CCNA Project Portfolio

Enterprise Network Implementation: Switching, Routing, and Services

A Technical Report

Prepared by:

AIT BEN IYCHE OMAR

2023-2024

Contents

General Introduction 1

1 WAN and LAN Addressing 2
- 1.1 Subnetting with the VLSM Method . . . 2
- 1.2 DHCP Pool Configuration on the Cork Router . . . 3

2 Configuration of Default Routes, OSPF Routing, and HSRP 4
- 2.1 Configure each router with a hostname and the required passwords . . . 4
  - 2.1.1 For the Galway Router . . . 4
- 2.2 Configure each interface for every router . . . 4
  - 2.2.1 For the Limerick Router . . . 4
- 2.3 Configure multi-area OSPF on the routers (Galway, Cork, Limerick, and Belfast) . . . 5
  - 2.3.1 For the routers in Area 0 . . . 5
  - 2.3.2 For the Cork Router (ABR between Area 0 and Area 1) . . . 6
  - 2.3.3 For the Galway Router in Area 1 . . . 6
  - 2.3.4 Routing Table for Each Router . . . 7
- 2.4 Configure route summarization for Area 1 . . . 7
- 2.5 Configure a default route on Belfast and redistribute it into the OSPF process . . . 9
- 2.6 Configure MD5 authentication between OSPF routers on all WAN links . . . 9
- 2.7 Set the Hello timer to 40 and the Dead timer to 160 on the link between Cork and Galway . . . 10
- 2.8 Verify that the Limerick, Belfast, Galway, and Cork routers are connected through Layers 1-7 . . . 10

3 Virtual Local Area Network (VLAN) Configuration 12
- 3.1 Apply basic switch configuration . . . 12
  - 3.1.1 Configure the hostname and passwords for each switch . . . 12
  - 3.1.2 Configure VTP Server on S1 . . . 13
  - 3.1.3 Configure the Root Bridge (PVST+) . . . 13
- 3.2 Configure the *Belfast* LAN . . . 14
  - 3.2.1 Create and name three data VLANs and one management VLAN on a switch 14
- 3.3 Configure ports *G0/0* as Trunk links (802.1Q) on S1 and S2 . . . 15
- 3.4 Configure S1, S2, and S3 so that ports 1 to 4 are trunks using the 802.1Q protocol . 15
- 3.5 Access mode configuration on S3 . . . 16
- 3.6 Connect G0/0 of the 2 Belfast routers to G0/0 of S1 and S2, and also a workstation per VLAN . . . 16

4 ACL Configurations **17**
4.1 Configure a `Reflexive ACL` in Belfast and use an ACL to control VTY access for Limerick . . . 17

5 DHCP Configurations **18**
5.1 Configuration of DHCP service for hosts in the Belfast LANs . . . 18
5.2 DHCP services configuration on the Cork Router . . . 18
5.3 Verification that each VLAN receives its address from DHCP . . . 18

6 NAT Configurations **20**
6.1 Configuration of the Cork Router . . . 20
6.1.1 NAT pool configuration . . . 20
6.1.2 Define an Access Control List (ACL) . . . 20
6.1.3 Dynamic Source Address Translation (NAT) . . . 21
6.1.4 Specify the internal and external NAT interfaces . . . 21
6.2 Connect a workstation to port Fa0/0 of Belfast to simulate an ISP server . . . 22
6.3 Configure the workstation to act as a web server . . . 23

7 Verification and Testing **24**
7.1 Verify communication between the different hosts on the network . . . 24

List of Figures

1 Working Network Topology 1

1.1 Network summary, including required sizes and addressing details for different subnets 2
1.2 Summary of VLAN configurations, including required and allocated sizes, IP addresses, subnet masks, assignable ranges, and broadcast addresses 2
1.3 DHCP services configuration on the Cork router for Belfast's VLANs 2, 3, and 4 . . 3

2.1 Configuration of hostname and password for the Galway router 4
2.2 Interface configuration for the Limerick router 5
2.3 For the Limerick Router 5
2.4 For the Belfast1 Router 5
2.5 Configuring the Cork router with OSPF in both areas 6
2.6 Configuring the Galway router with OSPF in Area 1 6
2.7 Routing table for the Belfast1 Router 8
2.8 Routing table for the Cork Router 8
2.9 Routing table for the Galway Router 8
2.10 Routing table for the Limerick Router 8
2.11 Configuration of route summarization for the Galway Router 9
2.12 Configuring the default route on Belfast and redistributing it into OSPF 9
2.13 Configuration of OSPF MD5 authentication on WAN links 10
2.14 For the Galway Router 10
2.15 For the Cork Router 10
2.16 Successful ping results from the `Limerick` router to various IPs 11
2.17 Successful ping results from the `Galway` router 11

3.1 Configuration of hostname and password on a switch 12
3.2 Configuration of the VTP domain, VLANs, and their names on the *S1* switch . . . 13
3.3 Setting the priority of switch S1 to 0 to designate it as the network's Root Bridge . 13
3.4 Configuring the priority for VLANs 1-4094 on switch S2 to 4096 14
3.5 Configuring the priority for VLANs 1-4094 on switch S3 to 4096 14
3.6 Configuration of VLANs and their names on the *S1* switch 14
3.7 Trunk mode configuration on S1 15
3.8 Trunk mode configuration on S2 15
3.9 Trunk mode configuration on S2 for ports 1-4 15
3.10 Access mode configuration on S3 16
3.11 Connecting the G0/0 ports of the two Belfast routers to the G0/0 ports of S1 and S2 respectively, and also connecting one workstation per VLAN. 16

4.1 Configuration of a `Reflexive ACL` in Belfast 17

4.2 Configuration of VTY access on the Limerick router using an ACL 17

5.1 Configuring workstations to obtain their IP address automatically 18
5.2 Configuring DHCP services on the Cork router 18
5.3 PC in VLAN 2 19
5.4 PC in VLAN 3 19
5.5 PC in VLAN 4 19

6.1 NAT pool configuration 20
6.2 Defining the ACL for NAT 21
6.3 Configuring dynamic source NAT with an ACL 21
6.4 Configuring the internal and external NAT interfaces 22
6.5 Connecting a workstation to simulate an ISP server 22
6.6 Configuring the workstation to act as a web server 23

7.1 Ping between a station in VLAN 2 and a station in the Galway network 24
7.2 Ping between different stations across the network 24

General Introduction

As part of the implementation of the company's network, we will configure VLANs to control broadcasts, enhance security, and group users. We will use RFC 1918 private addresses for the entire autonomous system, as well as DHCP on most LAN segments and NAT for Internet connectivity. We will also configure OSPF for internal routing and HSRP for gateway redundancy. The objective is to limit Internet access to web traffic while allowing multiple protocols within our WAN. To optimize the use of IP addresses and minimize waste, we will use VLSM where appropriate. Here is how we will proceed to configure the VLANs in Limerick, Galway, Cork, and Belfast as part of Phase I. Subsequently, we will address the next steps of the network configuration. Therefore, we will be working with the following schema:

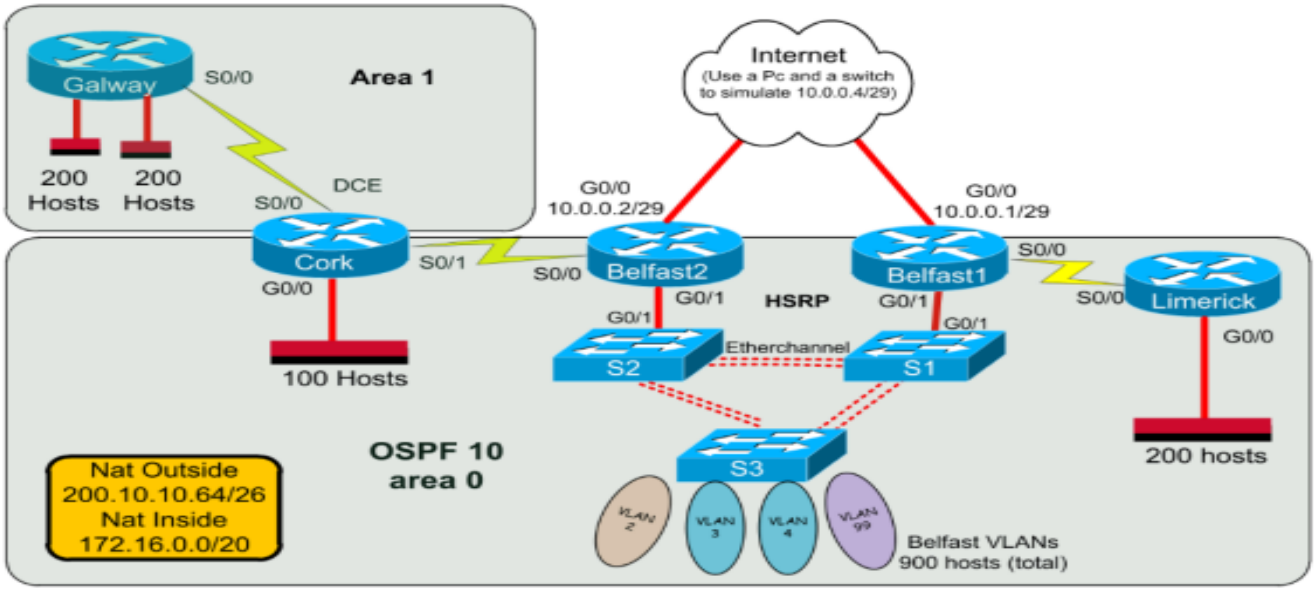

Figure 1: Working Network Topology

Chapter 1

WAN and LAN Addressing

The objective of this phase is to establish a coherent and efficient addressing plan for our network, using appropriate subnets for each VLAN to minimize address waste and optimize performance.

