



SEPTEMBER 2025

TFB2043

INFORMATION ASSURANCE AND SECURITY

GROUP PROJECT

LECTURER'S NAME:

Ts. Dr. Kamaluddeen Usman Danyaro

PREPARED BY:

GROUP 26

NO	NAME	STUDENT ID	PROGRAMME
1.	Adam Ajmal Bin Mohd Shukri	24006385	IT
2.	Dayangku Alyaa Maisarah Binti Awg Mohamad Syeruji	22011486	IT
3.	Muhammad Hazyq Bin Zulkarnine	24007516	IT
4.	Sharifah Huda Binti Syed Mohd Husainy	22011420	IT
5.	Mohamad Najwan Bin Jaimey	24007403	IS
6.	Muhammad Faris Aiman Bin Ramli	24006497	IT

Group Video Simulation Link: <https://youtu.be/fNiL13j5jfs>

INTRODUCTION

The development of secure network infrastructures is a critical requirement for modern organisations. This project addresses this need through the design and implementation of a network for a company comprising of four departments which are Information Technology (IT), Customer Service (CS), Human Resources (HR), and Information Security (IS). By using Cisco Packet Tracer, the objective of this project is to construct a functional network that integrates specific topological designs for each department while also implementing information assurance and security principles. The project applies various key concepts such as access control, secure remote management and network monitoring. The process involves configuring encrypted router passwords, implementing Secure Shell (SSH) for administrative access, and deploying the Simple Network Management Protocol (SNMP) for surveillance. The result of this project serves to combine theoretical knowledge with practical application, demonstrating a better understanding of information assurance and security.

PROBLEM DESCRIPTION

1. The Scenario

There are 38 active employees now, divided into four departments. Information Technology (IT), Customer Service (CS), Human Resource (HR), and Information Security (IS) are the four departments. Additionally, a server room that is situated in the middle of the four departments is there. The routers and switches link the various departments together. The gadgets in each department are interconnected using their own topology types. To prevent hackers and other online criminals from accessing their company's data, they have established encrypted passwords for each router. Each router's CLI allows for the configuration of a different password for each department's router. To access and remotely control the connected remote devices, the corporation additionally activated Secure Shell (SSH) on its routers. By enabling SSH, all network data, including usernames and passwords, is encrypted, and made impenetrable to eavesdroppers. Upon establishing the connection, a network administrator can provide commands to the remote devices. Finally, the business enabled Simple Network Management Protocol (SNMP) as a handy protocol for managing and keeping an eye on the connected servers and network devices in the business. These setups have made the network secure and protected from any online attacks.

1.1 IT Department

Implement a star topology for this department since each device is connected to the switch, which serves as the network's hub. It prohibits direct connection between devices; instead, each device must go through the hub. Up to 14 hosts are present in total.

1.2 CS Department

For this company's CS division, implement a tree topology, in which numerous connected pieces are grouped like the branches of a tree. The devices in this department can only be connected to the network via Wi-Fi, unlike the equipment in the other departments. With the help of our 3 access points, 14 hosts can be connected.

1.3 HR Department

You may implement a tree topology for the HR department, as well as a tree structure with all the devices connected like the branches of a tree. These topology's key benefits are greater scalability and flexibility.

1.4 IS Department

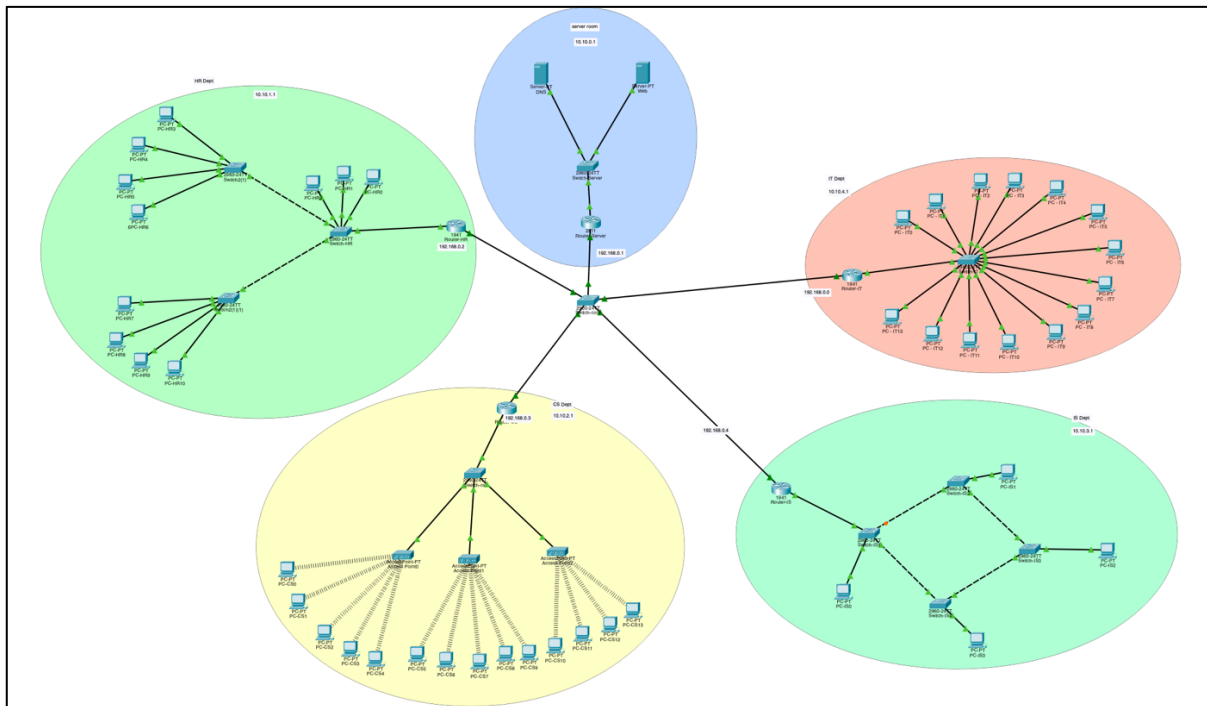
You may implement the link in the IS division using a ring and meshed topology combination. Each device is connected to the two devices on either side of it thanks to the ring topology. With the devices on either side of it, a device has two dedicated point-to-point links. According to the meshed topology, as shown in the topology, each device is linked to every other device on the network by a specific point-to-point link.

