5-2016

Design and Troubleshooting Of a TCP/IP Based IPV4 Enterprise Network

Raj Bahadur Pun
St. Cloud State University, rpun@stcloudstate.edu

DESIGN AND TROUBLESHOOTING OF A TCP/IP BASED IPV4 ENTERPRISE NETWORK

by

Raj Bahadur Pun

A Thesis

Submitted to the Graduate Faculty

of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Information Assurance

St. Cloud, Minnesota

April, 2016

Thesis Committee:
Dr. Dennis Guster, Chairperson
Dr. Susantha Herath
Dr. Ezzat Kirmani

ACKNOWLEDGEMENTS

Firstly, I would like to express my sincere gratitude to my thesis advisor Prof. Dennis Guster for the continuous support and guidance in my Thesis study and research, for his patience, encouragement, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis.

Besides my advisor, I would like to thank the rest of my thesis committee: Prof. Susantha Herath and Prof. Ezzat Kirmani, for their insightful advice and encouragement.

Last but not the least, I would like to thank my family for supporting me throughout writing this thesis and my life in general.

ABSTRACT

In today's enterprise world Businesses are totally driven by technology and Computer Networking is the core technology that makes Data communication possible. As organizations grow larger and larger, their network size increases and also becomes more complex. Without a structured and systematic troubleshooting approach it would be arduous to fix network issues and restore IT services. Troubleshooting is a skill, and like all skills, one will get better at it the more one has to perform it. The more troubleshooting situations one is placed in, the more skills will improve, and as a result of this, the more confidence will grow. Although there is no right or wrong way to troubleshoot, Network Engineers should follow a structured troubleshooting approach that provides common methods to enhance efficiency.

TABLE OF CONTENTS

Chapter I

INTRODUCTION

Introduction

Troubleshooting is the process of responding to a problem, diagnosing the cause of the problem, and finally resolving the problem. Troubleshooting issues may arise out of proactive network monitoring or can be reactive in nature. There are network monitoring softwares which use SNMP to proactively monitor network. A ticket can also be raised by someone actually facing the issue. After an issue is identified, the first step toward resolution is clearly understanding the issue. Without clear understanding of the issue information collection will be arduous and may not be accurate. From the information collected one should be able to better define the issue. Then based on the diagnosis, a hypothesis may be proposed about what is most likely causing the issue. Then the evaluation of these likely causes leads to the identification of the suspected underlying root cause of the issue and then finally resolving the issue.

This research is based on using the above approach of identifying, defining, diagnosing and eventually resolving network issues. An IPV4 network is designed and implemented on a Virtualized Linux platform using a Network simulation software. There are 8 case studies performed on the implemented network

Problem Statement

Without fully understanding a problem, in most cases it is not possible to provide a solution to fix the problem. Hence without a systematic approach and methodology it is extremely difficult to troubleshoot a network when a network outage occurs. By following the systematic approach of identifying, defining, diagnosing and resolving maintenance and troubleshooting of the network becomes easy and manageable.

Nature and Significance of the Problem

Network outage and downtime usually affects the productivity of users and systems which in turn will affect Business as well as profitability. Hence every step should be taken to ensure uptime of networks. With a systematic approach Network operations and support Engineers will spend less time understanding the issue and hence quicker resolution time can be expected. This study will be very useful in environments where uptime of networks are critical, a structured approach will definitely assist network engineers restore services which in turn will assist employees to be more productive and eventually improving profitability for businesses.

Objective of the Study

The objective of this study is to improve the efficiency of Network Engineers by using the structured process of Identifying, Defining, Diagnosing and resolving will make it easy for network support personnel to resolve network issues sooner which in turn will improve uptime of network without disruption to IT services driving businesses.

Study Questions/Hypotheses

- How easy is it to understand network issues without a structured approach?
- How can uptime of networks improved?

Limitations of the Study

Troubleshooting skills vary from person to person. There's no doubt that using a structured approach of identifying, defining, diagnosing and resolving network issues will definitely help during troubleshooting however a lot also depends on technical skills, communication skills, experience and familiarity with the network topology. Troubleshooting gets better with experience, regular learning and updating technical skills however is important to be efficient and efficiency comes by following a structured troubleshooting approach.

Definition of Terms

SNMP: Simple Network Management protocol

Structured Troubleshooting: A systematic step-by-step approach while troubleshooting

Identify: Single out or pinpoint the issue

Define: Clearly and correctly explaining the issue.

Diagnose: Identify the nature and cause of the issue

Resolution: Solving the issue

Summary

This chapter discussed the importance of having a structured troubleshooting approach. However it also identifies that network engineers also need to have other skills to be efficient while troubleshooting. There is no “one-stop shop” for all the requirements when it comes to diagnosing, troubleshooting and maintaining networks. It is more of a skill that develops with experience, continuously learning new technologies and improving communication skills.

Chapter II

BACKGROUND AND REVIEW OF LITERATURE

Introduction

This chapter discusses the background and literature related to the problem of not using structured troubleshooting approach and also points out frequently used troubleshooting approaches.

Background Related to the Problem

Lacoste and Wallace (2015) stated that "If you do not follow a structured approach, you might find yourself moving around troubleshooting tasks in a fairly random way based on instinct. Although in one instance you might be fast at solving the issue, in the next instance you end up taking an unacceptable amount of time. In addition, it can become confusing to remember what you have tried and what you have not. Eventually, you find yourself repeating solutions you have already tried, hoping it works. Also, if another administrator comes to assist you, communicating to that administrator the steps you have already gone through becomes a challenge. Therefore, following a structured troubleshooting approach helps you reduce the possibility of trying the same resolution more than once and inadvertently skipping a task. It also aids in communicating to someone else possibilities that you have already eliminated"

Literature Related to the Problem

Moreover Ranjbar, A. (2014) describes the importance of structured troubleshooting in the following manner “Troubleshooting is not an exact science, and a particular problem can be diagnosed and sometimes even solved in many different ways. However, when you perform structured troubleshooting, you make continuous progress, and usually solve the problem faster than it would take using an ad hoc approach. There are many different structured troubleshooting approaches. For some problems, one method might work better, whereas for others, another method might be more suitable. Therefore, it is beneficial for the troubleshooter to be familiar with a variety of structured approaches and select the best method or combination of methods to solve a particular problem. A structured troubleshooting method is used as a guideline through a troubleshooting process. The key to all structured troubleshooting methods is systematic elimination of hypothetical causes and narrowing down on the possible causes. By systematically eliminating possible problem causes, you can reduce the scope of the problem until you manage to isolate and solve the problem. If at some point you decide to seek help or hand the task over to someone else, your findings can be of help to that person and your efforts are not wasted”.

Following a single troubleshooting procedure may not be sufficient to address all conceivable network issues because there are too many variables in today's networks For Eg: End user triggered issues. However, following a structured troubleshooting approach would help to ensure that troubleshooting procedures have a similar flow whenever an issue arises irrespective of who is assigned the task. This approach also allows one troubleshooter to more efficiently take over from another troubleshooter in a seamless manner.

This section describes each step in a structured troubleshooting approach.

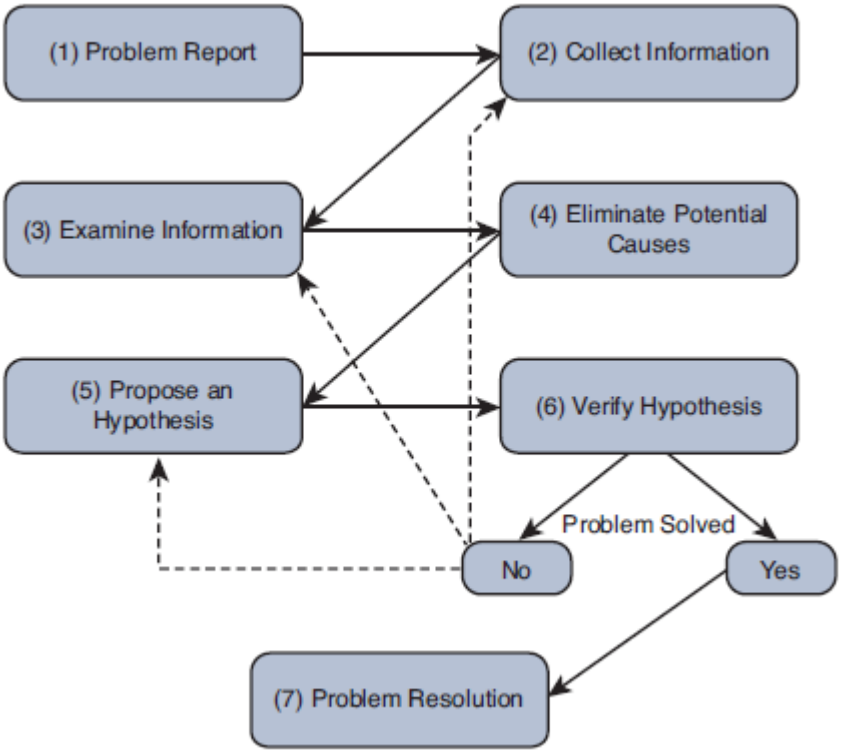


Figure 2.1

Retrieved page no. 13 from CCNP routing and switching TSHOOT 300-135 official cert guide. Indianapolis IN: Pearson Education.

Problem report

A problem report is when an end user would report an issue to the Helpdesk or the Support team. A user may report an issue as “Network is broken”. So at this stage the support personnel should start asking questions to get a better understanding of the issue. Without clear understanding it would be very arduous to provide quick fix to the issue.

Collect Information

It is important to be efficient and effective while collecting information about a network related issue. Questions like “How long has it been since the issue started”, “Was there anything that was done to trigger the issue”, “What happen when you try to access so and so“? These are very good questions to gather information which would eventually help to better and have clear understanding of the issue. Also logs in the network devices should be checked in addition to running ‘show, debug, ping and traceroute’ commands to gather as much information as possible.

Examine Information

The primary goal of examining information is to find if there are any indicators which may lead to the cause of the issue. The troubleshooter should have a sound knowledge of applications and protocols running in the network to be able to identify the underlying cause of the issue. Many a times the issue may be very complex so if there are data sets available to compare the current data would also be very helpful. Past documentation if available can also be very helpful while trying to solve network issues.

Eliminate Potential cause

Network troubleshooter should not jump to conclusions right away. All the steps discussed till now should be following diligently before concluding on Potential cause/causes of the issue. Efficiency and effectiveness comes only by carefully examining the collected information. It would be a good idea to explain the rationale with a coworker to ensure that the cause identified is correct so that an effective solution can be applied.

Propose Hypothesis

At this point, the troubleshooter should be able to list all the potential causes of the issue and rank them from most likely to least likely. Troubleshooter should then focus on the most likely cause of the issue and propose a Hypothesis based on the most likely cause.

Verify Hypothesis

Once most likely cause is identified it is important to develop a plan to address the suspected cause of the issue. In larger organizations which have defined processes the troubleshooter may need to work with the change management team before implementing the solution. There has to be a balance between the Urgency of the issue versus the potential overall loss of productivity. If the impact is high it is better to wait after business hours to implement the change.

Problem Resolution

This is the final step of a structured troubleshooting approach. This is the most important step however many a times once the issue is resolved it is forgotten. Every effort should be made to document the solution as quickly as possible so as to ensure that the implemented solution is available for other engineers and troubleshooters. Last but not the least the troubleshooter should report the solution provided to the respective parties and also get confirmation from the user that the issue has been resolved.

Literature Related to the Methodology

Commonly used troubleshooting approaches include the following:

- The top-down method
- The bottom-up method
- The divide-and-conquer method
- Following the traffic path
- Comparing configurations
- Component Swapping

For the most part “Following the traffic path” methodology will be used during the case studies. This is a very useful approach, For Eg: If a client is unable to reach a server, then trace route will be performed from the client to the server. Then based on which hop trace is stopping further investigation will be performed to find the fault domain and resolve the issue.

Summary

This chapter discussed the background and literature related to the problem and also introduced some of the commonly used troubleshooting approaches. These approaches can be used in various situations which would help narrow down the cause of the issue and resolve the issue as early as possible ensuring uptime of networks with minimal business impact and disruption to IT services and functions.

Chapter III

METHODOLOGY

Introduction

This chapter discusses the design and implementation of the study.

Design of the Study

Clearly one understands how important structured troubleshooting is and some of the troubleshooting approaches one can use while try to resolve network issues. In this study we will use these troubleshooting approaches after the IPv4 enterprise network is implemented in GNS3. GNS3 or Graphical Network Simulator-3 is a network software emulator first released in 2008. It allows the combination of virtual and real devices, used to simulate complex networks. It uses Dynamips emulation software to simulate Cisco IOS (Retrieved March 15, 2016, from https://en.wikipedia.org/wiki/Graphical_Network_Simulator-3).

Tools and Techniques

Virtualization, Linux and Network simulation software have been used to design and implement an enterprise IPv4 network for this study. In VMware player which is a type-2 hypervisor a Virtual machine has been created and Ubuntu Linux installed on the Virtual machine. In the Ubuntu Virtual machine GNS3 has been installed and an IPV4 network has been designed and implemented using GNS3. There are 8 case studies on various networking technologies which are solved in the simulated environment. Necessary screenshots with

configurations and validation results has been captured to validate the working of the solution implemented.

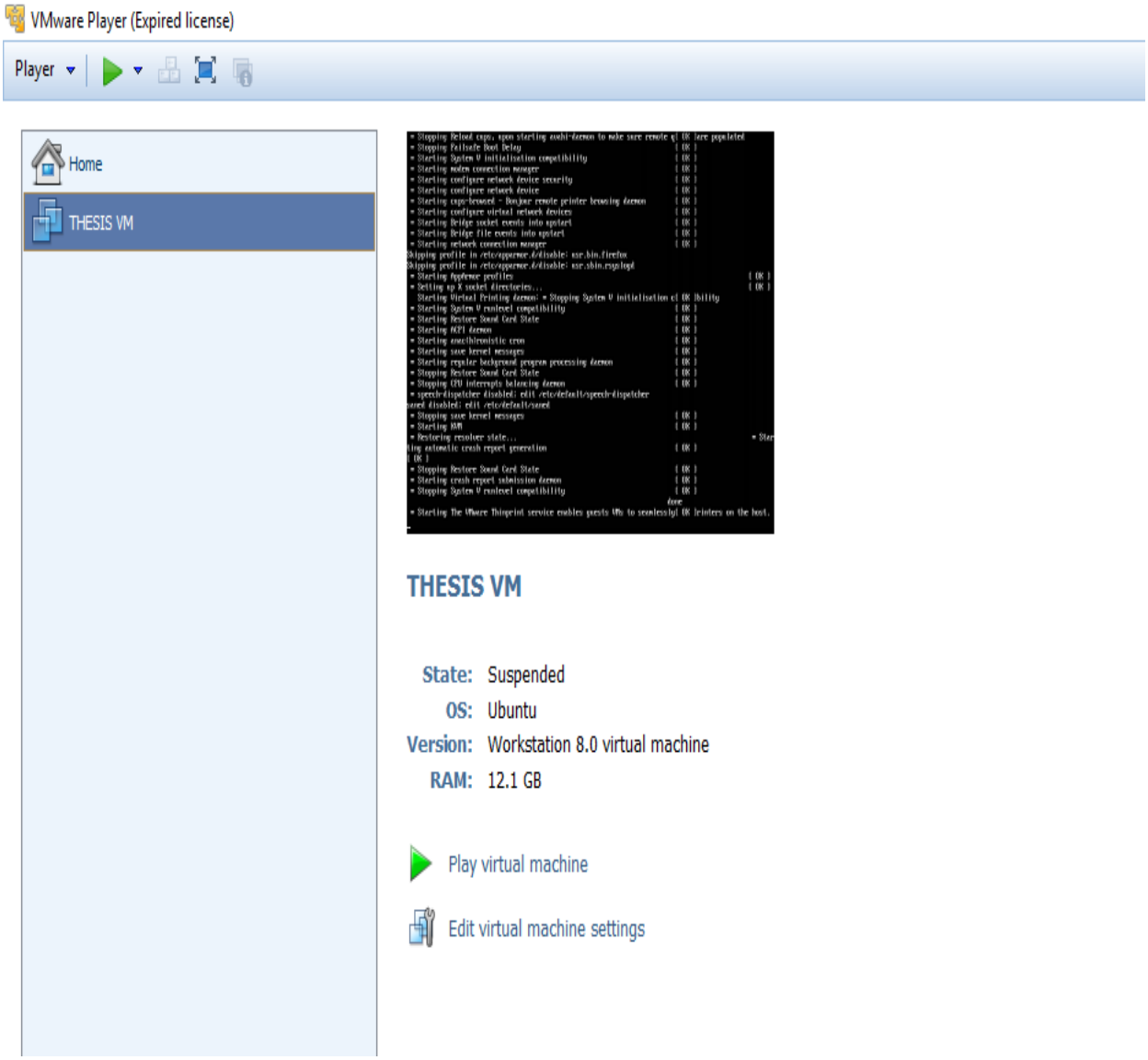


Figure 3.1

Thesis Virtual machine specification

The picture below depicts the amount of hardware resources allocated to the virtual machine.

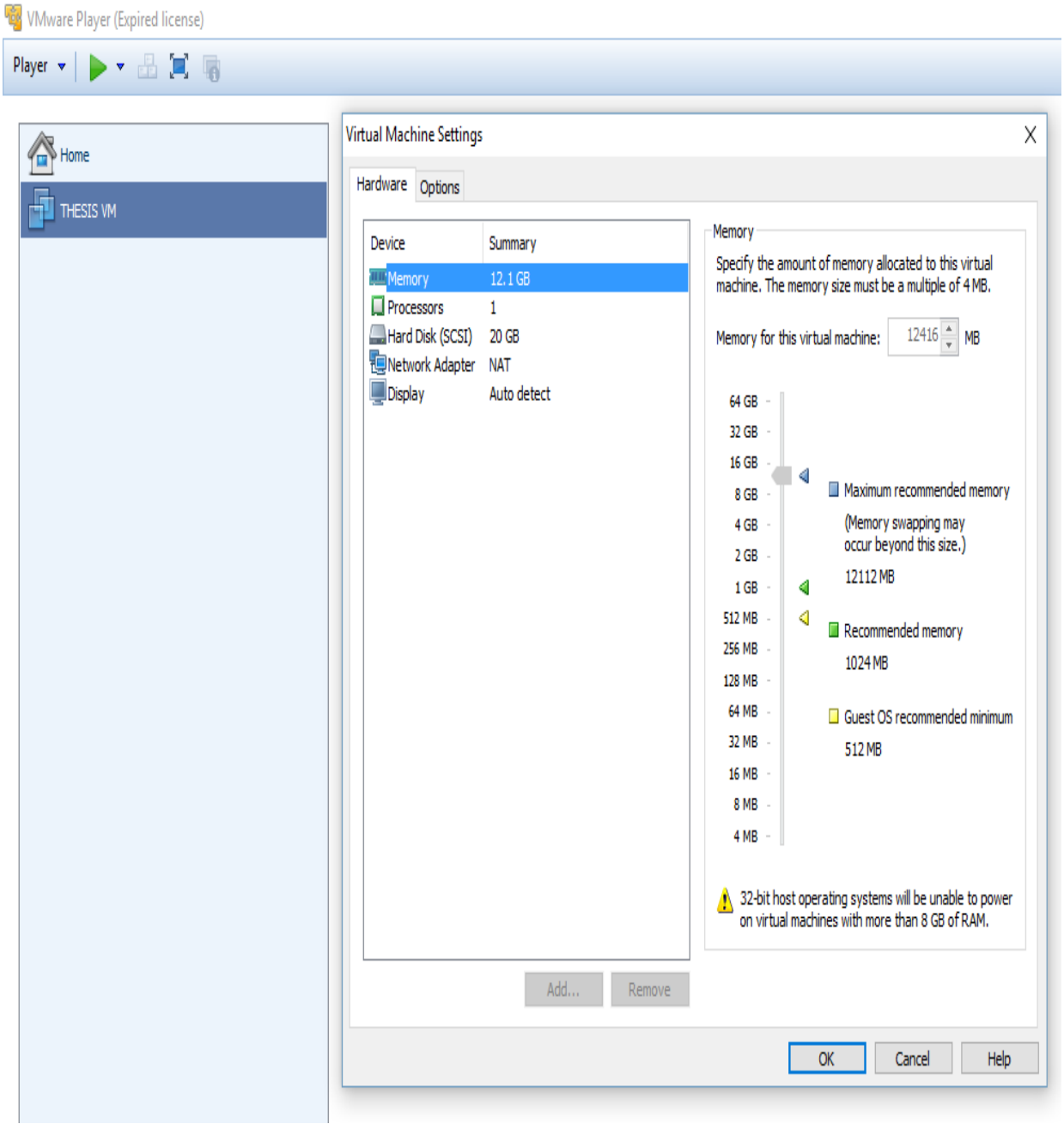


Figure 3.2

Virtual machine instance

The picture below represents the virtual machine built for the study.

