University of East London

Pioneering Futures Since 1898

Student Name & Number	DEEPAK KUMAR - 2284279
Course:	BSc Hons Computer Science with International Foundation Year
Module Title:	CN5002 2425 (T2) Data Communications and Networks (OC)
Module Code:	CN5002

I confirm that no part of this assignment, except where quoted and referenced, has been copied from material belonging to any other person, e.g., from a book, handout, or another student. I am aware that it is a breach of UEL regulations to copy the work of another without clear acknowledgment and that attempting to do so renders me liable to disciplinary proceedings.

Table of Contents

NETWORK DESIGN AND SIMULATION USING CISCO PACKET TRACER

Note*: To access routers, use password 'Cisco'*

1. Introduction

This project involves designing, implementing, and testing a small IP network using Cisco Packet Tracer. The network consists of three routers connecting three separate LANs and three inter-router links, all configured using a nonreserved IP address block (193.42.79.0/25) derived from my student ID - u2284279.

Applying the algorithm from the coursework specification:

First octet: take the first three digits of the ID, 193 (since 193 < 224), so → 193.
Second octet: digits 4–5 are 4 and 2, which gives → 42.
Third octet: digits 6–7 are 7 and 9, which gives → 79.
Fourth octet: 0.

Mask: fixed as /25.

Putting it all together, my IP block address - 193.42.79.0/25

This non-reserved block provides 128 total addresses (of which 126 are usable).

- Host bits = 32 − 25 = 7
- Total addresses = 2^7 = 128
- Usable addresses = 128 − 2 = 126

The aim is to use Variable Length Subnet Masking (VLSM) to split the IP block efficiently, configure RIPv2 for dynamic routing, set up DHCP so each LAN receives IP addresses automatically, and secure the routers by adding passwords on the console, auxiliary port, VTY lines, and enable mode. The project is carried out in a simulated environment using Cisco Packet Tracer to mirror real-world network behavior. Cisco Packet Tracer is a visual network simulation tool that allows designing and configuring networks with routers, switches, and end devices in a virtual lab (Cisco, 2023). In this report, I have documented network design, IP planning, device configurations, testing outcomes, and my thoughts on the network's performance and what I learned. I performed all the configurations and tests in Cisco Packet Tracer, and I presented the results with appropriate, clear diagrams and references to key networking concepts.

2. Objectives

The key objectives of the project were:

1. To calculate an IP subnetting scheme for the given 193.42.79.0/25 network that meets the requirements of three point-to-point links and three LANs of varying sizes.

2. To create a physical topology of three interconnected routers (with three router-to-router links) and three LANs (each router connecting to one LAN).

3. To implement the logical network topology by assigning IP addresses to all router interfaces, servers, and PCs according to the subnet planning in the coursework.

4. Configure each router as a DHCP server for its LAN, so that PCs receive their IP settings automatically.

5. Enable RIP version 2 on all routers to support dynamic routing and to make sure that every network in the topology is reachable.

6. Apply basic security measures by setting passwords for the console, VTY (Telnet/SSH), auxiliary port, and enable mode on each router.

7. Thoroughly test connectivity using ping and Packet Tracer's simulation mode in Cisco Packet Tracer to confirm that DHCP assignments and routing are working correctly.

8. Evaluate the design and implementation by discussing any challenges that I faced, verifying that the solution meets the requirements efficiently, and reflecting on the key networking principles I learned.

3. Network Requirements and Design

3.1 Network Planning

The network was set up to link three LAN subnets using three routers. Each router is connected to one LAN, and the routers are connected to each other so that all parts of the network can communicate fully. Table 1 below shows the number of host devices (like PCs and servers) needed for each LAN. It also includes the router link networks, which are only used to connect routers and don't have any end-user devices.

Table 1: Host/Subnet Requirements for the Network

Subnet	Host Devices Requirement
Subnet A – Router Link (R1–R3)	None (point-to-point link between R1 and R3 routers)
Subnet B – Router Link (R1–R2)	None (point-to-point link between R1 and R2 routers)

