



FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BITS 2343 COMPUTER NETWORK

Student ID Number	Full Name
B032010454	(S1G1) NURIN FARZANA BINTI MUJIBUR RAHMAN
B032010234	(S1G2) NURUL SYAFIQAH BINTI SAFIAN
B032020039	(S2G1) MUHAMMAD IZHAM BIN NORHAMADI
B032010222	(S1G1) KHAIRUL RIDZWAN BIN MUHAMAD ZARIN
B032010078	(S1G2) SYAFI BIN ABD RAZAK

Title	MINI PROJECT
Group	GROUP 8
Lecturer	TS. DR. NAZRULAZHAR BAHAMAN

Submission Date : 22 JANUARY 2022

TABLE OF CONTENTS

TITLE	PAGE
1.0 Introduction	1
2.0 Summary	2
3.0 Topology Diagram and Addressing Table	3
4.0 Routers and Switch Final Configuration	
4.1 Router Configuration	6
4.2 Switch Configuration	15
5.0 Requirement 1	18
6.0 Requirement 2	21
7.0 Requirement 3	23
8.0 Requirement 4	25
9.0 Requirement 5	27
10.0 Requirement 6	37
11.0 Requirement 7	41
12.0 Requirement 8	46
13.0 Conclusion	48

TABLE OF FIGURES

FIGURE	PAGE
3.0 Topology Diagram and Addressing Table	
Figure 3.1: The Topology Diagram with Corresponding Addresses	3
4.0 Routers and Switch Final Configuration	
Figure 4.01: Final HQ Router Configuration Part 1	6
Figure 4.02: Final HQ Router Configuration Part 2	7
Figure 4.03: Final HQ Router Configuration Part 3	8
Figure 4.04: Final BRCH1 Router Configuration Part 1	9
Figure 4.05: Final BRCH1 Router Configuration Part 2	10
Figure 4.06: Final BRCH1 Router Configuration Part 3	11
Figure 4.07: Final BRCH2 Router Configuration Part 1	12
Figure 4.08: Final BRCH2 Router Configuration Part 2	13
Figure 4.09: Final BRCH2 Router Configuration Part 3	14
Figure 4.10: Final S01 Switch Configuration	15
Figure 4.11: Final S1 Switch Configuration	16
Figure 4.12: Final S2 Switch Configuration	17
5.0 Requirement 1	
Figure 5.1: Evidence Showing Orange VLAN has Statically Assigned IP Addresses According to the Addressing Table	19
Figure 5.2: Evidence Showing All Other Networks Have Dynamically Assigned IP Addresses Through DHCP Server According to the Addressing Table	20
6.0 Requirement 2	
Figure 6.1: Evidence that VLANs Have Been Configured (S01 and S1)	21
Figure 6.2: Evidence that VLANs Have Been Configured (S2)	22
7.0 Requirement 3	
Figure 7.1: Evidence that Switch Ports have Been Assigned (S01 and S1)	23
Figure 7.2: Evidence that Switch Ports have Been Assigned (S2)	23

Figure 7.3: Evidence that Trunk Ports have Been Configured (S01 and S1)	24
Figure 7.4: Evidence that Trunk Ports have Been Configured (S2)	25
8.0 Requirement 4	
Figure 8.1: Evidence that HQ Router has been Configured According to The Addressing Table	26
9.0 Requirement 5	
Figure 9.01: Evidence that Routers Have Been Configured with RIPv2 Protocol (BRCH1 and BRCH2)	27
Figure 9.02: Evidence that Routers Have Been Configured with RIPv2 Protocol (HQ)	28
Figure 9.03: Evidence that Routers Have Been Configured with ACL	29
Figure 9.04: Using Ping to Verify ACL From Purple Network Host	30
Figure 9.05: Using Ping to Verify ACL From Green Network Host	31
Figure 9.06: Using Tracert from Green Host	32
Figure 9.07: Using Tracert from Purple Host	33
Figure 9.08: Verifying Access-List Configurations at HQ Router	34
Figure 9.09: Using Ping to Verify Access-List Configurations from Blue Host	35
Figure 9.10: Using Ping to Verify Access-List Configurations from Red Host 26	36
10.0 Requirement 6	
Figure 10.1: Red DHCP Server Configuration	37
Figure 10.2: Blue DHCP Server Configuration	38
Figure 10.3: Purple DHCP Server Configuration	38
Figure 10.4: BRCH2 Router as a DHCP Relay Agent	39
Figure 10.5: Evidence of IP Address Assignment from DHCP Server G1	39
Figure 10.5: Evidence of IP Address Assignment from DHCP Server M8	40
11.0 Requirement 7	
Figure 11.1: DNS Server Configuration	41
Figure 11.2: Web Server Configuration	41

Figure 11.3: Mail Server Configuration	42
Figure 11.4: Mail Configuration for G1	43
Figure 11.5: Mail Configuration for M8	43
Figure 11.6: Composing Email from G1	44
Figure 11.7: Sent Email from G1	44
Figure 11.8: Mail Received by J1	45
Figure 11.9: Mail Received by J1 Verified	45
12.0 Requirement 8	
Figure 12.1: Adding Image Files	46
Figure 12.2: Editing HTML Code	46
Figure 12.3: Searching for Webpage from P3	47
Figure 12.4: Group Member Images from Web Page from G1	47

TABLE OF TABLES

TITLE	PAGE
3.0 Topology Diagram and Addressing Table	
Table 3.1: Addressing Table	4
5.0 Requirement 1	
Table 5.1: IP Addressing Scheme	18
6.0 Requirement 2	
Table 6.1: Initial Port Assignments (Switches 01, 1 and 2)	21

1.0 Introduction

This mini project requires a simulation network to be developed according to the specified requirements. To develop and test the network, the software Packet Tracer was used. A website called draw.net which provides free diagram software online was used to draw the complete network schematic diagram. In the following chapters, a summary will be given to address the successes and failures of the mini project and the topology diagram and addressing table will also be discussed. Furthermore, the final router and switch configurations as well as proof that each requirement was met will be provided.

2.0 Summary

The aim for this mini project is to develop a simulated network with many different configurations. These configurations include access control lists, VLANs and dynamically assigned Internet Protocol (IP) addresses through the specified DHCP servers. Although there were many errors made throughout the development of the network, all requirements were met successfully.

All devices were assigned with IP address blocks as specified, VLANs were configured and switch ports were assigned to those VLANs. Next, routers were configured for InterVLAN routing and with suitable routing protocol and Access Control List (ACL). Moreover, DHCP servers were configured for the network. Finally, Web Server, DNS server and the Mail Server were also configured in addition to customising the homepage.

3.0 Topology Diagram and Addressing Table

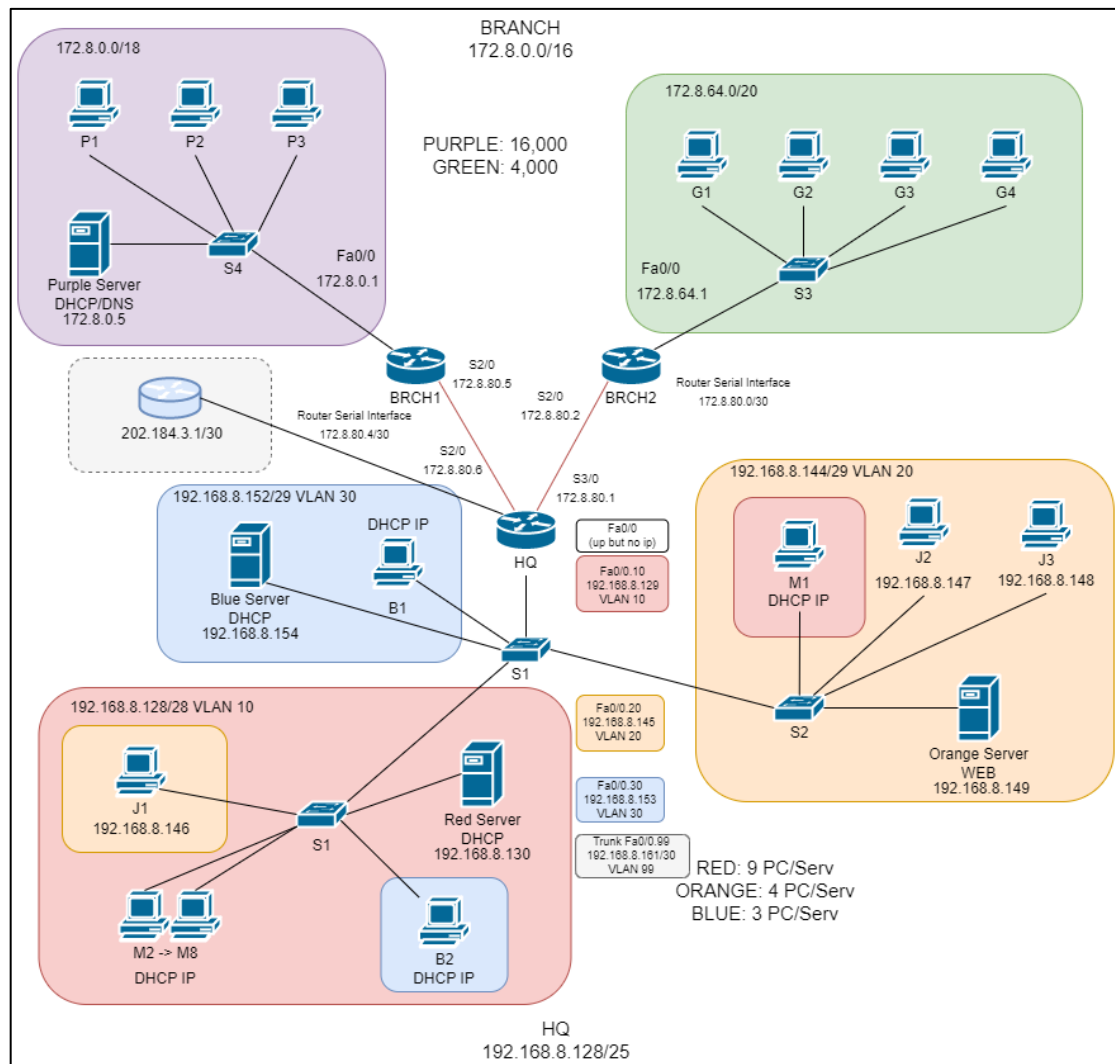


Figure 3.1: The Topology Diagram with Corresponding Addresses

Device	Interface	IP Address	Subnet Mask	Default
BRCH1	Fa0/0	172.8.0.1	255.255.192.0	N/A
	S2/0	172.8.80.5	255.255.255.252	N/A
BRCH2	Fa0/0	172.8.64.1	255.255.240.0	N/A
	S2/0	172.8.80.2	255.255.255.252	N/A
HQ	Fa0/0	N/A	N/A	N/A
	Fa0/0.10	192.168.8.129	255.255.255.240	N/A
	Fa0/0.20	192.168.8.145	255.255.255.248	N/A
	Fa0/0.30	192.168.8.153	255.255.255.248	N/A
	Fa0/0.99	192.168.8.161	255.255.255.252	N/A
	S2/0	172.8.80.1	255.255.255.252	N/A
	S3/0	172.8.80.6	255.255.255.252	N/A
Red Server	Fa0/1	192.168.8.130	255.255.255.240	192.168.8.129
M1	Fa0/2	DHCP Assigned	255.255.255.240	192.168.8.129
M2	Fa0/3	DHCP Assigned	255.255.255.240	192.168.8.129
M3	Fa0/4	DHCP Assigned	255.255.255.240	192.168.8.129
M4	Fa0/5	DHCP Assigned	255.255.255.240	192.168.8.129
M5	Fa0/6	DHCP Assigned	255.255.255.240	192.168.8.129
M6	Fa0/7	DHCP Assigned	255.255.255.240	192.168.8.129
M7	Fa0/8	DHCP Assigned	255.255.255.240	192.168.8.129
M8	Fa0/9	DHCP Assigned	255.255.255.240	192.168.8.129
Orange Server	Fa0/11	192.168.8.149	255.255.255.248	192.168.8.145
J1	Fa0/12	192.168.8.146	255.255.255.248	192.168.8.145
J2	Fa0/13	192.168.8.147	255.255.255.248	192.168.8.145
J3	Fa0/14	192.168.8.148	255.255.255.248	192.168.8.145
Blue Server	Fa0/16	192.168.8.154	255.255.255.248	192.168.8.153
B1	Fa0/17	DHCP Assigned	255.255.255.248	192.168.8.153
B2	Fa0/18	DHCP Assigned	255.255.255.248	192.168.8.153

Purple Server	Fa0/2	172.8.0.5	255.255.192.0	172.8.0.1
P1	Fa0/3	DHCP Assigned	255.255.192.0	172.8.0.1
P2	Fa0/4	DHCP Assigned	255.255.192.0	172.8.0.1
P3	Fa0/5	DHCP Assigned	255.255.192.0	172.8.0.1
G1	Fa0/2	DHCP Assigned	255.255.240.0	172.8.64.1
G2	Fa0/3	DHCP Assigned	255.255.240.0	172.8.64.1
G3	Fa0/4	DHCP Assigned	255.255.240.0	172.8.64.1
G4	Fa0/5	DHCP Assigned	255.255.240.0	172.8.64.1
Loopback	Loopback0	202.184.3.1	255.255. 255.252	N/A

Table 3.1: Addressing Table



The screenshot shows a window titled 'HQ' with three tabs: 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The configuration text is as follows:

```
interface FastEthernet0/0
  no ip address
  duplex auto
  speed auto
  !
interface FastEthernet0/0.10
  encapsulation dot1Q 10
  ip address 192.168.8.129 255.255.255.240
  ip access-group EXTND-3 in
  !
interface FastEthernet0/0.20
  encapsulation dot1Q 20
  ip address 192.168.8.145 255.255.255.248
  !
interface FastEthernet0/0.30
  encapsulation dot1Q 30
  ip address 192.168.8.153 255.255.255.248
  ip access-group EXTND-4 in
  !
interface FastEthernet0/0.99
  encapsulation dot1Q 99 native
  ip address 192.168.8.161 255.255.255.252
  !
interface FastEthernet1/0
  no ip address
  duplex auto
  speed auto
  shutdown
  !
interface Serial2/0
  ip address 172.8.80.6 255.255.255.252
  clock rate 64000
  !
interface Serial3/0
  ip address 172.8.80.1 255.255.255.252
  clock rate 64000
  !
interface FastEthernet4/0
  no ip address
  shutdown
  !
interface FastEthernet5/0
  no ip address
  shutdown
  !
interface Serial6/0
  no ip address
  clock rate 2000000
  shutdown
  !
```

At the bottom right of the window, there are two buttons: 'Copy' and 'Paste'.