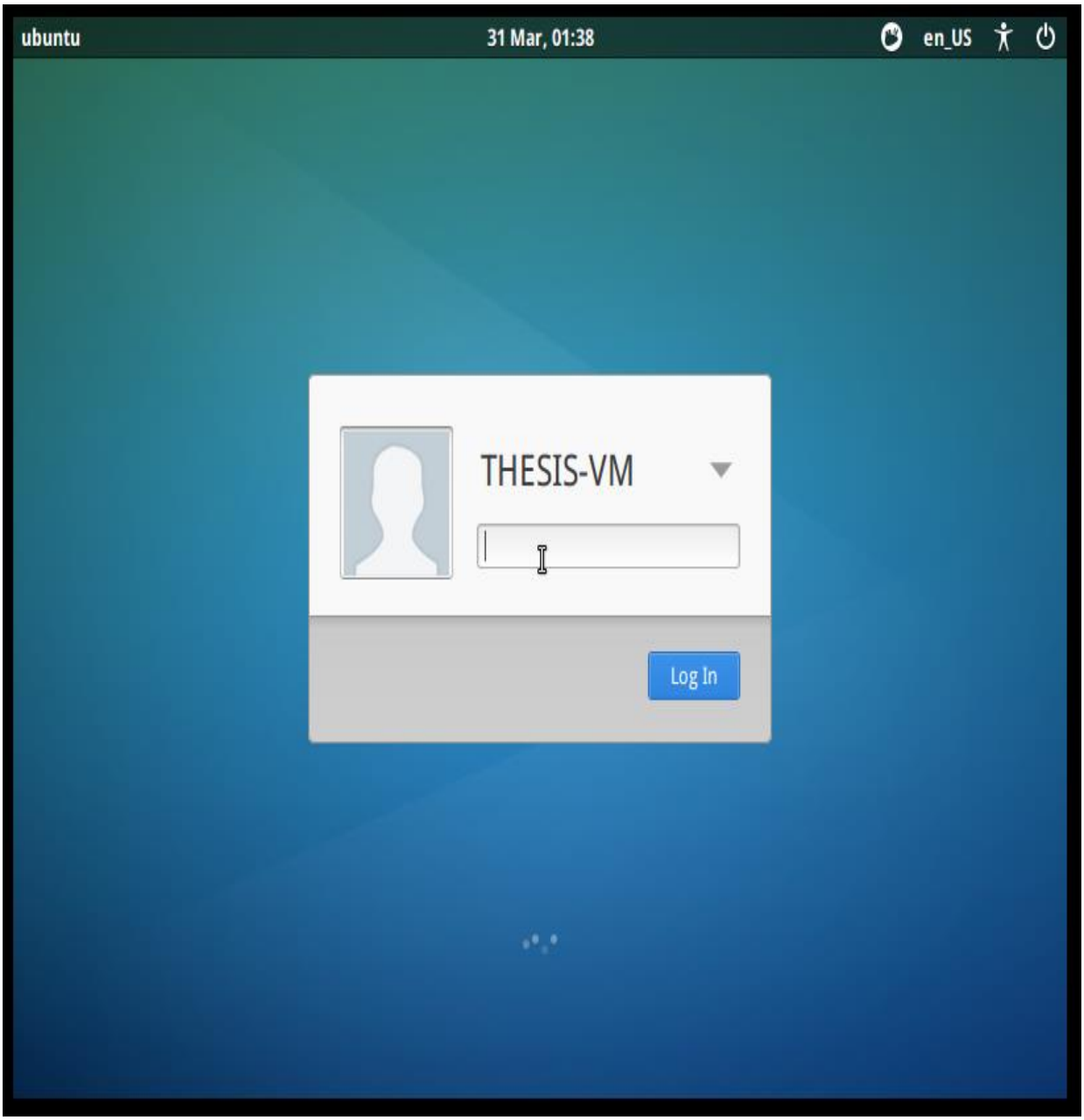


Figure 3.3

Network Topology

The picture below depicts the Network designed using GNS3 for the study.

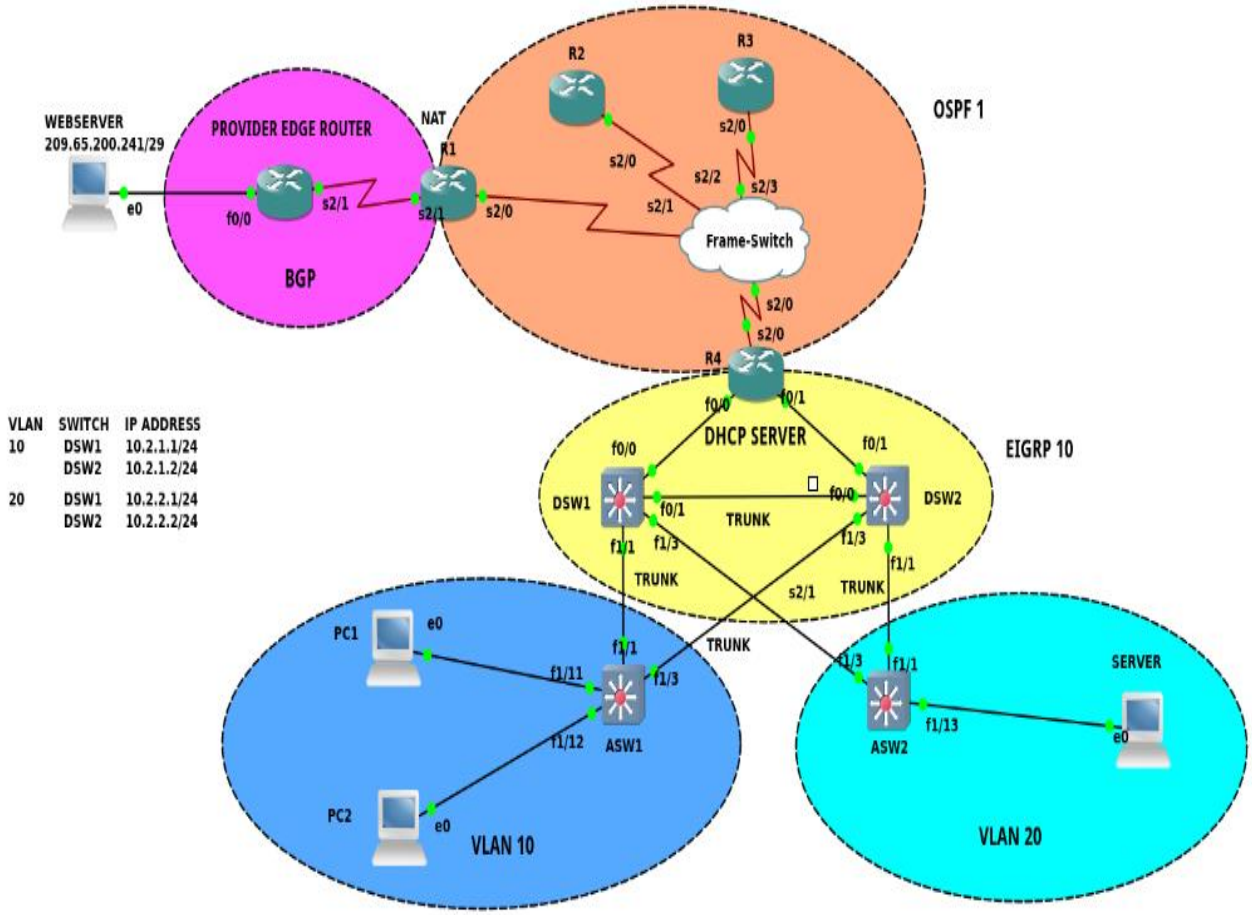


Figure 3.4

There are three virtual Local area networks created for this study, VLAN 10 is the client VLAN, VLAN 20 is the server VLAN and VLAN 200 is the management VLAN. PC1 and PC2 are in client VLAN and connected to the access switch ASW1. Server is in VLAN 20 is connected to access switch ASW2. Both ASW1 and ASW2 have redundant connections to distribution layer switches DSW1 and DSW2. All the connections between access layer and distributions layer switches are configured as trunk links so that the devices in different VLANs can communicate

with each other. R4 plays the role of a Customer edge router which is also configured as a DHCP server. There are DHCP Pools configured in R4 for both VLAN 10 and VLAN 20 subnets. DSW1 and DSW2 are also configured for DHCP relay so that any DHCP discover broadcast messages originating from the end devices are forwarded to R4 which is the DHCP server.

EIGRP is the routing protocol chosen to route LAN traffic; so R4, DSW1 and DSW2 are running EIGRP. All the external OSPF routes learnt by R4 are redistributed into EIGRP and also all the EIGRP routes are redistributed into OSPF so that there is reachability between the LAN and WAN parts of the network. R1, R2, R3 and R4 are in OSPF domain. Routers R4 and R3 are configured in OPPF area 34; R3 and R3 are in OSPF area 0 which is the backbone of the OSPF domain and R2 and R1 are in area 12. Routers R1 through R4 are all connected to the frame-relay switch. Frame-relay has been used as the layer-2 encapsulation protocol to provide Layer2 connectivity over the WAN. R1 is running both OSPF and BGP, in R1 OSPF has been configured to generate a default route and advertise to OSPF neighbors so that OSPF neighbor routers can reach R1, e-BGP has been chosen to run between R1 and the ISP-WEB-ROUTER. A Loopback IP address (209.65.200.241/29) has been configured in the ISP-WEB-ROUTER to simulate the presence of a Web Server so that reachability to the web server can be tested while working on the case studies.

IOS used in the simulation

Router: 7200 Software (C7200-ADVIPSERVICESK9-M), Version 15.2(4)S5, RELEASE SOFTWARE (fc1)

```
R4#sh ver
Cisco IOS Software, 7200 Software (C7200-ADVIPSERVICESK9-M), Version 15.2(4)S5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Feb-14 06:51 by prod_rel_team

ROM: ROMMON Emulation Microcode
BOOTLDR: 7200 Software (C7200-ADVIPSERVICESK9-M), Version 15.2(4)S5, RELEASE SOFTWARE (fc1)

R4 uptime is 1 day, 22 hours, 42 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"
Last reload type: Normal Reload
Last reload reason: unknown reload cause - suspect boot_data[BOOT_COUNT] 0x0, BOOT_COUNT 0, BOOTDATA 19
```

Switches: 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(12), RELEASE SOFTWARE (fc1)

```
DSW1#sh ver
Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(12), R
ELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 14:48 by prod_rel_team

ROM: ROMMON Emulation Microcode
ROM: 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(12), RELEASE SOFTWARE
 (fc1)
```

Summary

In this chapter we discussed the network design, Topology and various Tools used to design and implement an IPv4 Enterprise network. In the next chapter we will start performing case studies relating to various technologies in the areas of routing and switching.

Chapter IV

DATA PRESENTATION AND ANALYSIS

Introduction

In this chapter we will perform case studies on the implemented IPv4 network where-in we will try to solve various technical issues in the area of routing and switching by using the systematic troubleshooting process of Identifying, Defining, Diagnosing and resolving.

CASE STUDY 1: PC1 unable to ping Webserver

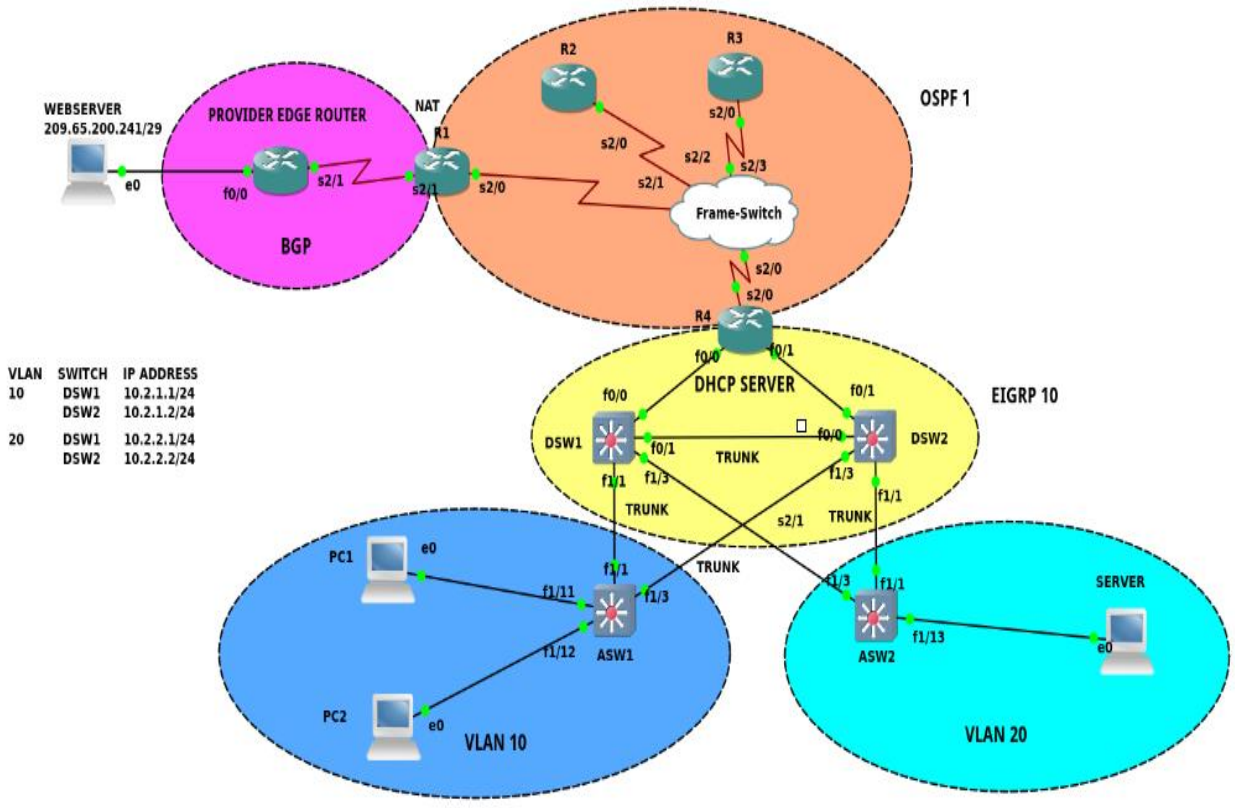


Figure 4.1

Identify and Define: PC1 which is in VLAN 10 is unable to ping the webserver at IP address 209.65.200.241

Diagnose starts here, the troubleshooting methodology used here is 'Following the traffic path'. It can be see that PC1 can reach the DHCP server at 4.4.4.4, However when trying to trace the reachability to the webserver it stops at 10.1.1.1

```
PC1> ip dhcp
DDD
Can't find dhcp server

PC1> ip dhcp
DDORA IP 10.2.1.6/24 GW 10.2.1.254

PC1> ping 4.4.4.4
84 bytes from 4.4.4.4 icmp_seq=1 ttl=254 time=51.155 ms
84 bytes from 4.4.4.4 icmp_seq=2 ttl=254 time=56.627 ms
^C
PC1> ping 209.65.200.241
209.65.200.241 icmp_seq=1 timeout
^C
^@
^@
^@
^@
PC1>
PC1>
PC1>
PC1> trace 209.65.200.241
trace to 209.65.200.241, 8 hops max, press Ctrl+C to stop
 1   10.2.1.1   32.576 ms  20.657 ms  40.264 ms
 2   10.1.4.5   103.354 ms  30.132 ms  51.645 ms
 3   10.1.1.9   103.625 ms  72.659 ms  61.636 ms
 4   10.1.1.5   189.217 ms  93.156 ms  187.771 ms
 5   10.1.1.1   321.059 ms  155.723 ms  166.782 ms
 6     *  *  *
 7     *  *  *
 8     *  *  *
```

As can be seen in below picture that 10.1.1.1 is the IP address configured on R1's Ser2/0.12 interface facing R2.

```
R1#
R1#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES NVRAM  administratively down down
FastEthernet0/1        unassigned      YES NVRAM  administratively down down
GigabitEthernet1/0     unassigned      YES NVRAM  administratively down down
Serial2/0              unassigned      YES NVRAM  up                    up
Serial2/0.12           10.1.1.1        YES NVRAM  up                    up
Serial2/1              209.65.200.225  YES NVRAM  up                    up
Serial2/2              unassigned      YES NVRAM  administratively down down
Serial2/3              unassigned      YES NVRAM  administratively down down
Ethernet3/0            unassigned      YES NVRAM  administratively down down
Ethernet3/1            unassigned      YES NVRAM  administratively down down
Ethernet3/2            unassigned      YES NVRAM  administratively down down
Ethernet3/3            unassigned      YES NVRAM  administratively down down
R1#
```

Below is the filter from R1's running configuration for both the interfaces where IP addresses are configured. Looking in Serial2/1 configuration it can be confirmed that Network address translation has been configured in the interface

```
R1#sh run int serial2/0.12
Building configuration...

Current configuration : 182 bytes
!
interface Serial2/0.12 point-to-point
 ip address 10.1.1.1 255.255.255.252
 ip nat inside
 ipv6 address 2026::12:1/122
 ipv6 ospf 6 area 12
 frame-relay interface-dlci 122
end

R1#sh run int serial2/1
Building configuration...

Current configuration : 156 bytes
!
interface Serial2/1
 ip address 209.65.200.225 255.255.255.252
 ip access-group DEFEND in
 ip nat outside
 encapsulation ppp
 serial restart-delay 0
end
```

PC1 has an IP address of 10.2.1.6/24 which will be denied by the implicit deny in access list Go-NAT-Go

```
R1#show access-lists
Standard IP access list Go-NAT-Go
    10 permit 10.1.0.0, wildcard bits 0.0.255.255
    20 permit 10.2.0.0, wildcard bits 0.0.0.255
Extended IP access list DEFEND
    10 deny ip 10.0.0.0 0.255.255.255 any
    20 deny ip 172.16.0.0 0.15.255.255 any
    30 deny ip 192.168.0.0 0.0.255.255 any
    40 deny ip host 255.255.255.255 any
    50 deny ip host 0.0.0.0 any
    60 permit ip any any (9 matches)
```

The below picture confirms that access-list Go-NAT-Go is used by Network address translation due to which PC1's IP address will be denied by the ACL and hence will not be natted causing the packet to drop at 10.1.1.1

```
R1#sh run | in nat
 ip nat inside
 ip nat outside
 default-information originate
ip nat inside source list Go-NAT-Go interface Serial2/1 overload
R1#
```

This issue can be solved by allowing PC1's subnet in the access-control list which is not allowing PC1's IP address to be natted. First of all line 20 of access list Go-NAT-Go is removed then line 20 is added back with a new wild card mask which will allow PC1 IPs address to be natted.

```
R1(config)#ip access-list standard Go-NAT-Go
R1(config-std-nacl)#no 20
R1(config-std-nacl)#
R1(config-std-nacl)#20 perm
R1(config-std-nacl)#20 permit 10.2.0.0 0.0.255.255
R1(config-std-nacl)#end
R1#
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show access-list
R1#show access-lists
Standard IP access list Go-NAT-Go
    10 permit 10.1.0.0, wildcard bits 0.0.255.255
    20 permit 10.2.0.0, wildcard bits 0.0.255.255
Extended IP access list DEFEND
    10 deny ip 10.0.0.0 0.255.255.255 any
    20 deny ip 172.16.0.0 0.15.255.255 any
    30 deny ip 192.168.0.0 0.0.255.255 any
    40 deny ip host 255.255.255.255 any
    50 deny ip host 0.0.0.0 any
    60 permit ip any any (13 matches)
```

It can be now observed that PC1 is able to ping the webserver at 209.65.200.241

```
PC1>
PC1>
PC1> ping 209.65.200.241
84 bytes from 209.65.200.241 icmp_seq=1 ttl=250 time=419.415 ms
84 bytes from 209.65.200.241 icmp_seq=2 ttl=250 time=509.931 ms
84 bytes from 209.65.200.241 icmp_seq=3 ttl=250 time=177.689 ms
84 bytes from 209.65.200.241 icmp_seq=4 ttl=250 time=197.281 ms
84 bytes from 209.65.200.241 icmp_seq=5 ttl=250 time=190.758 ms

PC1>
PC1>
PC1> ping 209.65.200.241
84 bytes from 209.65.200.241 icmp_seq=1 ttl=250 time=340.891 ms
84 bytes from 209.65.200.241 icmp_seq=2 ttl=250 time=221.044 ms
84 bytes from 209.65.200.241 icmp_seq=3 ttl=250 time=548.895 ms
84 bytes from 209.65.200.241 icmp_seq=4 ttl=250 time=266.352 ms
84 bytes from 209.65.200.241 icmp_seq=5 ttl=250 time=192.336 ms

PC1>
PC1>
PC1>
PC1>
PC1> ping 209.65.200.241
84 bytes from 209.65.200.241 icmp_seq=1 ttl=250 time=192.793 ms
84 bytes from 209.65.200.241 icmp_seq=2 ttl=250 time=196.315 ms
84 bytes from 209.65.200.241 icmp_seq=3 ttl=250 time=199.273 ms
84 bytes from 209.65.200.241 icmp_seq=4 ttl=250 time=197.253 ms
84 bytes from 209.65.200.241 icmp_seq=5 ttl=250 time=186.721 ms
```

It can also be seen that icmp ping packets are getting translated with PC1's IP address of 10.2.1.6 getting natted to a public IP address of 209.65.200.225

```
R1#
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.65.200.225:1029 10.2.1.6:32870   209.65.200.241:32870 209.65.200.241:1029
icmp 209.65.200.225:1030 10.2.1.6:33126   209.65.200.241:33126 209.65.200.241:1030
icmp 209.65.200.225:1031 10.2.1.6:33382   209.65.200.241:33382 209.65.200.241:1031
icmp 209.65.200.225:1032 10.2.1.6:33894   209.65.200.241:33894 209.65.200.241:1032
icmp 209.65.200.225:1033 10.2.1.6:34150   209.65.200.241:34150 209.65.200.241:1033
icmp 209.65.200.225:1034 10.2.1.6:37990   209.65.200.241:37990 209.65.200.241:1034
icmp 209.65.200.225:1035 10.2.1.6:38502   209.65.200.241:38502 209.65.200.241:1035
icmp 209.65.200.225:1024 10.2.1.6:38758   209.65.200.241:38758 209.65.200.241:1024
icmp 209.65.200.225:1025 10.2.1.6:39014   209.65.200.241:39014 209.65.200.241:1025
icmp 209.65.200.225:1026 10.2.1.6:39270   209.65.200.241:39270 209.65.200.241:1026
R1#
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.65.200.225:1029 10.2.1.6:32870   209.65.200.241:32870 209.65.200.241:1029
icmp 209.65.200.225:1030 10.2.1.6:33126   209.65.200.241:33126 209.65.200.241:1030
icmp 209.65.200.225:1031 10.2.1.6:33382   209.65.200.241:33382 209.65.200.241:1031
icmp 209.65.200.225:1032 10.2.1.6:33894   209.65.200.241:33894 209.65.200.241:1032
icmp 209.65.200.225:1033 10.2.1.6:34150   209.65.200.241:34150 209.65.200.241:1033
icmp 209.65.200.225:1034 10.2.1.6:37990   209.65.200.241:37990 209.65.200.241:1034
icmp 209.65.200.225:1035 10.2.1.6:38502   209.65.200.241:38502 209.65.200.241:1035
icmp 209.65.200.225:1024 10.2.1.6:38758   209.65.200.241:38758 209.65.200.241:1024
icmp 209.65.200.225:1025 10.2.1.6:39014   209.65.200.241:39014 209.65.200.241:1025
icmp 209.65.200.225:1026 10.2.1.6:39270   209.65.200.241:39270 209.65.200.241:1026
R1#
R1#
```

In this case study the fault domain was router R1, access-list was the technology where the issue was and the solution was to modify the access-list to allow PC1's subnet from being natted so that packets originating from PC1 could reach the webserver.