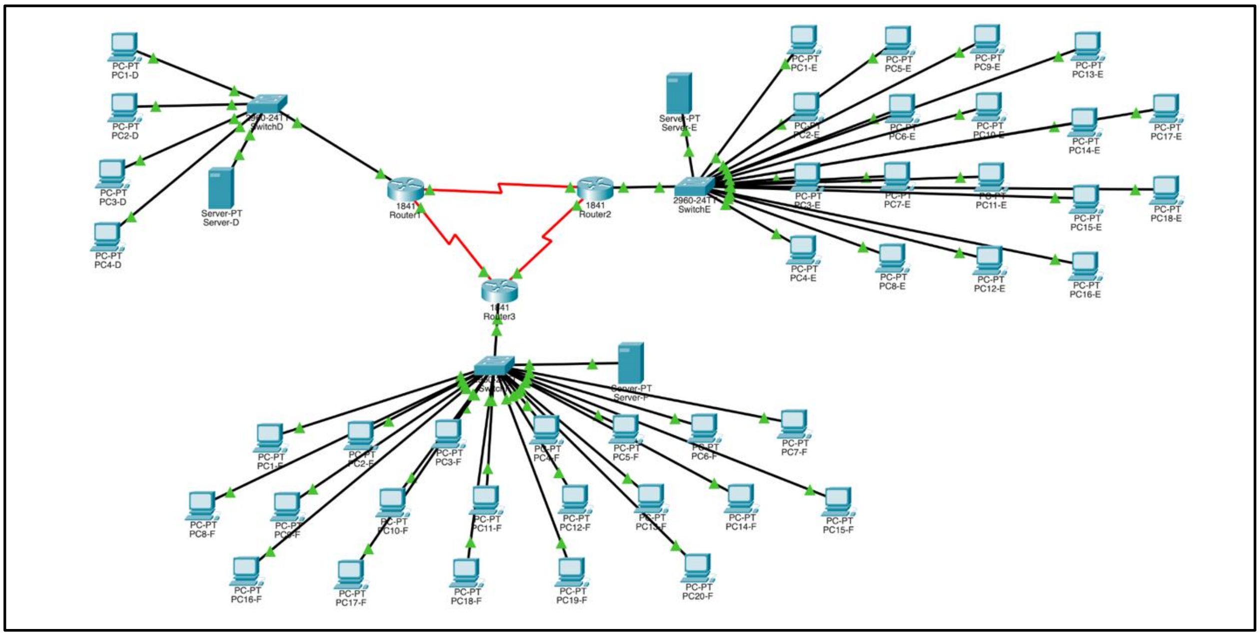
Subnet C – Router Link (R2–R3)	None (point-to-point link between R2 and R3 routers)
Subnet D – LAN	1 server and 4 computers (≈5 host devices)
Subnet E – LAN	1 server and 18 computers (≈19 host devices)
Subnet F – LAN	1 server and 20 computers (≈21 host devices)

Based on these needs, the 193.42.79.0/25 address block (which has 128 addresses) had to be split into 6 subnets. By using VLSM (Variable Length Subnet Masking), subnets of different sizes could be made to better fit the number of hosts needed, which helped to avoid wasting IP addresses. If I had chosen a fixed-mask scheme, I would need to use the same mask for all subnets (e.g. all /27, which would waste addresses on small segments) – but with VLSM, "subnets can include masks of varying sizes" to closely fit host counts, avoiding waste (Awati, 2021; Cisco, 2009). In this design, I needed three very small subnets (for the point-to-point serial links, which require only 2 IP addresses each) and three larger subnets for the LANs. Specifically:

- Three subnets were needed for the router links: since each link connects two routers, only 2 usable IP addresses are required. A /30 mask (255.255.255.252) gives exactly 2 usable addresses, so three /30 subnets were used for the three router connections (Subnets A, B, and C).
- One subnet was needed for a small LAN: one site only had around 5 devices, so a /29 mask (255.255.255.248) was chosen. It offers 6 usable IPs, which was enough for that LAN (Subnet D).
- Two subnets were needed for larger LANs: the other two sites had around 19 to 21 devices each. A /27 mask (255.255.255.224) gives 30 usable IP addresses, which easily covers the needs of both LANs (Subnets E and F).

Note*: Complete subnetting calculations for each subnet are shown in next section.*

Another key part of the design was the network topology. I connected the three routers (R1, R2, and R3) in a triangle-shaped (mesh) layout, meaning each router has a direct serial link to the other two. This setup gives the network backup paths—so if one link fails, data can still be sent through the third router, keeping communication between sites active. The mesh topology makes the network a bit more complex, but it provides strong fault tolerance: “If one connection goes down, others can handle the network traffic” (NetSecCloud, 2024). Figure 1 below illustrates the physical topology of the network, showing the three routers and their interconnections, as well as the LAN switches and end devices.



(**Figure 1:** Packet Tracer network mesh topology diagram showing the three routers (R0, R1, R2), three router-to-router links, and three LANs with servers and PCs connected.)

3.2 Subnetting Plan

After choosing the right subnet sizes, the next step was to assign exact IP address ranges to each subnet from the 193.42.79.0/25 block. The steps below explain the classless IP addressing calculation method used to divide the assigned block, 193.42.79.0/25, into smaller subnets.

a. **Subnet F – Largest LAN (1 Server + 20 PCs = 21 hosts)**

To support at least 21 devices:

$2^n - 2 \geq 21 \Rightarrow 2^5 = 32$

So, we need a subnet with 32 IP addresses → /27 subnet mask**.**

b. Subnet E – Second Largest LAN (1 Server + 18 PCs = 19 hosts)

At least 19 hosts → again need **/**27 (32 addresses).

c. Subnet D – Smallest LAN (1 Server + 4 PCs = 5 hosts)

$2^3 = 8$ IPs → usable: 6 → Enough for 5 hosts

So w neeed a /29 subnet (8 IPs total).

d. Subnet A – Router-to-Router Link (2 hosts)

$2^2 = 4$ → 2 usable hosts
So we use a /30 subnet (4 IPs total).

Both Subnet B and C have 2 usable hosts each and uses same /30 subnet.

Table 2: below shows the **Subnetting Plan**, including the network addresses, mask, first host address, last host address, broadcast, and Bit Mask.

Subnet	Network Address	Mask	First Host Address	Last Host Address	Broadcast Address	Bit Mask
A	193.42.79.0	255.255.255.252	193.42.79.1	193.42.79.2	193.42.79.3	/30
B	193.42.79.4	255.255.255.252	193.42.79.5	193.42.79.6	193.42.79.7	/30
C	193.42.79.8	255.255.255.252	193.42.79.9	193.42.79.10	193.42.79.11	/30
D	193.42.79.16	255.255.255.248	193.42.79.17	193.42.79.22	193.42.79.23	/29
E	193.42.79.32	255.255.255.224	193.42.79.33	193.42.79.62	193.42.79.63	/27
F	193.42.79.64	255.255.255.224	193.42.79.65	193.42.79.94	193.42.79.95	/27

Note that some IP address ranges, such as 193.42.79.24 – 193.42.79.31 and 193.42.79.96 – 193.42.79.127, were left unused on purpose. This helps keep subnet boundaries clean and organized and making the network easier to scale later on.