1.5 Server Room

There are two servers connected to a switch in the company's server room. The router is linked to the switch, and the router in turn is linked to other routers from various departments.

Activity 1

Topology Design

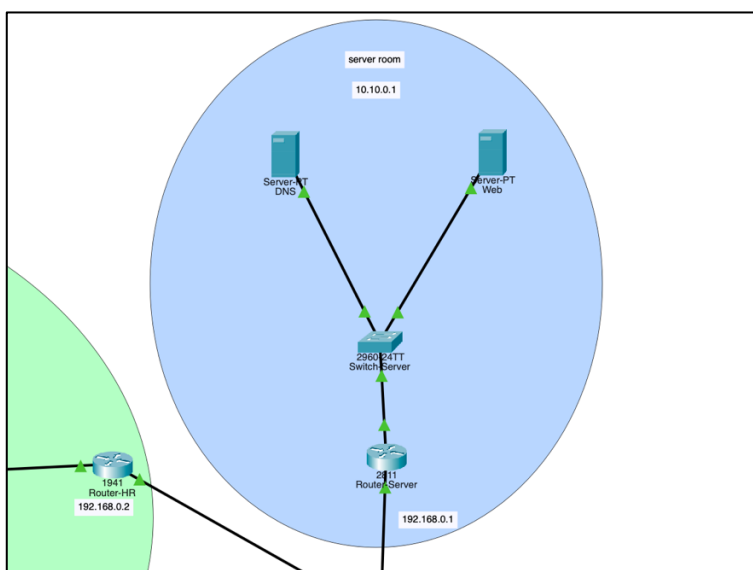


Departmental Topology Design

Server Room

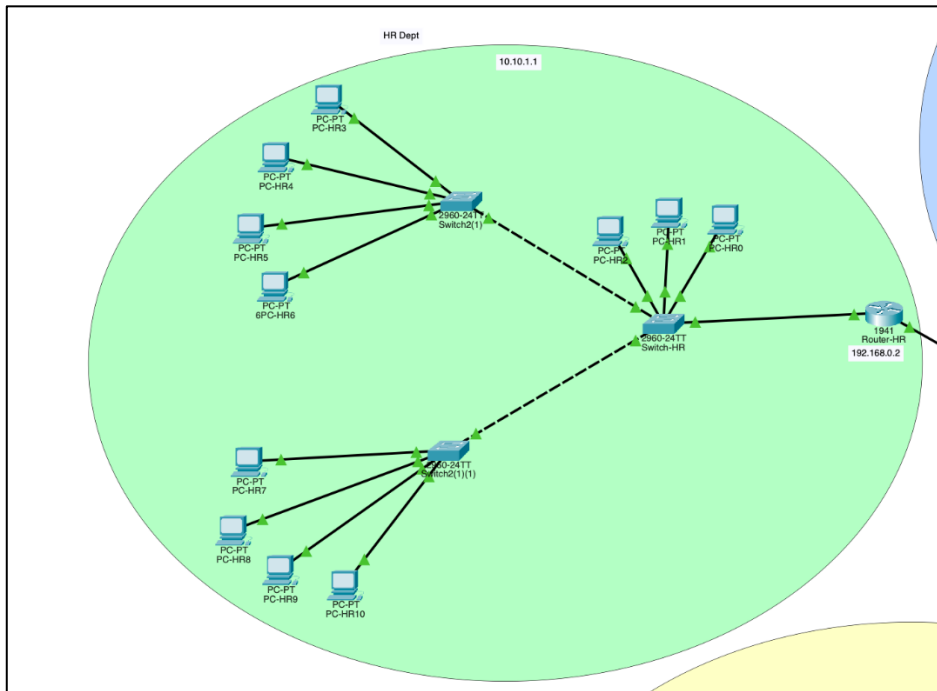
The Server Room contains:

- 1 Switch
- 2 Servers (DNS, DHCP, HTTP)
- A main router connected to the departmental routers