Case Study 2: PC1 in VLAN 10 is unable to reach the Server in VLAN 20

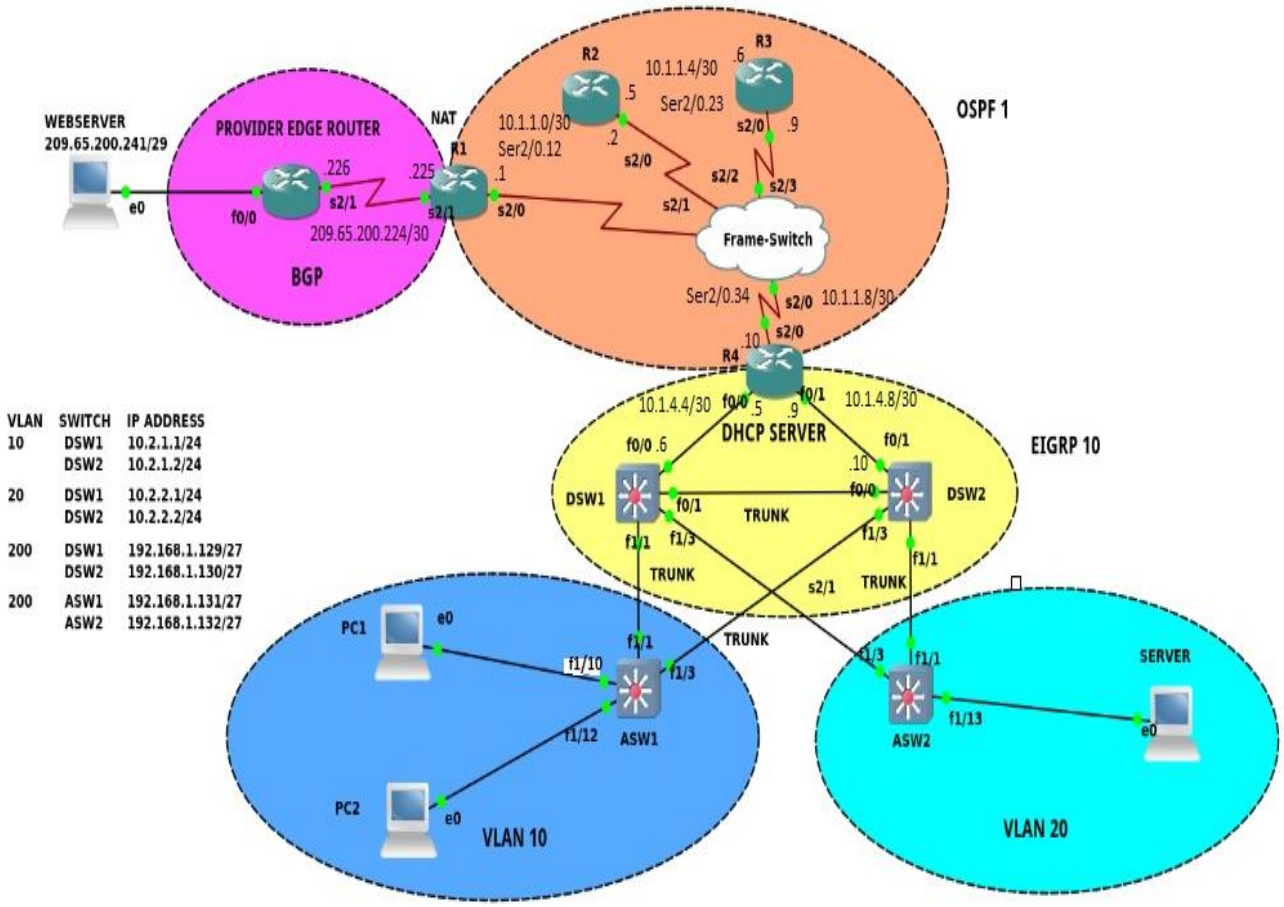


Figure 4.2

Identify and Define: PC1 which is in VLAN 10 is unable to reach the server in VLAN 20.

Diagnose starts here, the troubleshooting methodology is still to be decided because as of now it is not very clear where the issue is.

Due to some reason PC1 is not receiving an IP address.

```
PC1> show ip

NAME        : PC1[1]
IP/MASK     : 0.0.0.0/0
GATEWAY     : 0.0.0.0
DNS         :
MAC         : 00:50:79:66:68:01
LPORT       : 20502
RHOST:PORT  : 127.0.0.1:10008
MTU:        : 1500

PC1> ip dhcp
DDD
Can't find dhcp server

PC1>
PC1>
PC1> show ip

NAME        : PC1[1]
IP/MASK     : 0.0.0.0/0
GATEWAY     : 0.0.0.0
DNS         :
MAC         : 00:50:79:66:68:01
LPORT       : 20502
RHOST:PORT  : 127.0.0.1:10008
MTU:        : 1500
```

However Server which is in VLAN 20 is receiving IP address as shown below

```
SVR> ip dhcp
DDORA IP 10.2.2.6/24 GW 10.2.2.254
```

It is clear from the network topology that PC1 is connected to port fa1/10 in the access layer switch ASW1.

```
ASW1#show interfaces status

Port      Name               Status       Vlan       Duplex Speed Type
Fa1/0                        notconnect   1            auto    auto 10/100BaseTX
Fa1/1                        connected    trunk        full     100 10/100BaseTX
Fa1/2                        disabled     1            auto    auto 10/100BaseTX
Fa1/3                        connected    trunk        full     100 10/100BaseTX
Fa1/4                        disabled     1            auto    auto 10/100BaseTX
Fa1/5                        notconnect   1            auto    auto 10/100BaseTX
Fa1/6                        notconnect   1            auto    auto 10/100BaseTX
Fa1/7                        notconnect   1            auto    auto 10/100BaseTX
Fa1/8                        notconnect   1            auto    auto 10/100BaseTX
Fa1/9                        notconnect   1            auto    auto 10/100BaseTX
Fa1/10                       connected    1          a-full   a-100 10/100BaseTX
Fa1/11                       notconnect   10           full     100 10/100BaseTX
Fa1/12                       connected    10           full     100 10/100BaseTX
Fa1/13                       notconnect   1            full     100 10/100BaseTX
Fa1/14                       notconnect   10           full     100 10/100BaseTX
Fa1/15                       notconnect   10           full     100 10/100BaseTX
ASW1#
ASW1#
ASW1#
```

However it can be seen that port fa0/10 is in VLAN 1 instead of VLAN 10

```
ASW1#vl

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active    Fa1/0, Fa1/2, Fa1/4, Fa
                                                Fa1/6, Fa1/7, Fa1/8, Fa
                                                Fa1/10, Fa1/11, Fa1/13
10   User-Network                     active    Fa1/12, Fa1/14, Fa1/15
200  Management-Network               active
```

Let’s go ahead and configure fa1/10 as access port, assign it to vlan 10 and also configure portfast, speed & duplex for faster convergence.

All the VLANs are allowed in the trunk links between ASW1, DSW1 and DSW2.

```
ASW1(config)#int fastEthernet 1/10
ASW1(config-if)# switchport access vlan 10
ASW1(config-if)# duplex full
Duplex will not be set until speed is set to non-auto value
ASW1(config-if)# speed 100
ASW1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host.
 Connecting hubs, concentrators, switches,  bridges, etc.to this interface
 when portfast is enabled, can cause temporary spanning tree loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet1/10 but will only
 have effect when the interface is in a non-trunking mode.
ASW1(config-if)#
ASW1(config-if)#du
ASW1(config-if)#duplex full
ASW1(config-if)#
%LINK-3-UPDOWN: Interface FastEthernet1/10, changed state to up
```

```
ASW1#show interfaces trunk

Port      Mode         Encapsulation  Status        Native vlan
Fa1/1     on           802.1q         trunking      200
Fa1/3     on           802.1q         trunking      200

Port      Vlans allowed on trunk
Fa1/1     1-1005
Fa1/3     1-1005

Port      Vlans allowed and active in management domain
Fa1/1     1,10,200
Fa1/3     1,10,200

Port      Vlans in spanning tree forwarding state and not pruned
Fa1/1     1,10,200
Fa1/3     1,10,200
```

ASW1 Switch is unable to ping the Switched virtual interface i.e. interface vlan 10 configured on DSW1.

```
ASW1#ping 10.2.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
ASW1#
ASW1#
```

It can be observed that DSW1 has many down interfaces, fa0/0 and fa0/1 are connected to R4 and DSW2 and they should be in UP state.

```
DSW1#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.4.6        YES manual administratively down down
FastEthernet0/1            10.2.4.13       YES manual administratively down down
FastEthernet1/0            unassigned      YES unset  up                    down
FastEthernet1/1            unassigned      YES unset  up                    up
FastEthernet1/2            unassigned      YES unset  administratively down down
FastEthernet1/3            unassigned      YES unset  up                    up
FastEthernet1/4            unassigned      YES unset  administratively down down
FastEthernet1/5            unassigned      YES unset  up                    down
FastEthernet1/6            unassigned      YES unset  up                    down
FastEthernet1/7            unassigned      YES unset  up                    down
FastEthernet1/8            unassigned      YES unset  up                    down
FastEthernet1/9            unassigned      YES unset  up                    down
FastEthernet1/10           unassigned      YES unset  up                    down
FastEthernet1/11           unassigned      YES unset  up                    down
FastEthernet1/12           unassigned      YES unset  up                    down
FastEthernet1/13           unassigned      YES unset  up                    down
FastEthernet1/14           unassigned      YES unset  up                    down
FastEthernet1/15           unassigned      YES unset  up                    down
Serial2/0                  unassigned      YES manual administratively down down
Serial2/1                  unassigned      YES manual administratively down down
Serial2/2                  unassigned      YES manual administratively down down
Serial2/3                  unassigned      YES manual administratively down down
Vlan1                      unassigned      YES unset  up                    up
Vlan10                     10.2.1.1        YES manual up                    down
Vlan20                     10.2.2.2        YES manual up                    down
Vlan200                    192.168.1.129   YES manual up                    down
```

DSW1 also cannot reach 10.2.1.3 which is the switched virtual interface for vlan 10 in ASW1 and also it cannot reach R4 which is the DHCP server.

```
DSW1#ping 10.2.1.3
Translating "10.2.1.3"

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.1.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
DSW1#
DSW1#
DSW1#
DSW1#ping 4.4.4.4
Translating "4.4.4.4"

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

There’s no VLAN configuration found in DSW1

```
DSW1#sh vlan-switch br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/2, Fa1/4, Fa1/5
                                                Fa1/6, Fa1/7, Fa1/8, Fa1/9
                                                Fa1/10, Fa1/11, Fa1/12, Fa1/13
                                                Fa1/14, Fa1/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
DSW1#
```

VLANs 10, 20 and 200 were configured as shown below

```
DSW1#vlan database
DSW1(vlan)#
DSW1(vlan)#
DSW1(vlan)#vlan
DSW1(vlan)#vlan 10 na
DSW1(vlan)#vlan 10 name User-Network
VLAN 10 added:
    Name: User-Network
DSW1(vlan)#
DSW1(vlan)#
DSW1(vlan)#vlan 200 Management-Network
                    ^
% Invalid input detected at '^' marker.

DSW1(vlan)#vlan 200 name Management-Network
VLAN 200 added:
    Name: Management-Network
DSW1(vlan)#
DSW1(vlan)#
DSW1(vlan)#
DSW1(vlan)#
DSW1(vlan)#vlan 20  name Int-Server-Network
VLAN 20 added:
    Name: Int-Server-Network
```

Also administratively enabled the down interfaces

```
DSW1(config)#int fa0/0
DSW1(config-if)#
DSW1(config-if)#no shut
DSW1(config-if)#
DSW1(config-if)#exit
DSW1(config)#
DSW1(config)#
DSW1(config)#no shut
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
DSW1(config)#int fa0/0
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.1.4.5 (FastEthernet0/0) is up: new adjacency
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
DSW1(config)#itn fa
DSW1(config)#itn fa0/1
             ^
% Invalid input detected at '^' marker.

DSW1(config)#
DSW1(config)#itn fa
DSW1(config)#int fa0/1
DSW1(config-if)#no shut
DSW1(config-if)#
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
DSW1(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.2.4.14 (FastEthernet0/1) is up: new adjacency
DSW1(config-if)#
%HSRP-5-STATECHANGE: Vlan20 Grp 20 state Active -> Speak
DSW1(config-if)#
%HSRP-5-STATECHANGE: Vlan20 Grp 20 state Speak -> Standby
```

Both fa0/0 and fa0/1 are now up in DSW1

```
DSW1#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.4.6        YES manual up                    up
FastEthernet0/1            10.2.4.13       YES manual up                    up
FastEthernet1/0            unassigned      YES unset  up                    down
FastEthernet1/1            unassigned      YES unset  up                    up
FastEthernet1/2            unassigned      YES unset  administratively down down
FastEthernet1/3            unassigned      YES unset  up                    up
FastEthernet1/4            unassigned      YES unset  administratively down down
FastEthernet1/5            unassigned      YES unset  up                    down
FastEthernet1/6            unassigned      YES unset  up                    down
FastEthernet1/7            unassigned      YES unset  up                    down
FastEthernet1/8            unassigned      YES unset  up                    down
FastEthernet1/9            unassigned      YES unset  up                    down
FastEthernet1/10           unassigned      YES unset  up                    down
FastEthernet1/11           unassigned      YES unset  up                    down
FastEthernet1/12           unassigned      YES unset  up                    down
FastEthernet1/13           unassigned      YES unset  up                    down
FastEthernet1/14           unassigned      YES unset  up                    down
FastEthernet1/15           unassigned      YES unset  up                    down
Serial2/0                  unassigned      YES manual administratively down down
Serial2/1                  unassigned      YES manual administratively down down
Serial2/2                  unassigned      YES manual administratively down down
Serial2/3                  unassigned      YES manual administratively down down
Vlan1                      unassigned      YES unset  up                    up
Vlan10                     10.2.1.1        YES manual up                    up
Vlan20                     10.2.2.2        YES manual up                    up
Vlan200                    192.168.1.129   YES manual up                    up
DSW1#
DSW1#sh run | in 10.2.1.254
 standby 10 ip 10.2.1.254
```

HSRP configuration below indicates that HSRP Virtual IP address configured for vlan 10 is the default gateway for devices in VLAN 10

```
DSW1#sh run int vlan 10
Building configuration...

Current configuration : 228 bytes
!
interface Vlan10
 ip address 10.2.1.1 255.255.255.0
 ip helper-address 4.4.4.4
 standby 10 ip 10.2.1.254
 standby 10 priority 105
 standby 10 preempt
 standby 10 mac-address 0000.1234.5678
 standby 10 track 5 decrement 6
end
```

```
DSW1#sh run int vlan 20
Building configuration...

Current configuration : 149 bytes
!
interface Vlan20
 ip address 10.2.2.2 255.255.255.0
 ip helper-address 4.4.4.4
 standby preempt
 standby 20 ip 10.2.2.254
 standby 20 preempt
end
```

PC1 is now able to get an IP address and also able to ping itself and reach its default gateway which is the HSRP IP configured in DSW1

```
PC1> ip dhcp
DDORA IP 10.2.1.6/24 GW 10.2.1.254

PC1>
PC1>
PC1>
PC1>
PC1> show ip

NAME        : PC1[1]
IP/MASK     : 10.2.1.6/24
GATEWAY     : 10.2.1.254
DNS         :
DHCP SERVER : 10.1.4.5
DHCP LEASE  : 8957, 9000/4500/7875
MAC         : 00:50:79:66:68:01
LPORT       : 20502
RHOST:PORT  : 127.0.0.1:10008
MTU:        : 1500

PC1>
PC1>
PC1> ping 10.2.1.6
10.2.1.6 icmp_seq=1 ttl=64 time=0.001 ms
10.2.1.6 icmp_seq=2 ttl=64 time=0.001 ms
10.2.1.6 icmp_seq=3 ttl=64 time=0.001 ms
10.2.1.6 icmp_seq=4 ttl=64 time=0.001 ms
10.2.1.6 icmp_seq=5 ttl=64 time=0.001 ms

PC1>
PC1> ping 10.2.1.254
84 bytes from 10.2.1.254 icmp_seq=1 ttl=255 time=43.003 ms
84 bytes from 10.2.1.254 icmp_seq=2 ttl=255 time=21.149 ms
```

However PC1 still cannot ping the Server in VLAN 20

```
PC1> ping 10.2.2.6
10.2.2.6 icmp_seq=1 timeout
10.2.2.6 icmp_seq=2 timeout
^C
PC1>
PC1>
PC1> tracert 10.2.2.6
Bad command: "tracert 10.2.2.6". Use ? for help.

PC1>
PC1> trace10.2.2.6
Bad command: "trace10.2.2.6". Use ? for help.