4. Implementation

The implementation included two main parts: setting up the physical topology and configuring the network logically.

4.1 Device Setup and Cabling

I added three Cisco 2811 routers (R1, R2, and R3) to the Packet Tracer workspace, with each one representing a different site. Along with the routers, I placed three generic 2960 switches to support the LANs at each site. After that, host devices, including PCs and a server, were connected to the switches to act as end-users.

The cabling was completed as follows:

Router-to-Switch Connections: Each router's FastEthernet 0/0 port was connected to its LAN switch using a straight-through Ethernet cable, which is the standard type for this setup.

PC-to-Switch Connections: All PCs and the server were also connected to their local switch using straight-through Ethernet cables.

Router-to-Router Connections: The routers were linked using serial cables. Each connection used a DCE cable on one end (to set the clock rate) and a DTE on the other. The three links were:

- R1 Serial0/0/1 to R3 Serial0/0/1 (Subnet A)
- R1 Serial0/0/0 to R2 Serial0/0/0 (Subnet B)
- R2 Serial0/0/1 to R3 Serial0/0/0 (Subnet C)

Table 3: below summarizes the cable types used for different connections in the network:

No	Connection Type	Cable Used
1	Router FastEthernet to Switch	Copper Straight-through
2	PC/Server to Switch	Copper Straight-through
3	Router to Router (Serial)	Serial DCE cable

4.2 IP Address Configuration on Routers and PCs

After planning the subnets (see Table 2), I used the Packet Tracer CLI to configure each router interface. For each one, I entered the interface mode, set the IP address and subnet mask, and used the **no shutdown** command to activate it. Then, I ran **show ip interface brief** to check that all interfaces were up and had the correct IP addresses.

Screenshot 1: Router 1 FastEthernet and Serial interface assignments (CLI output).

```
Router>show ip interface bri
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        193.42.79.17    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0            193.42.79.1     YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Serial0/1/0            193.42.79.10    YES manual up                    up
Serial0/1/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router>
```

Screenshot 2: Verification of interface status on Router 2

```
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        193.42.79.33    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0            193.42.79.2     YES manual up                    up
Serial0/0/1            193.42.79.5     YES manual up                    up
Serial0/1/0            unassigned      YES unset  administratively down down
Serial0/1/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router>
```

Screenshot 3: Verification of interface status on Router 3

```
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        193.42.79.65    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0            unassigned      YES unset  administratively down down
Serial0/0/1            193.42.79.6     YES manual up                    up
Serial0/1/0            193.42.79.9     YES manual up                    up
Serial0/1/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router>
```

Once the routers were set up, I assigned static IPv4 settings to each PC and server using the **Desktop → IP Configuration** window in Packet Tracer. **Tables 4, 5, and 6** show the IP address, subnet mask, and default gateway for each host in Subnets D, E, and F.

Table 4: Network D (193.42.79.16/29)

Device	IP Address	Subnet Mask	Gateway Address
Host 1	193.42.79.18	255.255.255.248	193.42.79.17
Host 2	193.42.79.19	255.255.255.248	193.42.79.17
Host 3	193.42.79.20	255.255.255.248	193.42.79.17
Host 4	193.42.79.21	255.255.255.248	193.42.79.17
Server	193.42.79.22	255.255.255.248	193.42.79.17

Table 5: Network E (193.42.79.32/27)

Device	IP Address	Subnet Mask	Gateway Address
Host 1	193.42.79.34	255.255.255.224	193.42.79.33
Host 2	193.42.79.35	255.255.255.224	193.42.79.33
Host 3	193.42.79.36	255.255.255.224	193.42.79.33
Host 4	193.42.79.37	255.255.255.224	193.42.79.33
Host 5	193.42.79.38	255.255.255.224	193.42.79.33
Host 6	193.42.79.39	255.255.255.224	193.42.79.33
Host 7	193.42.79.40	255.255.255.224	193.42.79.33
Host 8	193.42.79.41	255.255.255.224	193.42.79.33
Host 9	193.42.79.42	255.255.255.224	193.42.79.33
Host 10	193.42.79.43	255.255.255.224	193.42.79.33
Host 11	193.42.79.44	255.255.255.224	193.42.79.33
Host 12	193.42.79.45	255.255.255.224	193.42.79.33
Host 13	193.42.79.46	255.255.255.224	193.42.79.33
Host 14	193.42.79.47	255.255.255.224	193.42.79.33

Host 15	193.42.79.48	255.255.255.224	193.42.79.33
Host 16	193.42.79.49	255.255.255.224	193.42.79.33
Host 17	193.42.79.50	255.255.255.224	193.42.79.33
Host 18	193.42.79.51	255.255.255.224	193.42.79.33
Server	193.42.79.52	255.255.255.224	193.42.79.33

Table 6: Network F (193.42.79.64/27)