HR Department

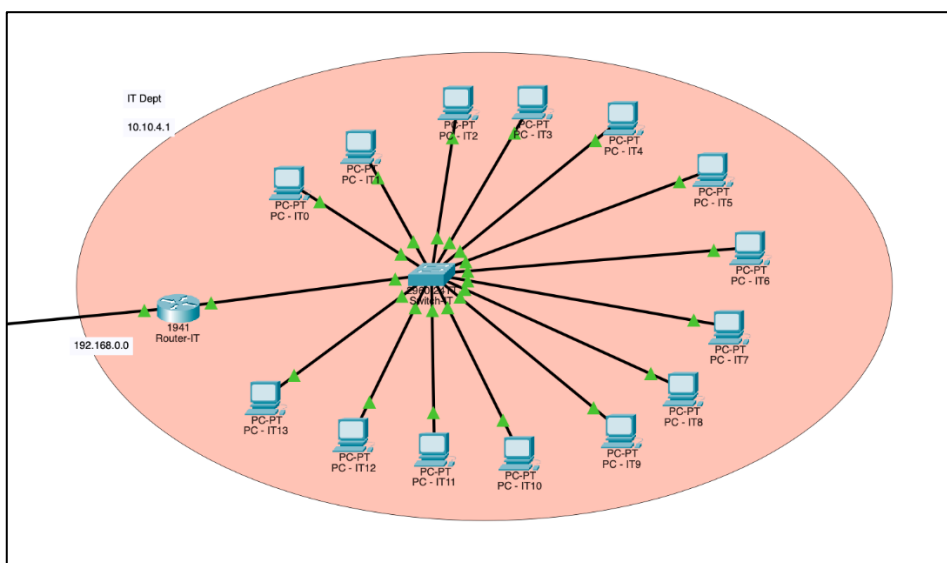
The HR department also uses a **Tree Topology**, supporting scalable branch-type device grouping.



IT Department

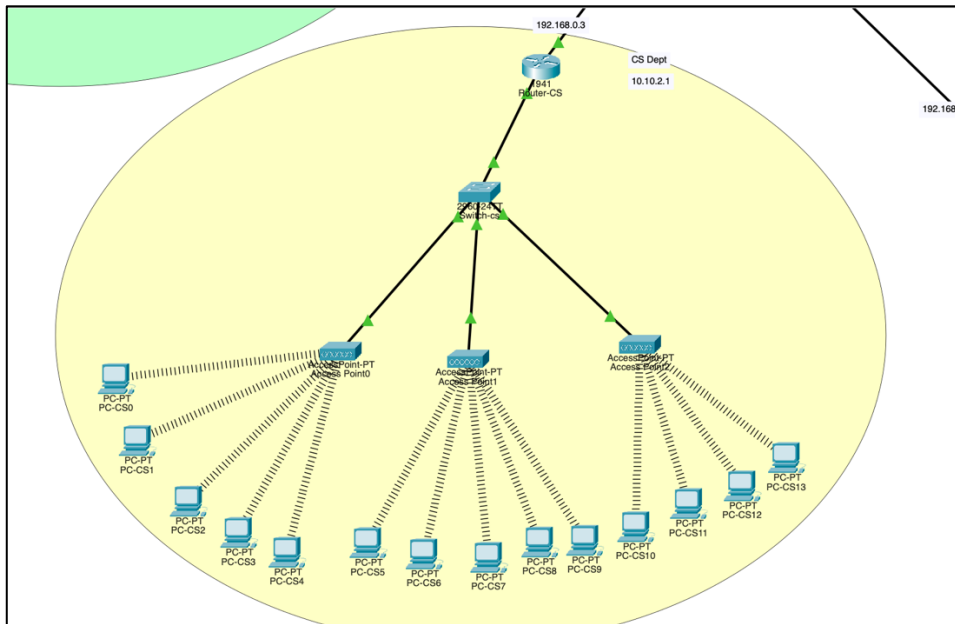
The IT Department uses a **Star Topology**, where all 14 hosts connect to a central switch. This setup provides:

- Easy troubleshooting
- Centralized management
- No direct device-to-device communication without passing through the switch