1.1 Subnetting with the VLSM Method

In this section, we started by applying the VLSM method to address our LANs (Galway, Cork, Limerick, Belfast), using the IP address 172.16.0.0/20. We then applied /30 subnets on all serial interfaces, as represented in the following table:

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
Belfst	900	1022	172.16.0.0	/22	255.255.252.0	172.16.0.1 - 172.16.3.254	172.16.3.255
Galway's	400	510	172.16.4.0	/23	255.255.254.0	172.16.4.1 - 172.16.5.254	172.16.5.255
Limerick	200	254	172.16.6.0	/24	255.255.255.0	172.16.6.1 - 172.16.6.254	172.16.6.255
Cork	100	126	172.16.7.0	/25	255.255.255.128	172.16.7.1 - 172.16.7.126	172.16.7.127
Serial betwen Galway's&Cork	2	2	172.16.7.128	/30	255.255.255.252	172.16.7.129 - 172.16.7.130	172.16.7.131
Serial betwen Limerick&Belfst1	2	2	172.16.7.132	/30	255.255.255.252	172.16.7.133 - 172.16.7.134	172.16.7.135
Serial btwen Cork&Belfst2	2	2	172.16.7.136	/30	255.255.255.252	172.16.7.137 - 172.16.7.138	172.16.7.139

Figure 1.1: Network summary, including required sizes and addressing details for different subnets

The **Belfast** subnet must be configured to support up to 900 devices, with the following distributions: 40 devices for VLAN 99 (Management VLAN), 120 hosts for VLAN 2, 250 hosts for VLAN 3, and 500 hosts for VLAN 4.

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
VLAN 4	500	510	172.16.0.0	/23	255.255.254.0	172.16.0.1 - 172.16.1.254	172.16.1.255
VLAN 3	250	254	172.16.2.0	/24	255.255.255.0	172.16.2.1 - 172.16.2.254	172.16.2.255
VLAN 2	120	126	172.16.3.0	/25	255.255.255.128	172.16.3.1 - 172.16.3.126	172.16.3.127
VLAN 99	40	62	172.16.3.128	/26	255.255.255.192	172.16.3.129 - 172.16.3.190	172.16.3.191

Figure 1.2: Summary of VLAN configurations, including required and allocated sizes, IP addresses, subnet masks, assignable ranges, and broadcast addresses

1.2 DHCP Pool Configuration on the Cork Router

Let's configure DHCP services on the Cork router. DHCP should provide services to the following LAN hosts:

- **VLAN 2, VLAN 3, and VLAN 4 of Belfast**

DHCP must transmit the following parameters to the hosts:

- **IP Address, Subnet Mask, Default Gateway, and DNS (10.0.0.4)**

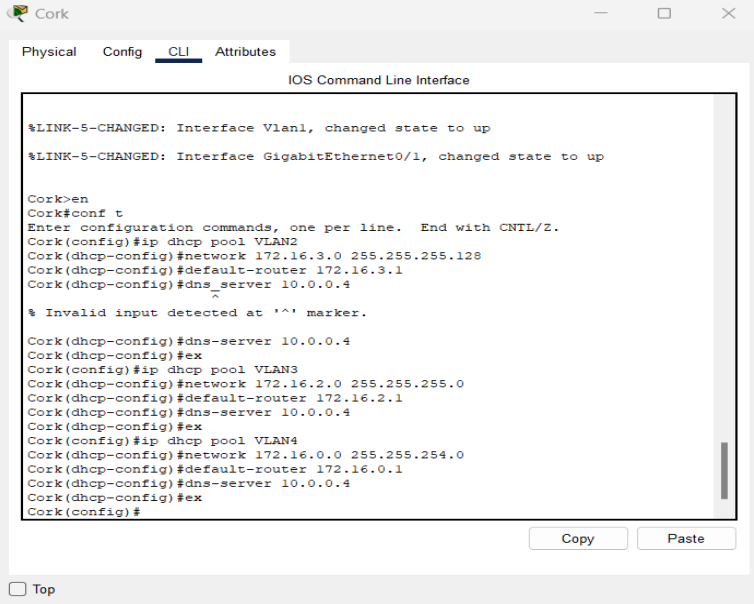

Figure 1.3: DHCP services configuration on the Cork router for Belfast's VLANs 2, 3, and 4

Chapter 2

Configuration of Default Routes, OSPF Routing, and HSRP

2.1 Configure each router with a hostname and the required passwords

2.1.1 For the Galway Router

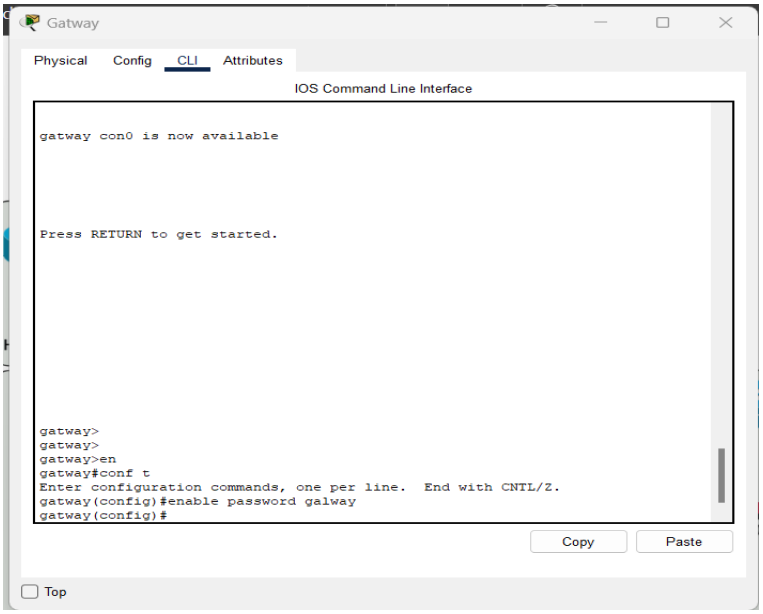

Figure 2.1: Configuration of hostname and password for the Galway router

$\Longrightarrow$ **The same configuration is applied to each router.**

2.2 Configure each interface for every router

2.2.1 For the Limerick Router

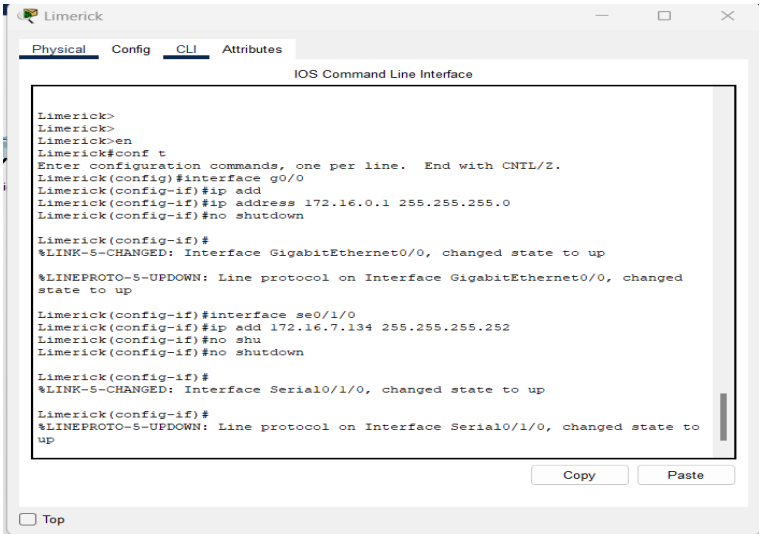

Figure 2.2: Interface configuration for the Limerick router

$\Longrightarrow$ **The same interface configuration is applied to each router.**

2.3 Configure multi-area OSPF on the routers (Galway, Cork, Limerick, and Belfast)

Multi-area OSPF configuration on the routers involves dividing the network into different OSPF areas and configuring communication between these areas. The Cork router is configured in two areas (Area 0 and Area 1), making it an Area Border Router (ABR).