Figure 4.02: Final HQ Router Configuration Part 2

```
!
router rip
  version 2
  network 172.8.0.0
  network 192.168.8.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended EXTND-3
  permit ip 192.168.8.128 0.0.0.15 host 192.168.8.149
  permit ip 192.168.8.128 0.0.0.15 192.168.8.152 0.0.0.7
ip access-list extended EXTND-4
  permit ip 192.168.8.152 0.0.0.7 host 192.168.8.149
  permit ip 192.168.8.152 0.0.0.7 192.168.8.128 0.0.0.15
!
no cdp run
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
  login
!
!
!
end
```

Copy Paste

Figure 4.03: Final HQ Router Configuration Part 3

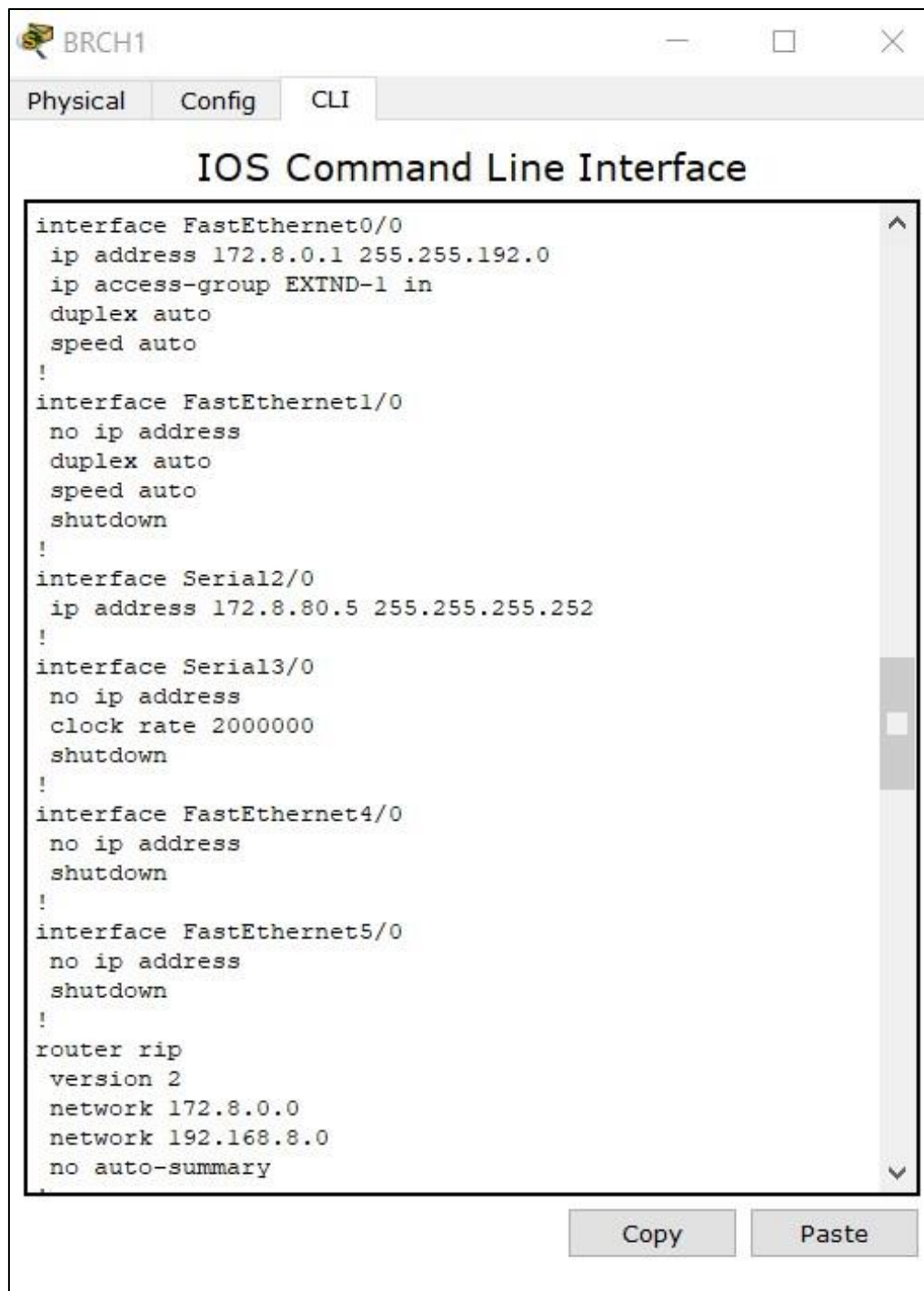


Figure 4.05: Final BRCH1 Router Configuration Part 2

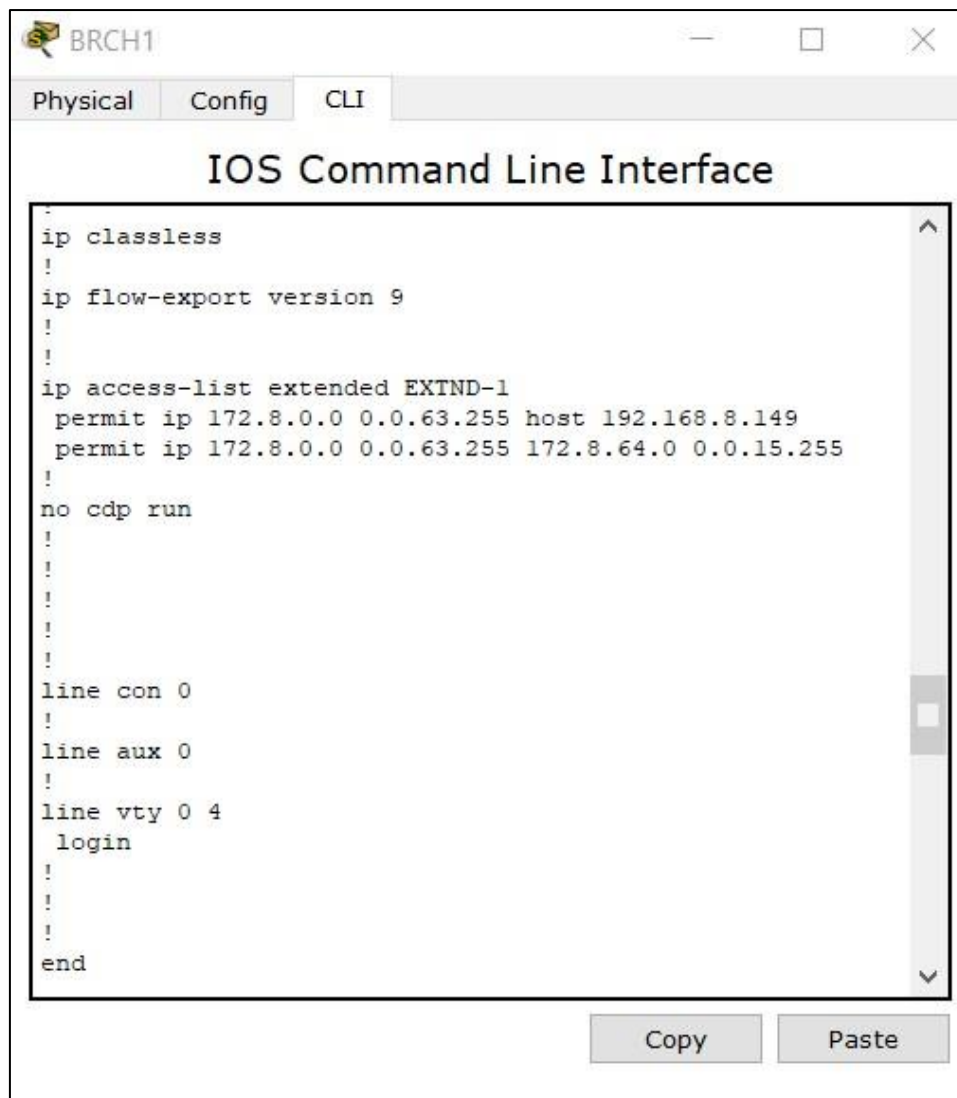


Figure 4.06: Final BRCH1 Router Configuration Part 3



Figure 4.07: Final BRCH2 Router Configuration Part 1



Figure 4.08: Final BRCH2 Router Configuration Part 2

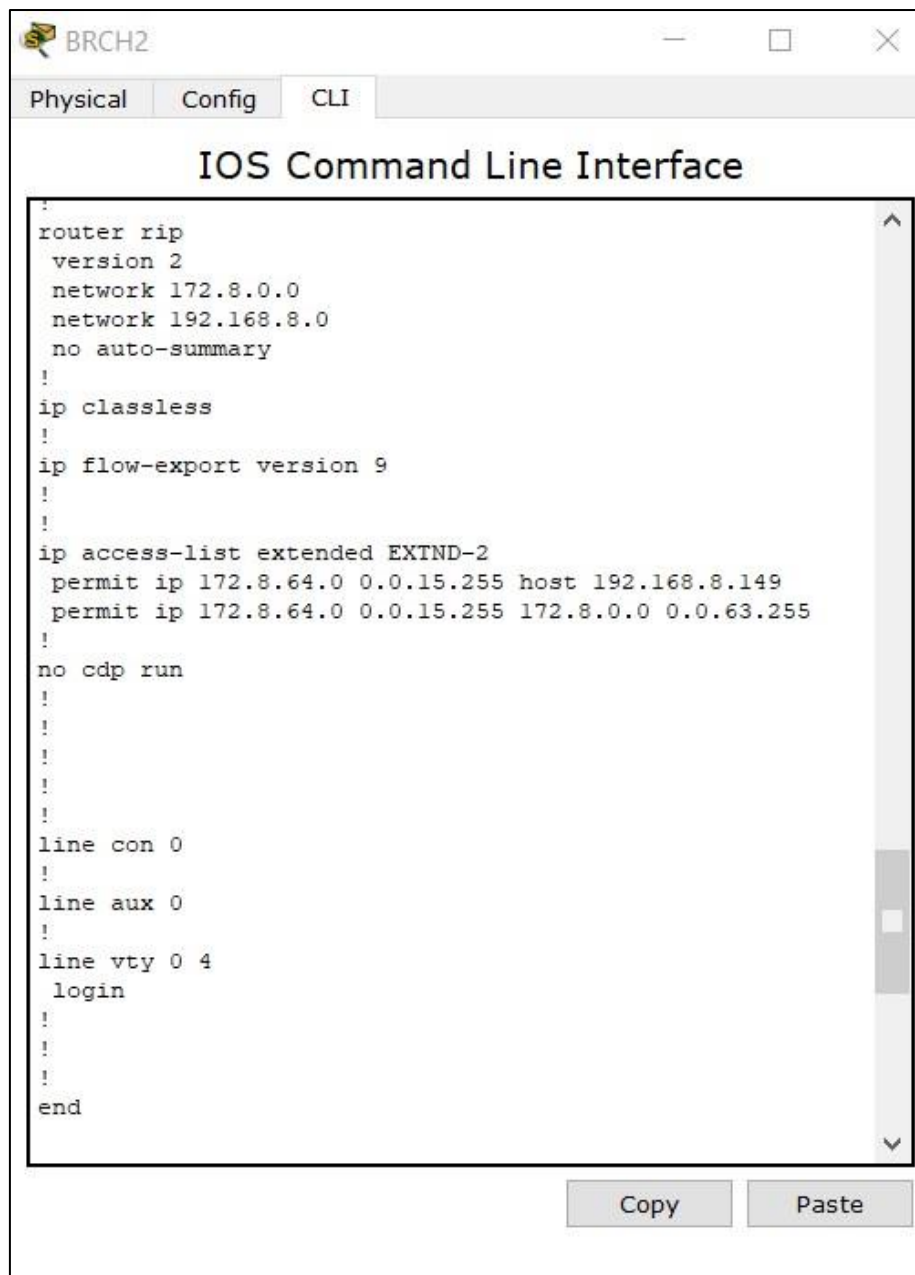
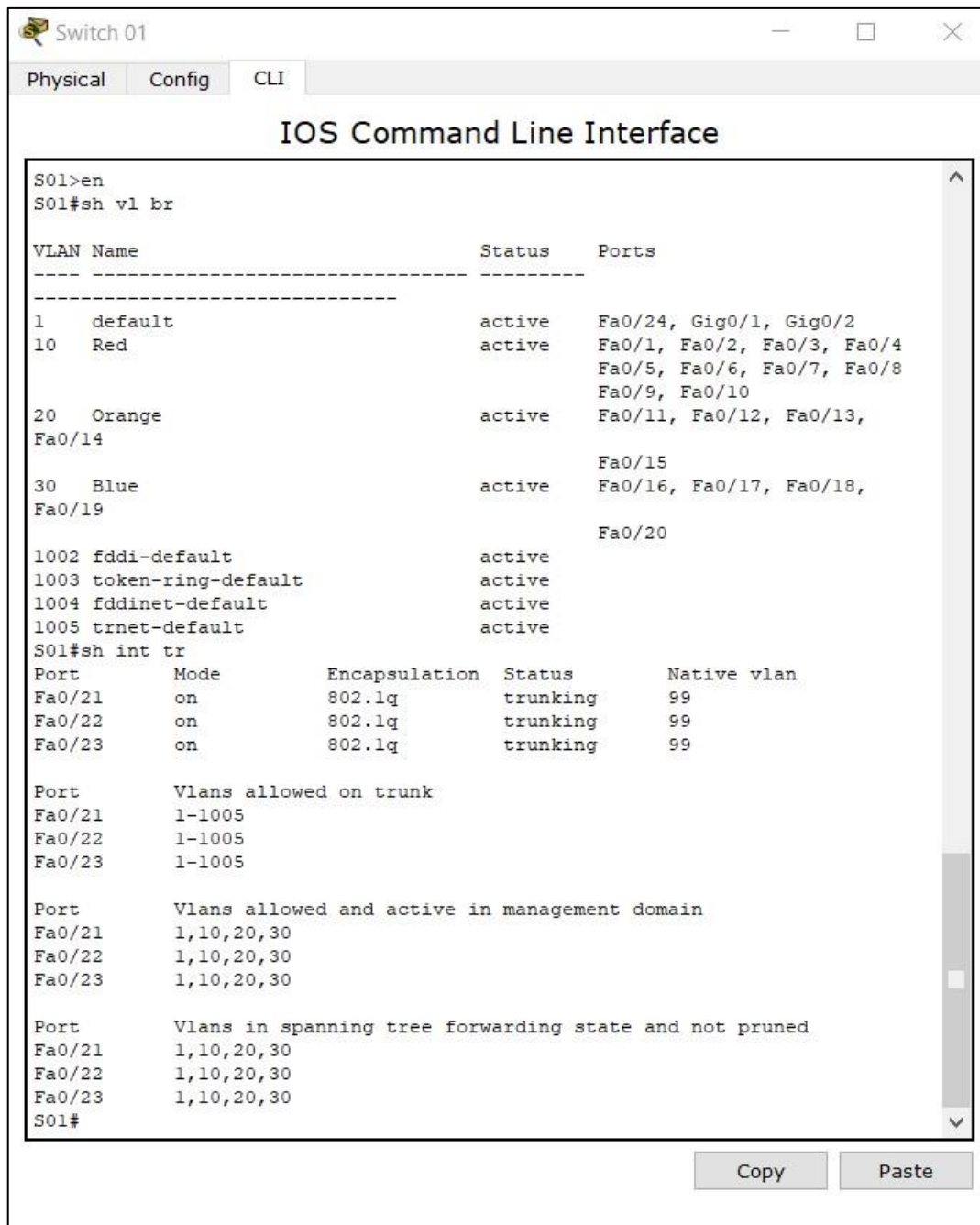


Figure 4.09: Final BRCH2 Router Configuration Part 3

4.2 Switch Configuration



The screenshot shows the CLI of a switch named S01. The 'Config' tab is active. The user has entered 'en' to enter privileged mode and 'sh vl br' to display the VLAN configuration. The output shows four active VLANs: 1 (default), 10 (Red), 20 (Orange), and 30 (Blue). Each VLAN is associated with specific ports. Additionally, the user has entered 'sh int tr' to display trunk configuration for ports Fa0/21, Fa0/22, and Fa0/23. The output shows these ports are in trunking mode with encapsulation 802.1q and native VLAN 99. It also lists the VLANs allowed on the trunk (1-1005) and the VLANs allowed and active in the management domain (1, 10, 20, 30).

```
S01>en
S01#sh vl br

VLAN Name                Status    Ports
-----
1    default                active    Fa0/24, Gig0/1, Gig0/2
10   Red                    active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
      Fa0/5, Fa0/6, Fa0/7, Fa0/8
      Fa0/9, Fa0/10
20   Orange                 active    Fa0/11, Fa0/12, Fa0/13,
      Fa0/14
      Fa0/15
30   Blue                   active    Fa0/16, Fa0/17, Fa0/18,
      Fa0/19
      Fa0/20
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active

S01#sh int tr

Port      Mode      Encapsulation  Status      Native vlan
Fa0/21    on        802.1q         trunking    99
Fa0/22    on        802.1q         trunking    99
Fa0/23    on        802.1q         trunking    99

Port      Vlans allowed on trunk
Fa0/21    1-1005
Fa0/22    1-1005
Fa0/23    1-1005

Port      Vlans allowed and active in management domain
Fa0/21    1,10,20,30
Fa0/22    1,10,20,30
Fa0/23    1,10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/21    1,10,20,30
Fa0/22    1,10,20,30
Fa0/23    1,10,20,30
S01#
```