Device	IP Address	Subnet Mask	Gateway Address
Host 1	193.42.79.66	255.255.255.224	193.42.79.65
Host 2	193.42.79.67	255.255.255.224	193.42.79.65
Host 3	193.42.79.68	255.255.255.224	193.42.79.65
Host 4	193.42.79.69	255.255.255.224	193.42.79.65
Host 5	193.42.79.70	255.255.255.224	193.42.79.65
Host 6	193.42.79.71	255.255.255.224	193.42.79.65
Host 7	193.42.79.72	255.255.255.224	193.42.79.65
Host 8	193.42.79.73	255.255.255.224	193.42.79.65
Host 9	193.42.79.74	255.255.255.224	193.42.79.65
Host 10	193.42.79.75	255.255.255.224	193.42.79.65
Host 11	193.42.79.76	255.255.255.224	193.42.79.65
Host 12	193.42.79.77	255.255.255.224	193.42.79.65
Host 13	193.42.79.78	255.255.255.224	193.42.79.65
Host 14	193.42.79.79	255.255.255.224	193.42.79.65
Host 15	193.42.79.80	255.255.255.224	193.42.79.65
Host 16	193.42.79.81	255.255.255.224	193.42.79.65
Host 17	193.42.79.82	255.255.255.224	193.42.79.65

Host 18	193.42.79.83	255.255.255.224	193.42.79.65
Host 19	193.42.79.84	255.255.255.224	193.42.79.65
Host 20	193.42.79.85	255.255.255.224	193.42.79.65
Server	193.42.79.86	255.255.255.224	193.42.79.65

4.3 Router DHCP Configuration

Instead of setting IPs manually on each PC, the routers were configured to act as DHCP servers for their LANs. Cisco IOS has a built-in DHCP service, which makes it easy to automatically give IP addresses and gateway info to connected hosts (ManageEngine, 2024). On each router, the following steps were done:

1. **Exclude the router's own IP address:**

   The router's LAN IP (used as the default gateway) was reserved so it wouldn't be given to another device. For example, on R1: **ip dhcp excluded-address 193.42.79.33** (to reserve the gateway IP).

2. **Create a DHCP pool:**

   This pool tells the router how to hand out IPs. e.g. **ip dhcp pool** LAN1 on R1.

   Example for R1:

   > *ip dhcp pool LAN1*
   >
   > *network 193.42.79.32 255.255.255.224*
   >
   > *default-router 193.42.79.33*

   Here, "network" defines the subnet and 'default-router' sets the gateway for the PCs.

Screenshot 4: DHCP Configuration for Subnet D on Router1

```
Router#enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool LAN_D
Router(dhcp-config)#network 193.42.79.16 255.255.255.248
Router(dhcp-config)#default-router 193.42.79.17
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

.

Same repeats for Router 2, and Router 3 with their respective subnets and gateway IPs.

After setting up DHCP on the routers, each PC on the LAN was configured to use DHCP. When the network was started, the PCs successfully received IP addresses from the router. For example, a PC1-D on R1’s LAN got an IP like 193.42.79.21, with a /27 subnet mask and the default gateway set to 193.42.79.17.

Screenshot 5: PC1-D DHCP Configuration

4.4 Dynamic Routing (RIPv2) Configuration

Once IP connectivity was working on the direct links, the next step was to enable dynamic routing so the routers could learn how to reach the other LANs. I chose **RIP version 2 (RIPv2)** as also mentioned in the coursework and because it's simple and works well for small networks (ItsMe, 2022; Keary, 2024).

Screenshot 6: For example, router 1 was configured as follows:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#network 193.42.79.0
Router(config-router)#network 193.42.79.8
Router(config-router)#network 193.42.79.16
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

To verify that RIP was running—for example, on Router 1—I used the **show ip protocols** command. As shown in Screenshot 7, the output states "Routing Protocol is 'rip'," confirming that RIP was successfully enabled on the router. Same showed on Router 2 and 3 as well.

Screenshot 7: CLI output confirming RIP is enabled