2.3.1 For the routers in Area 0

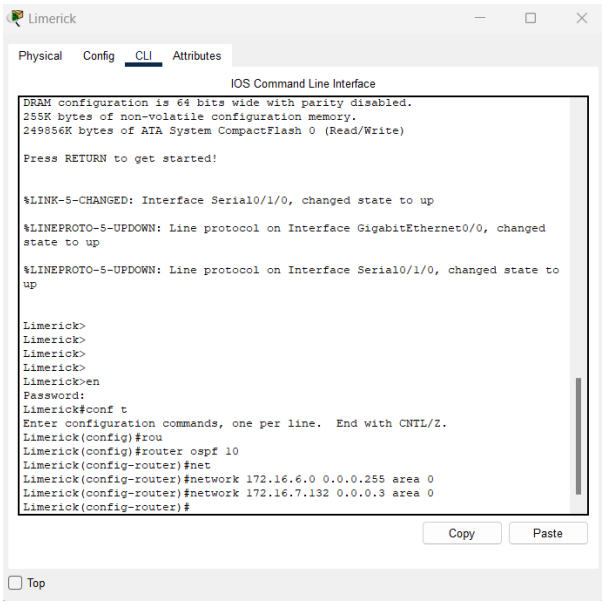

Figure 2.3: For the Limerick Router

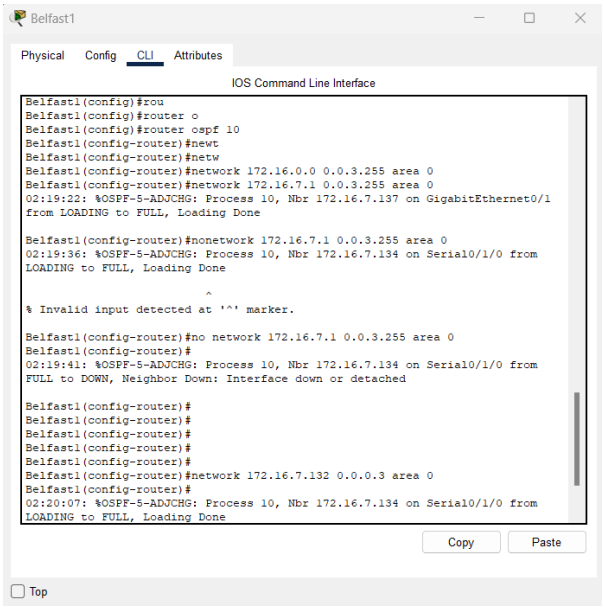

Figure 2.4: For the Belfast1 Router

$\Longrightarrow$ **The same for the Belfast2 Router.**

2.3.2 For the Cork Router (ABR between Area 0 and Area 1)

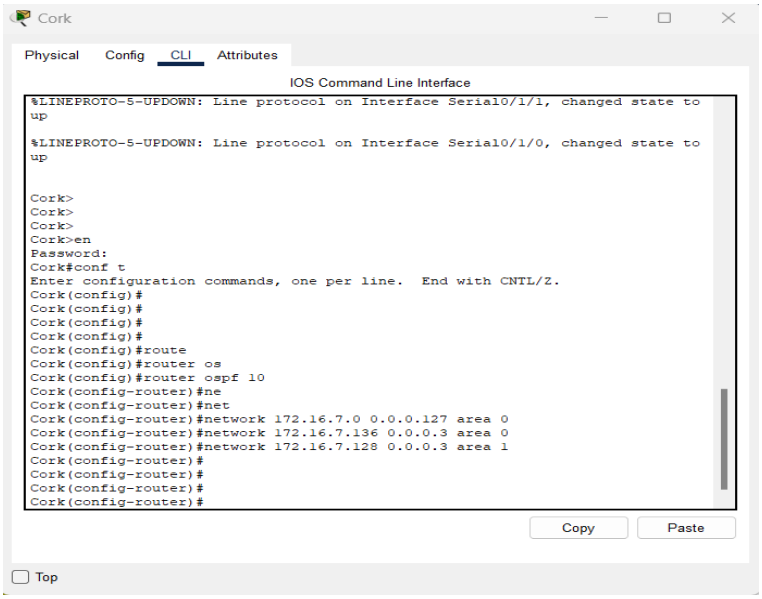

Figure 2.5: Configuring the Cork router with OSPF in both areas

2.3.3 For the Galway Router in Area 1

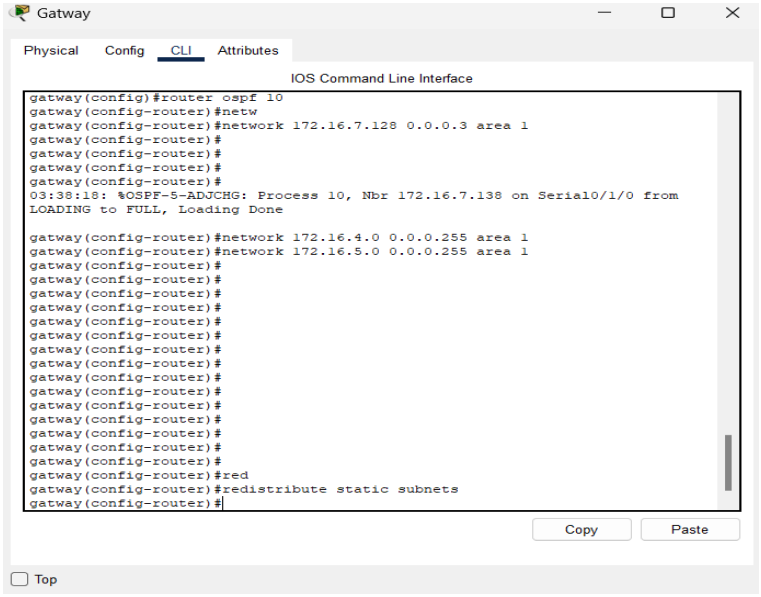

Figure 2.6: Configuring the Galway router with OSPF in Area 1

2.3.4 Routing Table for Each Router

2.4 Configure route summarization for Area 1

Figure 2.7: Routing table for the Belfast1 Router

Figure 2.8: Routing table for the Cork Router

Figure 2.9: Routing table for the Galway Router

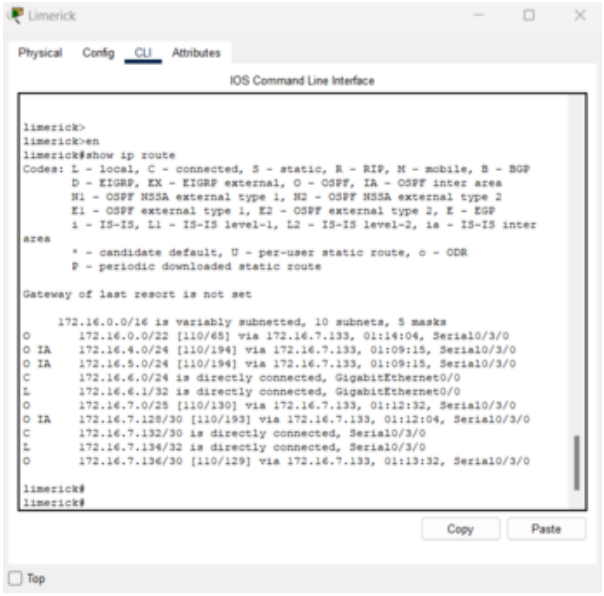

Figure 2.10: Routing table for the Limerick Router

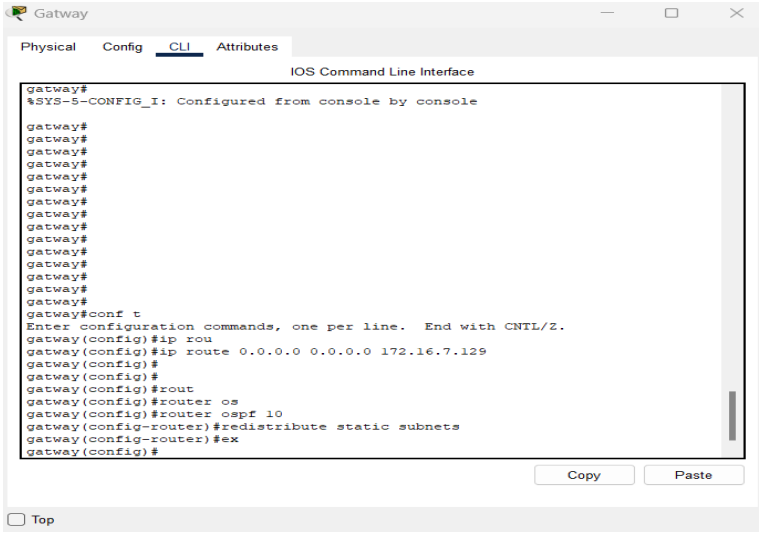

Figure 2.11: Configuration of route summarization for the Galway Router

2.5 Configure a default route on Belfast and redistribute it into the OSPF process

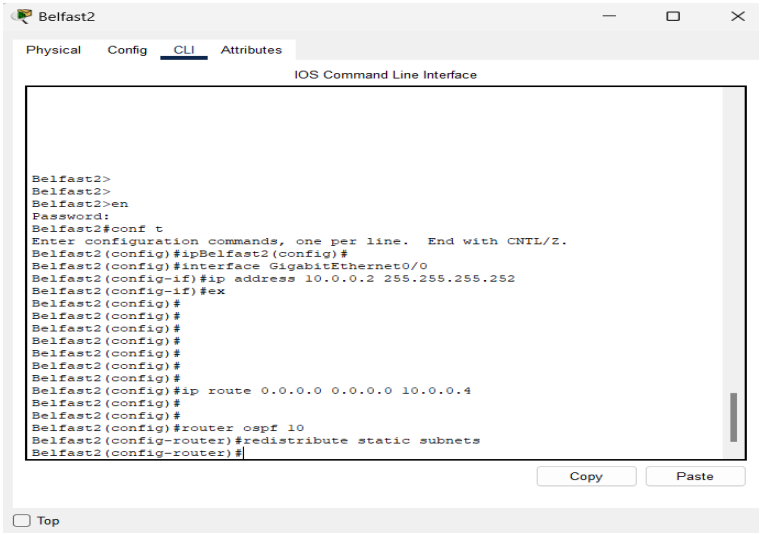

Figure 2.12: Configuring the default route on Belfast and redistributing it into OSPF

2.6 Configure MD5 authentication between OSPF routers on all WAN links