Figure 4.10: Final S01 Switch Configuration

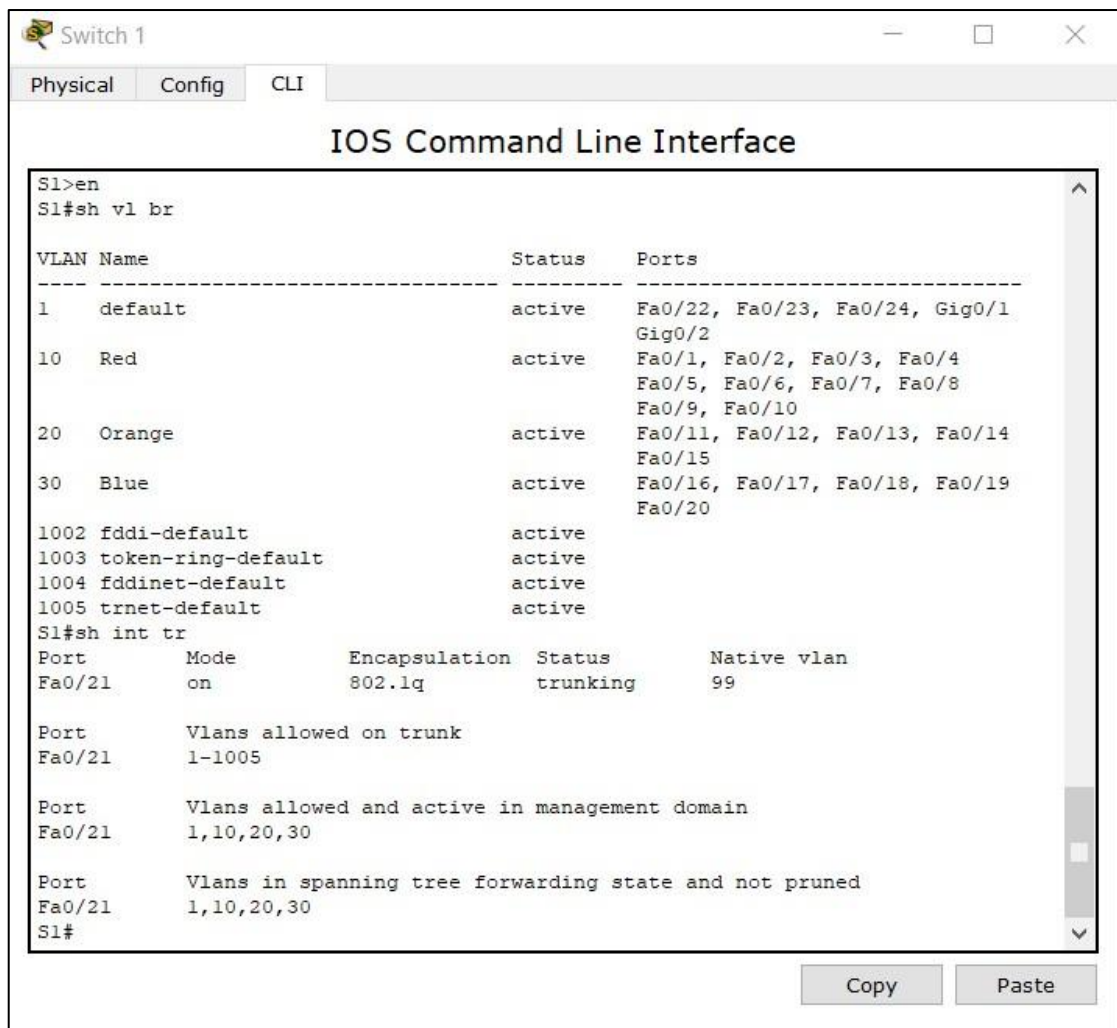


Figure 4.11: Final S1 Switch Configuration

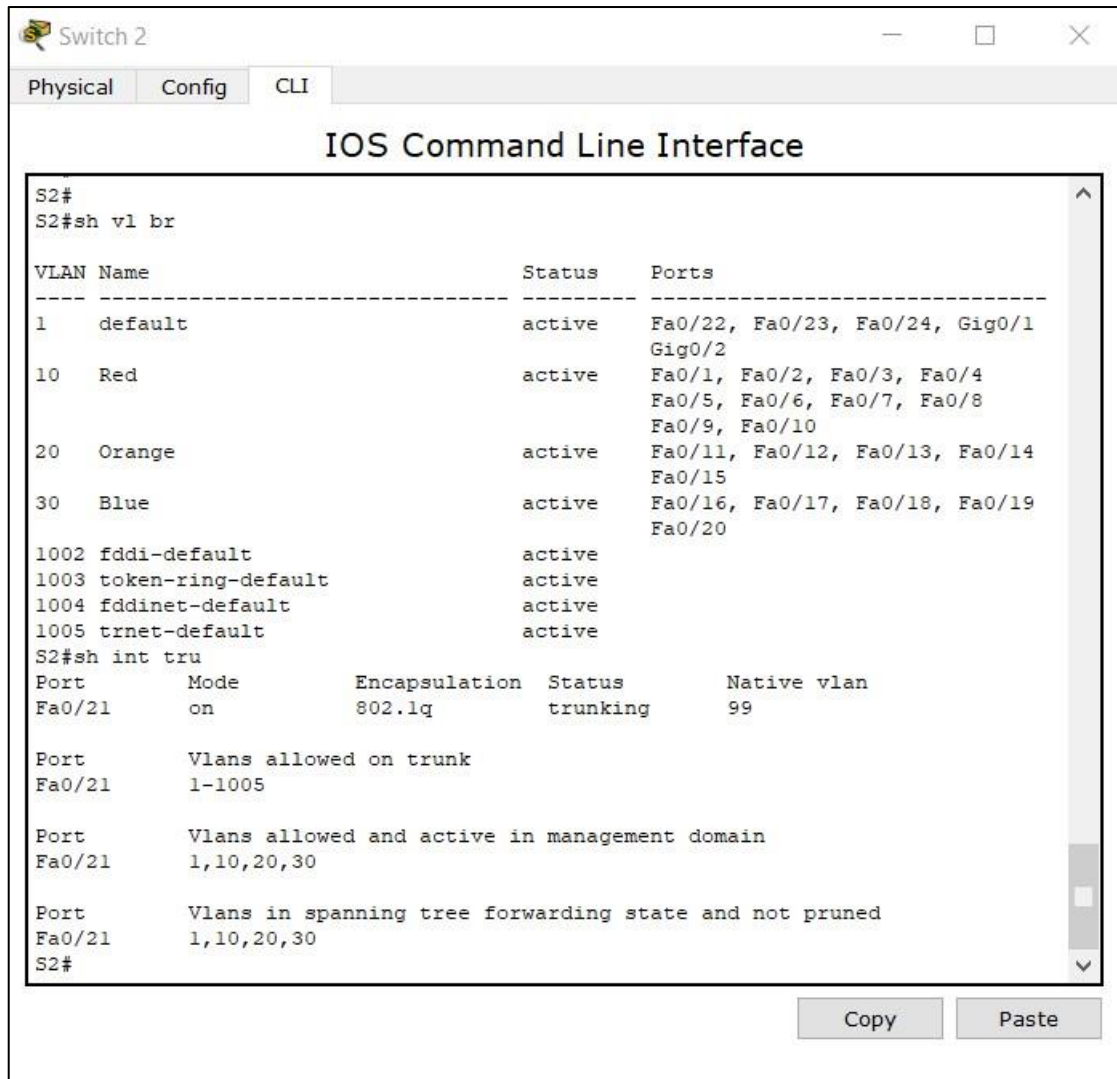


Figure 4.12: Final S2 Switch Configuration

5.0 Requirement 1

For this mini project, the network addresses were provided but the x value had to be replaced with our group number. The network addresses provided were 192.168.X.128/25 for the HQ networks and 172.X.0.0/16 for the branches network. As we are group 8, all x values were replaced with 8. Thus, for our mini project the HQ and branches addresses are 192.168.8.128/25 and 172.X.0.0/16 respectively.

For the branches network, there are four subnetworks, two of which are indicated by the purple and green coloured backgrounds. The other two subnetworks are the serial interfaces between the HQ router and the BRCH1 and BRCH2 routers. The purple network requires 16000 addresses whereas the green needs 4000 and the serial connections require 4 addresses. Thus, using VLSM we assign the subnetworks addresses from the 172.8.0.0/16 address block.

For the HQ network, there are 3 VLANs which require addresses. The Red, Orange and Blue VLAN have 9, 4 and 3 hosts which means they require 12, 7 and 6 addresses each respectively when including the network, broadcast and gateway address. Thus, using VLSM we assign the subnetworks addresses from the 192.168.8.128/25 address block. The following table shows IP addressing scheme for both the branch network and the HQ network.

Network	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
Purple	172.8.0.0/18	172.8.0.1	172.8.63.254	172.8.63.255
Green	172.8.64.0/20	172.8.64.1	172.8.79.254	172.8.79.255
BRCH1_HQ	172.8.80.0/30	172.8.80.1	172.8.80.2	172.8.80.3
BRCH2_HQ	172.8.80.4/30	172.8.80.5	172.8.80.6	172.8.80.7
Red VLAN	192.168.8.128/28	192.168.8.129	192.168.8.142	192.168.8.143
Orange VLAN	192.168.8.144/29	192.168.8.145	192.168.8.150	192.168.8.151
Blue VLAN	192.168.8.152/29	192.168.8.153	192.168.8.158	192.168.8.159

Table 5.1: IP Addressing Scheme

Once the IP addressing scheme has been designed and calculated, the IP addressing table was then filled out accordingly. Table 3.1 depicts the final addressing table, which also includes the ISP address which is loopback interface at the HQ router. The IP addressing table takes into account that requirement 6 specifies that only the Orange VLAN has statically assigned IP addresses whereas all other hosts will have their IP addresses dynamically assigned using a DHCP server.

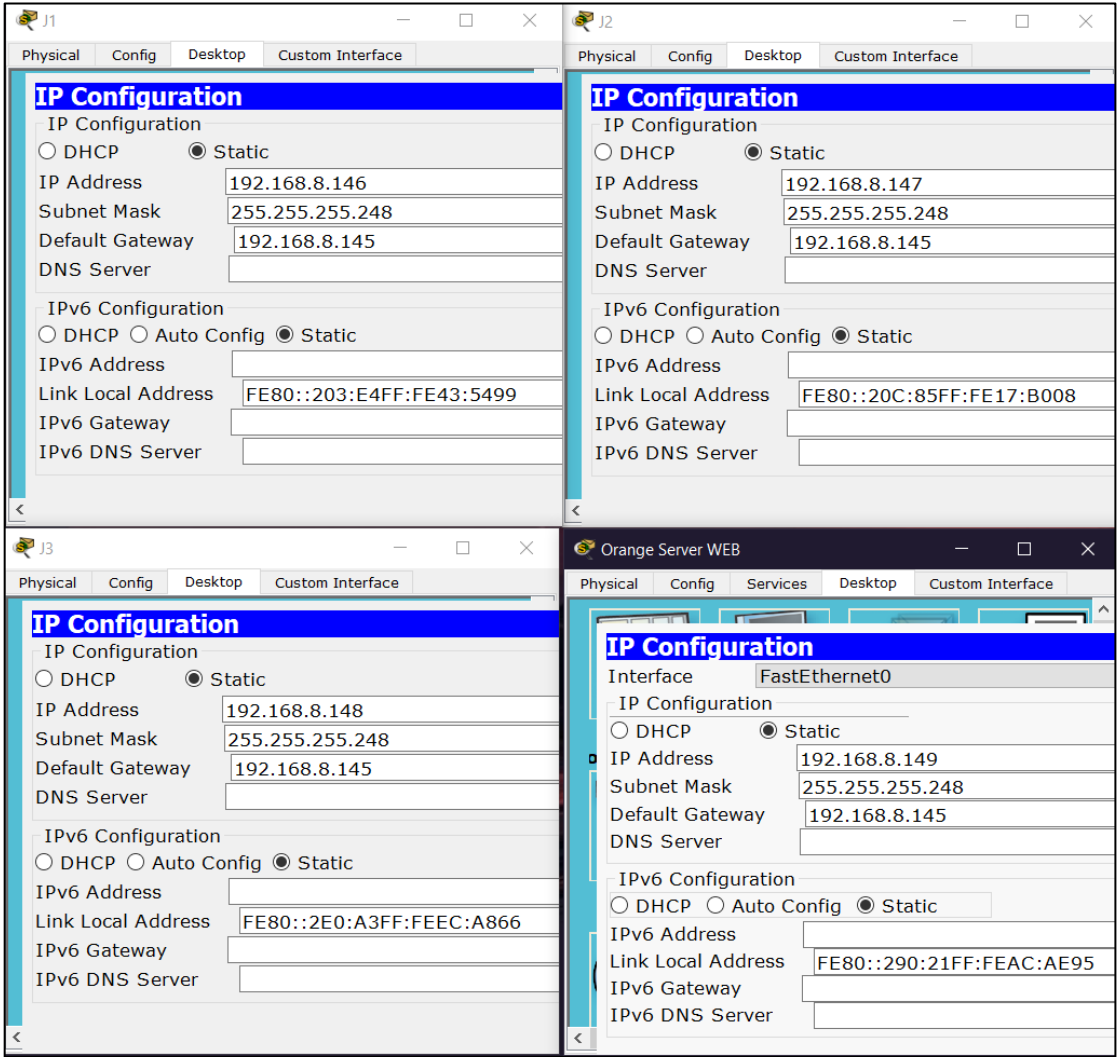


Figure 5.1: Evidence Showing Orange VLAN has Statically Assigned IP Addresses According to the Addressing Table

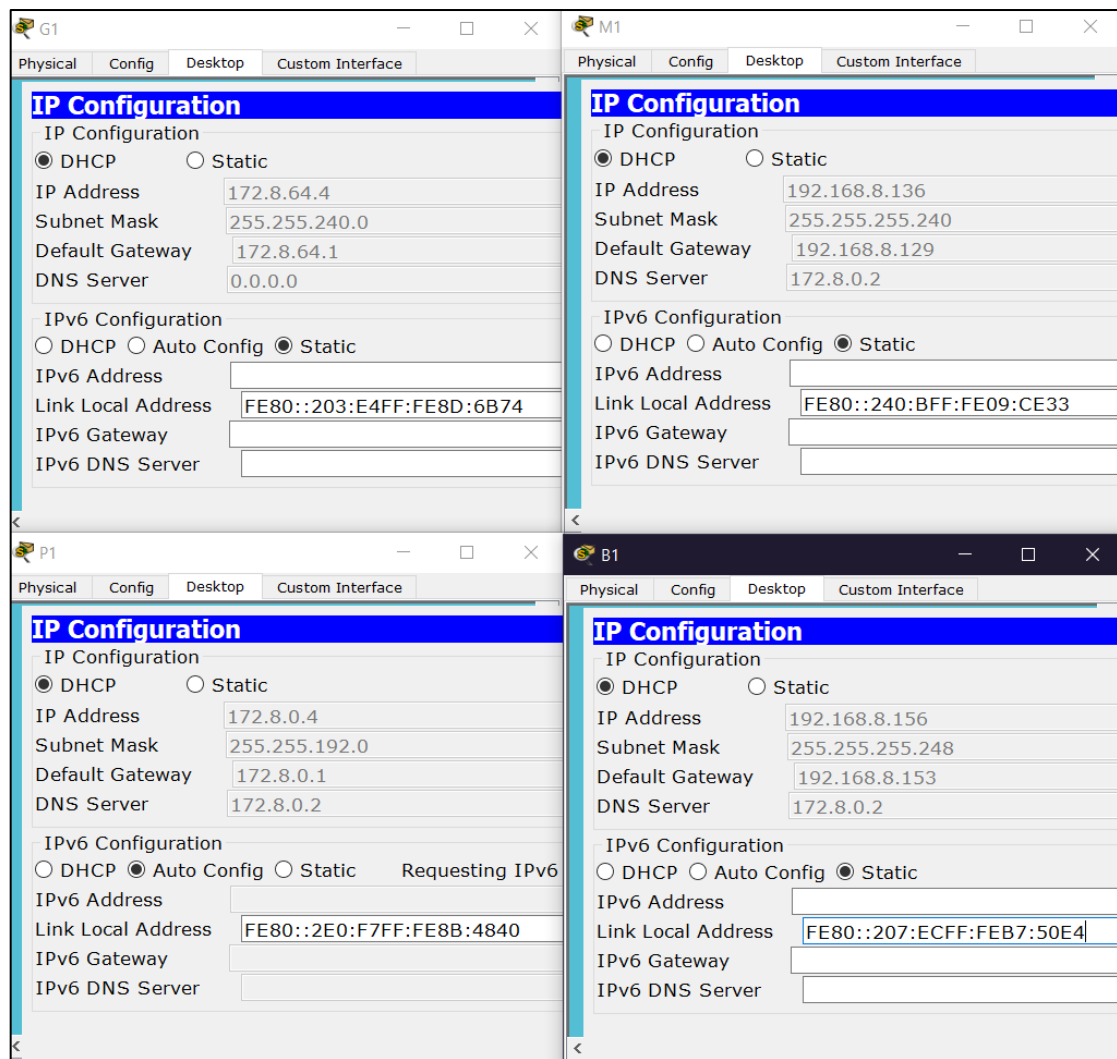


Figure 5.2: Evidence Showing All Other Networks Have Dynamically Assigned IP Addresses Through DHCP Server According to the Addressing Table

6.0 Requirement 2

Requirement 2 states that the Red, Orange and Blue VLANs are to be configure. We gave the VLAN IDs 10, 20, 30 and 99 to the Red, Orange, Blue and Native VLANs respectively. As requirement 3 requires the switch ports be assigned to the VLANs, planning is required when connecting the devices to the corresponding ports on the switch. Below is a table of the initial port assignments for switches S01, S1 and S2. Switches 2960-4TT were used for the network.