PC1>
PC1>
PC1> trace 10.2.2.6
trace to 10.2.2.6, 8 hops max, press Ctrl+C to stop
 1   10.2.1.1   43.071 ms  20.741 ms  10.108 ms
 2   *10.2.2.6   18.628 ms (ICMP type:3, code:3, Destination port unreachable)  10.152 ms
 3   *10.2.2.6   9.105 ms (ICMP type:3, code:3, Destination port unreachable)  30.297 ms  9.086 ms
```

Looking into the configuration of DSW2 there are no VLANs configured in DSW2

```
DSW2#sh vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/2, Fa1/4, Fa1/5
                                                Fa1/6, Fa1/7, Fa1/8, Fa1/9
                                                Fa1/10, Fa1/11, Fa1/12, Fa1/13
                                                Fa1/14, Fa1/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

Also there are many interfaces found administratively down in DSW2

```
DSW2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.2.4.14       YES manual administratively down down
FastEthernet0/1        10.1.4.10       YES manual administratively down down
FastEthernet1/0        unassigned      YES unset  up                    down
FastEthernet1/1        unassigned      YES unset  up                    up
FastEthernet1/2        unassigned      YES unset  administratively down down
FastEthernet1/3        unassigned      YES unset  up                    up
FastEthernet1/4        unassigned      YES unset  administratively down down
FastEthernet1/5        unassigned      YES unset  up                    down
FastEthernet1/6        unassigned      YES unset  up                    down
FastEthernet1/7        unassigned      YES unset  up                    down
FastEthernet1/8        unassigned      YES unset  up                    down
FastEthernet1/9        unassigned      YES unset  up                    down
FastEthernet1/10       unassigned      YES unset  up                    down
FastEthernet1/11       unassigned      YES unset  up                    down
FastEthernet1/12       unassigned      YES unset  up                    down
FastEthernet1/13       unassigned      YES unset  up                    down
FastEthernet1/14       unassigned      YES unset  up                    down
FastEthernet1/15       unassigned      YES unset  up                    down
Serial2/0              unassigned      YES manual administratively down down
Serial2/1              unassigned      YES manual administratively down down
Serial2/2              unassigned      YES manual administratively down down
Serial2/3              unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
Vlan10                 10.2.1.2        YES manual up                    down
Vlan20                 10.2.2.1        YES manual up                    down
Vlan200                192.168.1.130   YES manual up                    down
```

Configured VLANs in DSW2 as below

```
DSW2(vlan)#vlan 20  name Int-Server-Network
VLAN 20 added:
    Name: Int-Server-Network
DSW2(vlan)#vlan 10 name User-Network
VLAN 10 added:
    Name: User-Network
DSW2(vlan)#vlan 200  name Management-Network
VLAN 200 added:
    Name: Management-Network
```

Also enabled the administratively down interfaces

```
DSW2(config)#int fa0/0
DSW2(config-if)#no shut
DSW2(config-if)#
DSW2(config-if)#
DSW2(config-if)#ex
DSW2(config)#int fa0/0
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.2.4.13 (FastEthernet0/0) is up: new adjacency
DSW2(config)#int fa0/1
DSW2(config-if)#nos
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
DSW2(config-if)#nos hut
               ^
% Invalid input detected at '^' marker.

DSW2(config-if)#
DSW2(config-if)#
DSW2(config-if)#no shut
```

It can be observed that DSW2 is the Active default Gateway for devices in VLAN 20. Also all the down interfaces are up now.

```
DSW2#sh standby br
                  P indicates configured to preempt.
                  |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl10        10  100  P Standby  10.2.1.1        local           10.2.1.254
Vl20        20  105  P Active   local           10.2.2.2        10.2.2.254
DSW2#
DSW2#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.2.4.14       YES manual up                    up
FastEthernet0/1            10.1.4.10       YES manual up                    up
FastEthernet1/0            unassigned      YES unset  up                    down
FastEthernet1/1            unassigned      YES unset  up                    up
FastEthernet1/2            unassigned      YES unset  administratively down down
FastEthernet1/3            unassigned      YES unset  up                    up
FastEthernet1/4            unassigned      YES unset  administratively down down
FastEthernet1/5            unassigned      YES unset  up                    down
FastEthernet1/6            unassigned      YES unset  up                    down
FastEthernet1/7            unassigned      YES unset  up                    down
FastEthernet1/8            unassigned      YES unset  up                    down
FastEthernet1/9            unassigned      YES unset  up                    down
FastEthernet1/10           unassigned      YES unset  up                    down
FastEthernet1/11           unassigned      YES unset  up                    down
FastEthernet1/12           unassigned      YES unset  up                    down
FastEthernet1/13           unassigned      YES unset  up                    down
FastEthernet1/14           unassigned      YES unset  up                    down
FastEthernet1/15           unassigned      YES unset  up                    down
Serial2/0                  unassigned      YES manual administratively down down
Serial2/1                  unassigned      YES manual administratively down down
Serial2/2                  unassigned      YES manual administratively down down
Serial2/3                  unassigned      YES manual administratively down down
Vlan1                      unassigned      YES manual administratively down down
Vlan10                     10.2.1.2        YES manual up                    up
Vlan20                     10.2.2.1        YES manual up                    up
Vlan200                    192.168.1.130   YES manual up                    up
```

However PC1 still cannot ping the server

```
PC1> ping 10.2.1.1
84 bytes from 10.2.1.1 icmp_seq=1 ttl=255 time=19.107 ms
84 bytes from 10.2.1.1 icmp_seq=2 ttl=255 time=7.173 ms
^C
PC1>
PC1>
PC1> ping 10.2.2.2
84 bytes from 10.2.2.2 icmp_seq=1 ttl=255 time=56.193 ms
84 bytes from 10.2.2.2 icmp_seq=2 ttl=255 time=15.072 ms
^C
PC1>
PC1>
PC1>
PC1>
PC1> ping vlan 20  name Int-Server-Network
Cannot resolve vlan

PC1>
PC1>
PC1> ping 10.2.2.6
10.2.2.6 icmp_seq=1 timeout
10.2.2.6 icmp_seq=2 timeout
^C
```

Let’s go ahead and bounce vlan 10 & 20 interfaces at DSW2

```
DSW2(config)#int vlan 10
DSW2(config-if)#shut
DSW2(config-if)#
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Init
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.2.1.1 (Vlan10) is down: interface down
DSW2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
DSW2(config-if)#no shut
DSW2(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.2.1.1 (Vlan10) is up: new adjacency
DSW2(config-if)#
DSW2(config-if)#
DSW2(config-if)#
DSW2(config-if)#
DSW2(config-if)#
%LINK-3-UPDOWN: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
DSW2(config-if)#
DSW2(config-if)#
DSW2(config-if)#exit
DSW2(config)#int vlan 20
DSW2(config-if)#shut
DSW2(config-if)#
%HSRP-5-STATECHANGE: Vlan20 Grp 20 state Active -> Init
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.2.2.2 (Vlan20) is down: interface down
DSW2(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to down
DSW2(config-if)#
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
DSW2(config-if)#no shut
DSW2(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.2.2.2 (Vlan20) is up: new adjacency
```

PC1 in VLAN 10 is now successfully able to ping the Server is VLAN 20

```
PC1> ping 10.2.2.2
84 bytes from 10.2.2.2 icmp_seq=1 ttl=255 time=30.672 ms
84 bytes from 10.2.2.2 icmp_seq=2 ttl=255 time=19.107 ms
84 bytes from 10.2.2.2 icmp_seq=3 ttl=255 time=18.608 ms
^C
PC1>
PC1>
PC1> ping 10.2.2.6
10.2.2.6 icmp_seq=1 timeout
10.2.2.6 icmp_seq=2 timeout
^C
PC1>
PC1> ping 10.2.2.6
84 bytes from 10.2.2.6 icmp_seq=1 ttl=63 time=24.138 ms
84 bytes from 10.2.2.6 icmp_seq=2 ttl=63 time=28.694 ms
84 bytes from 10.2.2.6 icmp_seq=3 ttl=63 time=17.709 ms
^C
```

In this case study the fault domain was large, Switches ASW1, ASW2, DSW1 and DSW2 all had issues. Main issue was missing VLAN configuration and down interfaces in these devices and the issue was resolved by configuring VLANs and by bringing up the down interfaces.

Case Study 3: Server in VLAN 20 is unable to reach the Web server

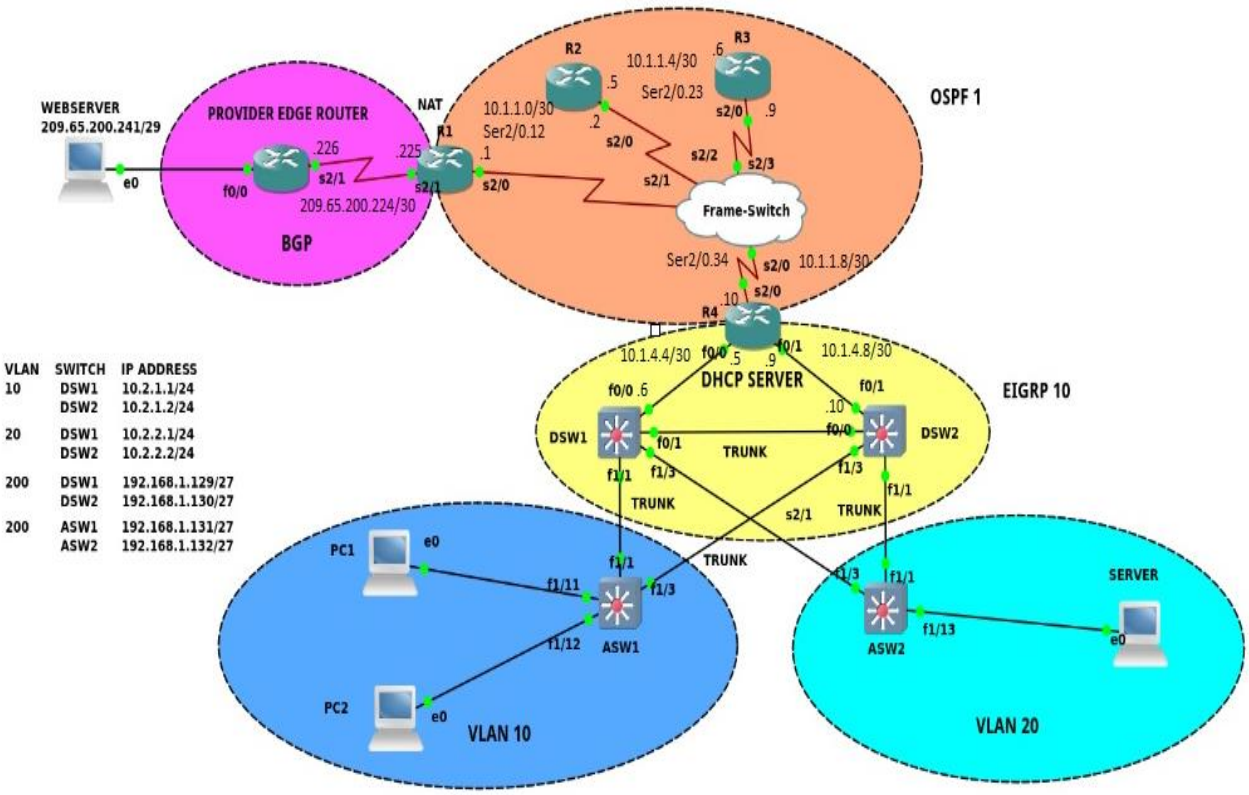
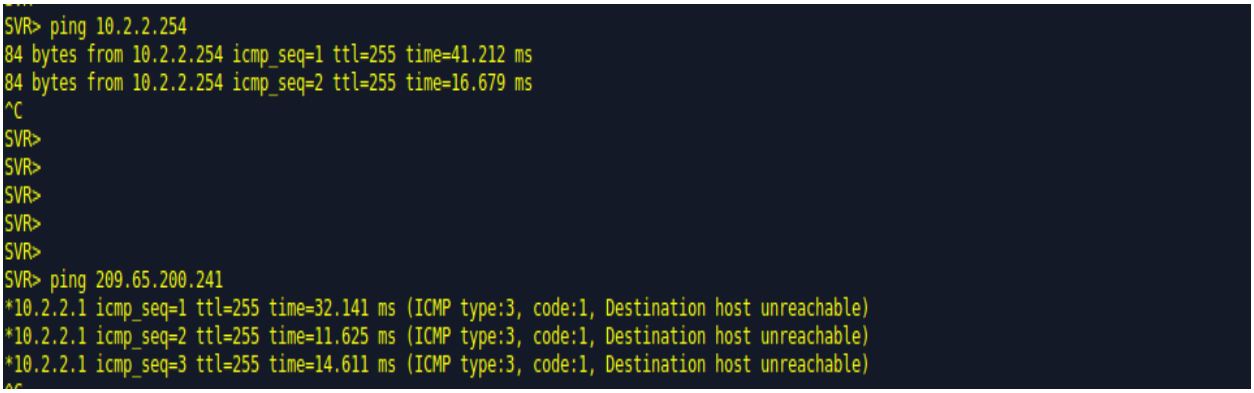


Figure 4.3

Identify and Define: In this case study the Server which is in VLAN 20 is unable to reach the web server at 209.65.200.241

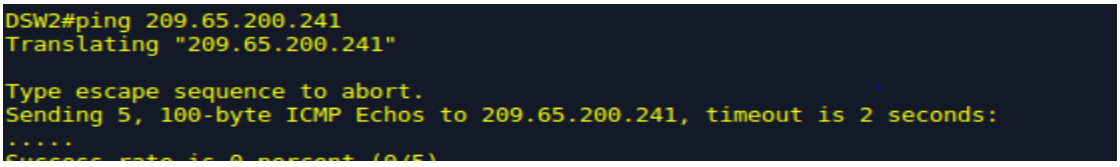
Diagnose starts here, the troubleshooting methodology used here is '**Following the traffic path'**.

It can be observed from the below image that that PC1 can reach its default gateway which is 10.2.2.254, however it cannot reach the web server at 209.65.200.241



While trying to trace the route to the web server from the Server we can observe that the Server can reach only till 10.2.2.1 which is the switched virtual interface i.e. interface vlan 20 configured at DSW2

DSW2 also cannot ping the web server



However while pinging the Web Server from R4 it is successful, due to some unknown reason the Web Server is not pingable from the Server at VLAN 20.

```
R4#ping 209.65.200.241
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.65.200.241, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/329/728 ms
R4#
```

Looking further into the routing table at DSW2 it is clear that DSW2 has no routes to reach outside the EIGRP domain. This means that the issue is at Router R4 which is the Border router between EIGRP and OSPF domains. This is a very important from a diagnosis perspective since we now know where the issue is.

```
DSW2#ping 209.65.200.241
Translating "209.65.200.241"

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.65.200.241, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
DSW2#
DSW2#
DSW2#
DSW2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     4.0.0.0/32 is subnetted, 1 subnets
D       4.4.4.4 [90/156160] via 10.1.4.9, 00:29:54, FastEthernet0/1
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.2.4.12/30 is directly connected, FastEthernet0/0
C       10.1.4.8/30 is directly connected, FastEthernet0/1
C       10.2.1.0/24 is directly connected, Vlan10
C       10.2.2.0/24 is directly connected, Vlan20
D       10.1.4.4/30 [90/30720] via 192.168.1.129, 00:29:54, Vlan200
                    [90/30720] via 10.2.2.2, 00:29:54, Vlan20
                    [90/30720] via 10.1.4.9, 00:29:55, FastEthernet0/1
     192.168.1.0/27 is subnetted, 1 subnets
C       192.168.1.128 is directly connected, Vlan200
DSW2#
DSW2#
```

By looking into the router configuration it can be confirmed that due to some reason OSPF is not redistributed into EIGRP however EIGRP is redistributed into OSPF.

```
R4#sh run | sec router eigrp
router eigrp 10
 default-metric 100 100 1 1 1
 network 4.4.4.4 0.0.0.0
 network 10.1.4.4 0.0.0.3
 network 10.1.4.8 0.0.0.3
```

```
R4#sh run | sec router ospf
router ospf 1
 area 34 nssa no-summary
 redistribute eigrp 10 subnets route-map EIGRP-into-OSPF
 network 10.1.1.8 0.0.0.3 area 34
ipv6 router ospf 6
 redistribute rip Get-Ripped include-connected
```

It is also important to observe the route-maps and access-lists configured at R4 to ensure that there is no misconfiguration. From the observation below route-map and access-list configuration looks good.

```
route-map OSPF-into-EIGRP permit 10
 match ip address OSPF-into-EIGRP
 set tag 6783
route-map EIGRP-into-OSPF permit 10
 match ip address EIGRP-into-OSPF
 set tag 777
R4#
```

```
R4#show access-lists
Standard IP access list EIGRP-into-OSPF
    10 permit 10.1.4.4, wildcard bits 0.0.0.3 (1 match)
    20 permit 10.1.4.8, wildcard bits 0.0.0.3 (1 match)
    30 permit 10.2.1.0, wildcard bits 0.0.0.255
    40 permit 10.2.2.0, wildcard bits 0.0.0.255
    50 permit 10.2.4.12, wildcard bits 0.0.0.3
    60 permit 192.168.1.128, wildcard bits 0.0.0.31
    70 permit 4.4.4.0, wildcard bits 0.0.0.255 (1 match)
Standard IP access list OSPF-into-EIGRP
    10 permit 0.0.0.0
    20 permit 10.1.1.8, wildcard bits 0.0.0.3
```

Let’s go ahead and ensure that OSPF is redistributed in EIGRP.

```
R4(config)#router eigrp 10
R4(config-router)#redis
R4(config-router)#redistribute ?
  bgp         Border Gateway Protocol (BGP)
  connected   Connected
  eigrp       Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis        ISO IS-IS
  mobile      Mobile routes
  odr         On Demand stub Routes
  ospf        Open Shortest Path First (OSPF)
  rip         Routing Information Protocol (RIP)
  static      Static routes
  vrf         Specify a source virtual routing/forwarding instance

R4(config-router)#redistribute osp
R4(config-router)#redistribute ospf 1  ?
  match       Redistribution of OSPF routes
  metric      Metric for redistributed routes
  route-map   Route map reference
  <cr>

R4(config-router)#redistribute ospf 1  rou
R4(config-router)#redistribute ospf 1  route-map ?
  WORD  Pointer to route-map entries

R4(config-router)#redistribute ospf 1  route-map OSPF-into-EIGRP ?
  match   Redistribution of OSPF routes
  metric  Metric for redistributed routes
  <cr>

R4(config-router)#redistribute ospf 1  route-map OSPF-into-EIGRP
```

We can now see that there is an External default route learnt via EIGRP which is due to the fact that OSPF is now redistributed into EIGRP.

```
DSW2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.4.9 to network 0.0.0.0

     4.0.0.0/32 is subnetted, 1 subnets
D       4.4.4.4 [90/156160] via 10.1.4.9, 00:02:22, FastEthernet0/1
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.2.4.12/30 is directly connected, FastEthernet0/0
D EX    10.1.1.8/30 [170/25628160] via 10.1.4.9, 00:00:11, FastEthernet0/1
C       10.1.4.8/30 is directly connected, FastEthernet0/1
C       10.2.1.0/24 is directly connected, Vlan10
C       10.2.2.0/24 is directly connected, Vlan20
D       10.1.4.4/30 [90/30720] via 192.168.1.129, 00:02:24, Vlan200
                    [90/30720] via 10.2.2.2, 00:02:24, Vlan20
                    [90/30720] via 10.1.4.9, 00:02:24, FastEthernet0/1
     192.168.1.0/27 is subnetted, 1 subnets
C       192.168.1.128 is directly connected, Vlan200
D*EX 0.0.0.0/0 [170/25628160] via 10.1.4.9, 00:00:14, FastEthernet0/1
DSW2#
DSW2#
DSW2#ping 209.65.200.241
Translating "209.65.200.241"

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.65.200.241, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 176/182/192 ms
DSW2#
```

Also DSW2 is able to ping the Web Server at 209.65.200.241, so there is a very good chance that the Server in VLAN 20 should be able to reach the Web Server now. The below ping confirms that the Server can Infact reach the Web Server at 209.65.200.241.

```
SVR> ping 209.65.200.241
209.65.200.241 icmp_seq=1 timeout
84 bytes from 209.65.200.241 icmp_seq=2 ttl=250 time=180.601 ms
84 bytes from 209.65.200.241 icmp_seq=3 ttl=250 time=195.767 ms
84 bytes from 209.65.200.241 icmp_seq=4 ttl=250 time=179.259 ms
84 bytes from 209.65.200.241 icmp_seq=5 ttl=250 time=195.210 ms
```

In this case study the fault domain was router R4. The technology causing the issue routing protocol redistribution and the issue was resolved by redistributing OSPF into EIGRP which generated a default route for DSW2 using which DSW2 and the Server in VLAN 20 were able to reach networks outside the EIGRP domain.

Case Study 4: PC2 in VLAN 10 is unable to reach the Web Server at 209.65.200.241

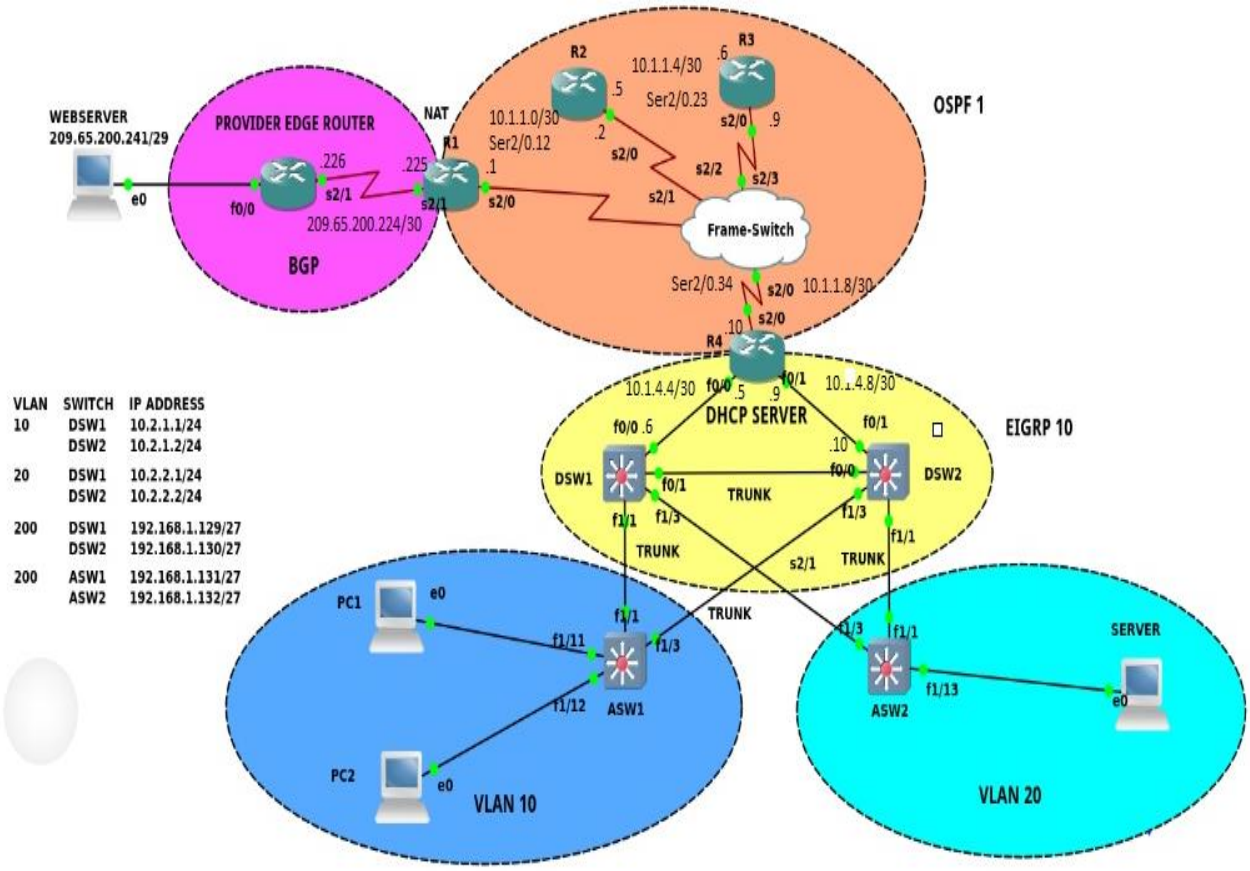


Figure 4.4

Identify and Define: In this case study PC2 which is in VLAN 10 is unable to reach the web server at 209.65.200.241

Diagnose starts here, the troubleshooting methodology used here is '**Following the traffic path'**.