MD5 authentication is a security method used to secure OSPF routing exchanges. When enabled, it verifies the authenticity of OSPF packets using an MD5 hashing algorithm, preventing unauthorized routers from injecting false information. The configuration is shown in the following figure:
$\Longrightarrow$ **The same for each router.**

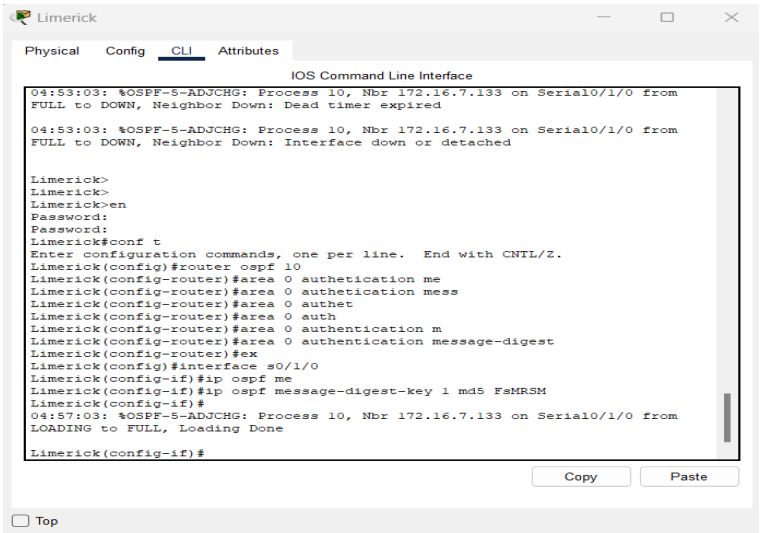

Figure 2.13: Configuration of OSPF MD5 authentication on WAN links

2.7 Set the Hello timer to 40 and the Dead timer to 160 on the link between Cork and Galway

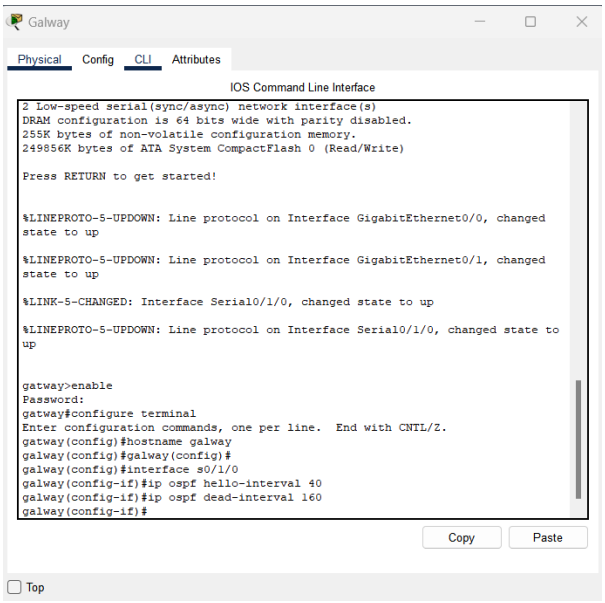

Figure 2.14: For the Galway Router

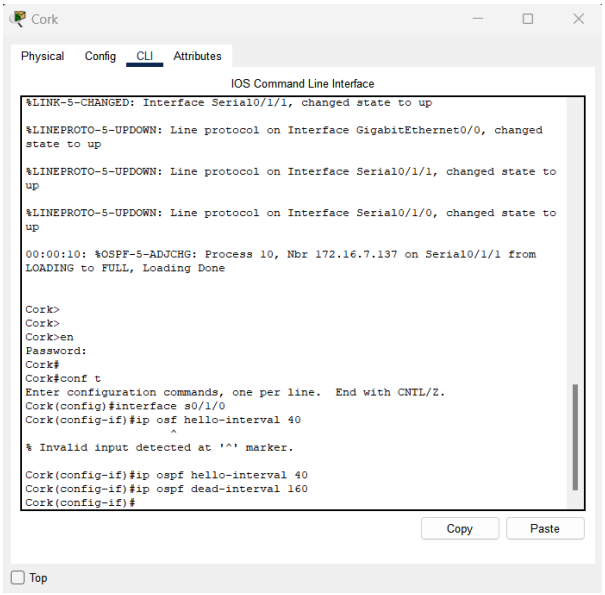

Figure 2.15: For the Cork Router

2.8 Verify that the Limerick, Belfast, Galway, and Cork routers are connected through Layers 1-7

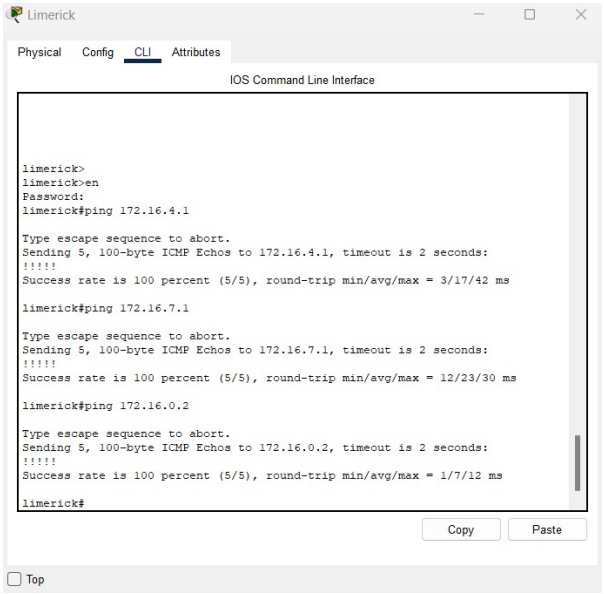

Figure 2.16: Successful ping results from the `Limerick` router to various IPs

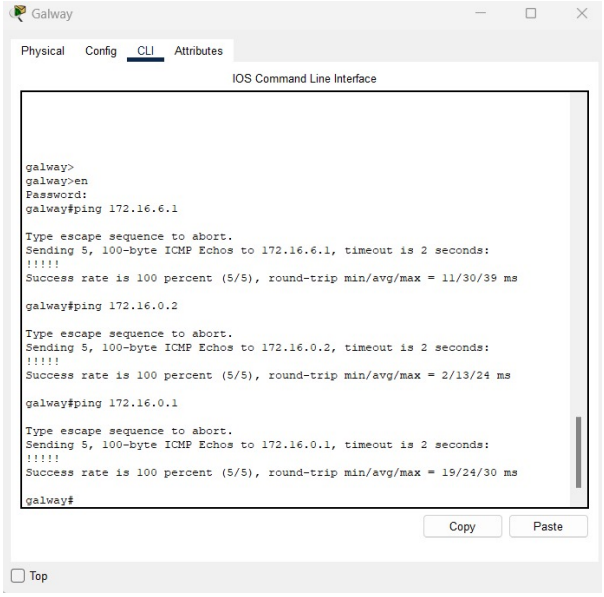

Figure 2.17: Successful ping results from the `Galway` router

Chapter 3

Virtual Local Area Network (VLAN) Configuration

3.1 Apply basic switch configuration

To configure a basic switch, it is important to set a hostname and passwords to secure access. Additionally, it is often necessary to configure specific features such as the Root Bridge for the Spanning Tree Protocol (STP) and server mode for specific interfaces. These basic steps are essential for ensuring the proper functioning and security of our network.