Ports	Assignment	Network
Fa0/1-10	VLAN 10 - Red	192.168.8.128/28
Fa0/11-15	VLAN 20 - Orange	192.168.8.144/29
Fa0/16-20	VLAN 30 - Blue	192.168.8.152/29
Fa0/21-23	802.1q Trunks (Native VLAN 99)	192.168.8.160/30

Table 6.1: Initial Port Assignments (Switches 01, 1 and 2)

The command **vlan** *vlan-id* in global configuration mode was used to add a vlan and the command **name** *vlan-name* was used to name the VLANs. Using the command **show vlan brief**, we can identify that the vlans for every host have been configured. The **show vlan brief** command can be shortened to **sh vl br**, which is the command used in the figures below.

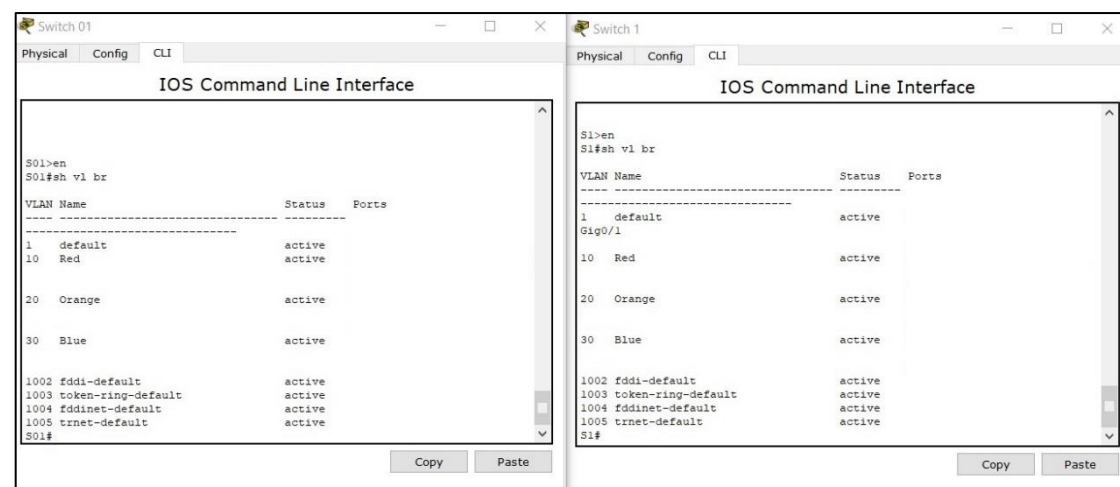


Figure 6.1: Evidence that VLANs Have Been Configured (S01 and S1)

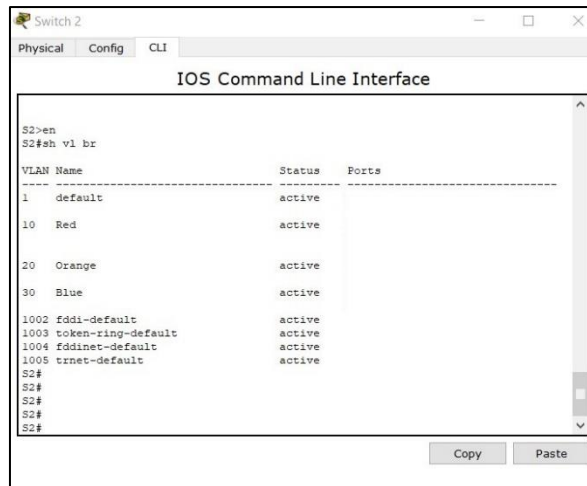
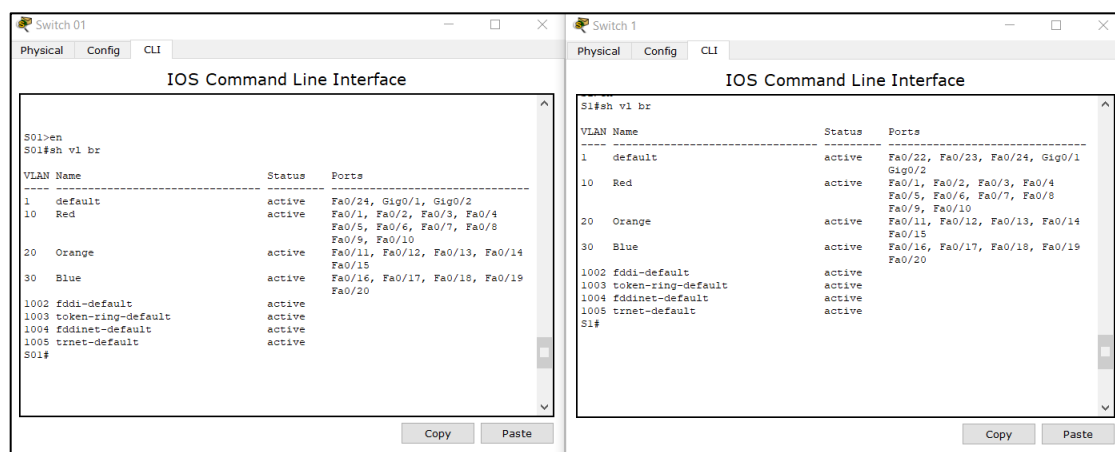


Figure 6.2: Evidence that VLANs Have Been Configured (S2)

As mentioned earlier, the Orange hosts have statically assigned IP addresses. Figure 5.1 is proof that they were configured according to the addressing table with the correct IP address, subnet mask and gateway address. All hosts were connected to the corresponding switches according to the initial port assignments as shown in Table 6.1.

7.0 Requirement 3

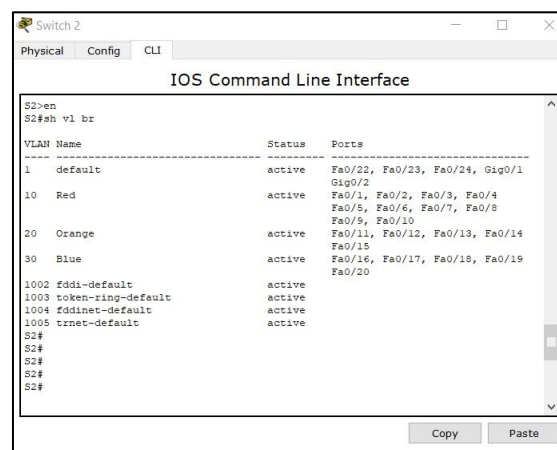
To assign switch ports to the VLANs on S01, S1 and S2, we use the **switchport access vlan *vlan-id*** command. Table 6.1 shows the initial port assignments for switches in the HQ network where we have assigned a range for each assignment. Thus, we used the **interface range** command to simplify the task. After assigning the appropriate ports to each VLAN and connecting the hosts accordingly, we use the **sh vl br** command to verify that they have been assigned appropriately.



The figure shows two side-by-side screenshots of network switch CLI interfaces. The left window is titled 'Switch 01' and the right window is titled 'Switch 1'. Both windows show the 'IOS Command Line Interface' with the 'sh vl br' command output. The output displays a table of VLANs with their names, statuses, and assigned ports.

VLAN Name	Status	Ports
1 default	active	Fa0/24, Gig0/1, Gig0/2
10 Red	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10
20 Orange	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15
30 Blue	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Figure 7.1: Evidence that Switch Ports have Been Assigned (S01 and S1)



The figure shows a screenshot of a network switch CLI interface titled 'Switch 2'. The window displays the 'IOS Command Line Interface' with the 'sh vl br' command output. The output displays a table of VLANs with their names, statuses, and assigned ports.

VLAN Name	Status	Ports
1 default	active	Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2
10 Red	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10
20 Orange	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15
30 Blue	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Figure 7.2: Evidence that Switch Ports have Been Assigned (S2)

Next, to allow the VLANs to exchange information or packets, we need to configure the trunk ports. We are using 802.1Q encapsulation with VLAN 99 as the Native VLAN. Again, we use the **interface range** command in the global configuration mode to enable us to simplify the configuration on the trunk ports. As shown in Table 6.1, the interface range used is Fa0/21-23 for the trunk ports. Thus, for S01, trunk ports were configured for all three of the assigned ports. For S1 and S2, only Fa0/21 was configured for the trunk port. To verify the configuration of trunk ports, we use the command **show interface trunk** or we can use the shortened version which is **sh int tr**.

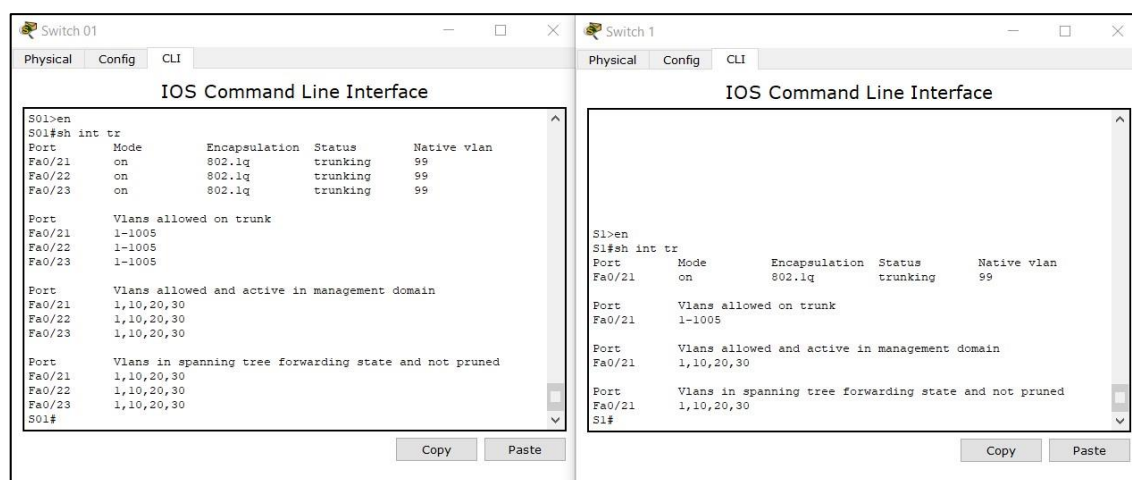


Figure 7.3: Evidence that Trunk Ports have Been Configured (S01 and S1)



Figure 7.4: Evidence that Trunk Ports have Been Configured (S2)

8.0 Requirement 4

Connectivity between VLANs requires routing at the network layer using layer three devices such as a router. We use the approach where we create Fast Ethernet connections between the router and the distribution layer switch and configure the connections as dot1q trunks. This will allow inter-VLAN traffic to be carried to and from the routing device on a single trunk. To do this, we need the router to be configured with multiple addresses by creating virtual interfaces (called subinterfaces) on one of the router Fast Ethernet ports and configuring them to be dot1q aware. We are configuring the interface Fa0/0 as the trunk port from the router.

First, we need to enter the interface for Fa0/0 using the command **int fa0/0** from the global configuration mode. For configuring the trunk for the VLAN 10 (Red VLAN), we enter the subinterface using the command **int fa0/10**. Next, we use the command **encapsulation dot1q 10** to establish trunking encapsulation and associate a VLAN with the subinterface followed by the command **ip add 192.168.8.129 255.255.255.248** to assign an IP address from the VLAN 10 to this interface. We repeat the steps for VLANs 20, 30 and 99 replacing the VLAN ID 10 accordingly. Once the configuration for the trunk port at the HQ router is done, we assign the IP addresses for the serial connections. For verification that the ip addresses have been configured correctly, we use the command **sh ip int br** which is the shortened version of the command **show ip interface brief**.

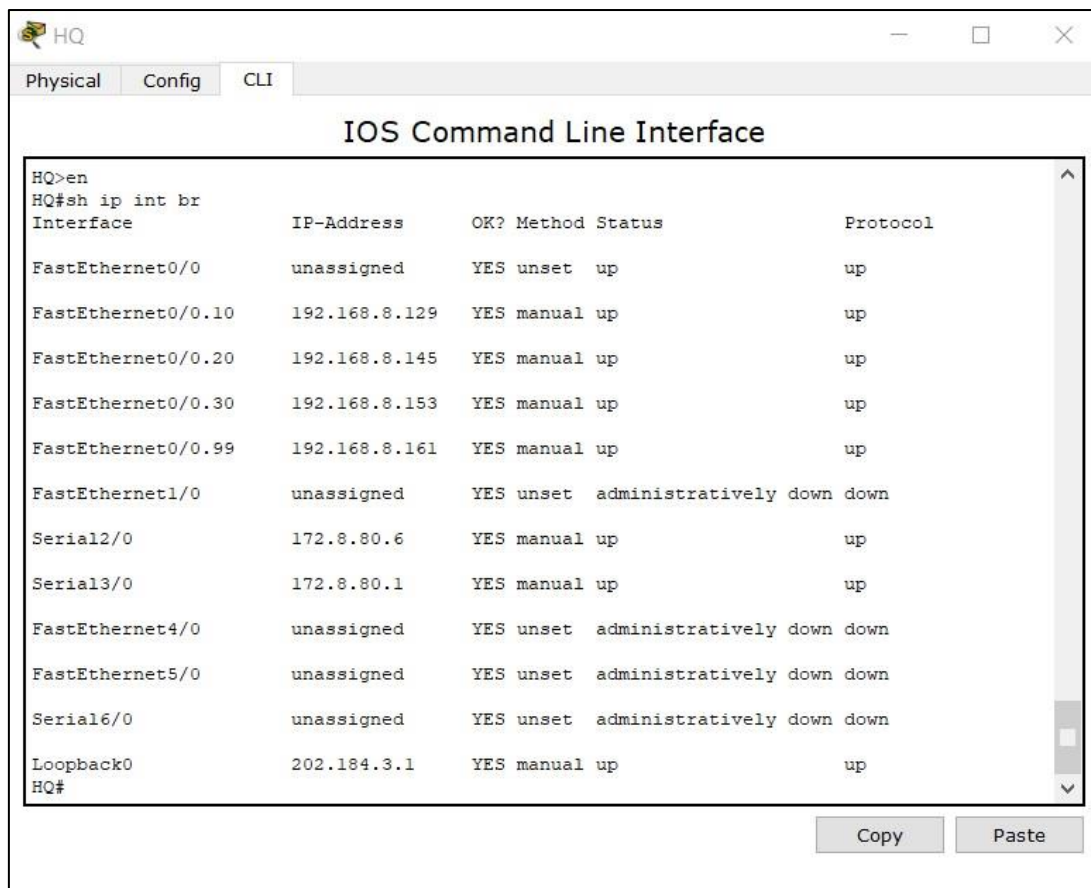


Figure 8.1: Evidence that HQ Router has been Configured According to The Addressing Table

9.0 Requirement 5

RIPv2 is a Distance Vector Routing Protocol that uses hop counts as its metric. The maximum number of hops is set to be 15 and any router farther than 15 hops away is considered unreachable. RIPv2 improves on its predecessor RIPv1 by sending subnet mask with the updates. This feature is the reason the RIPv2 is considered a classless routing protocol. For our network, we need RIPv2 as we subnet the network addresses that were provided.