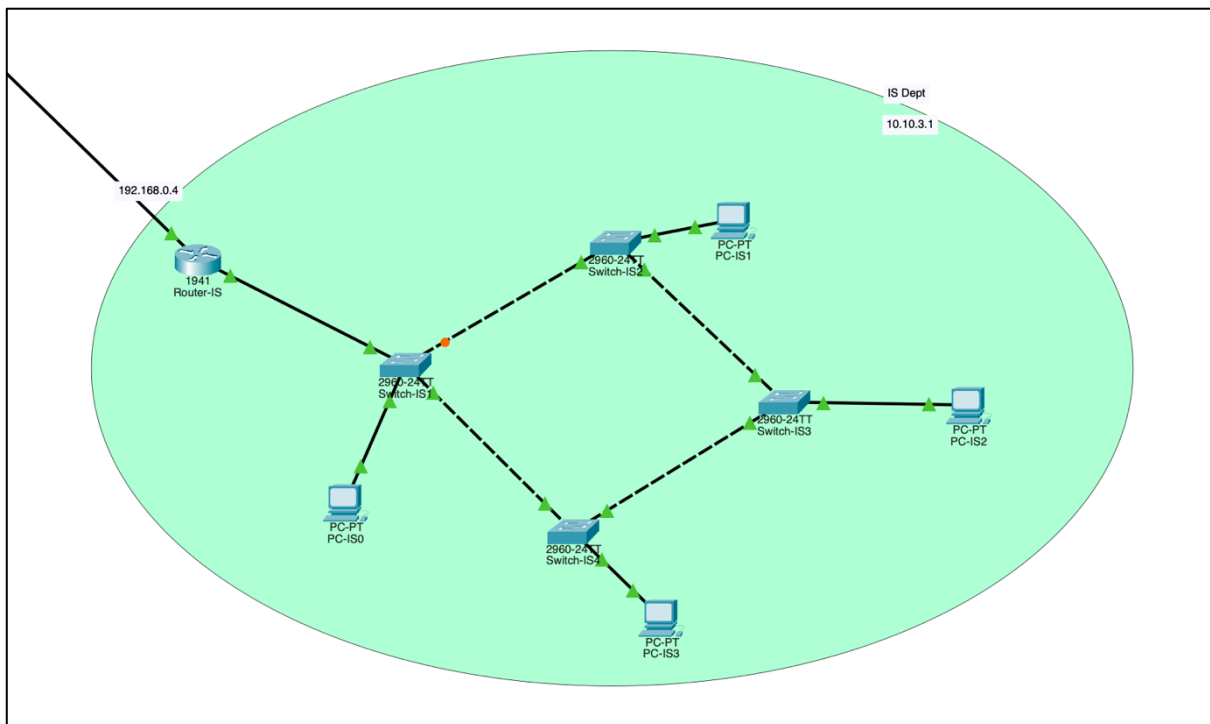
CS Department

This department uses a **Tree Topology** but entirely Wi-Fi based. Three access points branch from a central switch and support 14 hosts.



IS Department

The IS Department uses a **combined Ring + Mesh** topology for high redundancy.



IP address

Department	Network Address	Subnet Mask
Server Room	192.168.0.1	255.255.255.0
HR	192.168.0.2	255.255.255.0
IT	192.168.0.0	255.255.255.0
CS	192.168.0.3	255.255.255.0
IS	192.168.0.4	255.255.255.0

Server Room Device Labelling

Device Name	IP address	Subnet Mask
Router-Server	192.168.0.1	255.255.255.0
	10.10.0.1	255.255.255.0
Switch-Server	-	-
Server-PT DNS	10.10.0.11	255.255.255.0
Server-PT Web	10.10.0.10	255.255.255.0

IT Department Device Labelling

Device Name	IP address	Subnet Mask
Router-IT	192.168.0.5	255.255.255.0
	10.10.4.1	255.255.255.0
Switch-IT	-	-
PC-IT0	10.10.4.10	255.255.255.0
PC-IT1	10.10.4.11	255.255.255.0
PC-IT2	10.10.4.12	255.255.255.0
PC-IT3	10.10.4.13	255.255.255.0
PC-IT4	10.10.4.14	255.255.255.0
PC-IT5	10.10.4.15	255.255.255.0
PC-IT6	10.10.4.16	255.255.255.0
PC-IT7	10.10.4.17	255.255.255.0
PC-IT8	10.10.4.18	255.255.255.0
PC-IT9	10.10.4.19	255.255.255.0

PC-IT10	10.10.4.20	255.255.255.0
PC-IT11	10.10.4.21	255.255.255.0
PC-IT12	10.10.4.22	255.255.255.0
PC-IT13	10.10.4.23	255.255.255.0

IS Department Device Labelling

Device Name	IP address	Subnet Mask
Router-IS	192.168.0.4	255.255.255.0
	10.10.3.1	255.255.255.0
Switch-IS1	-	-
Switch-IS2	-	-
Switch-IS3	-	-
Switch-IS4	-	-
PC-IS0	10.10.3.10	255.255.255.0
PC-IS1	10.10.3.11	255.255.255.0
PC-IS2	10.10.3.12	255.255.255.0
PC-IS3	10.10.3.13	255.255.255.0

CS Department Device Labelling

Device Name	IP address	Subnet Mask
Router-cs	192.168.0.3	255.255.255.0
	10.10.2.1	255.255.255.0
Access Point0	-	-
Access Point1	-	-
Access Point3	-	-
PC-CS0	10.10.2.10	255.255.255.0
PC-CS1	10.10.2.11	255.255.255.0
PC-CS2	10.10.2.12	255.255.255.0
PC-CS3	10.10.2.13	255.255.255.0
PC-CS4	10.10.2.14	255.255.255.0
PC-CS5	10.10.2.15	255.255.255.0

PC-CS6	10.10.2.16	255.255.255.0
PC-CS7	10.10.2.17	255.255.255.0
PC-CS8	10.10.2.18	255.255.255.0
PC-CS9	10.10.2.19	255.255.255.0
PC-CS10	10.10.2.20	255.255.255.0
PC-CS11	10.10.2.21	255.255.255.0
PC-CS12	10.10.2.22	255.255.255.0
PC-CS13	10.10.2.23	255.255.255.0
PC-CS14	10.10.2.24	255.255.255.0