3.1.1 Configure the hostname and passwords for each switch

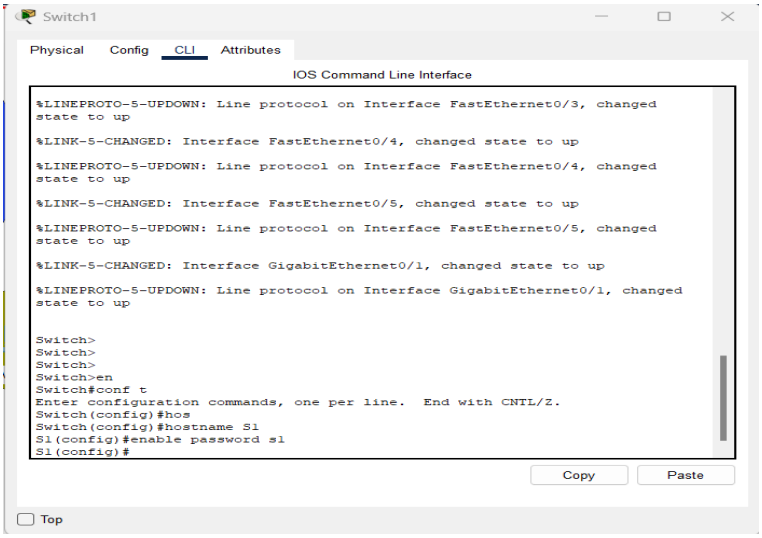

Figure 3.1: Configuration of hostname and password on a switch

$\Longrightarrow$ **The same configuration for each switch.**

3.1.2 Configure VTP Server on S1

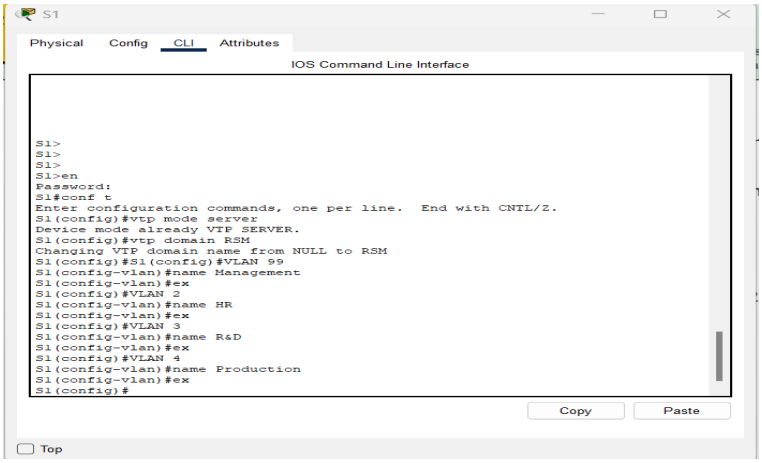

Figure 3.2: Configuration of the VTP domain, VLANs, and their names on the *S1* switch

3.1.3 Configure the Root Bridge (PVST+)

For *S1*

Giving S1 a priority of 0 means this switch has been configured to be the root bridge of the network. In a network using Spanning Tree Protocol (STP), the root bridge is the central point to which all other interfaces connect. A lower priority (0 being the lowest) ensures that S1 will be elected as the root bridge, which is desirable in our configuration to control the data propagation path.

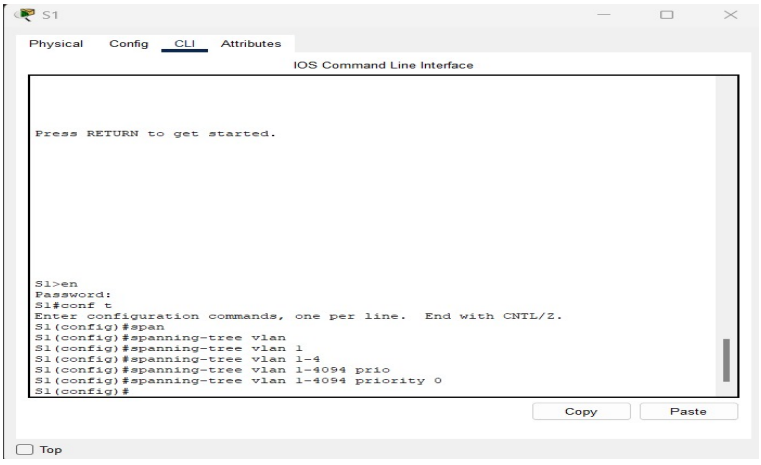

Figure 3.3: Setting the priority of switch S1 to 0 to designate it as the network's Root Bridge

For *S2* and *S3*

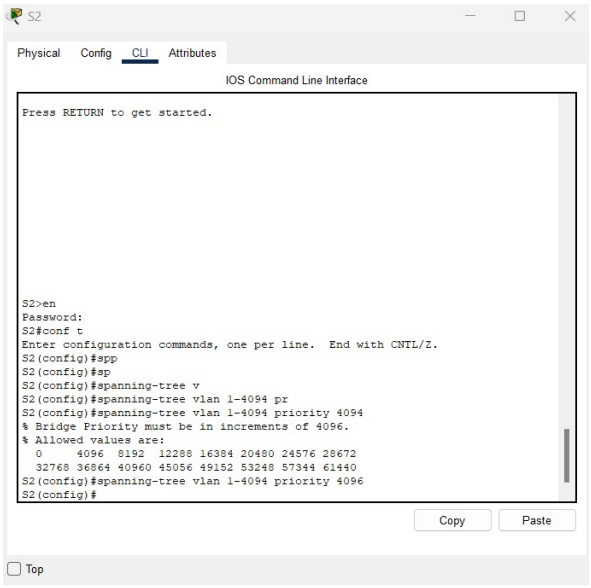

Figure 3.4: Configuring the priority for VLANs 1-4094 on switch S2 to 4096

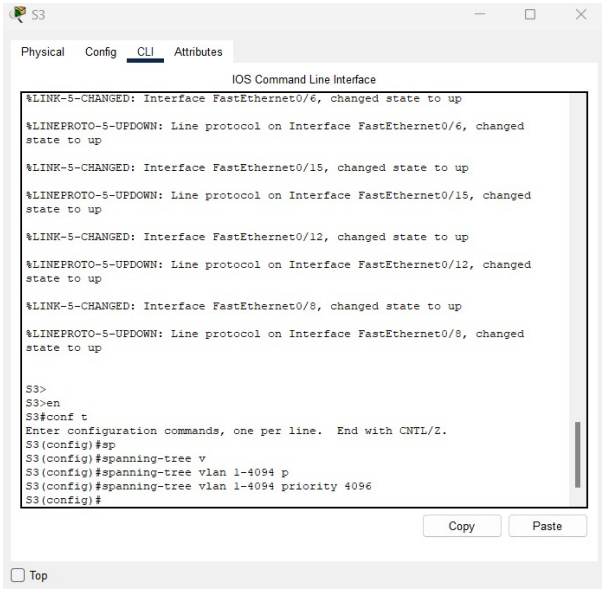

Figure 3.5: Configuring the priority for VLANs 1-4094 on switch S3 to 4096

3.2 Configure the *Belfast* LAN

3.2.1 Create and name three data VLANs and one management VLAN on a switch

We have already created the VLANs on the VTP server; the VTP client switches will share this database.

