FAKULTI TEKNOLOGI DAN KEJURUTERAAN ELEKTRONIK DAN KOMPUTER

BERL 2143

NETWORK SECURITY IMPLEMENTATION SEM 1 2024/2025

Prepared by:

MUHAMMAD AZRUL BIN REDZUAN

<B122310626>

Program:

BACHELOR OF TECHNOLOGY IN INDUSTRIAL ELECTRONICS WITH HONOURS (BERL)

1. INTRODUCTION

This report presents the configuration and implementation of a network topology based on the specifications provided in Table 1. The main objectives of this project are to design and configure a secure and synchronized network that includes NTP authentication, SSH remote management, access control policies, and OSPF routing with MD5 authentication.

Cisco Packet Tracer version 7.3 or later is used to simulate the network. The topology consists of three routers (R-Secondary, R-Tertiary, and R-Prime), three switches (S1, S2, and S3), three servers (Server-Secondary, Server-Tertiary, and Server-Prime), and three PCs (PC-Secondary, PC-Tertiary, and PC-Prime).

2. OBJECTIVE

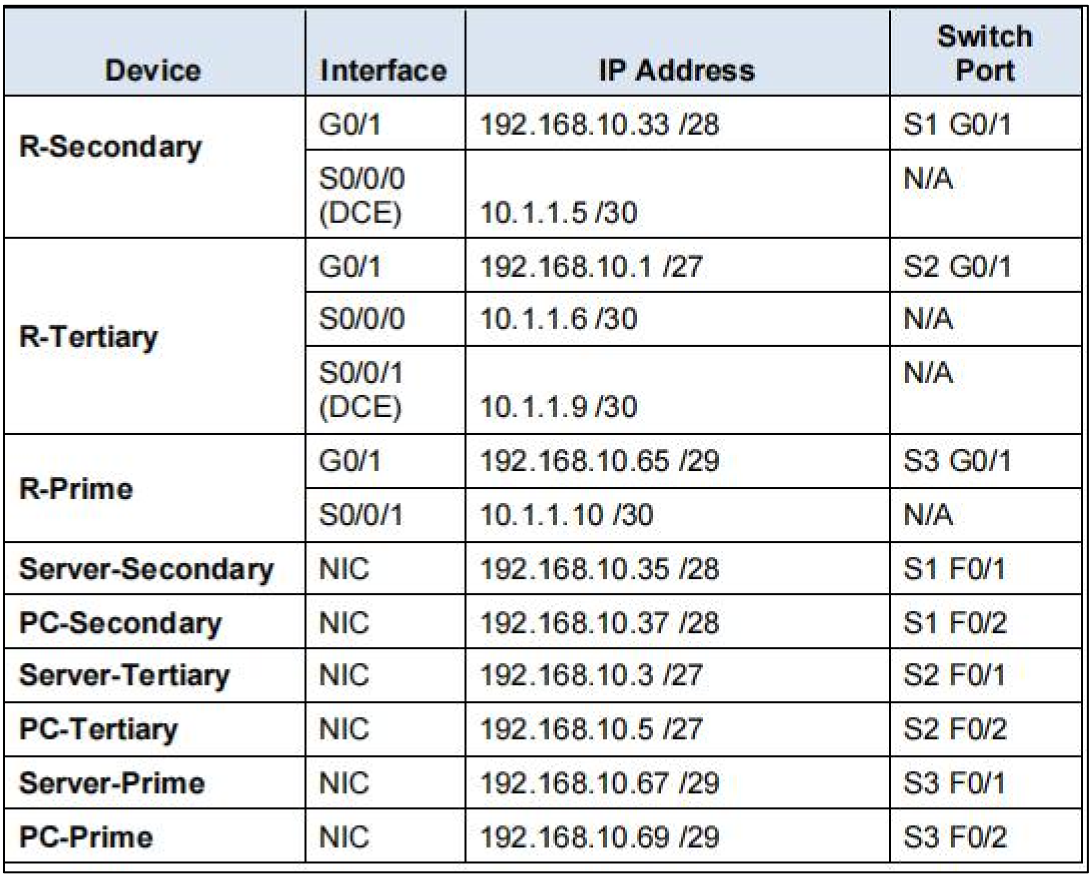
The objectives of this project are as follows:

i. To construct a network topology diagram based on the given IP addressing scheme.
ii. To configure NTP authentication between the Server-Prime and all routers.
iii. To synchronize the routers' software and hardware clocks with the NTP Server.
iv. To enable remote management access via SSH version 2 on R-Prime.
v. To implement access control policies allowing only web access from PC-Secondary to Server-Tertiary.
vi. To configure OSPF routing with MD5 authentication for secure routing updates.
vii. To verify network connectivity according to the given requirements.