HR Department Device Labelling

Device Name	IP address	Subnet Mask
Router-HR	192.168.0.2	255.255.255.0
	10.10.1.1	255.255.255.0
Switch-HR	-	-
Switch2(1)	-	-
Switch2(1)(1)	-	-
PC-HR0	10.10.1.10	255.255.255.0
PC-HR1	10.10.1.11	255.255.255.0
PC-HR2	10.10.1.12	255.255.255.0
PC-HR3	10.10.1.13	255.255.255.0
PC-HR4	10.10.1.14	255.255.255.0
PC-HR5	10.10.1.15	255.255.255.0
PC-HR6	10.10.1.16	255.255.255.0
PC-HR7	10.10.1.17	255.255.255.0
PC-HR8	10.10.1.18	255.255.255.0
PC-HR9	10.10.1.19	255.255.255.0
PC-HR10	10.10.1.20	255.255.255.0

Firewall Configuration

HTTP & ICMP

1. Configure firewall in a server and blocking packets and allowing web browser.

Web

Physical Config Services **Desktop** Programming Attributes

Firewall [X]

Service ☒ On ☐ Off

Interface FastEthernet0

Inbound Rules

Action Protocol

Remote IP Remote Wildcard Mask

Remote Port Local Port

Save Remove Add

	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Allow	IP	0.0.0.0	255.255.255.255	-	-
2	Deny	ICMP	0.0.0.0	255.255.255.255	-	-

☐ Top

2. Verifying the network by pinging the IP address of any PC

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.0.10

Pinging 10.10.0.10 with 32 bytes of data:

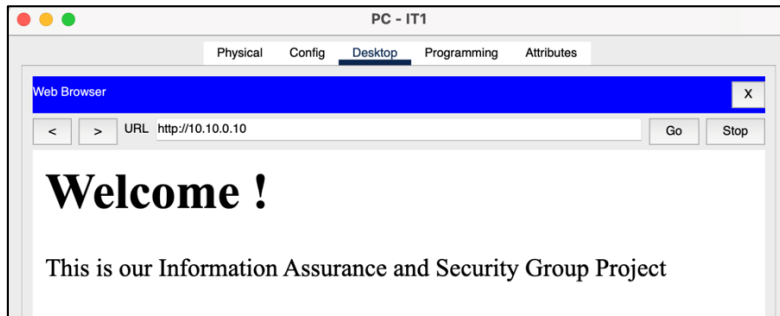
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

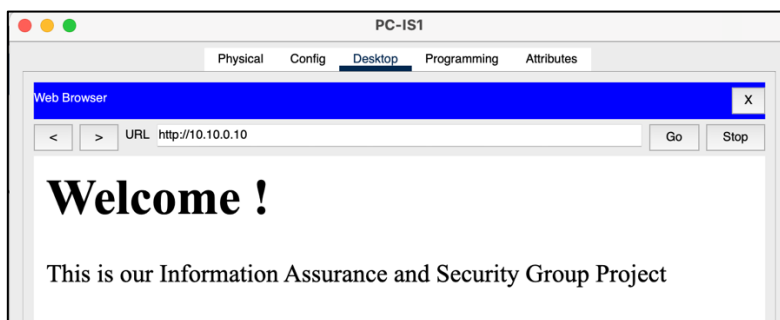
C:\>
```

3. Check the web browser by entering the IP address in the URL

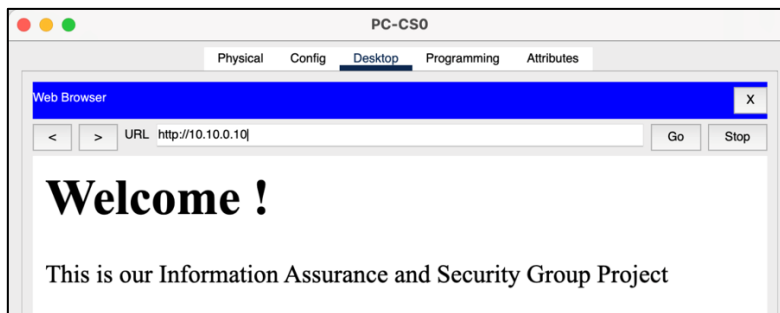
PC- IT



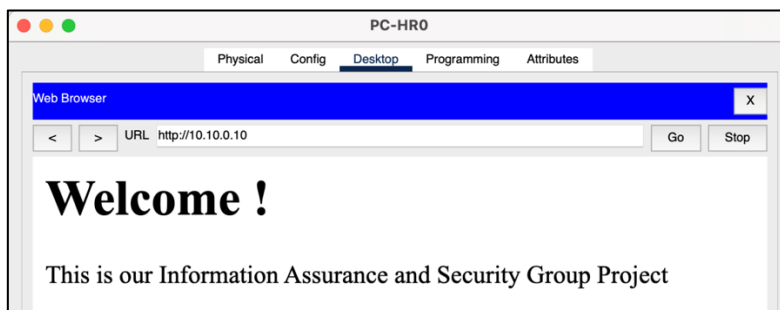
PC-IS



PC-CS



PC-HR



DNS SERVER

1. Configure DNS service on the generic server.

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

PRP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type

A Record

Address

Add

Save

Remove

No.	Name	Type	Detail
0	pc-cs0	A Record	10.10.0.11
1	pc-cs1	A Record	10.10.0.11
2	pc-hr0	A Record	10.10.0.11
3	pc-hr1	A Record	10.10.0.11
4	pc-is0	A Record	10.10.0.11
5	pc-is1	A Record	10.10.0.11
6	pc-it0	A Record	10.10.0.11
7	pc-it1	A Record	10.10.0.11

DNS Cache

2. Test domain name – IP resolution. Ping the hosts from one another using their names instead of their IP addresses.

2.1 Ping pc-is1 to pc-is0

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 10.10.3.11 255.255.255.0
C:\>ping pc-is0

Pinging 10.10.0.11 with 32 bytes of data:

Reply from 10.10.0.11: bytes=32 time<1ms TTL=126
Reply from 10.10.0.11: bytes=32 time=1ms TTL=126
Reply from 10.10.0.11: bytes=32 time<1ms TTL=126
Reply from 10.10.0.11: bytes=32 time<1ms TTL=126

Ping statistics for 10.10.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

2.2 Ping pc-hr1 to pc-hr0

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping pc-hr0

Pinging 10.10.0.11 with 32 bytes of data:

Reply from 10.10.0.11: bytes=32 time=1ms TTL=126
Reply from 10.10.0.11: bytes=32 time<1ms TTL=126
Reply from 10.10.0.11: bytes=32 time<1ms TTL=126
Reply from 10.10.0.11: bytes=32 time=2ms TTL=126

Ping statistics for 10.10.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

2.3 Ping pc-cs1 to pc-cs0