As can be seen in the below picture PC2 is able to ping its default gateway 10.2.1.254 and also Router R4 whose loopback IP address is 4.4.4.4. However while trying to trace to the webserver PC2 is not able to go beyond 10.1.1.9 which is router R3, so it makes sense to check router R3.

```
PC2> ip dhcp
DORA IP 10.2.1.6/24 GW 10.2.1.254

PC2>
PC2>
PC2> ping 10.2.1.254
84 bytes from 10.2.1.254 icmp_seq=1 ttl=255 time=22.174 ms
84 bytes from 10.2.1.254 icmp_seq=2 ttl=255 time=20.145 ms
^C
PC2>
PC2>
PC2>
PC2> ping 4.4.4.4
84 bytes from 4.4.4.4 icmp_seq=1 ttl=254 time=85.430 ms
4.4.4.4 icmp_seq=2 timeout
^C
PC2> ping 4.4.4.4
84 bytes from 4.4.4.4 icmp_seq=1 ttl=254 time=62.663 ms
84 bytes from 4.4.4.4 icmp_seq=2 ttl=254 time=38.718 ms
84 bytes from 4.4.4.4 icmp_seq=3 ttl=254 time=40.677 ms
84 bytes from 4.4.4.4 icmp_seq=4 ttl=254 time=17.649 ms
84 bytes from 4.4.4.4 icmp_seq=5 ttl=254 time=40.222 ms

PC2>
PC2>
PC2>
PC2>
PC2> trace 209.65.200.241
trace to 209.65.200.241, 8 hops max, press Ctrl+C to stop
 1   10.2.1.1   14.077 ms  31.144 ms  20.138 ms
 2   10.1.4.5   515.493 ms  291.815 ms  83.432 ms
 3   10.1.1.9   252.412 ms  82.722 ms  83.207 ms
 4   *10.1.1.9   105.171 ms (ICMP type:3, code:1, Destination host unreachable)
```

It can be observed that R3 does not have the 209.65.200.224/30 network in its routing table nor does it have a default route to reach R2 or R1.

```
R3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      4.0.0.0/32 is subnetted, 1 subnets
O N2     4.4.4.4 [110/20] via 10.1.1.10, 11:27:17, Serial2/0.34
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O IA     10.1.1.0/30 [110/128] via 10.1.1.5, 11:27:22, Serial2/0.23
C        10.1.1.4/30 is directly connected, Serial2/0.23
L        10.1.1.6/32 is directly connected, Serial2/0.23
C        10.1.1.8/30 is directly connected, Serial2/0.34
L        10.1.1.9/32 is directly connected, Serial2/0.34
O N2     10.1.4.4/30 [110/20] via 10.1.1.10, 11:27:17, Serial2/0.34
O N2     10.1.4.8/30 [110/20] via 10.1.1.10, 11:27:17, Serial2/0.34
```

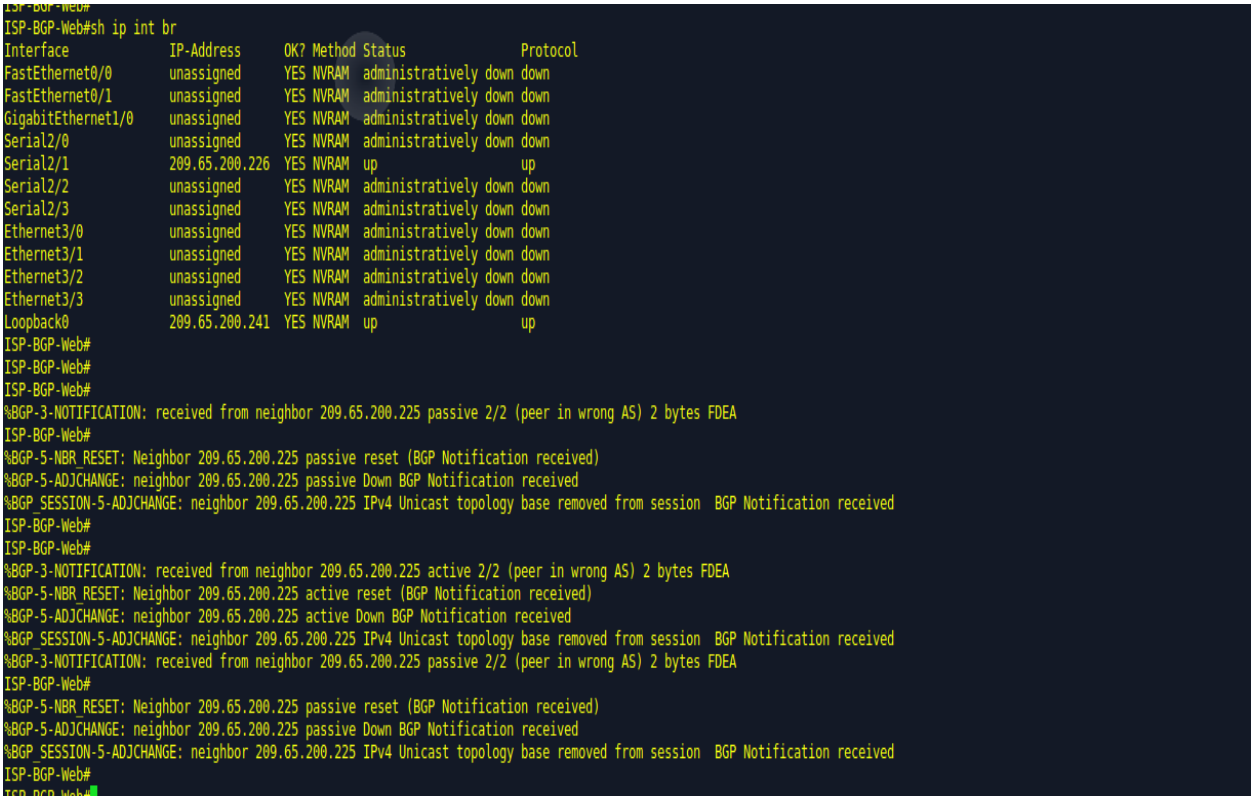
Let’s go ahead and check router R1, we can observe in router R1 that there’s flurry of console messages which is probably due to some issue in R1.

```
%BGP-3-NOTIFICATION: sent to neighbor 209.65.200.226 passive 2/2 (peer in wrong AS) 2 bytes FDEA
R1#
%BGP-4-MSGDUMP: unsupported or mal-formatted message received from 209.65.200.226:
FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 0039 0104 FDEA 00B4 D141 C8F1 1C02 0601
0400 0100 0102 0280 0002 0202 0002 0246 0002 0641 0400 00FD EA
R1#
%BGP-5-NBR_RESET: Neighbor 209.65.200.226 passive reset (BGP Notification sent)
%BGP-5-ADJCHANGE: neighbor 209.65.200.226 passive Down BGP Notification sent
R1#
%BGP-3-NOTIFICATION: sent to neighbor 209.65.200.226 active 2/2 (peer in wrong AS) 2 bytes FDEA
R1#
%BGP-4-MSGDUMP: unsupported or mal-formatted message received from 209.65.200.226:
FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 0039 0104 FDEA 00B4 D141 C8F1 1C02 0601
0400 0100 0102 0280 0002 0202 0002 0246 0002 0641 0400 00FD EA
R1#
%BGP-3-NOTIFICATION: sent to neighbor 209.65.200.226 passive 2/2 (peer in wrong AS) 2 bytes FDEA
R1#
%BGP-4-MSGDUMP: unsupported or mal-formatted message received from 209.65.200.226:
FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 0039 0104 FDEA 00B4 D141 C8F1 1C02 0601
0400 0100 0102 0280 0002 0202 0002 0246 0002 0641 0400 00FD EA
R1#
%BGP-5-NBR_RESET: Neighbor 209.65.200.226 active reset (BGP Notification sent)
%BGP-5-ADJCHANGE: neighbor 209.65.200.226 active Down BGP Notification sent
%BGP_SESSION-5-ADJCHANGE: neighbor 209.65.200.226 IPv4 Unicast topology base removed from session  BGP Notification sent
R1#
%BGP-5-NBR_RESET: Neighbor 209.65.200.226 passive reset (BGP Notification sent)
%BGP-5-ADJCHANGE: neighbor 209.65.200.226 passive Down BGP Notification sent
R1#
%BGP-3-NOTIFICATION: sent to neighbor 209.65.200.226 passive 2/2 (peer in wrong AS) 2 bytes FDEA
```

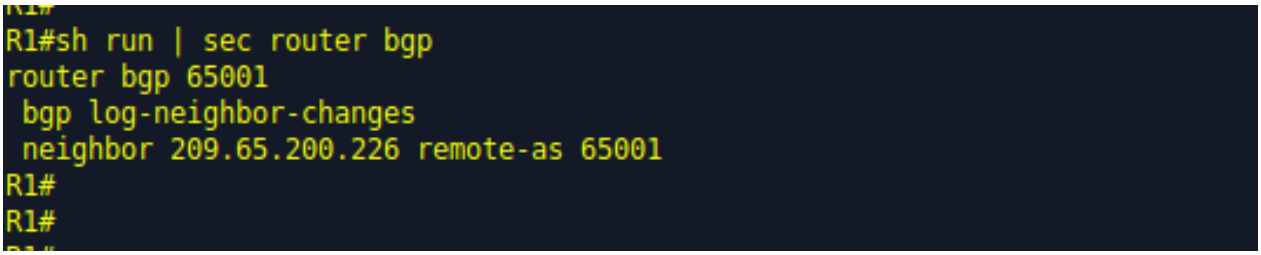
Looking into R1’S routing table it can be observed that R1 does not have default route nor does it have the Web Server’s subnet i.e. 209.65.241.240/30 subnet in its routing table.

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      4.0.0.0/32 is subnetted, 1 subnets
O E2     4.4.4.4 [110/20] via 10.1.1.2, 00:02:51, Serial2/0.12
      10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
C        10.1.1.0/30 is directly connected, Serial2/0.12
L        10.1.1.1/32 is directly connected, Serial2/0.12
O IA     10.1.1.4/30 [110/128] via 10.1.1.2, 00:02:51, Serial2/0.12
O IA     10.1.1.8/30 [110/192] via 10.1.1.2, 00:02:51, Serial2/0.12
O E2     10.1.4.4/30 [110/20] via 10.1.1.2, 00:02:51, Serial2/0.12
O E2     10.1.4.8/30 [110/20] via 10.1.1.2, 00:02:51, Serial2/0.12
O E2     10.2.1.0/24 [110/20] via 10.1.1.2, 00:02:51, Serial2/0.12
O E2     10.2.2.0/24 [110/20] via 10.1.1.2, 00:02:51, Serial2/0.12
O E2     10.2.4.12/30 [110/20] via 10.1.1.2, 00:02:51, Serial2/0.12
      192.168.1.0/27 is subnetted, 1 subnets
O E2     192.168.1.128 [110/20] via 10.1.1.2, 00:02:51, Serial2/0.12
      209.65.200.0/24 is variably subnetted, 3 subnets, 2 masks
C        209.65.200.224/30 is directly connected, Serial2/1
L        209.65.200.225/32 is directly connected, Serial2/1
C        209.65.200.226/32 is directly connected, Serial2/1
```

The IP addresses in ISP router are configured correctly how he same type of console message are also seem in the ISP router like in router R1.



As per the network topology router R1 and the ISP router should have an external BGP neighbor relationship however it can be observed from the below figure that the remote Autonomous system number is configured to be same as the Autonomous system number configured in R1, this becomes an iBGP relationship instead of eBGP. This is the reason why we are seeing ‘Peer in wrong AS’ message at the console of router R1.



The misconfiguration is corrected as below.

```
R1(config)#router bgp 65001
R1(config-router)#no neighbor 209.65.200.226 remote-as 65001
R1(config-router)#neighbor 209.65.200.226 remote-as 65002
```

It can be see that BGP is now converging and finally BGP is up and learning prefixes.

```
R1#sh ip bgp summ
R1#sh ip bgp summary
BGP router identifier 209.65.200.225, local AS number 65001
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
209.65.200.226  4        65002       1       2        1    0    0 00:00:00 OpenConfirm
R1#
R1#sh ip bgp summary
BGP router identifier 209.65.200.225, local AS number 65001
BGP table version is 3, main routing table version 3
2 network entries using 288 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 272 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 744 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
209.65.200.226  4        65002       6       4        3    0    0 00:00:00        2
```

Also R1 now has the Web Server's subnet i.e. 209.65.200.240/30 in its routing table and also there is a default route learnt from the ISP router.

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 209.65.200.226 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 209.65.200.226, 00:03:05
      4.0.0.0/32 is subnetted, 1 subnets
O E2     4.4.4.4 [110/20] via 10.1.1.2, 00:11:46, Serial2/0.12
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial2/0.12
L        10.1.1.1/32 is directly connected, Serial2/0.12
O IA     10.1.1.4/30 [110/128] via 10.1.1.2, 00:11:46, Serial2/0.12
O IA     10.1.1.8/30 [110/192] via 10.1.1.2, 00:11:46, Serial2/0.12
O E2     10.1.4.4/30 [110/20] via 10.1.1.2, 00:11:46, Serial2/0.12
O E2     10.1.4.8/30 [110/20] via 10.1.1.2, 00:11:46, Serial2/0.12
      209.65.200.0/24 is variably subnetted, 4 subnets, 3 masks
C        209.65.200.224/30 is directly connected, Serial2/1
L        209.65.200.225/32 is directly connected, Serial2/1
C        209.65.200.226/32 is directly connected, Serial2/1
B        209.65.200.240/29 [20/0] via 209.65.200.226, 00:03:05
```

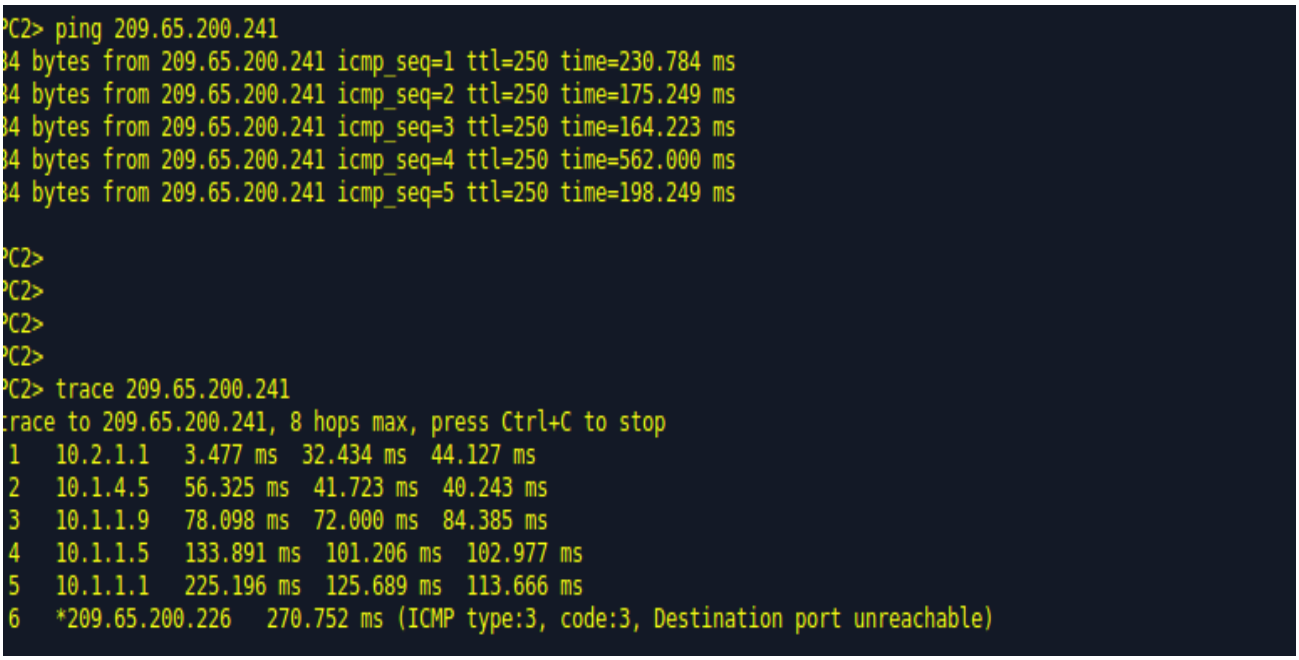
```
R1#sh ip bgp
BGP table version is 3, local router ID is 209.65.200.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  0.0.0.0          209.65.200.226                         0 65002 i
 *>  209.65.200.240/29
                      209.65.200.226           0             0 65002 i
R1#
```

Moving to router R4 and DSW1 it can been be seen that there is default route learnt which is required to forward the traffic moving to the Web Server coming from VLAN 10.

```
R4#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.9 to network 0.0.0.0

O*IA  0.0.0.0/0 [110/65] via 10.1.1.9, 01:27:08, Serial2/0.34
      4.0.0.0/32 is subnetted, 1 subnets
C        4.4.4.4 is directly connected, Loopback0
      10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
C        10.1.1.8/30 is directly connected, Serial2/0.34
L        10.1.1.10/32 is directly connected, Serial2/0.34
C        10.1.4.4/30 is directly connected, FastEthernet0/0
L        10.1.4.5/32 is directly connected, FastEthernet0/0
C        10.1.4.8/30 is directly connected, FastEthernet0/1
L        10.1.4.9/32 is directly connected, FastEthernet0/1
D        10.2.1.0/24 [90/30720] via 10.1.4.6, 00:40:36, FastEthernet0/0
D        10.2.2.0/24 [90/30720] via 10.1.4.6, 00:40:36, FastEthernet0/0
D        10.2.4.12/30 [90/284160] via 10.1.4.10, 00:45:54, FastEthernet0/1
                      [90/284160] via 10.1.4.6, 00:45:54, FastEthernet0/0
      192.168.1.0/27 is subnetted, 1 subnets
D        192.168.1.128 [90/30720] via 10.1.4.6, 00:40:36, FastEthernet0/0
R4#
```

Since PC2 was able to reach its default gateway at 10.2.1.254 and 10.1.4.4/30 is a directly connected network to R4, PC in VLAN 10 should now be able to reach the Web Server since the default route is now present in the routing tables of routers R4, R3, R2 and R1.

It can be seen that PC2 is now successfully able to ping the web server at 209.65.200.241.



In this case study the fault domain was router R1. The technology causing the issue was routing protocol BGP and the issue was resolved by correcting the Autonomous system number for BGP in router R1.