To enable RIPv2, we have to use the command **router rip** followed by the command **version 2**. Both of these commands can be shortened to **rou rip** and **ver 2** respectively. After the command **version 2**, we need to use the command **network network-address** for each network the router is connected to followed by **no auto-sum** to ensure the addresses are not summarised and no subnet will be overlooked. To verify that router rip has been enabled, we can use the command **sh runn** which is the shortened versioned of the command **show running-configuration**.

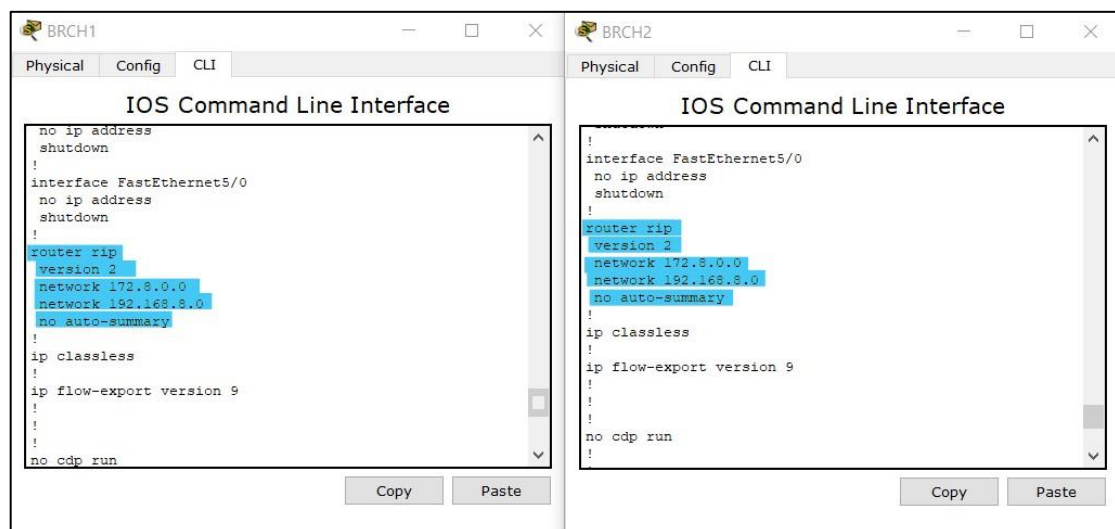


Figure 9.01: Evidence that Routers Have Been Configured with RIPv2 Protocol (BRCH1 and BRCH2)



Figure 9.02: Evidence that Routers Have Been Configured with RIPv2 Protocol (HQ)

Next, the requirements state that the purple and green networks should only be able to communicate between them and to the Orange Web Server. To do this we are going to apply an extended Access Control List (ACL). Extended ACL can deny or permit based on source and destination address not just destination address like standard ACL. With the extended ACL there is an implicit *deny any any* line which denies traffic from any source to any destination.

Thus, at the purple branch, we need to create an extended ACL and permit traffic from the source purple network to the host Orange Web Server and to the green network. For the green network, we need to permit traffic from the green network to the host Web Server and the purple network. In this way, the branches can communicate with each other and the Web Server but nothing else.

To do this, we first need to create an extended ACL list. As mentioned earlier, extended ACL needs to be applied closest to the source. Thus, both ACLs will be applied inbound

at BRCH1 and BRCH2 routers Fast Ethernet 0/0 port for the purple and green network respectively. Named access lists will be used for this mini-project.

For the purple network, we go to BRCH1 router and using the command **ip access-list extended EXTND-1** from the global configuration mode to create the access list. Next, use the commands **permit ip 172.8.0.0 0.0.63.255 host 192.168.8.149** and **permit ip 172.8.0.0 0.0.63.255 172.8.64.0 0.0.15.255**. Once we are back in global configuration mode, we need to apply the access list inbound at the interface fa0/0 using the command **int fa0/0** followed by **ip access-group EXTND-1 in**.

For the green network, we go to BRCH2 router and using the command **ip access-list extended EXTND-2** from the global configuration mode to create the access list. Next, use the commands **permit ip 172.8.64.0 0.0.15.255 host 192.168.8.149** and **permit ip 172.8.64.0 0.0.15.255 172.8.0.0 0.0.63.255**. Once we are back in global configuration mode, we need to apply the access list inbound at the interface fa0/0 using the command **int fa0/0** followed by **ip access-group EXTND-2 in**.

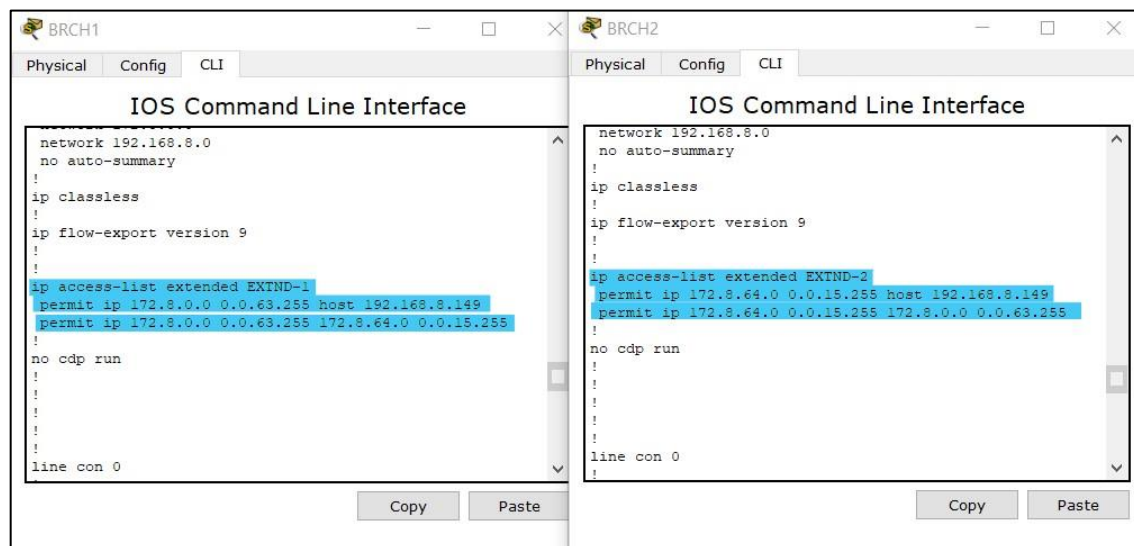
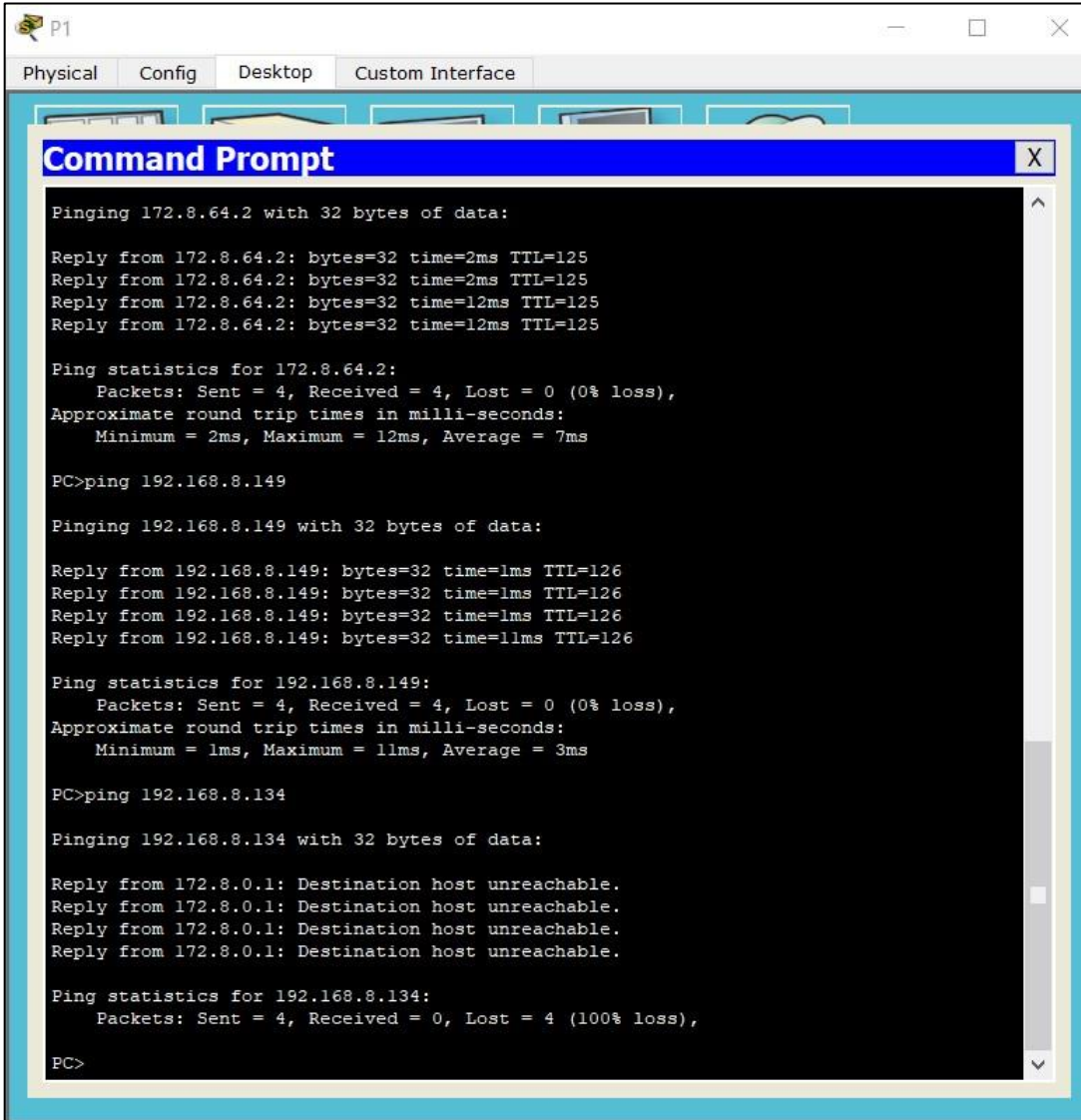