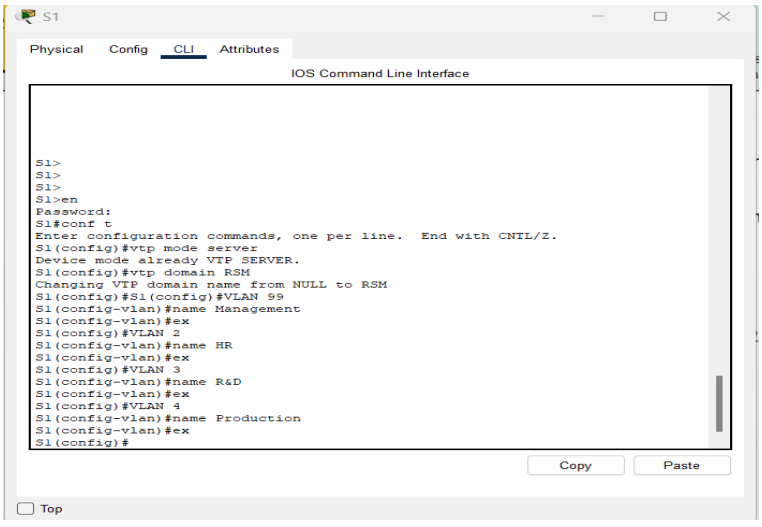

Figure 3.6: Configuration of VLANs and their names on the *S1* switch

$\Longrightarrow$ **The same configuration for each switch.**

3.3 Configure ports *G0/0* as Trunk links (802.1Q) on S1 and S2

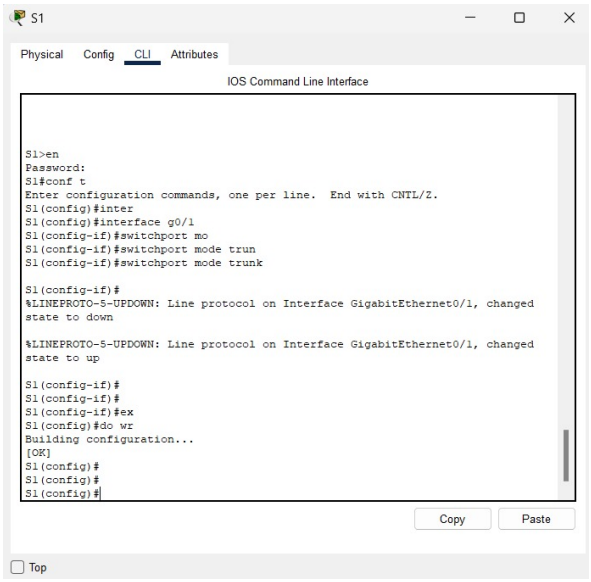

Figure 3.7: Trunk mode configuration on S1

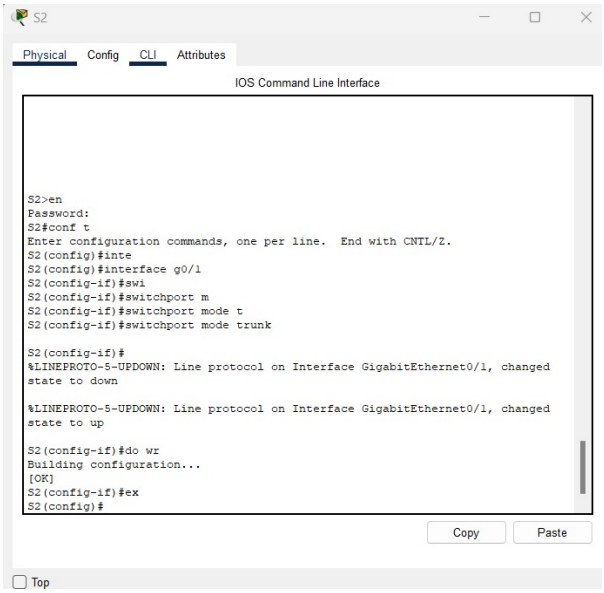

Figure 3.8: Trunk mode configuration on S2

3.4 Configure S1, S2, and S3 so that ports 1 to 4 are trunks using the 802.1Q protocol

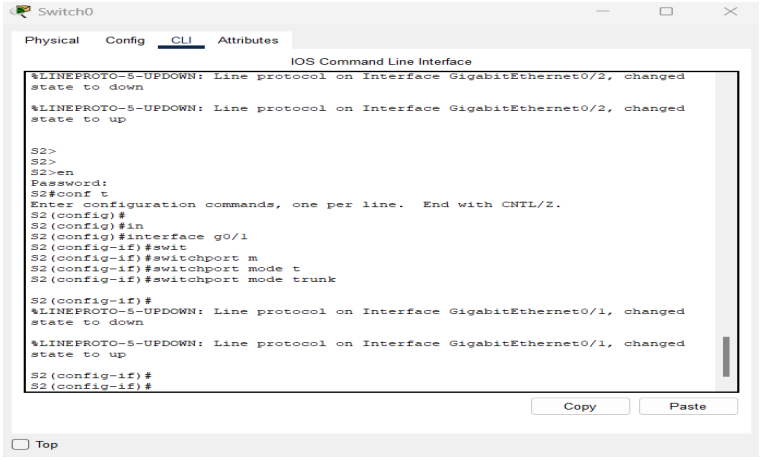

Figure 3.9: Trunk mode configuration on S2 for ports 1-4

$\Longrightarrow$ **The same configuration for each switch.**

3.5 Access mode configuration on S3

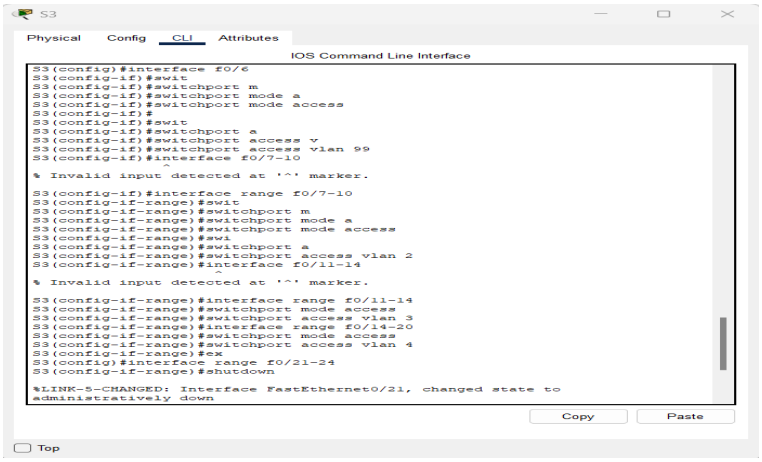

Figure 3.10: Access mode configuration on S3

3.6 Connect G0/0 of the 2 Belfast routers to G0/0 of S1 and S2, and also a workstation per VLAN

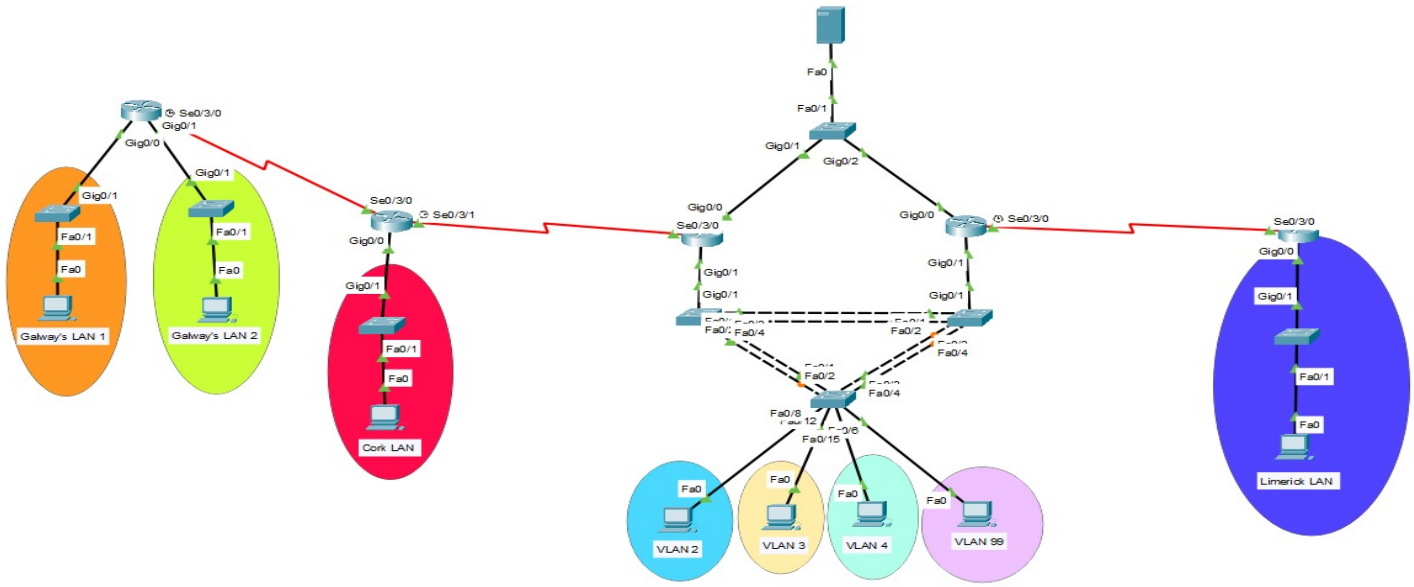

Figure 3.11: Connecting the G0/0 ports of the two Belfast routers to the G0/0 ports of S1 and S2 respectively, and also connecting one workstation per VLAN.