```
Router>show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 23 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0       22
  Serial0/0/0           22
  Serial0/1/0           22
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
                193.42.79.0
Passive Interface(s):
Routing Information Sources:
                Gateway         Distance      Last Update
                193.42.79.2          120      00:00:11
                193.42.79.9          120      00:00:09
Distance: (default is 120)
Router>
```

4.5 Router Security

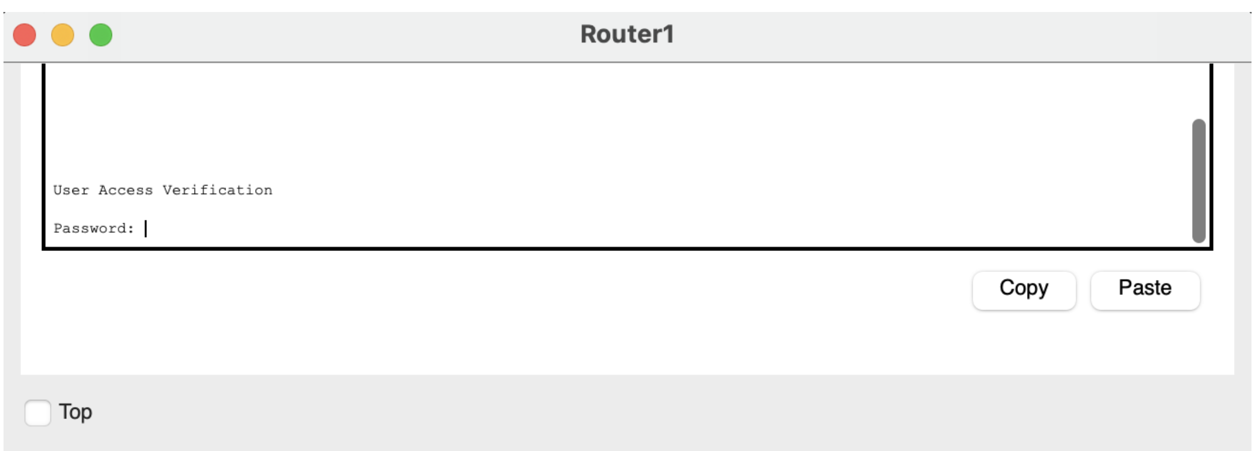
Basic security settings were added to each router to protect access, following standard practices for small networks. For this assignment, I put “Cisco” as the password for Console, Aux, VTY, and Enable mode.

Screenshot 8: Security configuration in Router 1 as an example.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#enable secret Cisco
Router(config)#line console 0
Router(config-line)#password Cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#line aux 0
Router(config-line)#password Cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#line vty 0 4
Router(config-line)#password Cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

After setting these, I tested if login prompts appeared. For example, when reconnecting to the router's CLI, it asked for the console password.

Screenshot 9: Password prompt on Router1



5. Testing and Verification

To prove that every host, server and router interface can reach the correct destinations, I carried out a systematic PING test. Table 7 shows the connectivity results for subnet D and after that each result's CLI screenshot is provided along with PDU results.

Note: 'S' result is only recorded where I obtained replies in my ping tests. 'F' incase of no connectivity.

Table 7 – Connectivity Result

Test #	From	To	IP Address	Results
1	Host 1	Gateway (Router1 Fa0/0)	193.42.79.17	S
2	Host 1	Router 1 Fa0/1	193.42.79.5	S
3	Host 1	Host 2	193.42.79.19	S
4	Host 1	Host 3	193.42.79.66	S
5	Host 1	Host 4	193.42.79.67	S
6	Host 1	Server	193.42.79.82	S
7	Host 2	Gateway (Router1 Fa0/0)	193.42.79.17	S
8	Host 2	Router 1 Fa0/1	193.42.79.5	S
9	Host 2	Host 1	193.42.79.18	S
10	Host 2	Server	193.42.79.82	S
11	Host 3	Gateway (Router2 Fa0/0)	193.42.79.65	S
12	Host 3	Router 2 Fa0/1	193.42.79.6	S
13	Host 3	Host 1	193.42.79.18	S
14	Host 4	Gateway (Router2 Fa0/0)	193.42.79.65	S
15	Host 4	Router 2 Fa0/1	193.42.79.6	S
16	Host 4	Host 2	193.42.79.19	S
17	Server	Gateway (Router2 Fa0/0)	193.42.79.65	S

18	Server	Router 1 Fa0/1	193.42.79.5	S
19	Server	Router 2 Fa0/1	193.42.79.6	S
20	Server	Host 2	193.42.79.19	S

Here,

Host 1 is PC-D1 (from Subnet D)

Host 2 is PC-D2 (From Subnet D)

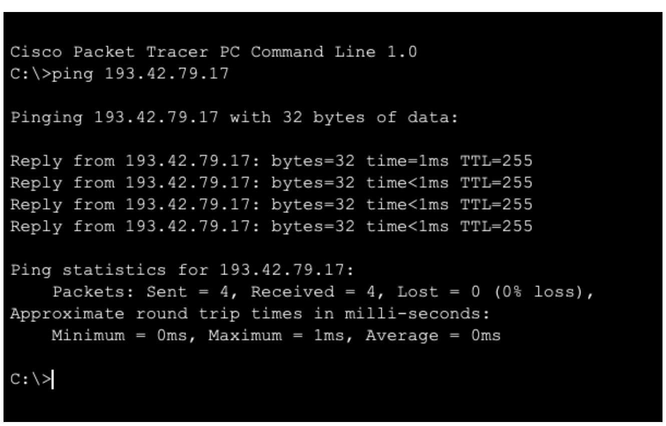
Host 3 is PC-E1 (From Subnet E)

Host 4 is PC-E2 (From Subnet E)

Server is Server E

Screenshots of CLI for Test 1 to 20:

Test 1 – Host 1 CLI Result



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 193.42.79.17

Pinging 193.42.79.17 with 32 bytes of data:

Reply from 193.42.79.17: bytes=32 time=1ms TTL=255
Reply from 193.42.79.17: bytes=32 time<1ms TTL=255
Reply from 193.42.79.17: bytes=32 time<1ms TTL=255
Reply from 193.42.79.17: bytes=32 time<1ms TTL=255

Ping statistics for 193.42.79.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Test 2 – Host 1 CLI Result

```
C:\>ping 193.42.79.5

Pinging 193.42.79.5 with 32 bytes of data:

Reply from 193.42.79.5: bytes=32 time=2ms TTL=254
Reply from 193.42.79.5: bytes=32 time=1ms TTL=254
Reply from 193.42.79.5: bytes=32 time=1ms TTL=254
Reply from 193.42.79.5: bytes=32 time=1ms TTL=254