3. EQUIPMENT USED

Device Type	**Model / Description**
Routers	Cisco 2911 with HWIC-2T Module
Switches	Cisco 2960
PCs and Servers	Generic PCs and Servers
Simulation Software	Cisco Packet Tracer 7.3 or newer
Cables	Ethernet and Serial cables

4. ADDRESSING TABLE



Device	Interface	IP Address	Switch Port
R-Secondary	G0/1	192.168.10.33 /28	S1 G0/1
	S0/0/0 (DCE)	10.1.1.5 /30	N/A
R-Tertiary	G0/1	192.168.10.1 /27	S2 G0/1
	S0/0/0	10.1.1.6 /30	N/A
	S0/0/1 (DCE)	10.1.1.9 /30	N/A
R-Prime	G0/1	192.168.10.65 /29	S3 G0/1
	S0/0/1	10.1.1.10 /30	N/A
Server-Secondary	NIC	192.168.10.35 /28	S1 F0/1
PC-Secondary	NIC	192.168.10.37 /28	S1 F0/2
Server-Tertiary	NIC	192.168.10.3 /27	S2 F0/1
PC-Tertiary	NIC	192.168.10.5 /27	S2 F0/2
Server-Prime	NIC	192.168.10.67 /29	S3 F0/1
PC-Prime	NIC	192.168.10.69 /29	S3 F0/2

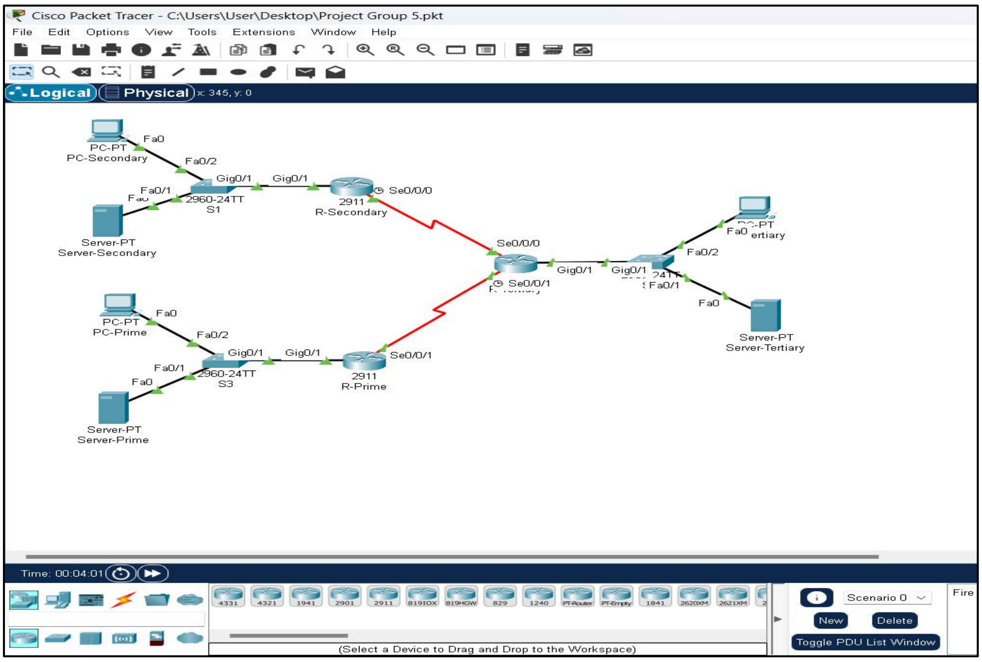
5. NETWORK TOPOLOGY

The network topology consists of three main segments, each connected through serial interfaces between routers. Each router connects to a local switch, which serves the corresponding PCs and servers.

Router Interconnections

R-Secondary ↔ R-Tertiary (Serial 10.1.1.5 /30 ↔ 10.1.1.6 /30)

R-Tertiary ↔ R-Prime (Serial 10.1.1.9 /30 ↔ 10.1.1.10 /30)



Router	Interface	IP Address / Subnet	Connected Devices
R-Secondary	G0/1	192.168.10.33 /28	Server-Secondary, PC-Secondary
R-Tertiary	G0/1	192.168.10.1 /27	Server-Tertiary, PC-Tertiary
R-Prime	G0/1	192.168.10.65 /29	Server-Prime, PC-Prime

6. BASIC ROUTER CONFIGURATION

Each router is configured with the following basic settings:

Hostname: R-Secondary, R-Tertiary, R-Prime

Banner: “Only <Group Number> is allowed to access!”