```
C:\>ping pc-cs0

Pinging 10.10.0.11 with 32 bytes of data:

Reply from 10.10.0.11: bytes=32 time=39ms TTL=126
Reply from 10.10.0.11: bytes=32 time=35ms TTL=126
Reply from 10.10.0.11: bytes=32 time=35ms TTL=126
Reply from 10.10.0.11: bytes=32 time=23ms TTL=126

Ping statistics for 10.10.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 39ms, Average = 33ms
```

2.4 Ping pc-it1 to pc-it0

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 10.10.4.11 255.255.255.0
C:\>ping pc-it0

Pinging 10.10.0.11 with 32 bytes of data:

Reply from 10.10.0.11: bytes=32 time=1ms TTL=126
Reply from 10.10.0.11: bytes=32 time=1ms TTL=126
Reply from 10.10.0.11: bytes=32 time<1ms TTL=126
Reply from 10.10.0.11: bytes=32 time<1ms TTL=126

Ping statistics for 10.10.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

DHCP Server

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

PRP

DHCP

Interface

FastEthernet0

Service

On

Off

Pool Name

serverPool2

Default Gateway

192.168.0.1

DNS Server

10.10.0.11

Start IP Address :

10

10

0

10

Subnet Mask:

255

255

255

0

Maximum Number of Users :

246

TFTP Server:

0.0.0.0

WLC Address:

0.0.0.0

Add

Save

Remove

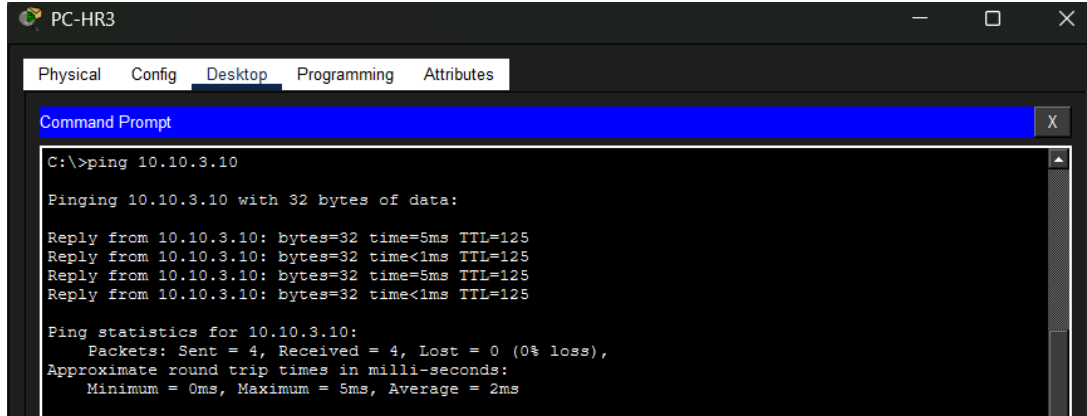
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool2	192.168.0.1	10.10.0.11	10.10.0.10	255.255....	246	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	10.10.0.0	255.255....	512	0.0.0.0	0.0.0.0

Activity 2

Test Configuration – Ping Command

1. Ping Different PCs from different departments

1.1 Ping PC-HR3 to PC-IS1



PC-HR3

Physical Config Desktop Programming Attributes

Command Prompt

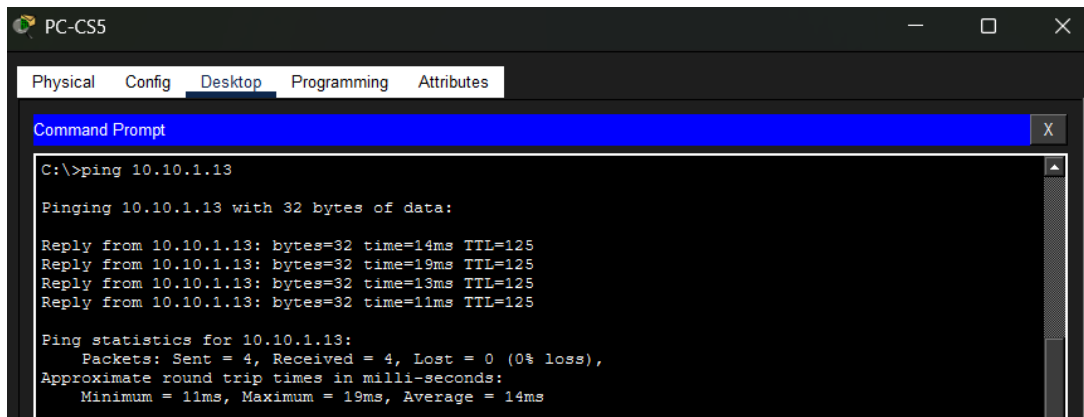
```
C:\>ping 10.10.3.10

