slowly resolve the ACL statements at each device one at a time.

Implementing network access controls and dot1x did not work at the start of implementation. It seemed like a Packet Tracer bug prevented the “radius server” command from saving within the running-configuration of an access switch. The first steps I took to resolve the issues were to create a small neighbor network to ensure Packet Tracer supports the feature, which proved that the feature works within Packet Tracer. Then I decided to restart the device in the capstone network that experienced the issue. That did not fix the issue. The last thing I tried was exporting the device configuration, adding the “radius server” commands in a notepad, and re-applying the configuration to the device. Exporting and re-applying device configurations resolved my issue and allowed me to implement dot1x.