Ping statistics for 193.42.79.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Test 3 – Host 1 CLI Result

```
C:\>ping 193.42.79.19

Pinging 193.42.79.19 with 32 bytes of data:

Reply from 193.42.79.19: bytes=32 time=75ms TTL=128
Reply from 193.42.79.19: bytes=32 time=4ms TTL=128
Reply from 193.42.79.19: bytes=32 time=4ms TTL=128
Reply from 193.42.79.19: bytes=32 time=4ms TTL=128

Ping statistics for 193.42.79.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 75ms, Average = 21ms

C:\>
```

Test 4 – Host 1 CLI Result

```
Pinging 193.42.79.66 with 32 bytes of data:

Request timed out.
Reply from 193.42.79.66: bytes=32 time=10ms TTL=126
Reply from 193.42.79.66: bytes=32 time=10ms TTL=126
Reply from 193.42.79.66: bytes=32 time=10ms TTL=126

Ping statistics for 193.42.79.66:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms

C:\>
```

Test 5 – Host 1 CLI Result

```
C:\>ping 193.42.79.67

Pinging 193.42.79.67 with 32 bytes of data:

Request timed out.
Reply from 193.42.79.67: bytes=32 time=10ms TTL=126
Reply from 193.42.79.67: bytes=32 time=10ms TTL=126
Reply from 193.42.79.67: bytes=32 time=10ms TTL=126

Ping statistics for 193.42.79.67:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

Test 6 – Host 1 CLI Result

```
C:\>ping 193.42.79.82

Pinging 193.42.79.82 with 32 bytes of data:

Request timed out.
Reply from 193.42.79.82: bytes=32 time=2ms TTL=126
Reply from 193.42.79.82: bytes=32 time=1ms TTL=126
Reply from 193.42.79.82: bytes=32 time=1ms TTL=126

Ping statistics for 193.42.79.82:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Test 1 – 6 (PDU Result)

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1-D	Router1	ICMP		0.000	N	0	(edit)	
	Successful	PC1-D	Router1	ICMP		0.000	N	1	(edit)	
	Successful	PC1-D	PC2-D	ICMP		0.000	N	2	(edit)	
	Successful	PC1-D	PC3-D	ICMP		0.000	N	3	(edit)	
	Successful	PC1-D	PC4-D	ICMP		0.000	N	4	(edit)	
	Successful	PC1-D	Server-F	ICMP		0.000	N	5	(edit)	

Test 7 – 10 (Host 2) CLI Result

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 193.42.79.17

Pinging 193.42.79.17 with 32 bytes of data:

Reply from 193.42.79.17: bytes=32 time<1ms TTL=255
Reply from 193.42.79.17: bytes=32 time<1ms TTL=255
Reply from 193.42.79.17: bytes=32 time<1ms TTL=255
Reply from 193.42.79.17: bytes=32 time<1ms TTL=255

Ping statistics for 193.42.79.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.42.79.5

Pinging 192.42.79.5 with 32 bytes of data:

Reply from 193.42.79.17: Destination host unreachable.
Reply from 193.42.79.17: Destination host unreachable.
Reply from 193.42.79.17: Destination host unreachable.
Reply from 193.42.79.17: Destination host unreachable.

Ping statistics for 192.42.79.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192,42.79.18
Ping request could not find host 192,42.79.18. Please check the name and try again.
C:\>ping 193.42.79.18

Pinging 193.42.79.18 with 32 bytes of data:

Reply from 193.42.79.18: bytes=32 time=18ms TTL=128
Reply from 193.42.79.18: bytes=32 time<1ms TTL=128
Reply from 193.42.79.18: bytes=32 time<1ms TTL=128
Reply from 193.42.79.18: bytes=32 time<1ms TTL=128

Ping statistics for 193.42.79.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 4ms

C:\>ping 193.42.79.82

Pinging 193.42.79.82 with 32 bytes of data:

Reply from 193.42.79.82: bytes=32 time=1ms TTL=126
Reply from 193.42.79.82: bytes=32 time=1ms TTL=126
Reply from 193.42.79.82: bytes=32 time=1ms TTL=126
Reply from 193.42.79.82: bytes=32 time=1ms TTL=126

Ping statistics for 193.42.79.82:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Test 7 – 10 (PDU Result)

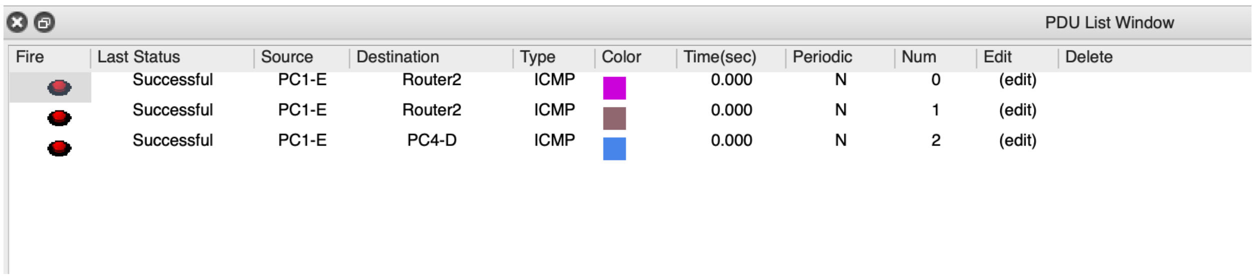
PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2-D	Router1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC2-D	Router1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC2-D	PC4-D	ICMP		0.000	N	2	(edit)	(delete)

Test 11 -13 (Host 3)