Case Study 5: PC1 to Web server is 7 hops but should always be 6 hops

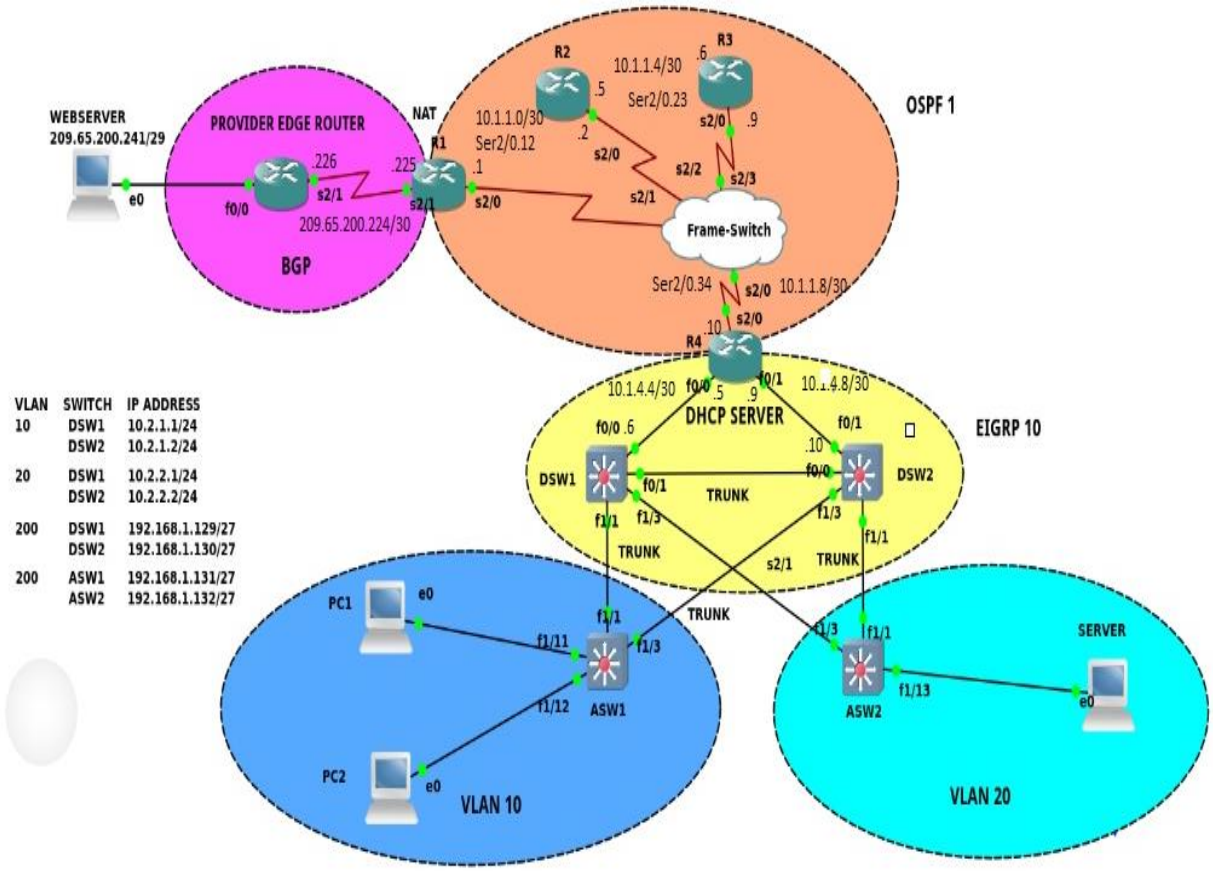


Figure 4.5

Identify and Define: Due to some issue in the network number of hops between PC1 and Web Server is 7. The requirement is to always maintain the number of hops between PC1 to Web Server to 6 by correcting and adjusting the configuration in the network devices..

Diagnose starts here, the troubleshooting methodology used here is '**Following the traffic path'**.

```
PC1> show ip

NAME        : PC1[1]
IP/MASK     : 10.2.1.6/24
GATEWAY     : 10.2.1.254
DNS         :
DHCP SERVER : 10.1.4.9
DHCP LEASE  : 5205, 9000/4500/7875
MAC         : 00:50:79:66:68:01
LPORT       : 20501
RHOST:PORT  : 127.0.0.1:10003
MTU:        : 1500

PC1>
PC1>
PC1> trace 209.65.200.241
trace to 209.65.200.241, 8 hops max, press Ctrl+C to stop
 1   10.2.1.1   9.494 ms  11.021 ms  20.340 ms
 2   10.2.1.2   972.964 ms  72.637 ms  30.635 ms
 3   10.1.4.9   138.709 ms  51.613 ms  41.144 ms
 4   10.1.1.9   167.804 ms  93.769 ms  229.811 ms
 5   10.1.1.5   261.689 ms  156.238 ms  615.774 ms
 6   10.1.1.1   291.580 ms  *  209.661 ms
 7     **209.65.200.226   631.881 ms (ICMP type:3, code:3, Destination port unreachable)
```

Looking into the above trace result the trace from PC1 comes to DSW1 then goes to DSW2 and then to R4, due to some issue DSW1 is not able to forward the packet to R4 so it is sending traffic to DSW2.

Looking into the network topology it is clear that 10.1.4.4/30 is a directly connected network to DSW1 hence DSW1 should be able to forward the ping packets to R4, so why is the traffic going from DSW1 to DSW2 need to be found out.

It can be further found out that 10.1.4.4/30 which is directly connected network to DSW1 is being learnt via EIGRP via next hop IPs 10.2.2.1 and 10.2.1.2 which are the IP addresses for interface VLAN20 and interface VLAN10 in DSW2.

```
DSW1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.2.2.1 to network 0.0.0.0

     4.0.0.0/32 is subnetted, 1 subnets
D       4.4.4.4 [90/158720] via 10.2.2.1, 00:00:26, Vlan20
                [90/158720] via 10.2.1.2, 00:00:26, Vlan10
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.2.4.12/30 is directly connected, FastEthernet0/1
D EX    10.1.1.8/30 [170/25630720] via 10.2.2.1, 00:00:26, Vlan20
                    [170/25630720] via 10.2.1.2, 00:00:26, Vlan10
D       10.1.4.8/30 [90/30720] via 10.2.2.1, 00:01:12, Vlan20
                    [90/30720] via 10.2.1.2, 00:01:12, Vlan10
C       10.2.1.0/24 is directly connected, Vlan10
C       10.2.2.0/24 is directly connected, Vlan20
D       10.1.4.4/30 [90/33280] via 10.2.2.1, 00:00:27, Vlan20
                    [90/33280] via 10.2.1.2, 00:00:27, Vlan10
     192.168.1.0/27 is subnetted, 1 subnets
C       192.168.1.128 is directly connected, Vlan200
D*EX 0.0.0.0/0 [170/25630720] via 10.2.2.1, 00:00:27, Vlan20
               [170/25630720] via 10.2.1.2, 00:00:27, Vlan10
```

The reason looks to be because Fa0/0 interface in DSW1 is down, hence DSW1 is learning the directly connected route from DSW2

```
DSW1#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.4.6        YES manual administratively down down
FastEthernet0/1            10.2.4.13       YES manual up                    up
FastEthernet1/0            unassigned      YES unset  up                    down
FastEthernet1/1            unassigned      YES unset  up                    up
FastEthernet1/2            unassigned      YES unset  administratively down down
FastEthernet1/3            unassigned      YES unset  up                    up
FastEthernet1/4            unassigned      YES unset  administratively down down
FastEthernet1/5            unassigned      YES unset  up                    down
FastEthernet1/6            unassigned      YES unset  up                    down
FastEthernet1/7            unassigned      YES unset  up                    down
FastEthernet1/8            unassigned      YES unset  up                    down
FastEthernet1/9            unassigned      YES unset  up                    down
FastEthernet1/10           unassigned      YES unset  up                    down
FastEthernet1/11           unassigned      YES unset  up                    down
FastEthernet1/12           unassigned      YES unset  up                    down
FastEthernet1/13           unassigned      YES unset  up                    down
FastEthernet1/14           unassigned      YES unset  up                    down
FastEthernet1/15           unassigned      YES unset  up                    down
Serial2/0                  unassigned      YES manual administratively down down
Serial2/1                  unassigned      YES manual administratively down down
Serial2/2                  unassigned      YES manual administratively down down
Serial2/3                  unassigned      YES manual administratively down down
Vlan1                      unassigned      YES manual administratively down down
Vlan10                     10.2.1.1        YES manual up                    up
Vlan20                     10.2.2.2        YES manual up                    up
Vlan200                    192.168.1.129   YES manual up                    up
```

The Default Gateway for PC1 is the HSRP virtual IP address configured in DSW1

```
DSW1#sh run int vlan10
Building configuration...

Current configuration : 228 bytes
!
interface Vlan10
 ip address 10.2.1.1 255.255.255.0
 ip helper-address 4.4.4.4
 standby 10 ip 10.2.1.254
 standby 10 priority 115
 standby 10 preempt
 standby 10 mac-address 0000.1234.5678
 standby 10 track 5 decrement 6
end
```

Below is the track configured in DSW1

```
DSW1#
DSW1#sh run | sec track
track 5 interface FastEthernet0/0 line-protocol
 standby 10 track 5 decrement 6
DSW1#
DSW1#
DSW1#
DSW1#
```

This means that if the line-protocol in interface fa0/0 goes down then the priority of HSRP group 10 will be decremented by a value 6 as shown in the above picture. Now looking into the HSRP configuration for VLAN 10 it is clear that the priority is set to a value of 115, since the track objects (fa0/0) line protocol is down the priority reduces to 109 but still keeping DSW1 as Active Switch for VLAN 10.

```
DSW1#show standby
Vlan10 - Group 10
  State is Active
    13 state changes, last state change 00:08:49
  Virtual IP address is 10.2.1.254
  Active virtual MAC address is 0000.1234.5678
    Local virtual MAC address is 0000.1234.5678 (confgd)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.000 secs
  Preemption enabled
  Active router is local
  Standby router is 10.2.1.2, priority 100 (expires in 9.164 sec)
  Priority 109 (configured 115)
    Track object 5 state Down decrement 6
  IP redundancy name is "hsrp-Vl10-10" (default)
```

Figure below confirms that DSW1 is still in the Active state for VLAN 10

```
DSW1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl10        10  109  P Active   local           10.2.1.2        10.2.1.254
Vl20        20  100  P Standby  10.2.2.1        local           10.2.2.254
```

Let’s change HSRP standby 10 priority to 105 so that when fa0/0 goes down the HSRP priority on DSW1 is decremented by 6 making DSW1 the standby HSRP Layer-3 switch for VLAN 10.

```
DSW1(config-if)#do sh run int vlan 10
Building configuration...

Current configuration : 228 bytes
!
interface Vlan10
 ip address 10.2.1.1 255.255.255.0
 ip helper-address 4.4.4.4
 standby 10 ip 10.2.1.254
 standby 10 priority 115
 standby 10 preempt
 standby 10 mac-address 0000.1234.5678
 standby 10 track 5 decrement 6
end

DSW1(config-if)#no standby 10 pri
DSW1(config-if)#no standby 10 priority 115
DSW1(config-if)#standby 10 priority 105
DSW1(config-if)#^Z
DSW1#
DSW1#
DSW1#sh run int vlan 10
Building configuration...

Current configuration : 228 bytes
!
interface Vlan10
 ip address 10.2.1.1 255.255.255.0
 ip helper-address 4.4.4.4
 standby 10 ip 10.2.1.254
 standby 10 priority 105
 standby 10 preempt
 standby 10 mac-address 0000.1234.5678
 standby 10 track 5 decrement 6
end
```

It can be observed now that DSW2 has become the Standby device for VLAN 10.

```
DSW1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl10        10  99   P Standby  10.2.1.2        local           10.2.1.254
Vl20        20  100  P Standby  10.2.2.1        local           10.2.2.254
DSW1#
```

Trace from PC1 shows first hop as 10.2.1.2 which is the IP address configured on vlan 10 interface in DSW2

```
PC1> ping 209.65.200.241
84 bytes from 209.65.200.241 icmp_seq=1 ttl=250 time=644.455 ms
84 bytes from 209.65.200.241 icmp_seq=2 ttl=250 time=409.888 ms
84 bytes from 209.65.200.241 icmp_seq=3 ttl=250 time=331.814 ms
84 bytes from 209.65.200.241 icmp_seq=4 ttl=250 time=309.843 ms
84 bytes from 209.65.200.241 icmp_seq=5 ttl=250 time=413.947 ms

PC1>
PC1>
PC1>
PC1> trace 209.65.200.241
trace to 209.65.200.241, 8 hops max, press Ctrl+C to stop
 1   10.2.1.2   115.799 ms  49.715 ms  59.951 ms
 2   10.1.4.9   296.316 ms  81.442 ms  101.154 ms
 3   10.1.1.9   315.291 ms  152.020 ms  139.796 ms
 4   10.1.1.5   245.765 ms  212.724 ms  182.653 ms
 5   10.1.1.1   626.978 ms  342.652 ms  332.459 ms
 6   *209.65.200.226   618.970 ms (ICMP type:3, code:3, Destination port unreachable)
```

We can see that the number of Hops have reduced to 6 from 7, this is due to the fact that now traffic from VLAN 10 is directly hitting DSW2.

We can also see that DSW2 is the active HSRP router for both VLAN 10 and VLAN 20

```
DSW2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl10        10  100  P Active   local           10.2.1.1        10.2.1.254
Vl20        20  105  P Active   local           10.2.2.2        10.2.2.254
DSW2#
DSW2#
DSW2#
DSW2#sh run int vlan 10
Building configuration...

Current configuration : 171 bytes
!
interface Vlan10
 ip address 10.2.1.2 255.255.255.0
 ip helper-address 4.4.4.4
 standby 10 ip 10.2.1.254
 standby 10 preempt
 standby 10 mac-address 0000.1234.5678
end
```

Now what if fa0/0 on DSW1 is brought up, ideally HSRP for vlan 10 should failover to DSW1 and traffic from PC1 should hit DSW1 and go to R4, let's do that

```
DSW1#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.4.6        YES manual administratively down down
FastEthernet0/1            10.2.4.13       YES manual up                    up
FastEthernet1/0            unassigned      YES unset  up                    down
FastEthernet1/1            unassigned      YES unset  up                    up
FastEthernet1/2            unassigned      YES unset  administratively down down
FastEthernet1/3            unassigned      YES unset  up                    up
FastEthernet1/4            unassigned      YES unset  administratively down down
FastEthernet1/5            unassigned      YES unset  up                    down
FastEthernet1/6            unassigned      YES unset  up                    down
FastEthernet1/7            unassigned      YES unset  up                    down
FastEthernet1/8            unassigned      YES unset  up                    down

DSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DSW1(config)#int fa0/0
DSW1(config-if)#no shut
DSW1(config-if)#logging console
DSW1(config)#
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.1.4.5 (FastEthernet0/0) is up: new adjacency
```

We can see console message for HSRP for vlan 10 failing over from DSW2 to DSW1 and also EIGRP neighborship is established between DSW1 and R4. Also network between DSW1 and R4 is showing directly connected now.

```
DSW1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl10        10  105  P Active   local           10.2.1.2        10.2.1.254
Vl20        20  100  P Standby  10.2.2.1        local           10.2.2.254
```

```
DSW1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.4.5 to network 0.0.0.0

     4.0.0.0/32 is subnetted, 1 subnets
D       4.4.4.4 [90/156160] via 10.1.4.5, 00:00:55, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.2.4.12/30 is directly connected, FastEthernet0/1
D EX    10.1.1.8/30 [170/25628160] via 10.1.4.5, 00:00:55, FastEthernet0/0
D       10.1.4.8/30 [90/30720] via 10.2.2.1, 00:00:55, Vlan20
                    [90/30720] via 10.2.1.2, 00:00:55, Vlan10
                    [90/30720] via 10.1.4.5, 00:00:55, FastEthernet0/0
C       10.2.1.0/24 is directly connected, Vlan10
C       10.2.2.0/24 is directly connected, Vlan20
C       10.1.4.4/30 is directly connected, FastEthernet0/0
     192.168.1.0/27 is subnetted, 1 subnets
C       192.168.1.128 is directly connected, Vlan200
D*EX 0.0.0.0/0 [170/25628160] via 10.1.4.5, 00:00:57, FastEthernet0/0
DSW1#
DSW1#sh ip eigrp nei
DSW1#sh ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.1.130           Vl200             13 00:00:53    1  5000  2  0
0   10.2.1.2                Vl10              14 00:01:03   32   200  0  490
4   10.1.4.5                Fa0/0             11 00:03:07  561  3366  0  56
3   10.2.4.14               Fa0/1             13 00:06:27   34   204  0  491
2   10.2.2.1                Vl20              12 00:06:27   43   258  0  492
```

Below shows that traffic from PC1 is hitting DSW1 and then R4 and we are also meeting the requirement of maintaining number of hops to 6 always.

```
PC1> ping 209.65.200.241
209.65.200.241 icmp_seq=1 timeout
84 bytes from 209.65.200.241 icmp_seq=2 ttl=250 time=385.954 ms
84 bytes from 209.65.200.241 icmp_seq=3 ttl=250 time=437.208 ms
84 bytes from 209.65.200.241 icmp_seq=4 ttl=250 time=373.898 ms
84 bytes from 209.65.200.241 icmp_seq=5 ttl=250 time=408.984 ms

PC1>
PC1>
PC1> trace 209.65.200.241
trace to 209.65.200.241, 8 hops max, press Ctrl+C to stop
 1     *10.2.1.1   38.465 ms  50.103 ms
 2   10.1.4.5   785.543 ms  242.952 ms  151.211 ms
 3   10.1.1.9   283.162 ms  131.946 ms  60.494 ms
 4   10.1.1.5   364.719 ms  193.981 ms  800.123 ms
 5   10.1.1.1   455.849 ms  291.052 ms  412.764 ms
 6   *209.65.200.226   658.767 ms (ICMP type:3, code:3, Destination port unreachable)
```

Again shutdown fa0/0 in DSW1 for testing

```
DSW1(config)#int fa0/0
DSW1(config-if)#shut
DSW1(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.1.4.5 (FastEthernet0/0) is down: interface down
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 192.168.1.130 (Vlan200) is down: Interface Goodbye received
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 192.168.1.130 (Vlan200) is up: new adjacency
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
DSW1(config-if)#
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Active -> Speak
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.2.1.2 (Vlan10) is down: peer restarted
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.2.1.2 (Vlan10) is up: new adjacency
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
```

We can see that DSW1 has become HSRP Standby for HSRP VLAN 10. Below shows traffic from PC1 is hitting DSW2, then R4 and then out to the internet. This shows that the hops between PC1 to webserver will always remain 6 hops.

```
PC1>
PC1> ping 209.65.200.241
84 bytes from 209.65.200.241 icmp_seq=1 ttl=250 time=776.472 ms
84 bytes from 209.65.200.241 icmp_seq=2 ttl=250 time=354.402 ms
84 bytes from 209.65.200.241 icmp_seq=3 ttl=250 time=507.497 ms
84 bytes from 209.65.200.241 icmp_seq=4 ttl=250 time=314.890 ms
84 bytes from 209.65.200.241 icmp_seq=5 ttl=250 time=333.504 ms

PC1>
PC1>
PC1>
PC1>
PC1> trace 209.65.200.241
trace to 209.65.200.241, 8 hops max, press Ctrl+C to stop
 1   10.2.1.2   53.533 ms  40.000 ms  30.669 ms
 2   10.1.4.9   345.706 ms  69.593 ms  59.796 ms
 3   10.1.1.9   141.607 ms  193.142 ms  130.709 ms
 4   10.1.1.5   225.594 ms  224.823 ms  422.293 ms
 5   10.1.1.1   680.393 ms  374.392 ms  415.991 ms
 6   *209.65.200.226   716.200 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

The fault domain was DSW1, technology was HSRP and the solution was to adjust the priority in DSW1 for HSRP to failover between DSW1 and DSW2 so as to ensure that the number of hops between PC1 and webserver always remains 6 hops.

Case Study 6: Fault tolerance for VLAN 10 completely fails if DSW1 is down

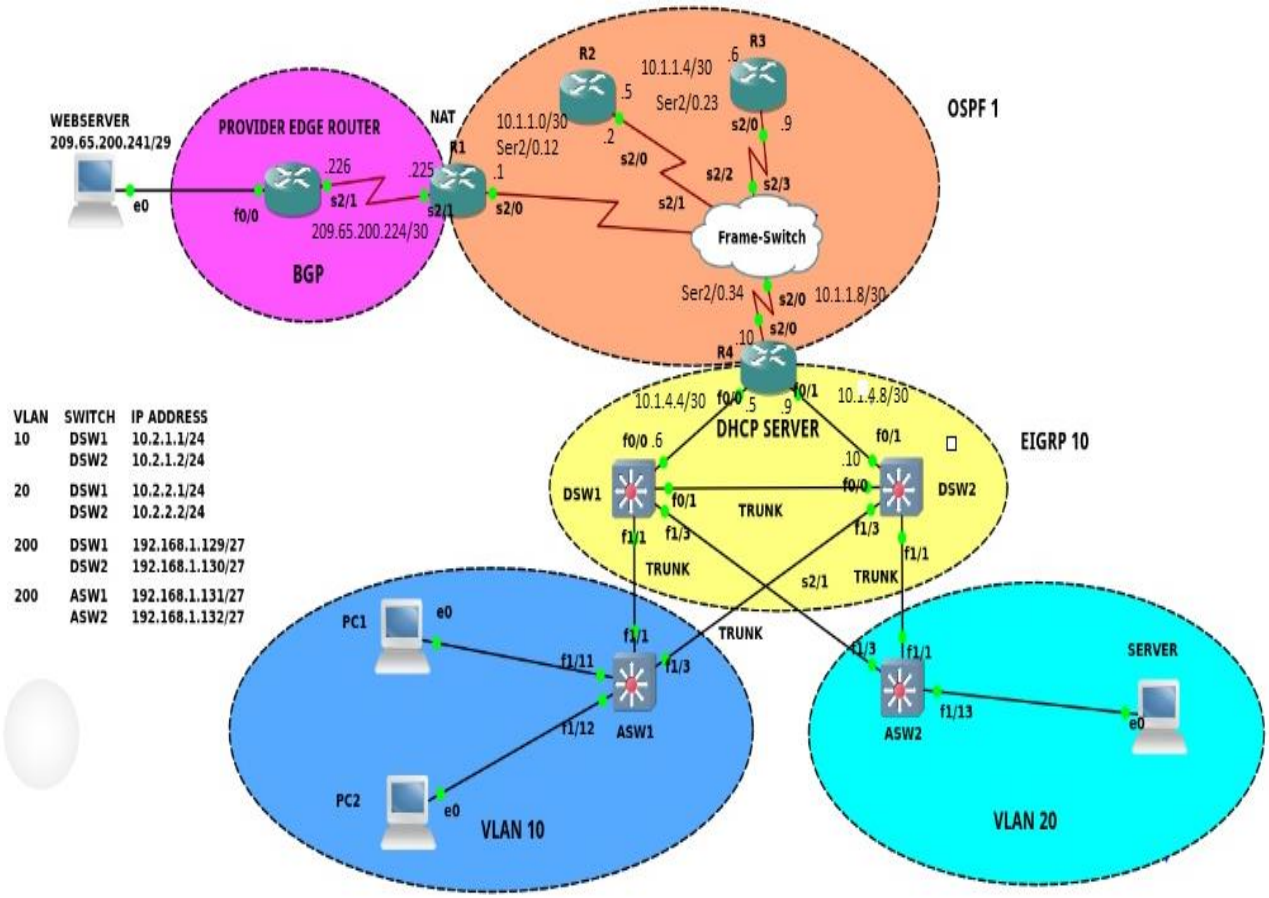


Figure 4.6

Identify and Define: Fault tolerance for VLAN 10 completely fails if DSW1 is down. This means that devices in VLAN 10 are incapable of receiving IP address from the DHCP server and hence unable to reach out to other devices neither in the internal network or out to the external network outside EIGRP domain. This issue was created by powering down DSW1 in GNS3.

It can be observed that due to some issue in the network PC1 is unable of getting an IP address from DHCP server.