Pinging 10.10.3.10 with 32 bytes of data:

Reply from 10.10.3.10: bytes=32 time=5ms TTL=125
Reply from 10.10.3.10: bytes=32 time<1ms TTL=125
Reply from 10.10.3.10: bytes=32 time=5ms TTL=125
Reply from 10.10.3.10: bytes=32 time<1ms TTL=125

Ping statistics for 10.10.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 2ms
```

1.2 Ping PC-CS5 to PC-HR3



PC-CS5

Physical Config Desktop Programming Attributes

Command Prompt

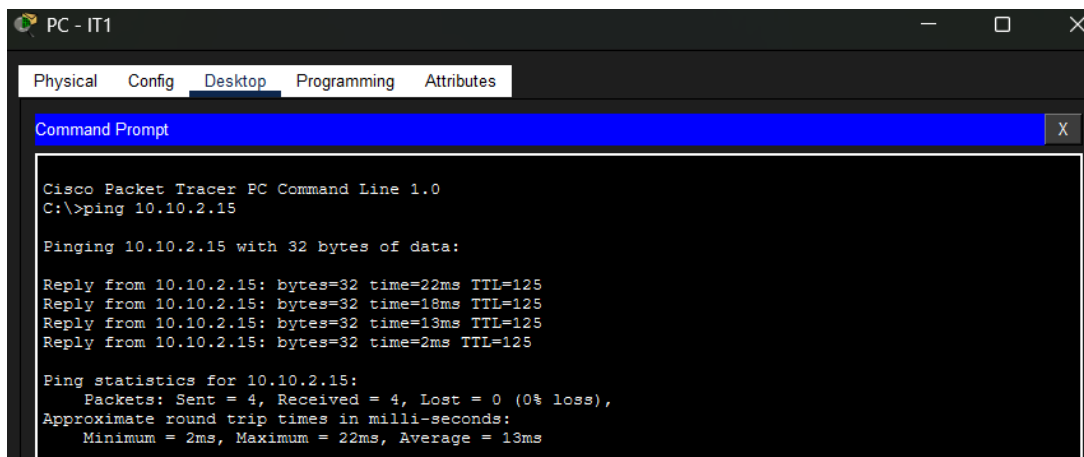
```
C:\>ping 10.10.1.13

Pinging 10.10.1.13 with 32 bytes of data:

Reply from 10.10.1.13: bytes=32 time=14ms TTL=125
Reply from 10.10.1.13: bytes=32 time=19ms TTL=125
Reply from 10.10.1.13: bytes=32 time=13ms TTL=125
Reply from 10.10.1.13: bytes=32 time=11ms TTL=125