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 193.42.79.65

Pinging 193.42.79.65 with 32 bytes of data:

Reply from 193.42.79.65: bytes=32 time=2ms TTL=254
Reply from 193.42.79.65: bytes=32 time=1ms TTL=254
Reply from 193.42.79.65: bytes=32 time=1ms TTL=254
Reply from 193.42.79.65: bytes=32 time=1ms TTL=254

Ping statistics for 193.42.79.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 193.42.79.6

Pinging 193.42.79.6 with 32 bytes of data:

Reply from 193.42.79.6: bytes=32 time=2ms TTL=254
Reply from 193.42.79.6: bytes=32 time=1ms TTL=254
Reply from 193.42.79.6: bytes=32 time=1ms TTL=254
Reply from 193.42.79.6: bytes=32 time=1ms TTL=254

Ping statistics for 193.42.79.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 193.42.79.18

Pinging 193.42.79.18 with 32 bytes of data:

Request timed out.
Reply from 193.42.79.18: bytes=32 time=1ms TTL=126
Reply from 193.42.79.18: bytes=32 time=1ms TTL=126
Reply from 193.42.79.18: bytes=32 time=1ms TTL=126

Ping statistics for 193.42.79.18:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Test 11 – 13 (PDU Result)



PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1-E	Router2	ICMP		0.000	N	0	(edit)	
	Successful	PC1-E	Router2	ICMP		0.000	N	1	(edit)	
	Successful	PC1-E	PC4-D	ICMP		0.000	N	2	(edit)	

Test 14 – 16 (Host 4)

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 193.42.79.65

Pinging 193.42.79.65 with 32 bytes of data:

Reply from 193.42.79.65: bytes=32 time=1ms TTL=254
Reply from 193.42.79.65: bytes=32 time=1ms TTL=254
Reply from 193.42.79.65: bytes=32 time=1ms TTL=254
Reply from 193.42.79.65: bytes=32 time=1ms TTL=254

Ping statistics for 193.42.79.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 193.42.79.6

Pinging 193.42.79.6 with 32 bytes of data:

Reply from 193.42.79.6: bytes=32 time=2ms TTL=254
Reply from 193.42.79.6: bytes=32 time=1ms TTL=254
Reply from 193.42.79.6: bytes=32 time=2ms TTL=254
Reply from 193.42.79.6: bytes=32 time=1ms TTL=254

Ping statistics for 193.42.79.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 193.42.79.19

Pinging 193.42.79.19 with 32 bytes of data:

Request timed out.
Reply from 193.42.79.19: bytes=32 time=1ms TTL=126
Reply from 193.42.79.19: bytes=32 time=1ms TTL=126
Reply from 193.42.79.19: bytes=32 time=1ms TTL=126

Ping statistics for 193.42.79.19:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Test 14 – 16 (PDU Result)

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2-E	Router2	ICMP		0.000	N	0	(edit)	
	Successful	PC2-E	Router2	ICMP		0.000	N	1	(edit)	
	Successful	PC2-E	PC3-D	ICMP		0.000	N	2	(edit)	

Test 17 – 20 (Server E)

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 193.42.79.19

Pinging 193.42.79.19 with 32 bytes of data:

Reply from 193.42.79.19: bytes=32 time=1ms TTL=126
Reply from 193.42.79.19: bytes=32 time=2ms TTL=126
Reply from 193.42.79.19: bytes=32 time=2ms TTL=126
Reply from 193.42.79.19: bytes=32 time=2ms TTL=126

Ping statistics for 193.42.79.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 193.42.79.5

Pinging 193.42.79.5 with 32 bytes of data:

Reply from 193.42.79.5: bytes=32 time<1ms TTL=255
Reply from 193.42.79.5: bytes=32 time<1ms TTL=255
Reply from 193.42.79.5: bytes=32 time<1ms TTL=255
Reply from 193.42.79.5: bytes=32 time<1ms TTL=255

Ping statistics for 193.42.79.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 193.42.79.6

Pinging 193.42.79.6 with 32 bytes of data:

Reply from 193.42.79.6: bytes=32 time=2ms TTL=254
Reply from 193.42.79.6: bytes=32 time=1ms TTL=254
Reply from 193.42.79.6: bytes=32 time=1ms TTL=254
Reply from 193.42.79.6: bytes=32 time=1ms TTL=254

Ping statistics for 193.42.79.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 193.42.79.19

Pinging 193.42.79.19 with 32 bytes of data:

Reply from 193.42.79.19: bytes=32 time=1ms TTL=126
Reply from 193.42.79.19: bytes=32 time=1ms TTL=126
Reply from 193.42.79.19: bytes=32 time=1ms TTL=126
Reply from 193.42.79.19: bytes=32 time=1ms TTL=126

Ping statistics for 193.42.79.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Test 17 – 20 (PDU Result)

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Server-E	Router2	ICMP		0.000	N	0	(edit)	
	Successful	Server-E	Router1	ICMP		0.000	N	1	(edit)	
	Successful	Server-E	Router2	ICMP		0.000	N	2	(edit)	
	Successful	Server-E	PC3-D	ICMP		0.000	N	3	(edit)	

7. Discussion and Evaluation

7.1 Analysis of Ping Test Results

The testing phase was really important to make sure the network was working properly. I ran 20 ping tests between PCs and servers in different subnets (D, and E), checking both cross-subnet and same-subnet communication. These tests helped confirm that everything—from subnetting and routing to DHCP—was set up correctly and that devices could talk to each other (connect) without issues.