```
PC1> ip dhcp
DDD
Can't find dhcp server

PC1>
PC1>
PC1>
PC1> ip dhcp
DDD
Can't find dhcp server
```

We can see from the below command “show standby brief” that DSW2 has taken over the role of active HSRP router for VLAN 10.

```
DSW2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl10        10  100  P Active   local           unknown         10.2.1.254
Vl20        20  99   P Active   local           unknown         10.2.2.254
DSW2#
DSW2#
DSW2#show standby vlan 10
Vlan10 - Group 10
  State is Active
    1 state change, last state change 00:01:36
  Virtual IP address is 10.2.1.254
  Active virtual MAC address is 0000.1234.5678
    Local virtual MAC address is 0000.1234.5678 (confgd)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.492 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Vl10-10" (default)
DSW2#
```

We can observe that IP helper address is configured in DSW2 but DSW2 cannot reach R4 which is the DHCP server.

```
DSW2#show ip helper-address
Interface                Helper-Address  VPN VRG Name            VRG State
Vlan10                   4.4.4.4         0   None                Unknown
Vlan20                   4.4.4.4         0   None                Unknown
DSW2#
DSW2#
DSW2#
DSW2#
DSW2#ping 4.4.4.4 source vlan 10
Translating "4.4.4.4"

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 10.2.1.2
.....
Success rate is 0 percent (0/5)
DSW2#
```

DSW2 is also not having any EIGRP routes in its routing table. DSW1, DSW2 and R4 are all running EIGRP, so definitely there's some issue with EIGRP in DSW2 or R4. There are no EIGRP learned routes in DSW2's routing table as can be seen below.

```
DSW2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.2.4.12/30 is directly connected, FastEthernet0/0
C       10.1.4.8/30 is directly connected, FastEthernet0/1
C       10.2.1.0/24 is directly connected, Vlan10
C       10.2.2.0/24 is directly connected, Vlan20
     192.168.1.0/27 is subnetted, 1 subnets
C       192.168.1.128 is directly connected, Vlan200
DSW2#
```

DSW2 cannot reach loopback of R4 but can ping 10.1.4.9 which is the IP address configured on the directly connected interface on R4.

```
DSW2#ping 4.4.4.4
Translating "4.4.4.4"

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
DSW2#
DSW2#
DSW2#
DSW2#ping 10.1.4.9
Translating "10.1.4.9"

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.4.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/32/52 ms
DSW2#
```

DSW2 and R4 should be reachable to each other via EIGRP however EIGRP is not working on DSW2's fast Ethernet 0/1 interface which is the interface in DSW2 connected to R4.

```
DSW2#show ip eigrp interfaces
IP-EIGRP interfaces for process 10

                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Vl10               0        0/0         0       0/1           50           0
Vl20               0        0/0         0       0/1           50           0
Fa0/0              0        0/0         0       0/1            0           0
Vl200              0        0/0         0       0/1           50           0
DSW2#
DSW2#
DSW2#show ip eigrp interfaces fa
DSW2#show ip eigrp interfaces fastEthernet 0/1
IP-EIGRP interfaces for process 10

                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
DSW2#
```

Looking into the “show ip protocols” command’s output we can see that DSW2 is advertising 10.1.4.8/30 network but the problem is fa0/1 is set as passive interface, due to this DSW2 will not form EIGRP neighbor relationship with the device connected to it on fa0/1 interface.

```
DSW2#show ip protocols
Routing Protocol is "eigrp 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 10
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.1.4.8/30
    10.2.1.0/24
    10.2.2.0/24
    10.2.4.12/30
    192.168.1.128/27
  Passive Interface(s):
    FastEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:22:13
    Gateway         Distance      Last Update
    10.1.4.9              90      00:12:43
    10.2.1.1              90      00:22:03
    10.2.2.2              90      00:22:03
    192.168.1.129         90      00:22:03
  Distance: internal 90 external 170
```

Looking into the running config for DSW2 it can be confirmed that fa0/1 is configured as passive interface.

```
DSW2#sh running-config | sec router eigrp
router eigrp 10
 passive-interface FastEthernet0/1
 network 10.1.4.8 0.0.0.3
 network 10.2.1.0 0.0.0.255
 network 10.2.2.0 0.0.0.255
 network 10.2.4.12 0.0.0.3
 network 192.168.1.128 0.0.0.31
 no auto-summary
DSW2#
```

Let's go ahead and disable passive-interface on fa0/1 at DSW2, as soon as this is done we can observe that EIGRP neighbor relationship with R4 (10.1.4.9) is up and established.

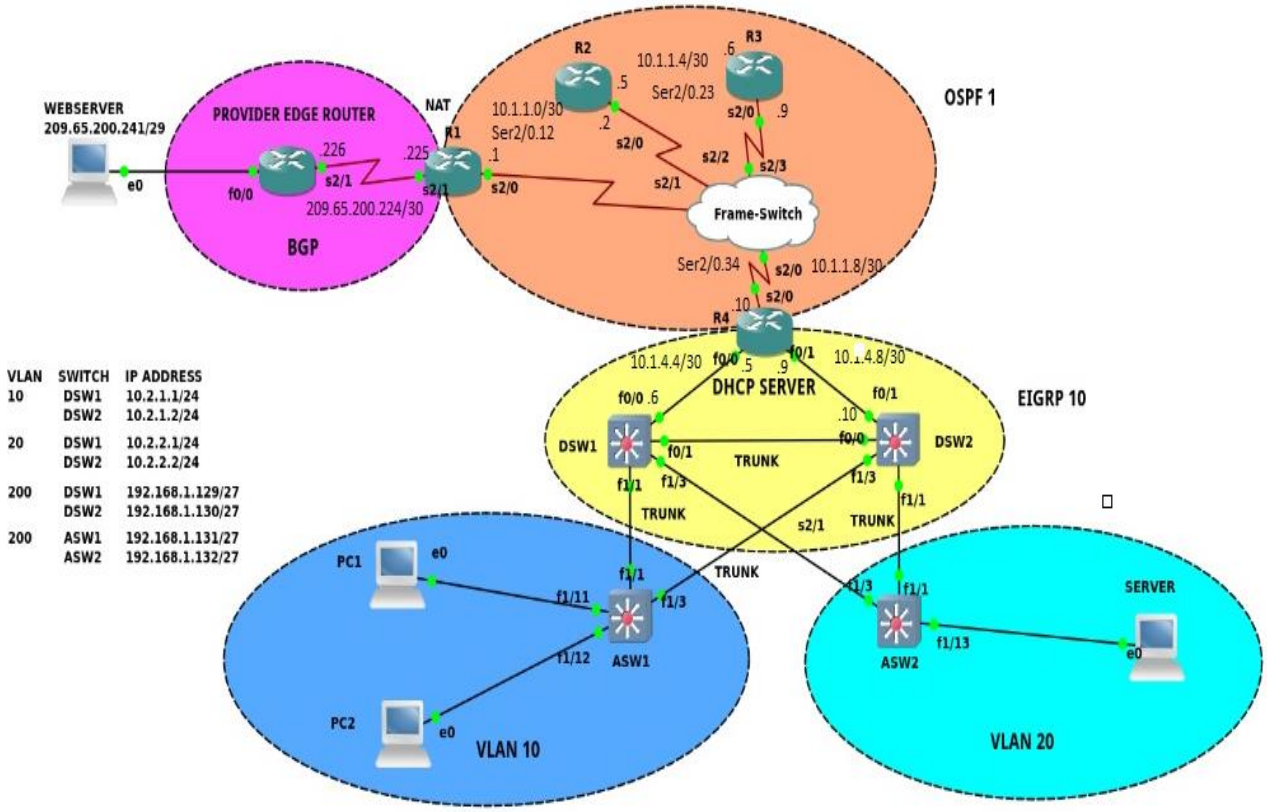
```
DSW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DSW2(config)#router eigrp 10
DSW2(config-router)#
DSW2(config-router)#no passive-interface fa 0/1
DSW2(config-router)#
DSW2(config-router)#
DSW2(config-router)#^Z
DSW2#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.1.4.9 (FastEthernet0/1) is up: new adjacency
DSW2#
%SYS-5-CONFIG_I: Configured from console by console
DSW2#
```

PC1 is now getting IP address and is now able to ping the web-server

```
PC1> ip dhcp
DDORA IP 10.2.1.6/24 GW 10.2.1.254

PC1>
PC1> ping 209.65.200.241
84 bytes from 209.65.200.241 icmp_seq=1 ttl=250 time
84 bytes from 209.65.200.241 icmp_seq=2 ttl=250 time
84 bytes from 209.65.200.241 icmp_seq=3 ttl=250 time
```

In this case study the fault domain was DSW2, technology was EIGRP and the solution was to disable passive interface for fa0/1 in DSW2 which brought up EIGRP neighbor relationship between DSW2 and R4. Then PC1 had reachability to R4 which is the DHCP server and PC1 was able to receive an IP address from the DHCP server and eventually ping the Web Server.

Case Study 7: ASW1 cannot reach the webserver



VLAN	SWITCH	IP ADDRESS
10	DSW1	10.2.1.1/24
	DSW2	10.2.1.2/24
20	DSW1	10.2.2.1/24
	DSW2	10.2.2.2/24
200	DSW1	192.168.1.129/27
	DSW2	192.168.1.130/27
200	ASW1	192.168.1.131/27
	ASW2	192.168.1.132/27

Figure 4.7

Identify and Define: In this case study the issue is that the access layer switch ASW1 which is primary serving VLAN10 is unable to reach the webserver at IP address 209.65.200.241. The objective is to find out the fault domain, the technology that is causing the issue and finally resolve the issue.

It can be observed that when ASW1 is trying to trace the web server it cannot go beyond 10.1.1.9.

```
ASW1#
ASW1#ping 209.65.200.241

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.65.200.241, timeout is 2 seconds:
.UUUU
Success rate is 0 percent (0/5)
ASW1#
ASW1#
ASW1#
ASW1#
ASW1#trace 209.65.200.241

Type escape sequence to abort.
Tracing the route to 209.65.200.241

  1 192.168.1.130 60 msec 12 msec 92 msec
  2 10.1.4.9 260 msec 68 msec 64 msec
  3 10.1.1.9 140 msec 112 msec 128 msec
  4 10.1.1.9 !H  !H  !H
ASW1#
ASW1#
```

Looking into the network topology, 10.1.1.9 is the IP address configured on R3's interface that is facing R4, let's login to R3 and check its routing table. It is clear that R3 does not have route to reach the webserver at 209.65.200.241 or the ISP subnet which is in 209.65.201.224/30 subnet.

```
R3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      4.0.0.0/32 is subnetted, 1 subnets
O N2     4.4.4.4 [110/20] via 10.1.1.10, 11:18:18, Serial2/0.34
      10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
O IA     10.1.1.0/30 [110/128] via 10.1.1.5, 11:18:18, Serial2/0.23
C        10.1.1.4/30 is directly connected, Serial2/0.23
L        10.1.1.6/32 is directly connected, Serial2/0.23
C        10.1.1.8/30 is directly connected, Serial2/0.34
L        10.1.1.9/32 is directly connected, Serial2/0.34
O N2     10.1.4.4/30 [110/20] via 10.1.1.10, 11:18:18, Serial2/0.34
O N2     10.1.4.8/30 [110/20] via 10.1.1.10, 11:18:18, Serial2/0.34
O N2     10.2.1.0/24 [110/20] via 10.1.1.10, 00:03:07, Serial2/0.34
O N2     10.2.2.0/24 [110/20] via 10.1.1.10, 00:03:07, Serial2/0.34
O N2     10.2.4.12/30 [110/20] via 10.1.1.10, 00:03:07, Serial2/0.34
      192.168.1.0/27 is subnetted, 1 subnets
O N2     192.168.1.128 [110/20] via 10.1.1.10, 00:03:07, Serial2/0.34
R3#
```

It can be observed that router R3 has OSPF neighborship with R2 (10.1.1.5)

```
R3#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.1.5          0   FULL/  -        00:00:32    10.1.1.5        Serial2/0.23
4.4.4.4           0   FULL/  -        00:00:35    10.1.1.10       Serial2/0.34
```

Looking into the routing table of R2, it also does not have route or default route to reach 209.65.200.224/30 network. Also it does not have OSPF neighborship with R1

```
R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      4.0.0.0/32 is subnetted, 1 subnets
O E2     4.4.4.4 [110/20] via 10.1.1.6, 11:23:32, Serial2/0.23
      10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
C        10.1.1.0/30 is directly connected, Serial2/0.12
L        10.1.1.2/32 is directly connected, Serial2/0.12
C        10.1.1.4/30 is directly connected, Serial2/0.23
L        10.1.1.5/32 is directly connected, Serial2/0.23
O IA     10.1.1.8/30 [110/128] via 10.1.1.6, 11:23:32, Serial2/0.23
O E2     10.1.4.4/30 [110/20] via 10.1.1.6, 11:23:32, Serial2/0.23
O E2     10.1.4.8/30 [110/20] via 10.1.1.6, 11:23:32, Serial2/0.23
O E2     10.2.1.0/24 [110/20] via 10.1.1.6, 00:07:58, Serial2/0.23
O E2     10.2.2.0/24 [110/20] via 10.1.1.6, 00:07:58, Serial2/0.23
O E2     10.2.4.12/30 [110/20] via 10.1.1.6, 00:07:58, Serial2/0.23
      192.168.1.0/27 is subnetted, 1 subnets
O E2     192.168.1.128 [110/20] via 10.1.1.6, 00:07:58, Serial2/0.23
R2#
R2#
R2#
R2#
R2#sh ip ospf nei
R2#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.1.9          0   FULL/  -        00:00:35    10.1.1.6        Serial2/0.23
```

We can see that OSPF is enabled in router R2

```
R2#show ip ospf interface br
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se2/0.23     1     0               10.1.1.5/30        64    P2P   1/1
Se2/0.12     1     12              10.1.1.2/30        64    P2P   0/0
R2#
```

From the show command ‘Show ip ospf interface Se2/0.12’ it can be seen that OSPF is running in R2’s interface facing R1, network type is point-to-point, Hello and Dead timers are 10 and 40 secs and there is no OSPF authentication configured.

```
R2#
R2#show ip ospf interface Se2/0.12
Serial2/0.12 is up, line protocol is up
  Internet Address 10.1.1.2/30, Area 12, Attached via Network Statement
  Process ID 1, Router ID 10.1.1.5, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R2#
```

Let’s check the same in R1, the network type configured in R1 is point-to-point, Hello and Dead timers are 11 and 44 secs respectively, due to this R1 and R2 will not form OSPF neighborship.

```
R1#show ip ospf interface br
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se2/0.12     1     12              10.1.1.1/30        64    P2P   0/0
R1#
R1#
R1#
R1#
R1#
R1#show ip ospf interface Se2/0.12
Serial2/0.12 is up, line protocol is up
  Internet Address 10.1.1.1/30, Area 12, Attached via Network Statement
  Process ID 1, Router ID 209.65.200.225, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 11, Dead 44, Wait 44, Retransmit 5
    oob-resync timeout 44
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Let's check OSPF configuration in R1 and it is clear that hello timer for OSPF is set to 11secs in router R1.

```
R1#sh run int Se2/0.12
Building configuration...

Current configuration : 209 bytes
!
interface Serial2/0.12 point-to-point
 ip address 10.1.1.1 255.255.255.252
 ip nat inside
 ip ospf hello-interval 11
 ipv6 address 2026::12:1/122
 ipv6 ospf 6 area 12
 frame-relay interface-dlci 122
end
```

Let's fix this, by running the 'no ip ospf hello-interval' command which will set OSPF Hello timer to the default value of 10 secs, we can see now that OSPF is forming neighbor relationship with R2.

```
R1(config)#int se2/0.12
R1(config-subif)#
R1(config-subif)#no ip ospf hello
R1(config-subif)#no ip ospf hello-interval
R1(config-subif)#
R1(config-subif)#
R1(config-subif)#
R1(config-subif)#
R1(config-subif)#
R1(config-subif)#^Z
R1#
%OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.5 on Serial2/0.12 from LOADING to FULL, Loading Done
R1#
```

```
R1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.1.5          0   FULL/  -        00:00:38    10.1.1.2        Serial2/0.12
R1#
```

However ASW1 still cannot reach the webserver

```
ASW1#
ASW1#ping 209.65.200.241

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.65.200.241, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
ASW1#
ASW1#
ASW1#traceroute 209.65.200.241

Type escape sequence to abort.
Tracing the route to 209.65.200.241

  1 192.168.1.130 36 msec 32 msec 36 msec
  2 10.1.4.9 340 msec 220 msec 64 msec
  3 10.1.1.9 172 msec 104 msec 168 msec
  4 10.1.1.5 220 msec 148 msec 152 msec
  5 10.1.1.1 224 msec 204 msec 176 msec
  6  *  *  *
  7  *
ASW1#
ASW1#
```

ASW1 can reach R1 i.e. 10.1.1.1 and R1 can reach the webserver.

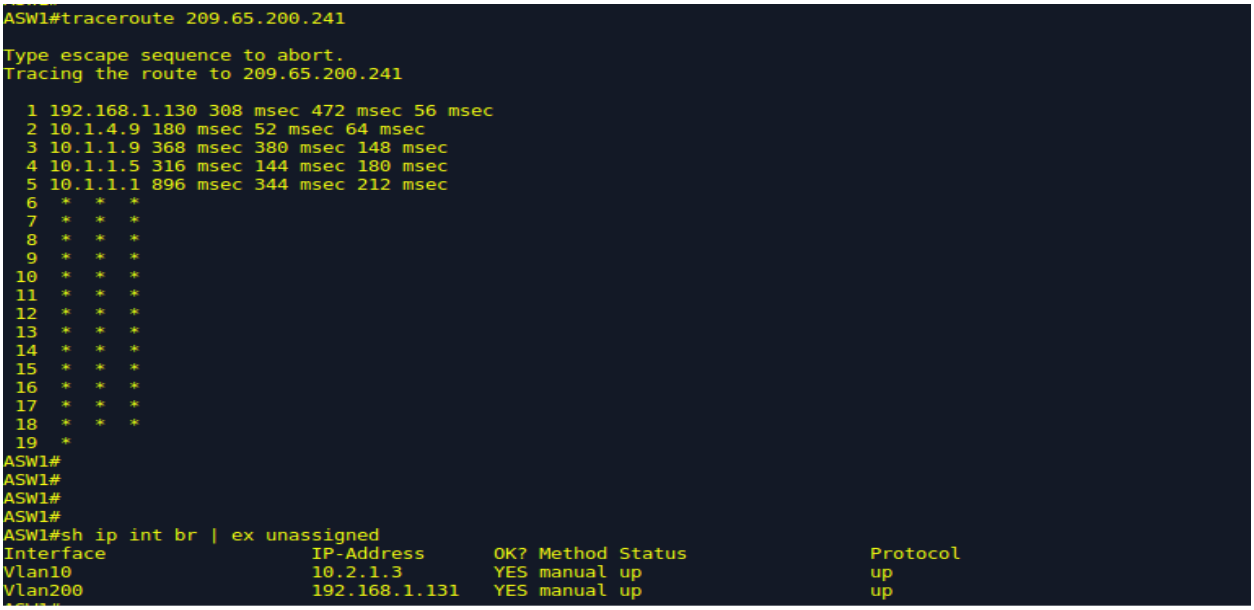
```
R1#ping 209.65.200.241
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.65.200.241, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/32/40 ms
R1#
```

So issue is something within R1 that is not allowing ASW1 to reach the webserver, maybe technology like access-list or Network address translation is causing the issue.