Console password: AssignCon

Privileged EXEC password: AssignEn

VTY password: AssignVty

6. Network Time Protocol (NTP) Configuration

NTP Authentication Key: 1

Password: Assignntp

NTP Server: Server-Prime (192.168.10.67)

All routers are configured to:

i. Authenticate the NTP source using key 1.
ii. Synchronize the **software clock** with the NTP server.
iii. Periodically update the **hardware clock** from the NTP time.

7. SSH Remote Management Configuration (R-Prime)

R-Prime is configured for secure remote management using **SSH version 2**.

Domain name: AAA.com

Username: AdminAAA

Password: AssignPass (encrypted)

RSA key modulus: 1024 bits

Access method: SSH only (Telnet disabled)

This allows administrators to access R-Prime securely using an encrypted connection.

8. Access Control Policy Configuration

Access Control Lists (ACLs) are implemented to meet the specified network access rules:

Requirement	**Description**
1. Web Access	Only HTTP (port 80) from PC-Secondary (192.168.10.37) to Server-Tertiary (192.168.10.3) is permitted.
2. FTP Access	Not permitted from PC-Secondary to Server-Tertiary.
3. ICMP (Ping)	Allowed from PC-Secondary to Server-Tertiary, but denied between Server-Prime and PC-Secondary.

These rules ensure secure and controlled communication across the network.

9. OSPF Routing Configuration

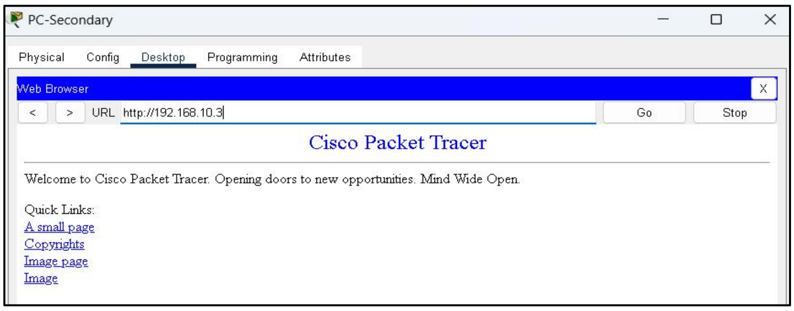
The OSPF routing protocol is implemented across all routers to enable dynamic routing between networks.

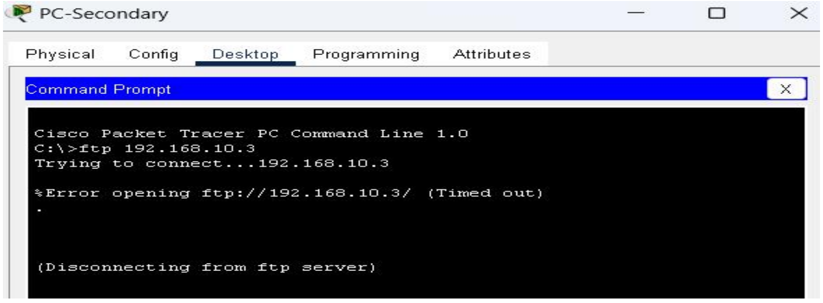
Routing Protocol	**OSPF**
Process ID	1
Authentication Type	MD5
Key ID	1
Password	Assignmd5

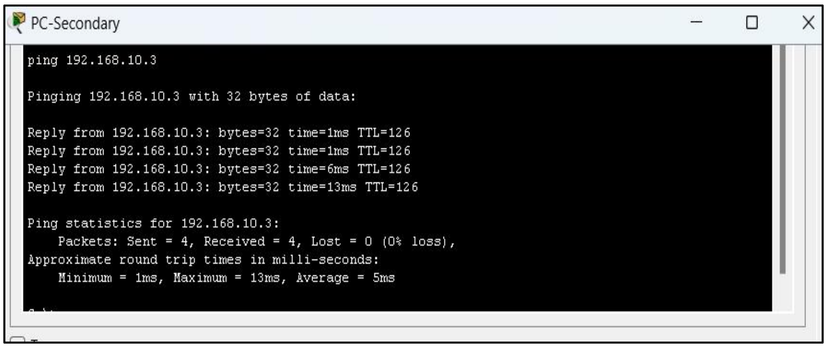
Each router advertises its directly connected networks, and MD5 authentication ensures that only authorized routers can exchange routing updates.