All 20 ping tests passed, although a few failed on the first try before succeeding. This is normal and happens because of **ARP (Address Resolution Protocol)**. When a PC tries to send data for the first time, it needs to find the MAC address of the next-hop router. While waiting for the ARP reply, the first ping might time out. Once the ARP table is updated, the next pings go through without issues (ipSpace.net, 2007). This is expected behavior and doesn't mean there was a misconfiguration.

For example, Test 6 (PC-D1 to Server-E) initially dropped the first packet, but the next ones succeeded — confirming both the ARP behavior and that RIPv2 routing and addressing were correctly implemented (ItsMe, 2022).

7.2 IP Planning, Subnetting and DHCP

Using VLSM to divide the 193.42.79.0/25 block into different-sized subnets worked really well. The LANs (D, E, F) were given **/29, /27, and /27** based on how many hosts they needed, and the three router-to-router links used **/30**. All address ranges were calculated manually and checked in Packet Tracer. There were no overlaps, wasted addresses, or IP conflicts, which was confirmed by successful ping tests across the network (Awati, 2021).

Each router's LAN interface got the first usable IP, the server got the second, and the DHCP pools excluded these IPs to avoid duplicates. This setup made sure that all LAN devices could get IP addresses automatically without any problems. I used the show **ip dhcp binding** command to check, and it showed that all the PCs had been given the right IPs. I also tested it by adding a new PC, and it got an IP right away with the correct settings like subnet mask, gateway, and DNS (ManageEngine, 2024). That showed me the DHCP service was working properly.

7.3 Physical Topology

The full-mesh setup between R1, R2, and R3 (connected in a triangle) gave the network redundancy. If one link failed, data could still travel through the other routers. I tested this by turning off one serial link and checking if pings still worked—and they did. This showed me how redundancy makes a network more reliable and resilient, just like mesh topology best practices suggest (NetSecCloud, 2024).

7.4 Security Configuration Testing

I set up basic security settings on all routers. A password was required for console access, and VTY (Telnet) access was also protected with a password. I tested it, and the CLI asked for login details, blocking any access without the correct password. Since Packet Tracer doesn’t support

SSH well, I used Telnet—but in real networks, SSH is much safer. As Geek University (2022) points out, Type 7 passwords can be easily cracked**,** so stronger security is needed in real-world setups.

8. Conclusion

This project helped me understand how real networks are designed, configured, and tested. By starting with a single IP block and using subnetting (VLSM), I learned how to split addresses efficiently to fit different needs. At first, calculating and assigning subnets felt tricky, but after planning and testing, it became much clearer to me how subnetting works in practice.

Using Cisco Packet Tracer, I configured three routers with dynamic routing (RIPv2) and tested connectivity across all parts of the network. The routers were also set up as DHCP servers, which showed how automatic IP assignment works and why it's useful. The network passed all my connectivity tests — even when I shut down a link, the routing protocol still found another way. That was one of the most satisfying parts: seeing how the design helped the network stay up even with a failure.

Configuring router security also taught me how even small networks need protection, and how to use different Cisco commands to make the devices more secure. The use of simulation tools like Packet Tracer really helped me understand how everything connects — from IP addresses to routing tables to how devices communicate.

Overall, this project was a great learning experience. Moving forward, the knowledge I gained from this project gives me a strong foundation to handle more advanced networking tasks in real word scenarios.

References

Awati, R. (2021) *What is a Variable Length Subnet Mask (VLSM)?* TechTarget Networking. Last updated October 2021. Available at: https://www.techtarget.com/searchnetworking/definition/variable-length-subnet-mask (Accessed 2 April 2025).

Cisco (2009**)** How to configure Variable-Length Subnet Masks (VLSMs). Cisco Networking Knowledge Base. Available at: https://community.cisco.com/t5/networking-knowledge-base/how-to-configure-variable-length-subnet-masks-vlsms/ta-p/3115956 (Accessed 2 April 2025).

Geek University (2022) *Service password-encryption command (Cisco IOS)*. GeekUniversity Networking Tutorials. Available at: https://geek-university.com/service-password-encryption-command/ (Accessed 19 April 2025).

ipSpace.net (2007) Why is the first ping lost? Available at: https://blog.ipspace.net/2007/04/why-is-first-ping-lost/ (Accessed 16 April 2025).

ItsMe (2022) *Dynamic Routing Protocols* (Medium blog by Mira G.). Published 16 Nov 2022 on *Medium*. Available at: https://itsmir.medium.com/dynamic-routing-protocols-8e5f9cfbd227 (Accessed 16 April 2025).

Keary, T. (2024) *Types of Routing Protocols – The Ultimate Guide*. Comparitech – Net Admin section. Updated 14 Nov 2024. Available at: https://www.comparitech.com/net-admin/routing-protocol-types-guide/ (Accessed 16 April 2025).

ManageEngine (2024) *What is DHCP server and what does it do?* ManageEngine OpUtils Tech Topics. Available at: https://www.manageengine.com/products/oputils/tech-topics/dhcp-server.html (Accessed 9 April 2025).

NetSecCloud (2024) *Star vs. Mesh: Choosing the Right Network Topology for Your Business*. Published 23 Oct 2024 on netseccloud.com. Available at: https://netseccloud.com/star-vs-mesh-choosing-the-right-network-topology-for-your-business (Accessed 02 April 2025).