Figure 9.03: Evidence that Routers Have Been Configured with ACL

Next, to verify that the ACL works, we try to ping various devices in the network. Only the devices located in the green or purple network and the Orange Web Server should succeed. The addresses for the green and purple network are DHCP assigned from the purple DHCP server, which will be discussed later in the following chapter. 172.8.64.2 is a green host address, 172.8.0.4 is a purple network host address, 192.168.8.149 is the Orange Web Server address and the 192.168.8.134 is the address for a red host.



```
P1
Physical Config Desktop Custom Interface

Command Prompt

Pinging 172.8.64.2 with 32 bytes of data:

Reply from 172.8.64.2: bytes=32 time=2ms TTL=125
Reply from 172.8.64.2: bytes=32 time=2ms TTL=125
Reply from 172.8.64.2: bytes=32 time=12ms TTL=125
Reply from 172.8.64.2: bytes=32 time=12ms TTL=125

Ping statistics for 172.8.64.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 7ms

PC>ping 192.168.8.149

Pinging 192.168.8.149 with 32 bytes of data:

Reply from 192.168.8.149: bytes=32 time=1ms TTL=126
Reply from 192.168.8.149: bytes=32 time=1ms TTL=126
Reply from 192.168.8.149: bytes=32 time=1ms TTL=126
Reply from 192.168.8.149: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.8.149:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 3ms

PC>ping 192.168.8.134

Pinging 192.168.8.134 with 32 bytes of data:

Reply from 172.8.0.1: Destination host unreachable.
Reply from 172.8.0.1: Destination host unreachable.
Reply from 172.8.0.1: Destination host unreachable.
Reply from 172.8.0.1: Destination host unreachable.

Ping statistics for 192.168.8.134:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Figure 9.04: Using Ping to Verify ACL From Purple Network Host

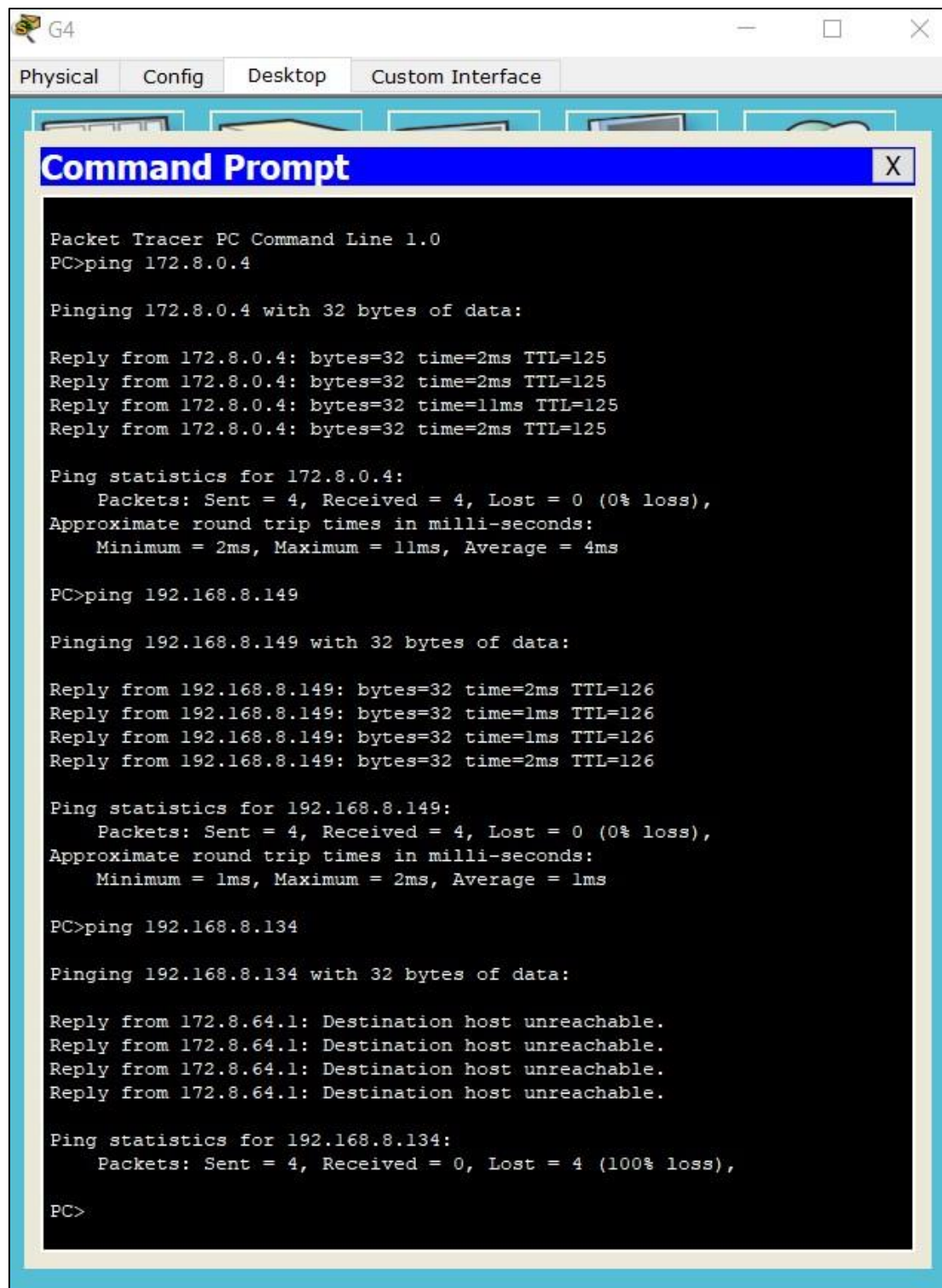
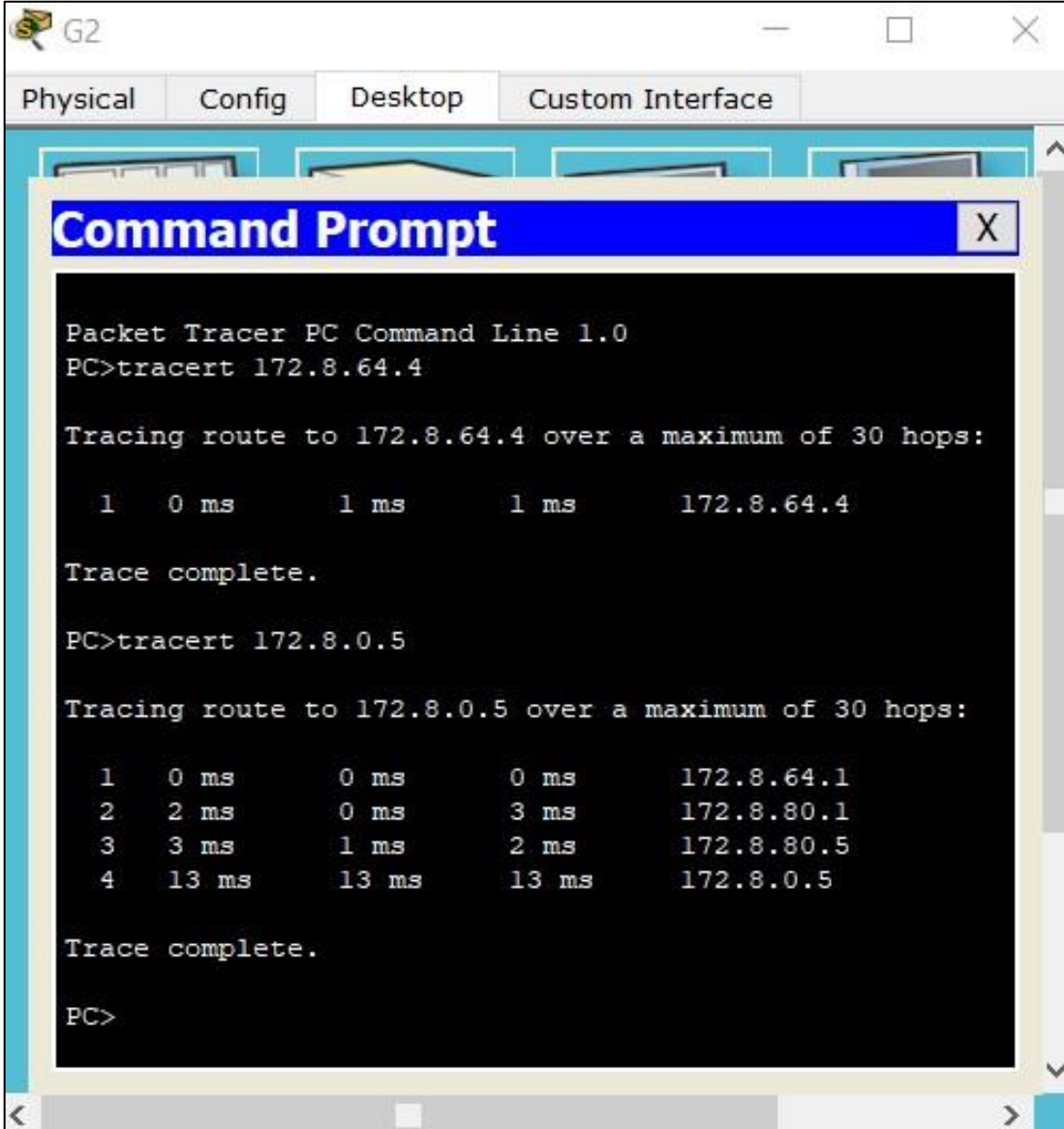


Figure 9.05: Using Ping to Verify ACL From Green Network Host

As shown in Figures 9.4 and 9.5, the purple and green hosts can communicate with each other and the Orange Web Server but cannot communicate with any other host.

The requirement also states that we need to identify the route each host passes through to communicate with other hosts in the branches network. To do this, we can use the command **tracert** from the command prompt of one of the host workstations. For a green network device, the route is shown below.



The screenshot shows a Packet Tracer PC Command Line window for a host named G2. The window has tabs for Physical, Config, Desktop, and Custom Interface. The Command Prompt window is open, displaying the following text:

```
Packet Tracer PC Command Line 1.0
PC>tracert 172.8.64.4

Tracing route to 172.8.64.4 over a maximum of 30 hops:

  1    0 ms      1 ms      1 ms      172.8.64.4

Trace complete.

PC>tracert 172.8.0.5

Tracing route to 172.8.0.5 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      172.8.64.1
  2    2 ms      0 ms      3 ms      172.8.80.1
  3    3 ms      1 ms      2 ms      172.8.80.5
  4   13 ms     13 ms     13 ms      172.8.0.5

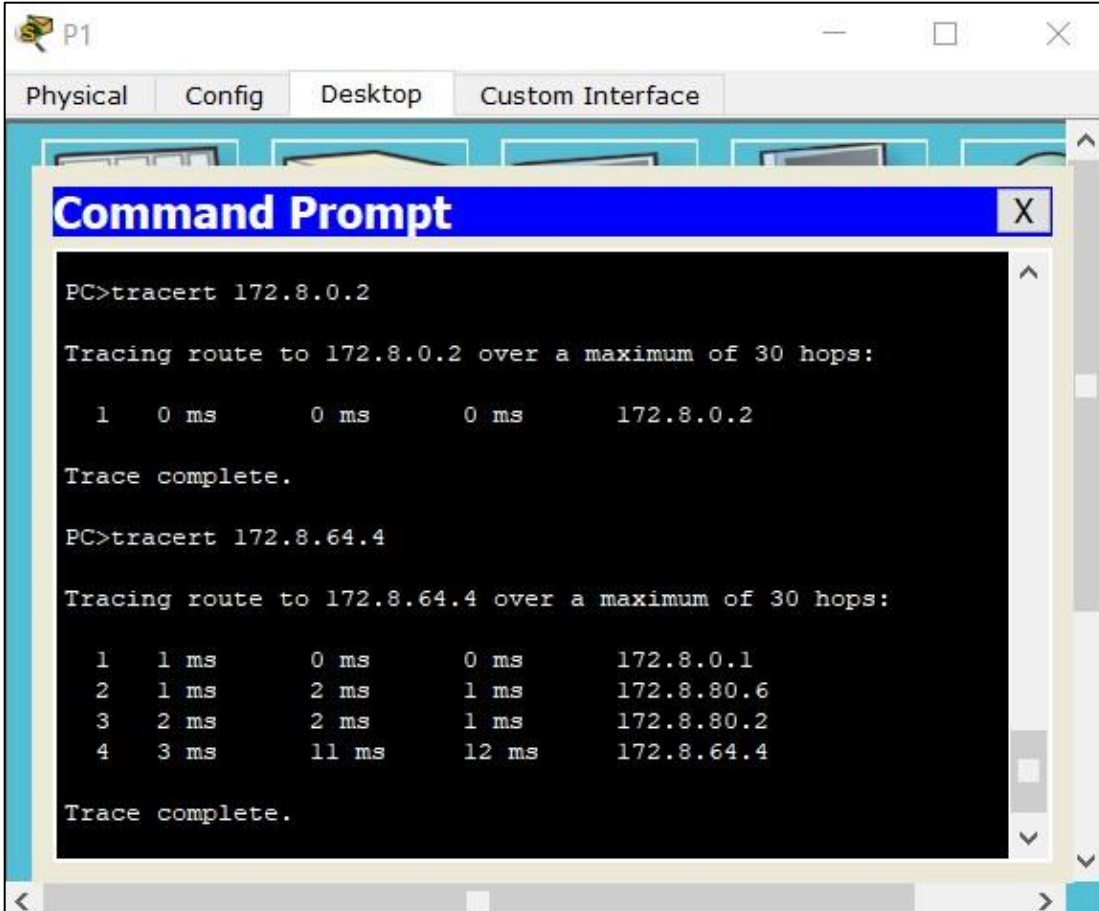
Trace complete.

PC>
```

Figure 9.06: Using Tracert from Green Host

In Figure 9.06, for the first tracert command, the destination IP address is within the green network. Thus, it only goes to the default gateway which 172.8.64.1 before reaching the destination address. The second tracert command has a destination IP address of host on the purple network. It has to go to the default gateway before reaching the serial interface of the HQ router which has an address of 172.8.80.1. Then, it hops

to the next serial interface at HQ router which has an address of 172.8.80.5 before reaching the destination address.



```
PC>tracert 172.8.0.2

Tracing route to 172.8.0.2 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    172.8.0.2

Trace complete.

PC>tracert 172.8.64.4

Tracing route to 172.8.64.4 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    172.8.0.1
  2  1 ms    2 ms    1 ms    172.8.80.6
  3  2 ms    2 ms    1 ms    172.8.80.2
  4  3 ms   11 ms   12 ms    172.8.64.4

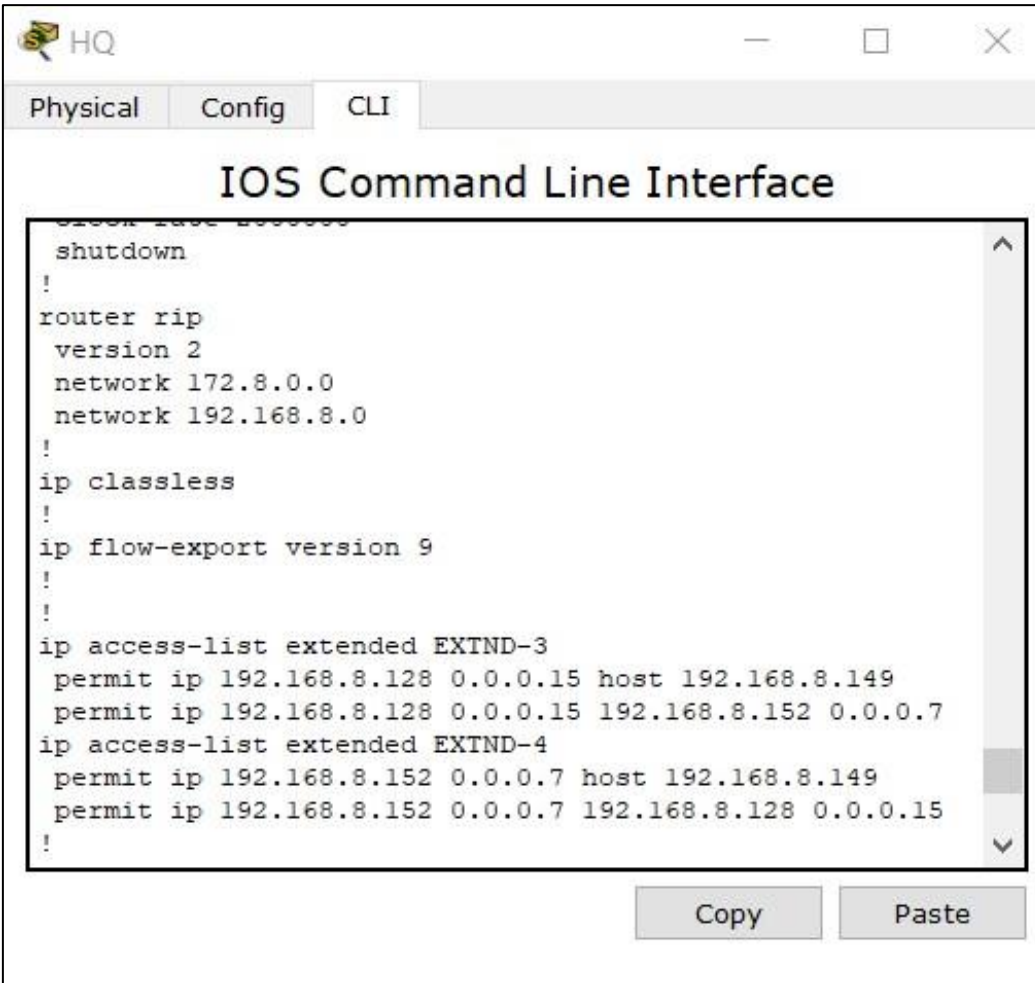
Trace complete.
```

Figure 9.07: Using Tracert from Purple Host

In Figure 9.07, the first tracert command has a destination IP address is within the purple network. Thus, it only goes to the default gateway which 172.8.0.1 before reaching the destination address. The second tracert command has a destination IP address of host on the green network. It has to go to the default gateway before reaching the serial interface of the HQ router which has an address of 172.8.80.6. Then, it hops to the next serial interface at HQ router which has an address of 172.8.80.2 before reaching the destination address.

The last specification for requirement 5 states that the Red and Blue VLANs should be able to communicate only with each other and the Orange Web Server. We use similar steps to when we were creating ACLs for the green and purple network. The ACLs will be applied to the HQ router as that is the closest to the source addresses. We need to

create two separate access-lists however as we will apply the lists to different subinterfaces. The commands to create and apply the ACL for the Red VLAN are as follows: **ip access-list extended EXTEND-3** followed by **permit ip 192.168.8.128 0.0.0.15 host 192.168.8.149** and then **permit ip 192.168.8.128 0.0.0.15 192.168.8.152 0.0.0.7** before **exit** then **int fa0/0.10** and **ip access-group EXTND-3 in**. For the Blue VLAN the commands are as follows: **ip access-list extended EXTEND-4** followed by **permit ip 192.168.8.152 0.0.0.7 host 192.168.8.149** and then **permit ip 192.168.8.152 0.0.0.7 192.168.8.128 0.0.0.15** before **exit** then **int fa0/0.30** and **ip access-group EXTND-4 in**. To verify the configurations, use **sh runn**.



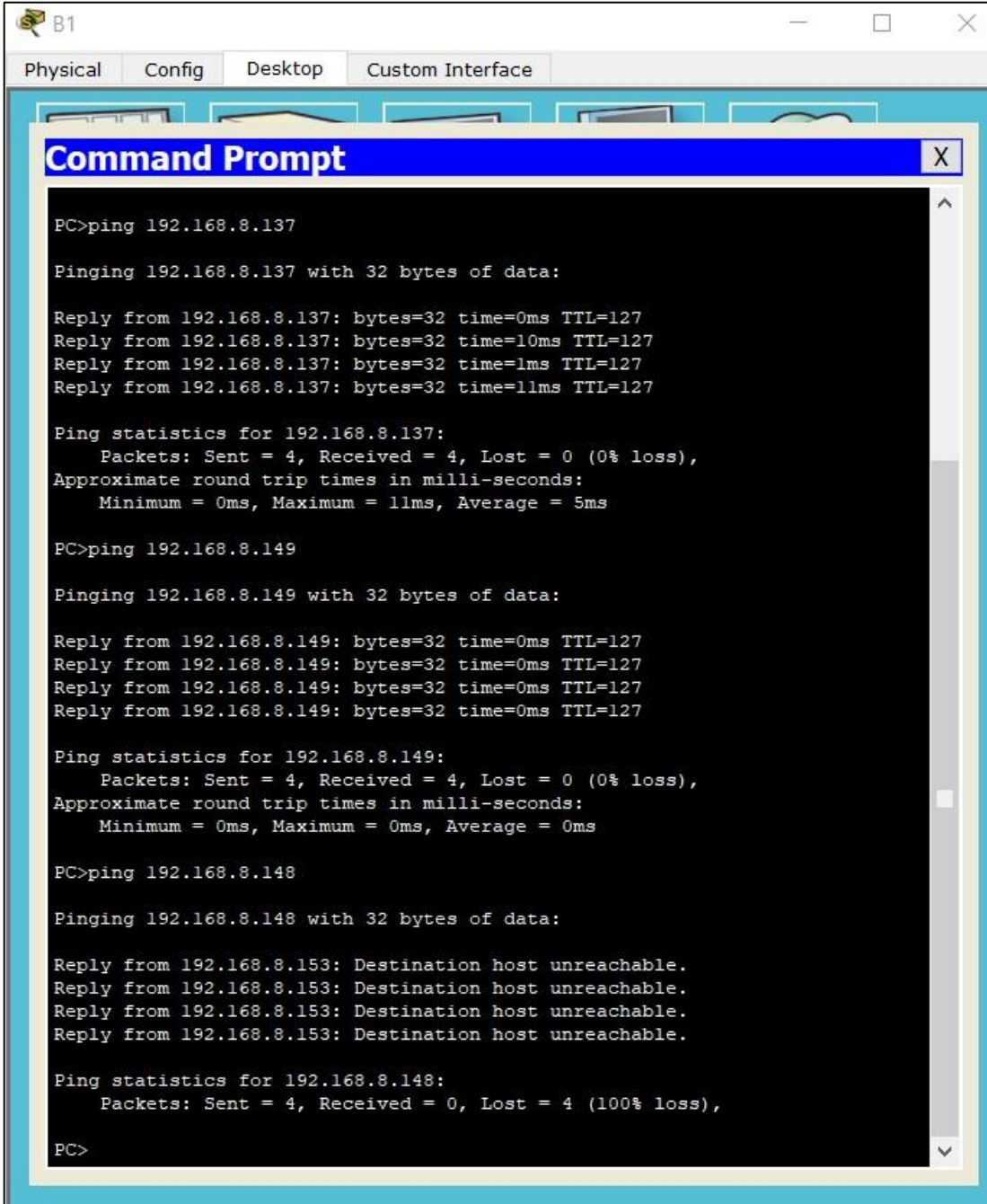
The screenshot shows a window titled 'HQ' with tabs for 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The command prompt is 'HQ#'. The configuration shown is as follows:

```
HQ#
shutdown
!
router rip
version 2
network 172.8.0.0
network 192.168.8.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended EXTND-3
 permit ip 192.168.8.128 0.0.0.15 host 192.168.8.149
 permit ip 192.168.8.128 0.0.0.15 192.168.8.152 0.0.0.7
ip access-list extended EXTND-4
 permit ip 192.168.8.152 0.0.0.7 host 192.168.8.149
 permit ip 192.168.8.152 0.0.0.7 192.168.8.128 0.0.0.15
!
```

At the bottom of the CLI window, there are 'Copy' and 'Paste' buttons.

Figure 9.08: Verifying Access-List Configurations at HQ Router

Next, to verify that the ACL for the Red and Blue VLANs work, we try to ping various devices from the command prompt. Only pings for devices located in the Red or Blue VLANs and the Orange Web Server should succeed. The addresses for the Red and Blue VLANs are DHCP assigned from their respective DHCP server, which will be discussed later in the following chapter. 192.168.8.156 is a Blue VLAN address, 192.168.8.137 is a Red VLAN address, 192.168.8.149 is the Orange Web Server address and the 192.168.8.148 is the address for an orange host.



The screenshot shows a Packet Tracer environment with a PC named B1. The PC has tabs for Physical, Config, Desktop, and Custom Interface. The Desktop tab is active, displaying a Command Prompt window. The Command Prompt shows the following output:

```
PC>ping 192.168.8.137

Pinging 192.168.8.137 with 32 bytes of data:

Reply from 192.168.8.137: bytes=32 time=0ms TTL=127
Reply from 192.168.8.137: bytes=32 time=10ms TTL=127
Reply from 192.168.8.137: bytes=32 time=1ms TTL=127
Reply from 192.168.8.137: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.8.137:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms

PC>ping 192.168.8.149

Pinging 192.168.8.149 with 32 bytes of data:

Reply from 192.168.8.149: bytes=32 time=0ms TTL=127
Reply from 192.168.8.149: bytes=32 time=0ms TTL=127
Reply from 192.168.8.149: bytes=32 time=0ms TTL=127
Reply from 192.168.8.149: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.8.149:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.8.148

Pinging 192.168.8.148 with 32 bytes of data:

Reply from 192.168.8.153: Destination host unreachable.
Reply from 192.168.8.153: Destination host unreachable.
Reply from 192.168.8.153: Destination host unreachable.
Reply from 192.168.8.153: Destination host unreachable.