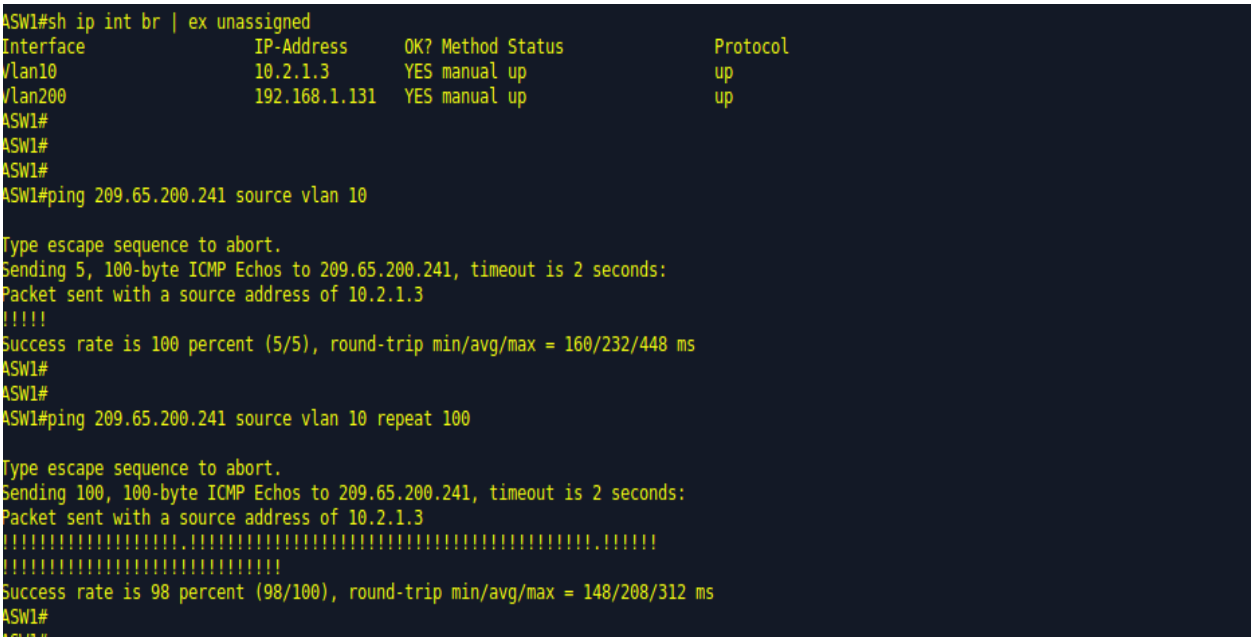
We can see that there's Network address translation configured which is using an access-list named Go-NAT-Go. This means that the Source IP addresses that router R1 is able to NAT are defined in access-list named Go-NAT-Go.

```
R1#sh run | in nat
 ip nat inside
 ip nat outside
 default-information originate
ip nat inside source list Go-NAT-Go interface Serial2/1 overload
R1#
R1#
R1#sh ip nat translations
R1#
R1#sh ip nat translations
R1#
R1#
R1#show access
R1#show access-lis
R1#show access-lists
Standard IP access list Go-NAT-Go
    10 permit 10.1.0.0, wildcard bits 0.0.255.255
    20 permit 10.2.0.0, wildcard bits 0.0.255.255
Extended IP access list DEFEND
    10 deny ip 10.0.0.0 0.255.255.255 any
    20 deny ip 172.16.0.0 0.15.255.255 any
    30 deny ip 192.168.0.0 0.0.255.255 any
    40 deny ip host 255.255.255.255 any
    50 deny ip host 0.0.0.0 any
    60 permit ip any any (1635 matches)
R1#
```

Traceroute from ASW1 shows that first hop is 192.168.1.130 which means that ASW1 is sending pings with a source of VLAN 200 which is the management VLAN and hence will be blocked by the implicit deny in access-list Go-NAT-Go configured in router R1.



Let’s ping using source of vlan 10, we can observe that the ping to the webserver with source as vlan 10 is successful.



We can see that pings are successful, so for normal pings to work we can allow 192.168.1.131 in the ACL and that should fix the issue, let's go ahead and do that.

```
R1(config-std-nacl)#30 permit 192.168.1.131 0.0.0.0
R1(config-std-nacl)#
R1(config-std-nacl)#
R1(config-std-nacl)#^Z
R1#
R1#
R1#
R1#
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show access-lists
Standard IP access list Go-NAT-Go
    30 permit 192.168.1.131
    10 permit 10.1.0.0, wildcard bits 0.0.255.255
    20 permit 10.2.0.0, wildcard bits 0.0.255.255 (2 matches)
Extended IP access list DEFEND
    10 deny ip 10.0.0.0 0.255.255.255 any
    20 deny ip 172.16.0.0 0.15.255.255 any
    30 deny ip 192.168.0.0 0.0.255.255 any
    40 deny ip host 255.255.255.255 any
    50 deny ip host 0.0.0.0 any
    60 permit ip any any (1758 matches)
R1#
```

We can see that now ASW1 is able to reach the webserver without using vlan 10 as the source

```
ASW1#ping 209.65.200.241

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.65.200.241, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 172/251/388 ms
ASW1#
ASW1#ping 209.65.200.241 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 209.65.200.241, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 98 percent (98/100), round-trip min/avg/max = 140/220/636 ms
ASW1#
```

In this case study the fault domain was router R1, technology was OSPF and Access-List and the solution was to make OSPF hello timer in router R1 to be same as that of router R2 so that OSPF neighbor relationship could be established between routers R1 and R2. Another thing that had to be done to allow pings to the webserver without source of vlan 10 was to allow IP address 192.168.1.131 in the access-list named Go-NAT-Go so that router R1 could perform network address translation on ASW's vlan200 IP address of 192.168.1.131

Case Study 8: PC1 in VLAN 10 can't ping the web server

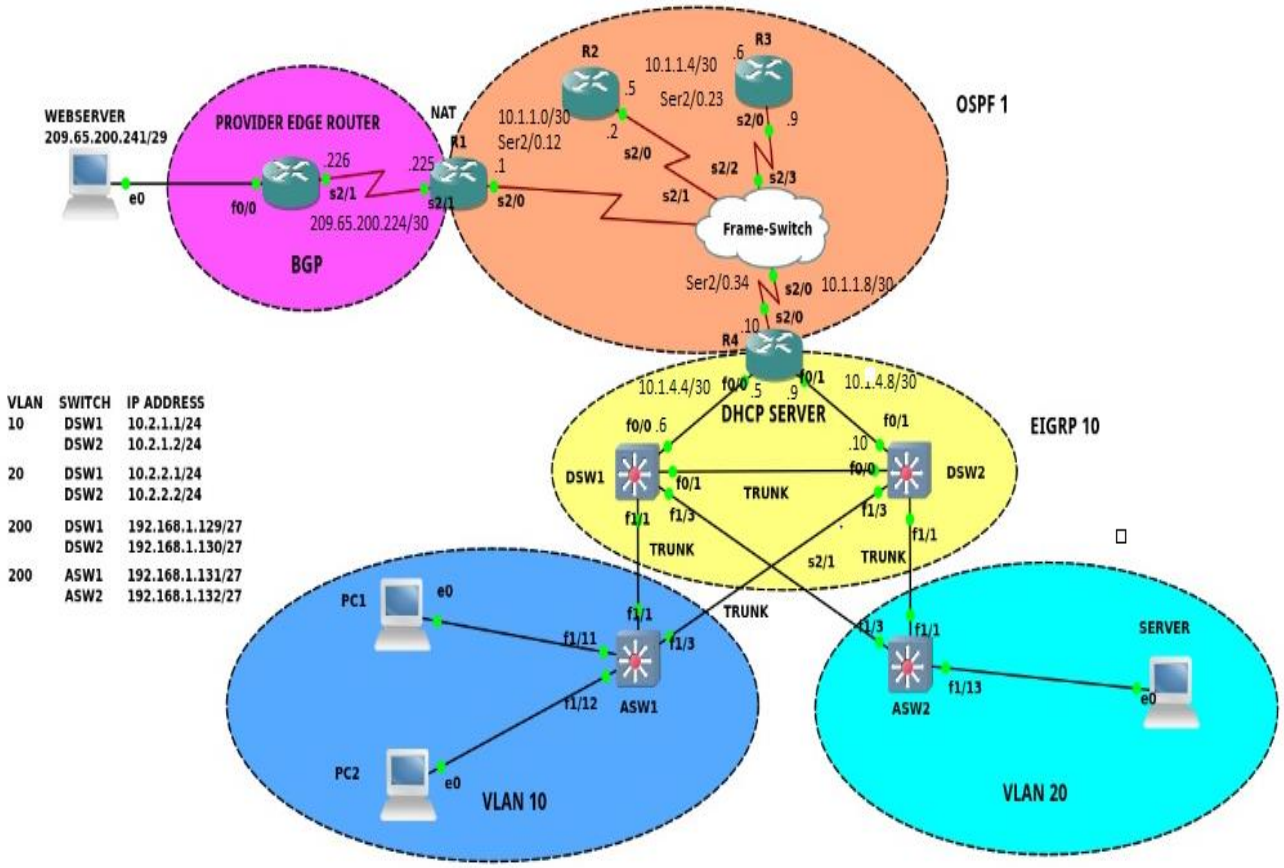


Figure 4.8

Identify and Define: In this case study PC1 which is in VLAN 10 is unable to ping the web server at 209.65.200.241. The objective is to find out the fault domain, the technology causing the issue and finally resolving the issue.

```
PC1>
PC1> ip dhcp
DORA IP 10.2.1.6/28 GW 10.2.1.254

PC1>
PC1> sh ip

NAME        : PC1[1]
IP/MASK     : 10.2.1.6/28
GATEWAY     : 10.2.1.254
DNS         :
DHCP SERVER : 10.1.4.9
DHCP LEASE  : 8994, 9000/4500/7875
MAC         : 00:50:79:66:68:01
LPORT       : 20501
RHOST:PORT  : 127.0.0.1:10003
MTU:        : 1500

PC1>
PC1> ping 10.2.1.254
host (10.2.1.254) not reachable
```

Looking closely into the IP configuration we can see from the above figure that PC1's IP address and the default gateway are in different subnets. This is the reason PC1 is unable to ping its default gateway. This looks to be a DHCP server issue.

R4 is the DHCP server in the topology, let's do some investigation in the DHCP server.

```
R4#sh ip dhcp pool

Pool SUBNET-10 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 14
 Leased addresses               : 1
 Excluded addresses             : 5
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 10.2.1.7             10.2.1.1        - 10.2.1.14         1     / 5     / 14

Pool SUBNET-20 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 5
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 10.2.2.1             10.2.2.1        - 10.2.2.254        0     / 5     / 254
```

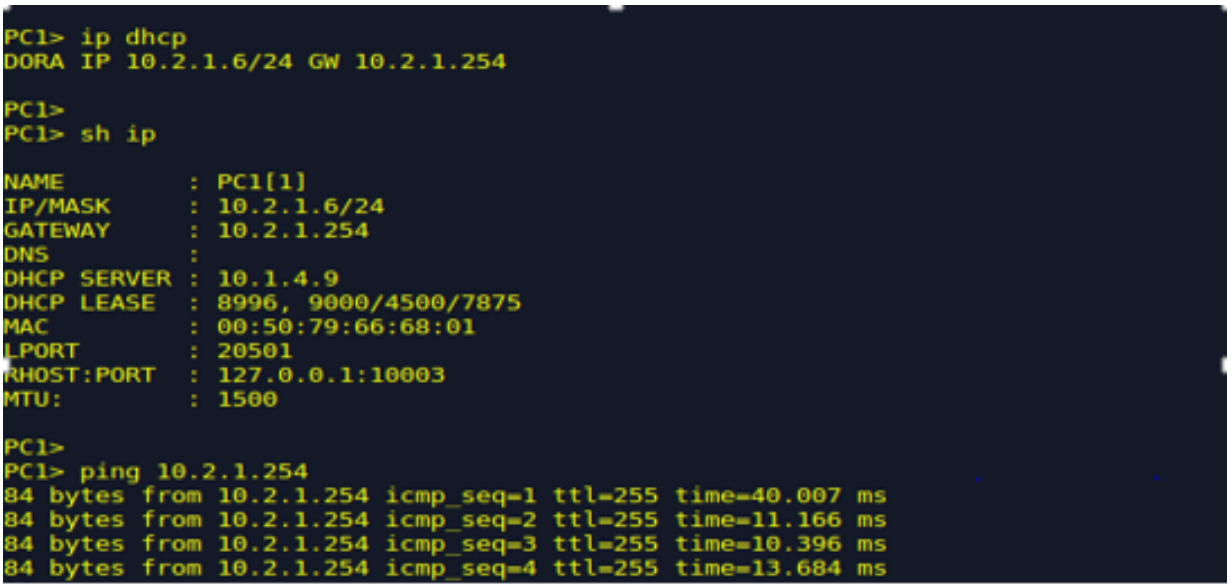
We can see that there are two DHCP pools defined in router R4, let's check the running configuration of DHCP in R4.

```
R4#sh run | sec dhcp
ip dhcp relay information option
ip dhcp relay information trust-all
ip dhcp excluded-address 10.2.1.0 10.2.1.5
ip dhcp excluded-address 10.2.2.0 10.2.2.5
ip dhcp pool SUBNET-10
 network 10.2.1.0 255.255.255.240
 default-router 10.2.1.254
 lease 0 2 30
ip dhcp pool SUBNET-20
 network 10.2.2.0 255.255.255.0
 default-router 10.2.2.254
 lease 0 2 30
```

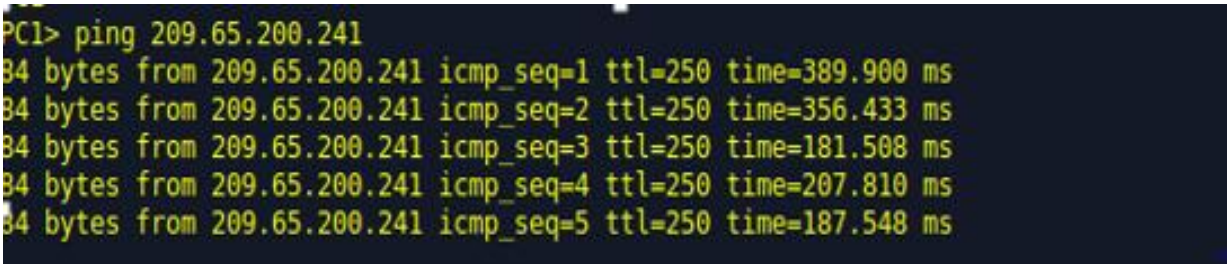
As we can see that the first DHCP pool named SUBNET-10 has subnet mask of 255.255.255.240 which is limiting the usable IPs in this subnet from 10.2.1.1 to 10.2.1.14. Let's correct the subnet mask for SUBNET-10

```
R4#
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#
R4(config)#ip dhcp pool SUBNET-10
R4(dhcp-config)#no network 10.2.1.0 255.255.255.240
R4(dhcp-config)#network 10.2.1.0 255.255.255.0
R4(dhcp-config)#
```

We can now see that PC1's IP address and default gateway are in the same subnet.



Let's ping the web server now, PC1 is able to successfully ping the web server.



The fault domain was router R4 which is the DHCP server, technology causing the issue was DHCP and the issue was resolved by changing the subnet mask of the DHCP Pool named SUBNET-10 from 255.255.255.240 to 255.255.255.0 which made PC1's IP address and its default gateway in the same subnet hence making PC1 to reach R4 which is the DHCP server.

Summary

In this chapter the design and setup of the implemented network is clearly explained. Eight different case studies were solved using the approach of Identify, Define, Diagnose and Resolution. The next chapter will discuss the results and recommendations from the study.

Chapter V

RESULTS, CONCLUSION, AND RECOMMENDATIONS

Introduction

Troubleshooting computer networks is an art, the more one spends time troubleshooting, the better one will become. Different people will have different methods and approaches to troubleshooting. What works for one person might not work for the other person. A seasoned professional will have vast knowledge and experience to call upon when needed whereas a beginner will have to do more research and may need help while trying to solve an issue. This chapter is devoted to explaining the results, recommendations and future work.

Results

How easy is it to resolve network issues without a structured approach?

How can uptime of networks improved?

Today's enterprise networks are large and complex. As the complexity increases resolution also becomes arduous. The technical skills one needs to have while trying to fix the issue is one aspect, however troubleshooting methodology and approach is another. After an issue is reported, the first step toward resolution is clearly defining the issue. When there is a clearly defined issue it helps with diagnosing the issue and a hypothesis about what is most likely causing the issue can be proposed. In some cases there may be number of likely causes and after identifying suspected underlying causes, one can define approaches to resolving the issue and

select what may be the best approach to solve the issue. The case studies implemented and solved in my research using methodical approach of "Following the traffic path" and troubleshooting approach of Identifying, Defining, Diagnosing and resolving clearly indicates that troubleshooting becomes easy when using a structured approach. In each of the case studies it can be noted that diagnosis has been done correctly and the issue has been resolved in the first attempt with the correct solution. This approach makes Network troubleshooting easy and simple which would help resolve network issues in a shorter span of time and eventually keep the networks up and running as much as possible.

Conclusion

Troubleshooting is one of the most challenging task that network professionals face. On top of that the need to find the root cause of a problem with a limited time under pressure is a tough job. Network usually don't fail during a favorable time. Networks may go down when businesses are running at their peak and the need to keep the network up and running is intense. After a problem has been identified and defined it is essential to isolate the true cause of the problem from irrelevant factors before trying to fix the problem. Troubleshooting is more of an art form than science. To be an effective and efficient troubleshooter one must approach the issue in an organized and methodical manner. It is important to note that the troubleshooter should look for the root cause of the issue rather than its symptoms. As an effective troubleshooter one needs to learn to quickly eliminate causes which are not relevant and not related to the issue. This allows the troubleshooter to concentrate on things that might help determine the root cause of the issue and resolve network issues faster. To achieve this, one must approach network issues with a systematic approach.

Future work

The future work should involve using IPv6 since IPv6 is the future of networking. IPv6 provides a much larger IP address space compared to IPv4, IPv6 is the future as far as IP addressing is concerned. Building a simulated environment using IPv6 addressing space and various networking technologies will be a great way to test how this methodology of Identifying ,Defining, Diagnosing and Troubleshooting works along with approaches like “Following the traffic path” , “Top-down”. “Bottom-up” approaches etc.

REFERENCES

[1] Kandula, S., Mahajan, R., Verkaik, P., Agarwal, S., Padhye, J., & Bahl, P. (2009). Detailed diagnosis in enterprise networks. Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication - SIGCOMM '09. doi:10.1145/1592568.1592597

[2] Savage, S., Wetherall, D., Karlin, A., & Anderson, T. (2000). Practical network support for IP traceback. ACM SIGCOMM Computer Communication Review SIGCOMM Comput. Commun. Rev., 30(4), 295-306. doi:10.1145/347057.347560

[3] Postel, J., "DoD standard Internet Protocol", RFC 760, DOI 10.17487/RFC0760, January 1980, <http://www.rfc-editor.org/info/rfc760>.

[4] White, K., "Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations", RFC 2925, DOI 10.17487/RFC2925, September 2000, http://www.rfc-editor.org/info/rfc2925

[5] Malkin, G., "Traceroute Using an IP Option", RFC 1393, DOI 10.17487/RFC1393, January 1993, <http://www.rfc-editor.org/info/rfc1393>.

[6] Lougheed, K. and Y. Rekhter, "Border Gateway Protocol (BGP)", RFC 1105, DOI 10.17487/RFC1105, June 1989, <http://www.rfc-editor.org/info/rfc1105>.

[7] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, DOI 10.17487/RFC1631, May 1994, <http://www.rfc-editor.org/info/rfc1631>.

[8] Waters, G., "The IPv4 Subnet Selection Option for DHCP", RFC 3011, DOI 10.17487/RFC3011, November 2000, <http://www.rfc-editor.org/info/rfc3011>.

[9] Chown, T., "Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks", RFC 4554, DOI 10.17487/RFC4554, June 2006, http://www.rfc-editor.org/info/rfc4554

[10] Psenak, P., Mirtorabi, S., Roy, A., Nguyen, L., and P. Pillay-Esnault, "Multi-Topology (MT) Routing in OSPF", RFC 4915, DOI 10.17487/RFC4915, June 2007, <http://www.rfc-editor.org/info/rfc4915>.

[11] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, DOI 10.17487/RFC7181, April 2014, <http://www.rfc-editor.org/info/rfc7181>

[12] O'Sullivan, T., "Telnet Protocol: A Proposed Document", RFC 158, DOI 10.17487/RFC0158, May 1971, <http://www.rfc-editor.org/info/rfc158>.

[13] Lacoste, R., & Wallace, K. (2015). CCNP routing and switching TSHOOT 300-135 official cert guide. Indianapolis IN: Pearson Education.

[14] Wallace, K. (2014). CCNP routing and switching ROUTE 300-101: Official cert guide. Indianapolis: Cisco press.

[15] Hucaby, D. (2014). CCNP routing and switching SWITCH 300-115: Official cert guide. Indianapolis: Cisco press.

[16] Ranjbar, A. (2014). Troubleshooting and Maintaining Cisco IP Networks (TSHOOT) Foundation Learning Guide: (ccnp Tshoot 300-135).

[17] Website Title: Wikipedia
URL:https://en.wikipedia.org/wiki/Graphical_Network_Simulator-3

[18] Website Title: www.cisco.com
URL:https://www.cisco.com/cgi-n/Support/OutputInterpreter/home.pl?locale=en

[19] Website Title: www.cisco.com
URL: https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

[20] Website Title: www.cisco.com
URL:http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1901.htm