Chapter 4

ACL Configurations

4.1 Configure a `Reflexive ACL` in Belfast and use an ACL to control VTY access for Limerick

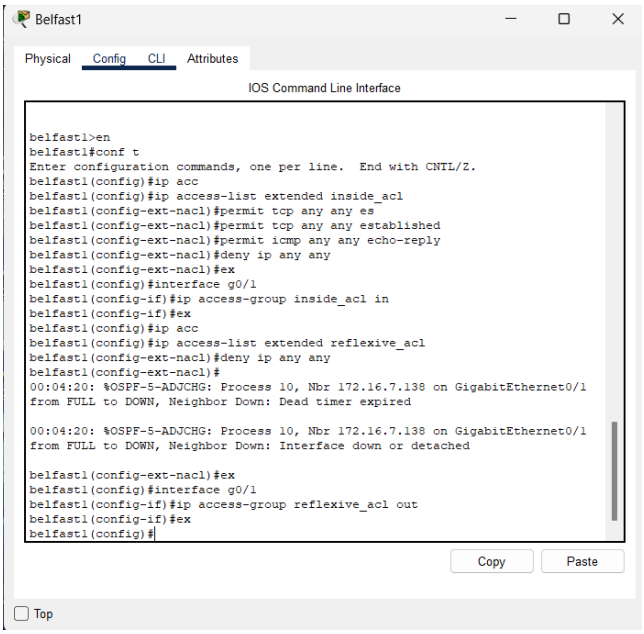

Figure 4.1: Configuration of a `Reflexive ACL` in Belfast

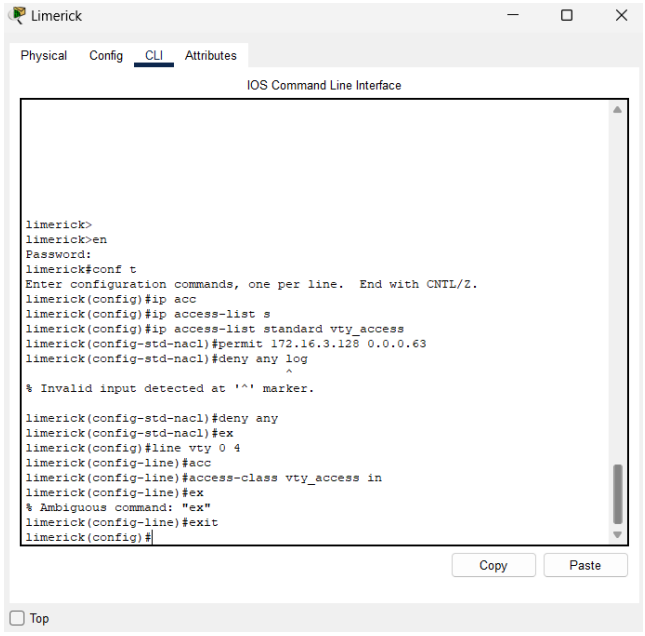

Figure 4.2: Configuration of VTY access on the Limerick router using an ACL

Chapter 5

DHCP Configurations

5.1 Configuration of DHCP service for hosts in the Belfast LANs

See the first chapter.

5.2 DHCP services configuration on the Cork Router

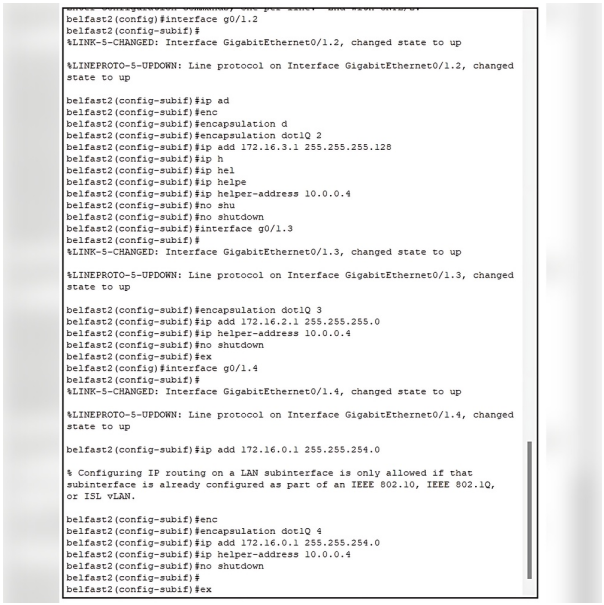

Figure 5.1: Configuring workstations to obtain their IP address automatically

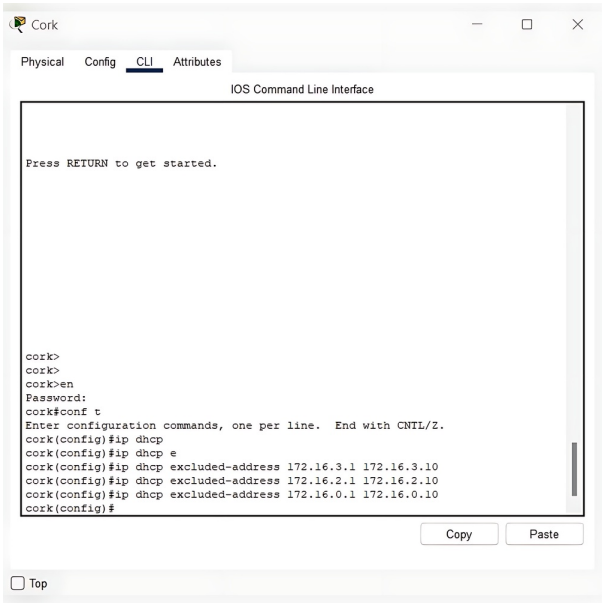

Figure 5.2: Configuring DHCP services on the Cork router

5.3 Verification that each VLAN receives its address from DHCP

The following figures show that each VLAN receives its address from the DHCP server.

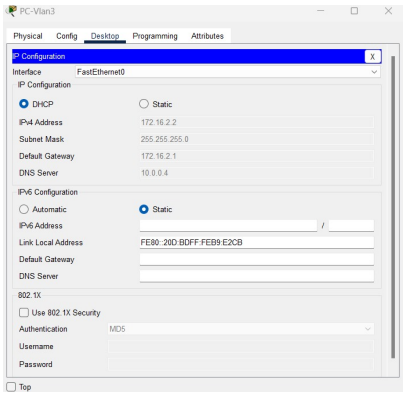

Figure 5.3: PC in VLAN 2

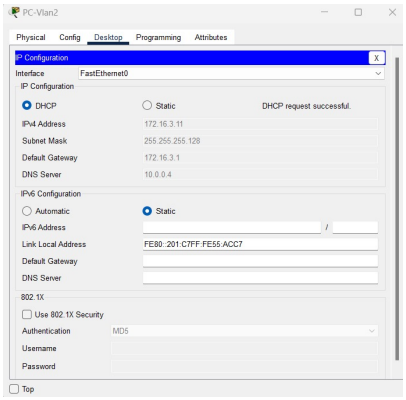

Figure 5.4: PC in VLAN 3

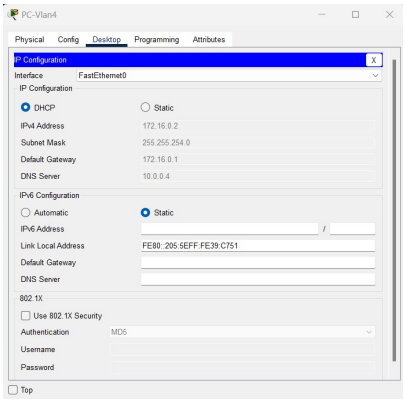

Figure 5.5: PC in VLAN 4

Chapter 6

NAT Configurations

6.1 Configuration of the Cork Router

6.1.1 NAT pool configuration

The pool consists of the public network address 200.10.10.64/26. Exclude the first 10 addresses from this pool (to be used for servers when necessary).

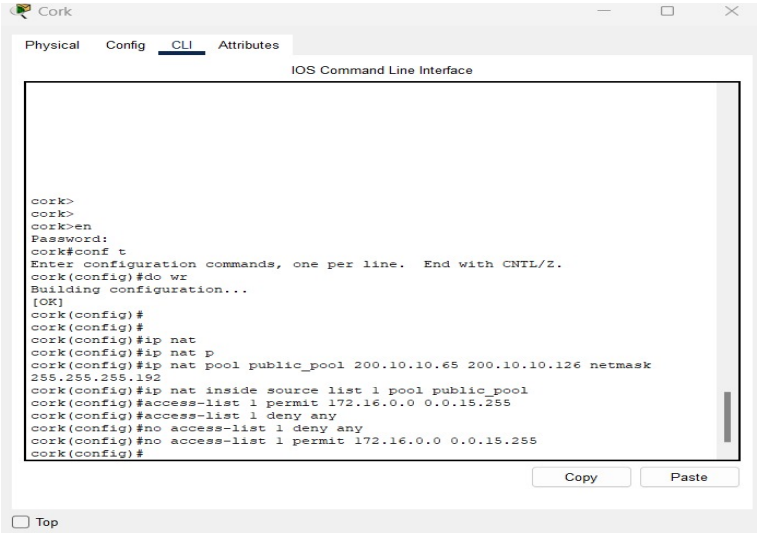

Figure 6.1: NAT pool configuration

6.1.2 Define an Access Control List (ACL)

To define an ACL that will translate all internal addresses (172.16.0.0/20) and deny all other traffic, we can use the following configuration:

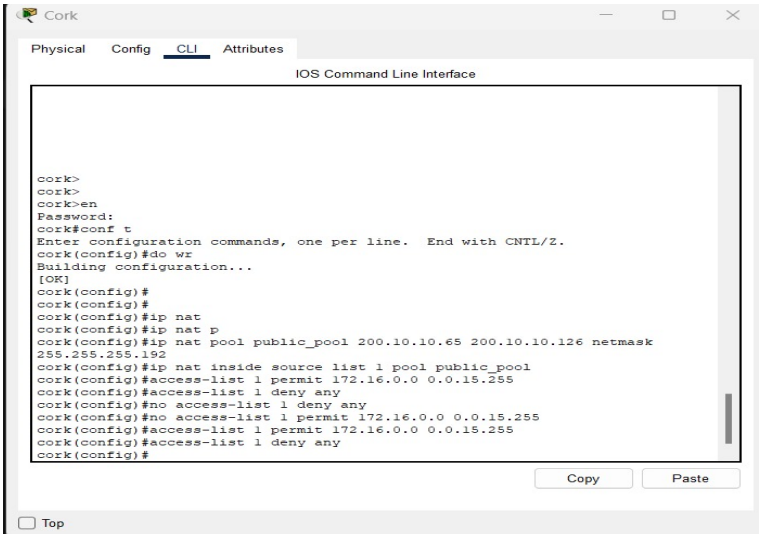

Figure 6.2: Defining the ACL for NAT

6.1.3 Dynamic Source Address Translation (NAT)

This configuration will apply NAT to all traffic from the internal network, translating their source addresses. Any traffic not matching the ACL will be denied.

