**Network Engineering Capstone  
Functionality Report**

# 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** | Emily Parker |
| **WGU Student ID** | 011200197 |
| **WGU Student Email** | epar255@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.*

 Config subnets ONLY. Point them to test case #2 for ACL configuration. Don’t configure DHCP, just configure static IP’s on the routers/L3 switches. DHCP is for Test Case #4.

  static route from r1 to r4

The functionality of this test case is exhibited by pinging from R1, at Fenrir site 1 to R4, at Fenrir site 2. For traffic to successfully flow from R1 to R4, there needs to be proper routes configured. Static routes were configured and were verified to be working correctly. Tools used include the “IP route” command, and the ping command which utilizes ICMP echo requests/replies. Allowing certain devices to access/not access resources will be configured in test case #2 (ACL’s) instead of here. Relevant devices include R1, R2, R3, and R4. Relevant subnets include 192.168.7.0 /24, 192.168.10.0 /24, and 192.168.11.0 /24.

## Network Diagram or Segment

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



## Testing Method

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

The testing method used here was the ping command. By pinging R4 from R1, I was able to verify that traffic is able to be forwarded between site 1 and 2. Metrics of success include the success rate of the pings being 5/5, meaning there was no loss, and all packets reached the destination.

## 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.*

After static IP’s were assigned, the next step to test reachability was to have routes configured. Test case #8 will cover OSPF configuration for dynamic routing. For now static routes will do, they will be deleted afterwards.





Ping from 192.168.7.0 to 192.168.11.0 should still fail, routes haven’t been configured on the other routers.

It does fail, this is expected behavior.



After configuring the other two static routes on R2 and R3, the ping between Fenrir 1 and Fenrir 2 was successful.



# 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.*

PC’S ON THE GUEST SUBNETS HAVE STATIC IP’S ONLY TEMPORARILY FOR THIS TEST CASE. THEY WILL ACQUIRE DYNAMIC IP’S LATER IN TEST CASE #4.

configuring a standard ACL – apply closest to destination

Functionality exhibited here includes the PC’s on each Guest subnet being able to access the Internet and only the Internet. The router labeled “Internet”; hostname “ISP-Router” is really a stand-in. Packet Tracer has limited functionality, so the PC’s cannot actually access the Internet. Access to internal network resources is denied by the use of a standard numbered ACL. Commands I have used here include the “ip access-list [*number*]” command to create the ACL, “access-list [*number*] permit/deny [*IP*] [*wildcard mask*]” to add an ACE to the list, and the “ip access-group [*number*] in/out” command to apply the ACL inbound or outbound on the interface. It is very important to use a wildcard mask instead of a standard subnet mask, or else it will not work correctly. For clarity, you must create the ACL in global config mode, and apply it in interface config mode.

## Network Diagram or Segment

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



## Testing Method

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

 The testing method I used to verify functionality of this test case is to use the ping command to verify the PC’s on the guest subnet cannot access internal network resources. I applied the ACL outbound on ISP-Router’s F1/0 interface so that when PC10 and PC11 try to communicate to the internal network, they are simply blocked from doing so. On top of that, **ONLY** those two subnets are blocked when ISP-Router checks its outbound ACL for matches. Pings from the guest PC’s to the internal network were successfully blocked, as shown below in the Process List.

## 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.*



Commands to add ACE’s to the ACL, then a show command to list all current IP access-lists. NOTE: The command to create a standard numbered ACL is “ip access-list [*number*]”. These commands must be run in global config mode.



Switching to interface F1/0, and applying the ACL outbound. The command here is a bit different, as you specify “access-group” rather than “access-list” This is done in interface config mode.



Verifying that pings from PC10 to ISP-Router’s F1/0 interface fail. This behavior is expected, and wanted. This proves that the configuration and application of the ACL is correct.



Again verifying that pings were unsuccessful, this time from PC11 to ISP-Router’s F1/0 interface. This behavior is expected, and wanted.

# 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.*

The functionality exhibited in this test case is meant to show the company Acceptable Use Policy to users when logging onto network devices. Relevant tools include the “banner motd” command, followed by a delimiter character of your choosing. This will allow you to write your login message, and then end it with the delimiter character. Relevant devices include every L2 switch, L3 switch, and router in the network. If Packet Tracer supported the functionality, the login banner would also be present on every end user device in the network.

## Network Diagram or Segment

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

A blue square with black lines and green triangles

Description automatically generated

## Testing Method

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

 The testing method in this case is very simple. Open a CLI connection on the selected device, and the AUP will show up.

## 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.*

The first step in creating login banners for the network devices is to use the “banner motd” command, followed by a delimiter of your choosing. This will allow the device to know which part is the command and which part is the login banner. NOTE: “motd” stands for message of the day.Then you can write your banner, and add the delimiter again.









As seen here. when logging onto a device, the login banner that I have configured is displayed. For brevity I have only configured login banners for 3 devices, SW1, SW2, and SW3. Configurations would be the exact same for other network devices. Packet Tracer does not have the functionality required for configuring login banners on the PC’s.

# 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.*

The desired functionality here is to have all end user devices to have IP addresses assigned dynamically by the use of DHCP. This way, devices that no longer need an IP address(ex. Device is powered off, or no longer in use) can release their IP’s back to the DHCP server for use by another device. This creates a smooth and dynamic IP allocation and release process. If necessary, devices can request a reservation so that they receive the same IP upon each boot up, for example. Network devices should receive static IP’s so we can reliably access and perform configuration changes with a previously known IP. For example, if each time you SSH into a device and the IP is different, it creates unneccsary confusion and effort. We want the process to be smooth and simple. Our guest networks should not communicate with the internal network, so they will receive IP’s from ISP-Router, configured as a DHCP server. The hosts on the internal network will receive IP’s from our internal DHCP servers. (**include relevant subnets and hosts here**!!!!)

## Network Diagram or Segment

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

A computer icons with numbers and letters

Description automatically generated with medium confidence

A computer with a sign

Description automatically generated



## Testing Method

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

## 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.*

Need to config vlans first - DHCP wasn’t working bc I forgot to config an IP/mask/gateway on the server…… major brain fart today. Come back to DHCP after configuring VLAN’s/trunking.

# 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.*

## Network Diagram or Segment

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

## Testing Method

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

## 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.*

# Test Case #6: Edge Device Syslog and NTP

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

## Functionality

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

## Network Diagram or Segment

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

## Testing Method

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

## 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.*

# 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.*

 Configure trunk ports between L2 switches.

## Network Diagram or Segment

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

## Testing Method

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

## 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.*

# Test Case #8: Basic or Advanced Networking

## Custom Test Case

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

## 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 Diagram or Segment

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

## Testing Method

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

## 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.*

# Test Case #9: IPSec

## 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.*

## 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 Diagram or Segment

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

## Testing Method

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

## 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.*

# Test Case #10: Network Security

## Custom Test Case

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

## 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 Diagram or Segment

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

## Testing Method

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

## 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.*

# Network Troubleshooting

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