Ping statistics for 192.168.8.148:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Figure 9.09: Using Ping to Verify Access-List Configurations from Blue Host

```
M8
Physical Config Desktop Custom Interface

Command Prompt
PC>ping 192.168.8.156

Pinging 192.168.8.156 with 32 bytes of data:

Reply from 192.168.8.156: bytes=32 time=0ms TTL=127
Reply from 192.168.8.156: bytes=32 time=14ms TTL=127
Reply from 192.168.8.156: bytes=32 time=9ms TTL=127
Reply from 192.168.8.156: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.8.156:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 5ms

PC>ping 192.168.8.149

Pinging 192.168.8.149 with 32 bytes of data:

Reply from 192.168.8.149: bytes=32 time=5ms TTL=127
Reply from 192.168.8.149: bytes=32 time=10ms TTL=127
Reply from 192.168.8.149: bytes=32 time=8ms TTL=127
Reply from 192.168.8.149: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.8.149:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 10ms, Average = 8ms

PC>ping 192.168.8.148

Pinging 192.168.8.148 with 32 bytes of data:

Reply from 192.168.8.129: Destination host unreachable.
Reply from 192.168.8.129: Destination host unreachable.
Reply from 192.168.8.129: Destination host unreachable.
Reply from 192.168.8.129: Destination host unreachable.

Ping statistics for 192.168.8.148:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Figure 9.10: Using Ping to Verify Access-List Configurations from Red Host

As shown in Figures 9.09 and 9.10, the orange host is unreachable and the message came from the respective Blue and Red default gateways.

10.0 Requirement 6

Based on the IP addressing scheme, each subnetwork has available addresses to assign to the hosts within that network. However, to configure them all statically is tedious and time consuming, especially when the number of hosts are high such as for the purple and green network which need 16000 and 4000 addresses respectively. Thus, DHCP servers are used to dynamically assign IP addresses.

First, the DHCP service must be turned on which can be done by going to the DHCP servers and then services then DHCP. Then, the different pools must be added by providing a pool name, default gateway, starting IP address, subnet mask and max user for this project. It is important to note that the starting address must be inputted carefully as there cannot be any overlapping IP addresses. The different fields are filled in based on the IP addressing scheme and the addressing table which are depicted in Table 5.1 and Table 3.1 respectively. Shown below are the final configuration for the DHCP servers in the entire network.

Red Server DHCP

Physical Config Services Desktop Custom Interface

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: Red Server

Default Gateway: 192.168.8.129

DNS Server: 0.0.0.0

Start IP Address : 192 168 8 130

Subnet Mask: 255 255 255 240

Maximum number of Users : 14

TFTP Server: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
Red Server	192.168.8.129	0.0.0.0	192.168.8.130	255.255.255.240	14	0.0.0.0
serverPool	192.168.8.129	0.0.0.0	192.168.8.128	255.255.255.240	14	0.0.0.0

Figure 10.1: Red DHCP Server Configuration

The screenshot shows the 'Blue Server DHCP' configuration window. The 'Services' tab is active, and the 'DHCP' service is selected. The interface is set to 'FastEthernet0' and the service is turned 'On'. The configuration fields are as follows:

- Pool Name: serverPool
- Default Gateway: 192.168.8.153
- DNS Server: 0.0.0.0
- Start IP Address: 192.168.8.152
- Subnet Mask: 255.255.255.248
- Maximum number of Users: 5
- TFTP Server: 0.0.0.0

Below the configuration fields is a table with columns: Pool Name, Default Gateway, DNS Server, Start IP Address, Subnet Mask, Max User, and TFTP Server. The table contains two entries:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
serverPool	192.168.8.153	0.0.0.0	192.168.8.152	255.255.255.248	5	0.0.0.0
Blue Server	192.168.8.153	0.0.0.0	192.168.8.154	255.255.255.248	5	0.0.0.0

Figure 10.2: Blue DHCP Server Configuration

The screenshot shows the 'Purple Server DHCP/DNS' configuration window. The 'Services' tab is active, and the 'DHCP' service is selected. The interface is set to 'FastEthernet0' and the service is turned 'On'. The configuration fields are as follows:

- Pool Name: Green Server
- Default Gateway: 172.8.64.1
- DNS Server: 172.8.0.2
- Start IP Address: 172.8.64.2
- Subnet Mask: 255.255.240.0
- Maximum number of Users: 4000
- TFTP Server: 0.0.0.0

Below the configuration fields is a table with columns: Pool Name, Default Gateway, DNS Server, Start IP Address, Subnet Mask, Max User, and TFTP Server. The table contains three entries:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
Purple Server	172.8.0.1	172.8.0.2	172.8.0.6	255.255.192.0	16000	0.0.0.0
Green Server	172.8.64.1	172.8.0.2	172.8.64.2	255.255.240.0	4000	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	512	0.0.0.0

Figure 10.3: Purple DHCP Server Configuration

Next, to ensure that the DHCP requests by the hosts are successful, we need to use the **ip helper-address** *DHCP-server-ip-address* command in order to configure the routers as a DHCP relay agent. Only the BRCH2 router needs to be configured as a DHCP relay agent as the green hosts are not within the same subnetwork as the DHCP server. We can verify that the configurations have been done correctly by using the **sh runn** command.



Figure 10.4: BRCH2 Router as a DHCP Relay Agent

Shown below are some examples of hosts with addresses from the DHCP servers as specified in the requirement and according to the IP addressing scheme which is shown in Table 5.1.

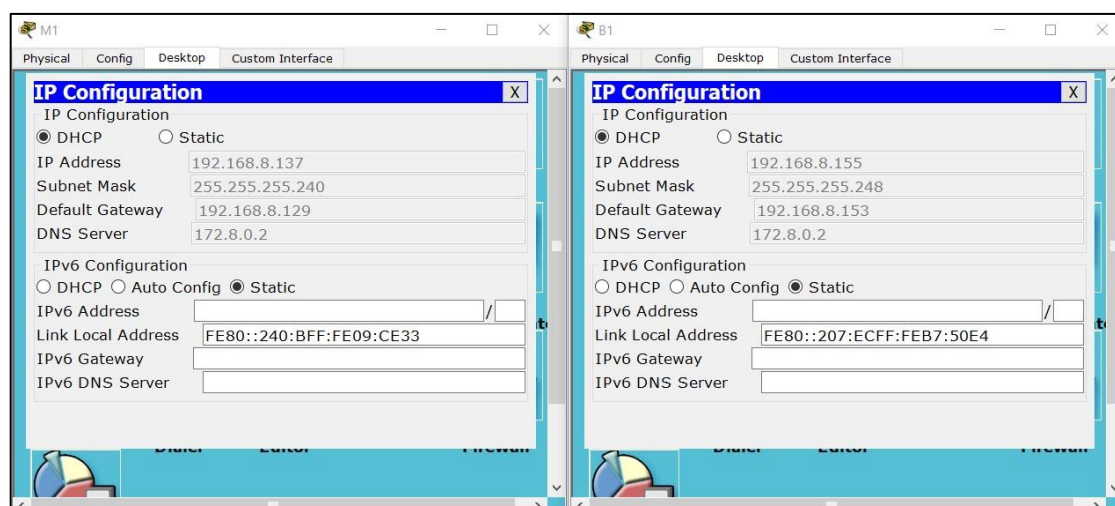


Figure 10.5: Evidence of IP Address Assignment from DHCP Server

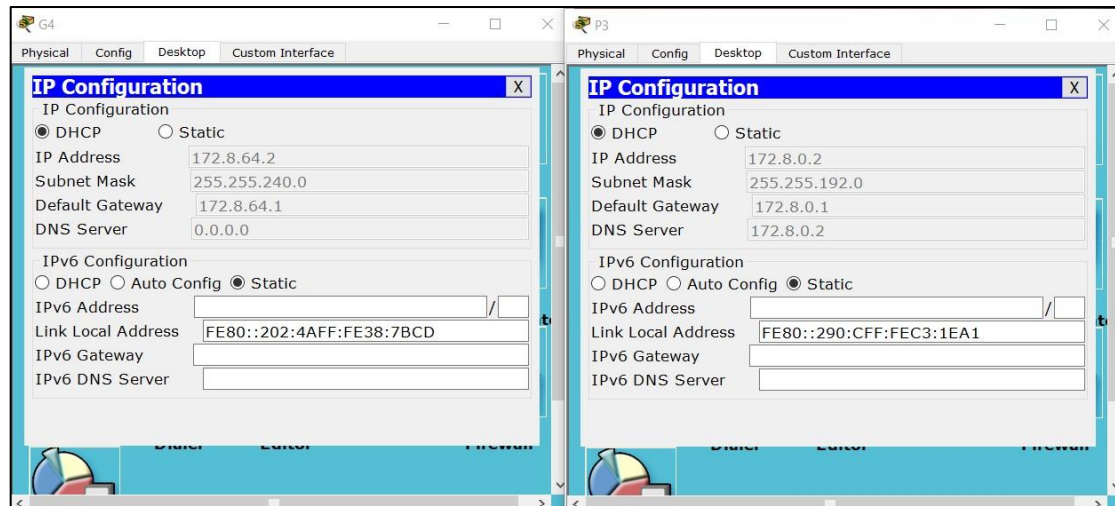


Figure 10.5: Evidence of IP Address Assignment from DHCP Server

11.0 Requirement 7

The DNS Server is located at the purple network. Thus, only the green and purple hosts will be able to access it due to the ACLs configured in Chapter 9. The Web Server is located on the Orange VLAN. However, all networks have access to this due to the ACLs permit command. The Mail Server will be set up on the Orange Web Server. This is so that there is some form of communication available between the BRANCHES and HQ network. Figure 11.1 show the configuration for the DNS Server.

Purple Server DHCP/DNS

Physical Config Services Desktop Custom Interface

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type A Record

Address

Add Save Remove

No.	Name	Type	Detail
0	dhcserver	A Record	172.8.0.5
1	dnserver	A Record	172.8.0.2
2	mailserver	A Record	192.168.8.149
3	www.group_8.utem.edu.my	A Record	192.168.8.149

DNS Cache

Figure 11.1: DNS Server Configuration

Orange Server WEB

Physical Config Services Desktop Custom Interface

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP

HTTP

HTTP ☒ On ☐ Off

HTTPS ☒ On ☐ Off

File Manager

	File Name	Edit	Delete
1	bridge.jpg		(delete)
2	index.html	(edit)	(delete)
3	izham.jpg		(delete)
4	khai.jpg		(delete)
5	syafi.jpg		(delete)
6	syafiqah.jpg		(delete)

New File Import

Figure 11.2: Web Server Configuration

Orange Server WEB

Physical Config Services Desktop Custom Interface

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP

EMAIL

SMTP Service ☒ ON ☐ OFF

POP3 Service ☒ ON ☐ OFF

Domain Name:

User Setup

User Password

P1
P2
P3
G1
G2
G3
G4
J1
J2
J3
M1
M2
M3
M4
M5
M6
M7
M8
B1
B2

Figure 11.3: Mail Server Configuration

For the hosts to actually communicate with each other however, email configuration must be done for each host. Shown below are some examples of the host mail configurations.

The screenshot shows a window titled 'G1' with tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. The 'Config' tab is active, showing a 'Configure Mail' dialog. The dialog has three sections: 'User Information' with fields for 'Your Name' (G1) and 'Email Address' (G1@email.com); 'Server Information' with fields for 'Incoming Mail Server' (192.168.8.149) and 'Outgoing Mail Server' (192.168.8.149); and 'Logon Information' with fields for 'User Name' (G1) and 'Password' (masked with dots). At the bottom are 'Save', 'Clear', and 'Reset' buttons.

Figure 11.4: Mail Configuration for G1

The screenshot shows a window titled 'M8' with tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. The 'Config' tab is active, showing a 'Configure Mail' dialog. The dialog has three sections: 'User Information' with fields for 'Your Name' (M8) and 'Email Address' (M8@email.com); 'Server Information' with fields for 'Incoming Mail Server' (192.168.8.149) and 'Outgoing Mail Server' (192.168.8.149); and 'Logon Information' with fields for 'User Name' (M8) and 'Password' (masked with dots). At the bottom are 'Save', 'Clear', and 'Reset' buttons.

Figure 11.5: Mail Configuration for M8

As the Mail Server is located at 192.168.8.149, all hosts can access this which enables communication between the BRANCHES and HQ network. Shown below, an email is sent from G1 host and received by the J1 host.

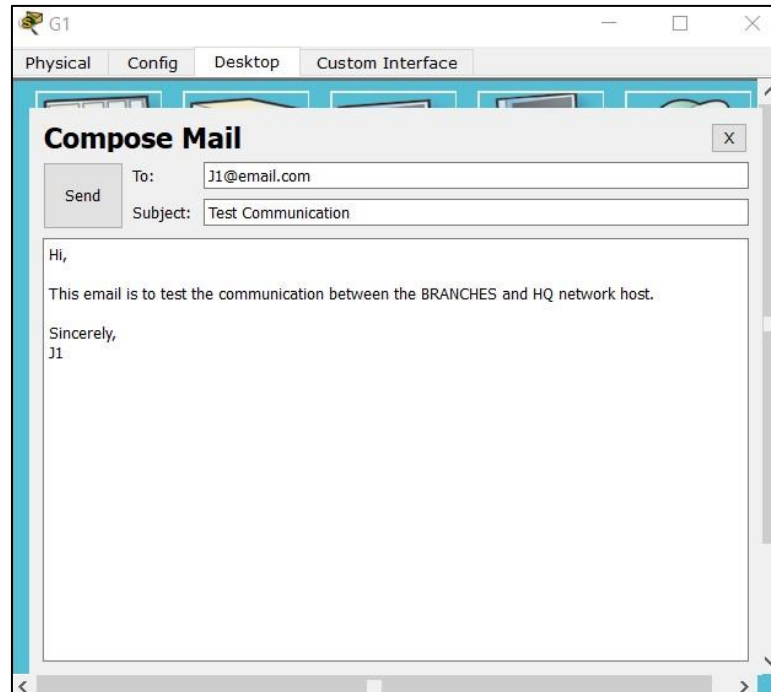


Figure 11.6: Composing Email from G1

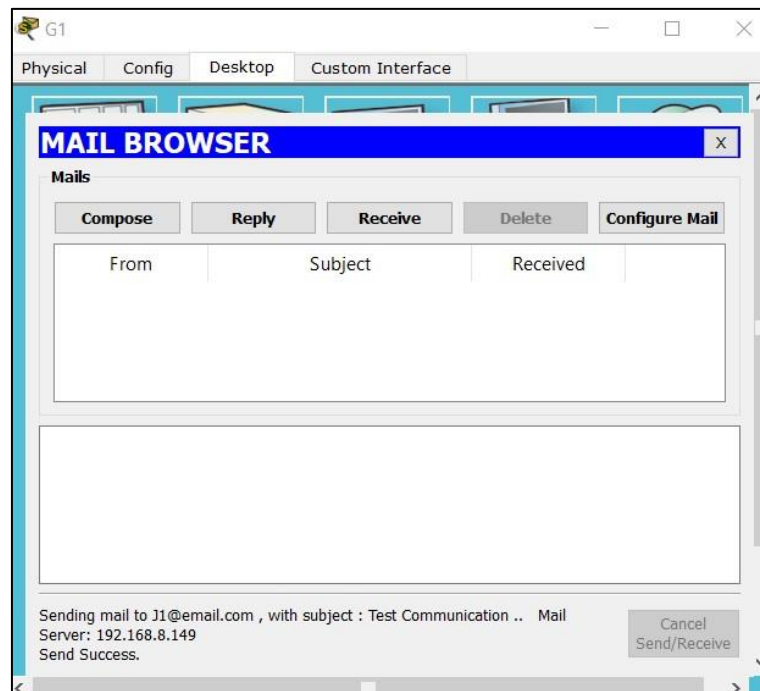


Figure 11.7: Sent Email from G1

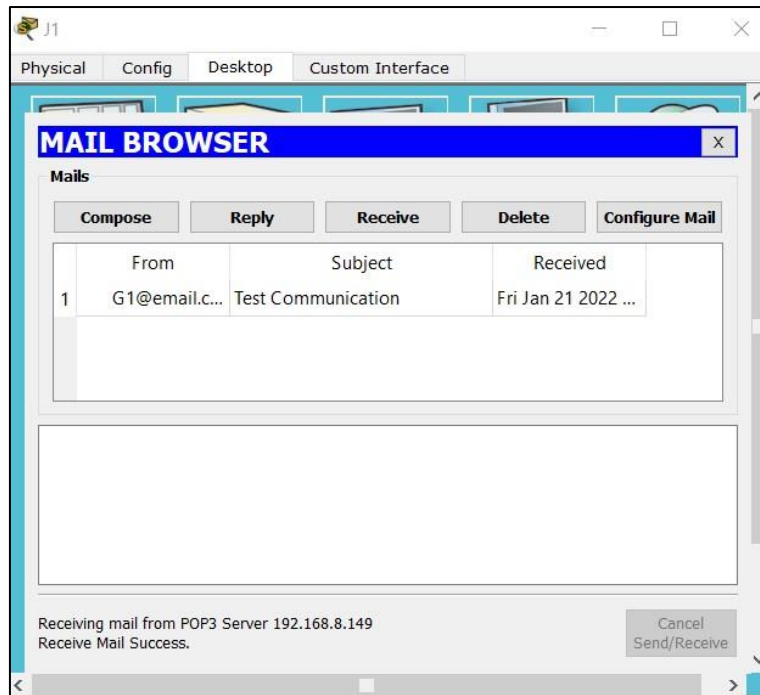


Figure 11.8: Mail Received by J1

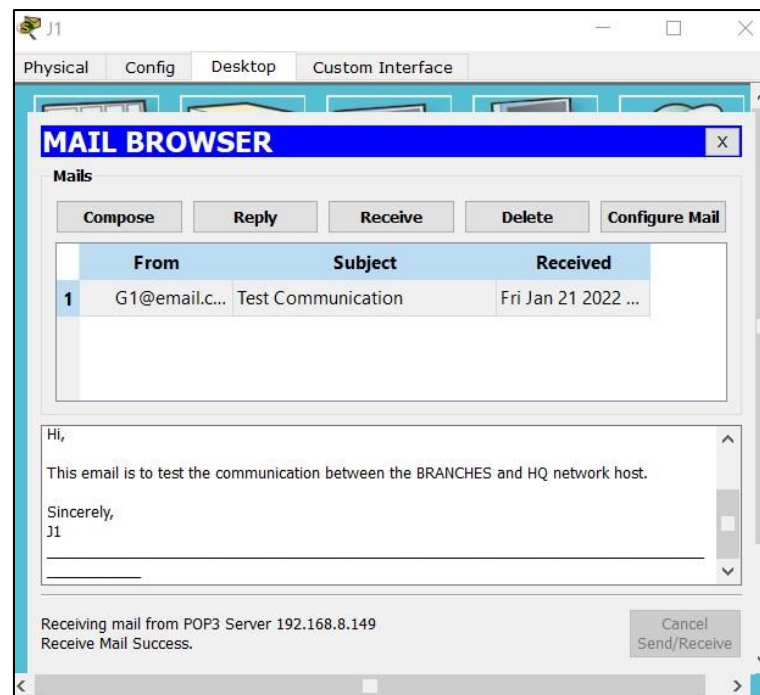


Figure 11.9: Mail Received by J1 Verified

12.0 Requirement 8

To build a webpage, html code was used. All group member names were added and two different colours were used. Individual pictures were also added as stated in the requirement. The pictures can be accessed by the links under the main body of text.

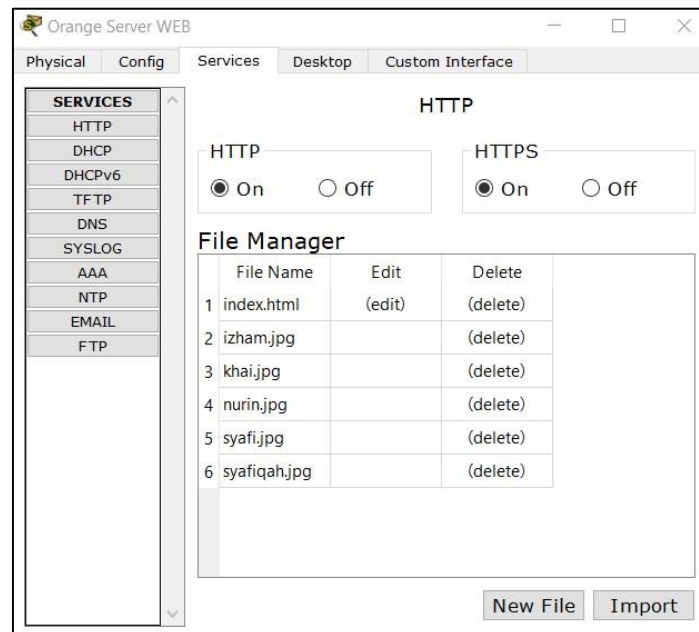


Figure 12.1: Adding Image Files

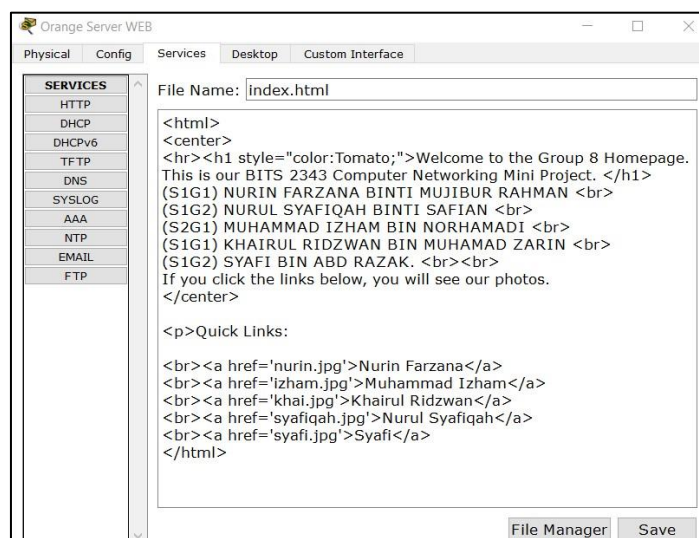


Figure 12.2: Editing HTML Code

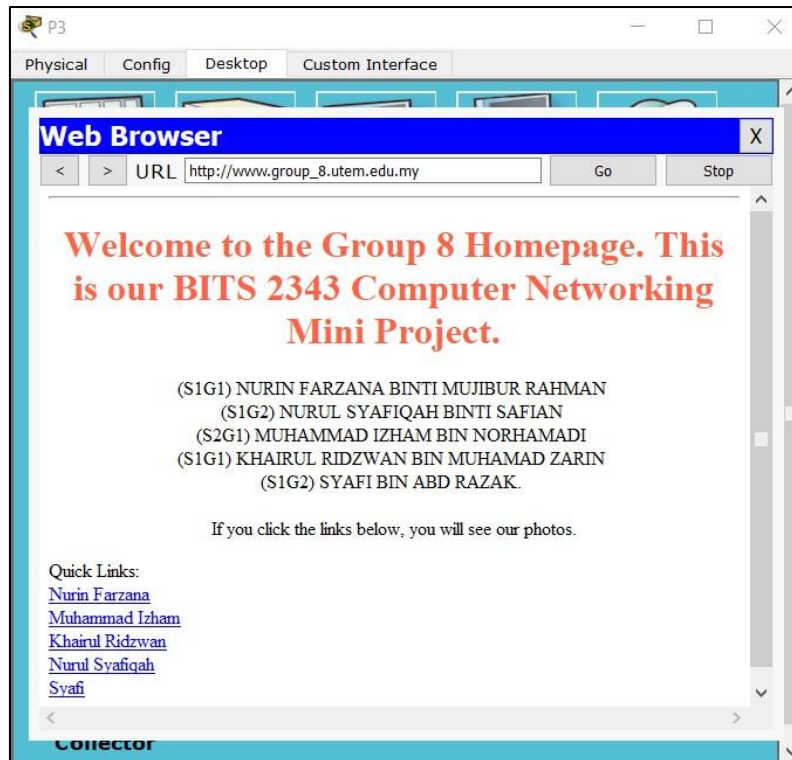


Figure 12.3: Searching for Webpage from P3

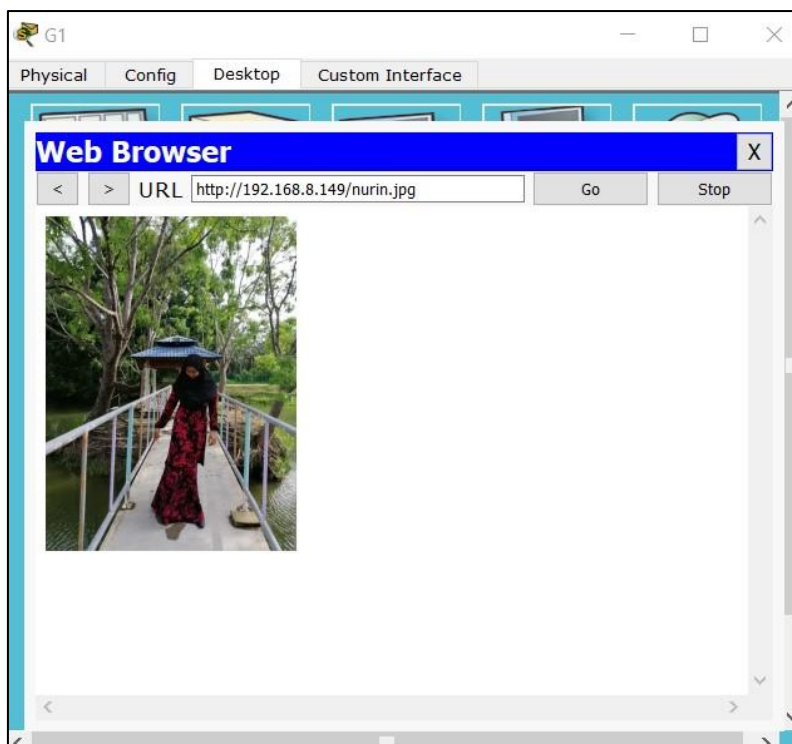


Figure 12.4: Group Member Images from Web Page from G1

13.0 Conclusion

In conclusion, the mini project was a success as all requirements were met satisfactorily. As a group, we were able to demonstrate our proficiency in developing a simulated network using packet tracer. We were able to implement access control lists as well as virtual local area network (VLAN) networks. Moreover, we displayed our ability to set up DHCP, DNS and Mail servers successfully.