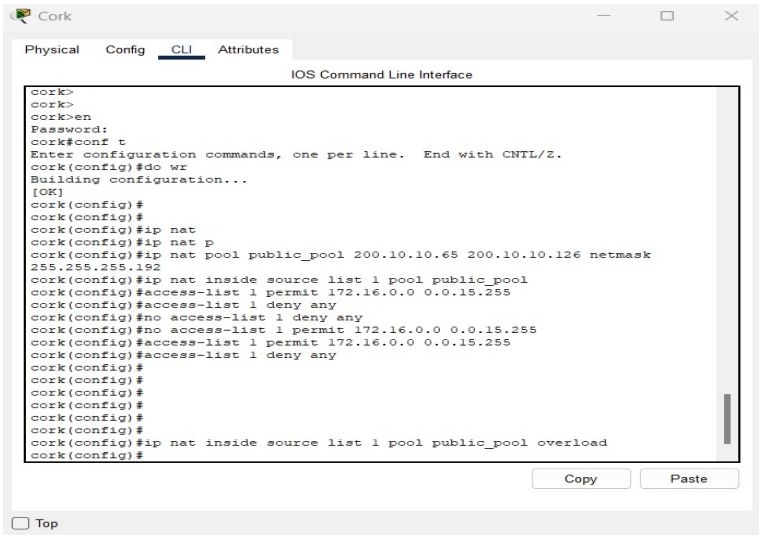

Figure 6.3: Configuring dynamic source NAT with an ACL

6.1.4 Specify the internal and external NAT interfaces

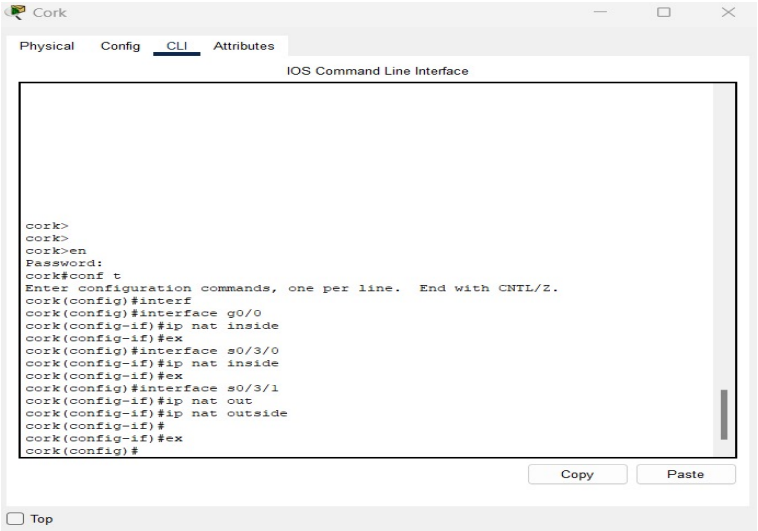

Figure 6.4: Configuring the internal and external NAT interfaces

6.2 Connect a workstation to port Fa0/0 of Belfast to simulate an ISP server

Configure this workstation as follows:

- Configure the IP address
- The subnet mask as 10.0.0.4/29
- Configure the default gateway

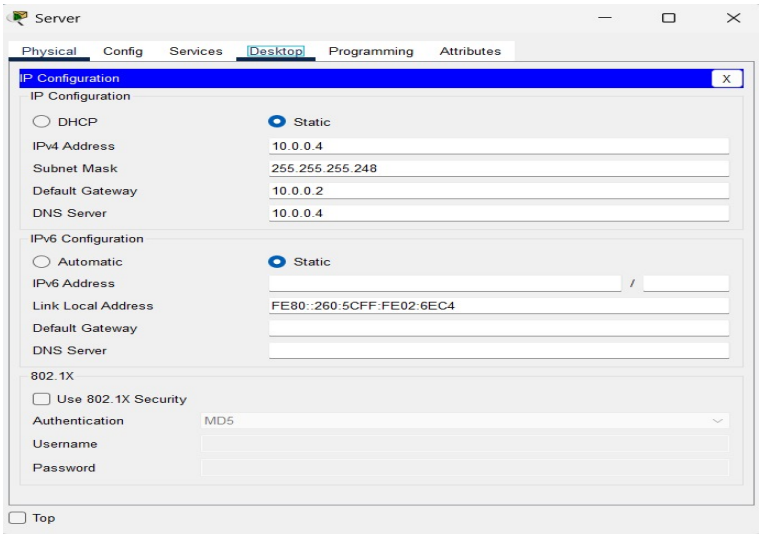

Figure 6.5: Connecting a workstation to simulate an ISP server

6.3 Configure the workstation to act as a web server

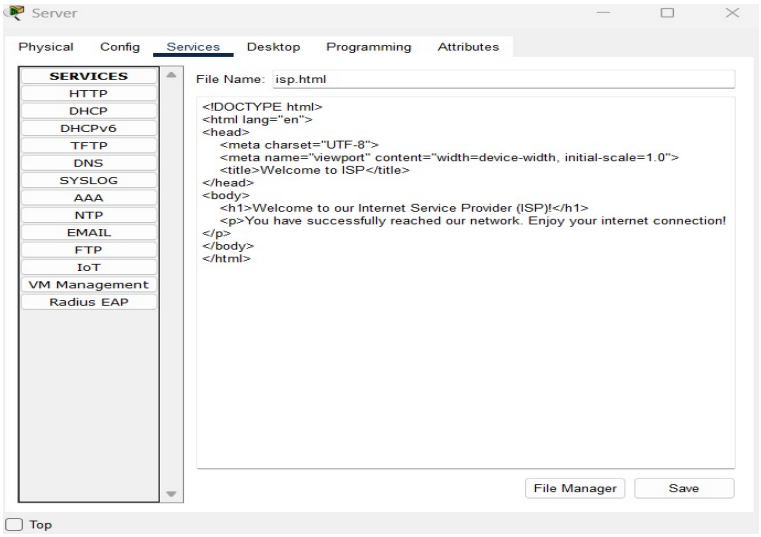

Figure 6.6: Configuring the workstation to act as a web server

Chapter 7

Verification and Testing

7.1 Verify communication between the different hosts on the network

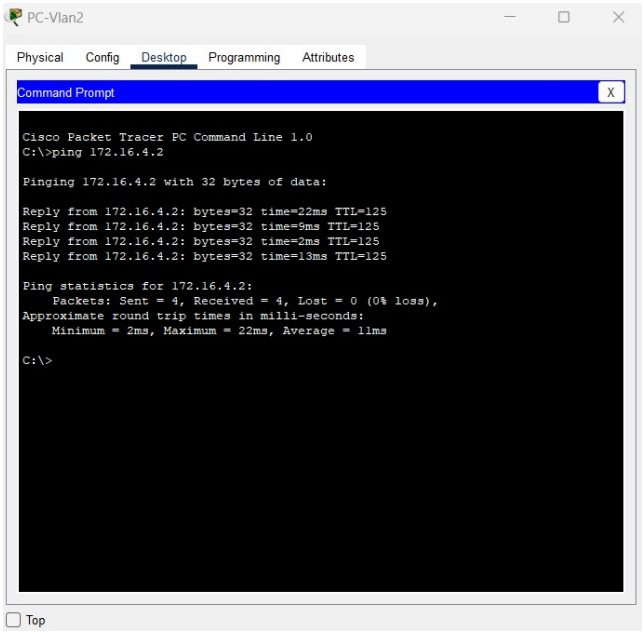

Figure 7.1: Ping between a station in VLAN 2 and a station in the Galway network

Figure 7.2: Ping between different stations across the network