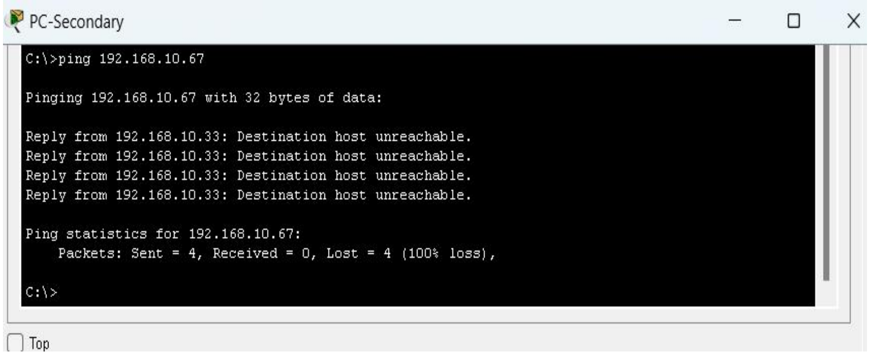
10. Verification Tests

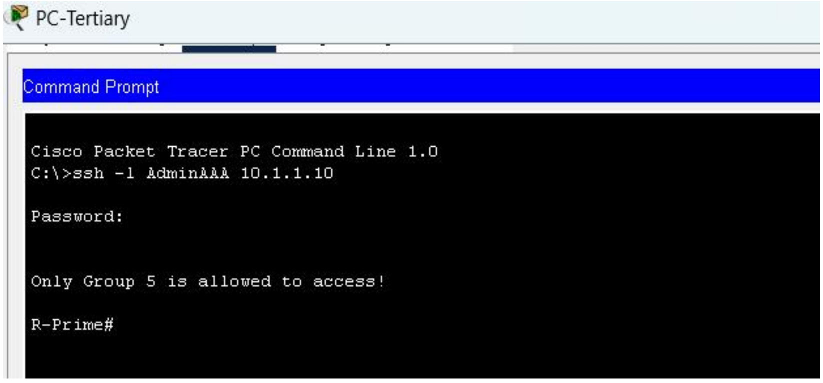
After configuration, the following connectivity tests are performed to verify the system:

Test Description	Expected Result
1. Web access from PC-Secondary to Server-Tertiary	SUCCESS  PC-Secondary Physical Config Desktop Programming Attributes Web Browser URL http://192.168.10.3 Go Stop Cisco Packet Tracer Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open. Quick Links: A small page Copyrights Image page Image

2. FTP access from PC-Secondary to Server-Tertiary	FAIL
	
	PC-Secondary
	Physical Config Desktop Programming Attributes
	Command Prompt
	`Cisco Packet Tracer PC Command Line 1.0`
	`C:\>ftp 192.168.10.3`
	`Trying to connect...192.168.10.3`
	`%Error opening ftp://192.168.10.3/ (Timed out)`
	`.`
	`(Disconnecting from ftp server)`

3. Ping from PC-Secondary to Server-Tertiary	SUCCESS
	
	PC-Secondary
	`ping 192.168.10.3`
	`Pinging 192.168.10.3 with 32 bytes of data:`
	`Reply from 192.168.10.3: bytes=32 time=1ms TTL=126`
	`Reply from 192.168.10.3: bytes=32 time=1ms TTL=126`
	`Reply from 192.168.10.3: bytes=32 time=6ms TTL=126`
	`Reply from 192.168.10.3: bytes=32 time=13ms TTL=126`
	`Ping statistics for 192.168.10.3:`
	`    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),`
	`Approximate round trip times in milli-seconds:`
	`    Minimum = 1ms, Maximum = 13ms, Average = 5ms`

4. Ping from PC-Secondary to Server-Prime	FAIL
	
	PC-Secondary
	`C:\>ping 192.168.10.67`
	`Pinging 192.168.10.67 with 32 bytes of data:`
	`Reply from 192.168.10.33: Destination host unreachable.`
	`Reply from 192.168.10.33: Destination host unreachable.`
	`Reply from 192.168.10.33: Destination host unreachable.`
	`Reply from 192.168.10.33: Destination host unreachable.`
	`Ping statistics for 192.168.10.67:`
	`    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),`
	`C:\>`
	□ Top

5. SSH access from PC-MITC to R-Prime	SUCCESS 

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l AdminAAA 10.1.1.10

Password:


Only Group 5 is allowed to access!

R-Prime#
```

11. Conclusion

The network topology was successfully designed and configured according to the given requirements.

The implementation included:

i. NTP authentication and synchronization,
ii. Secure SSH remote access,
iii. ACL-based traffic control,
iv. OSPF routing with MD5 authentication for security.

All configurations were verified through connectivity tests, confirming that the system operates according to the specified access and routing policies.