Ping statistics for 10.10.1.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 19ms, Average = 14ms
```

1.3 Ping PC-IT1 to PC-CS5



PC - IT1

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.2.15

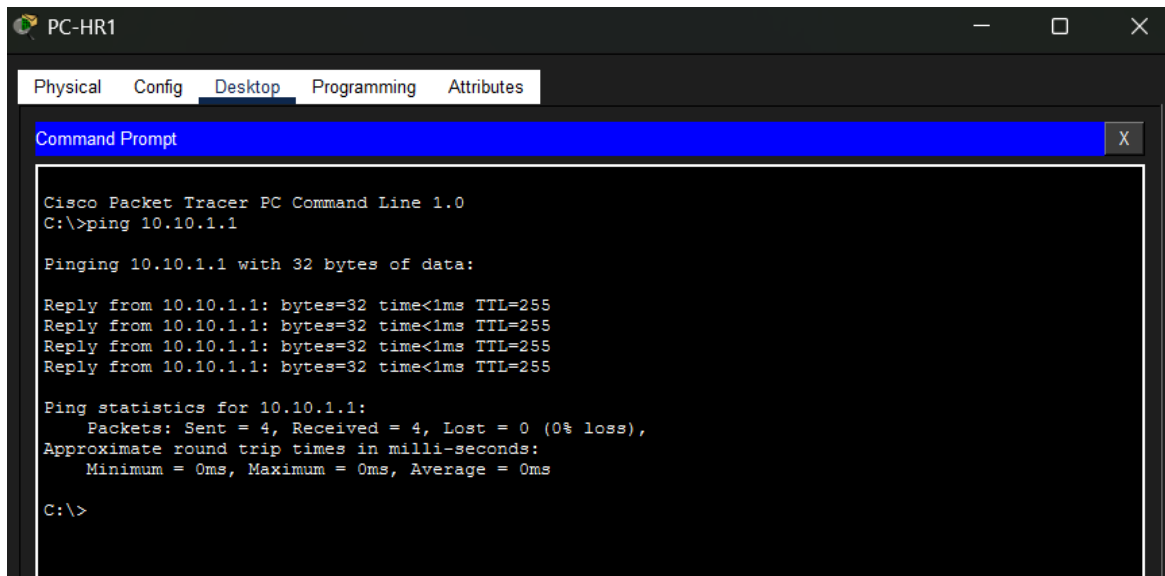
Pinging 10.10.2.15 with 32 bytes of data:

Reply from 10.10.2.15: bytes=32 time=22ms TTL=125
Reply from 10.10.2.15: bytes=32 time=18ms TTL=125
Reply from 10.10.2.15: bytes=32 time=13ms TTL=125
Reply from 10.10.2.15: bytes=32 time=2ms TTL=125

Ping statistics for 10.10.2.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 22ms, Average = 13ms
```

2. Ping from PC to its gateway

2.1 ping from PC-HR1 to its gateway



The screenshot shows the 'PC-HR1' window in Cisco Packet Tracer. The 'Desktop' tab is selected, and the 'Command Prompt' application is open. The command prompt displays the output of the command 'ping 10.10.1.1'. The output shows four successful replies with 32 bytes of data, a time of less than 1ms, and a TTL of 255. The ping statistics indicate that 4 packets were sent and received, with 0% loss, and the round trip times are all 0ms.

```
PC-HR1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.1.1

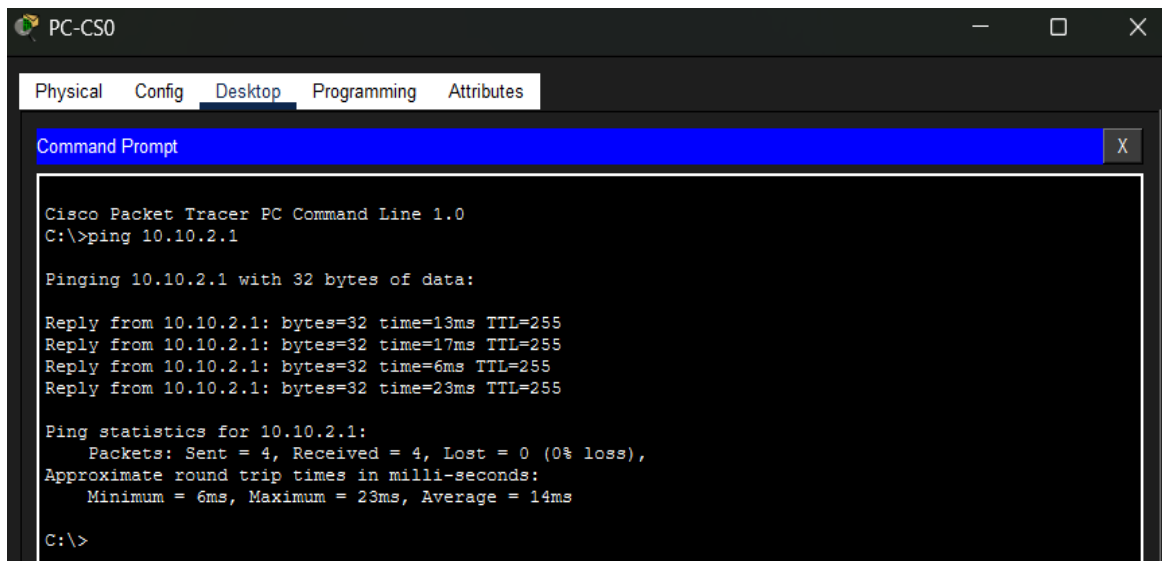
Pinging 10.10.1.1 with 32 bytes of data:

Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

2.2 ping from PC-CS0 to its gateway



The screenshot shows the 'PC-CS0' window in Cisco Packet Tracer. The 'Desktop' tab is selected, and the 'Command Prompt' application is open. The command prompt displays the output of the command 'ping 10.10.2.1'. The output shows four successful replies with 32 bytes of data, a time of 13ms, 17ms, 6ms, and 23ms, and a TTL of 255. The ping statistics indicate that 4 packets were sent and received, with 0% loss, and the round trip times are 6ms, 23ms, and 14ms.

```
PC-CS0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.2.1

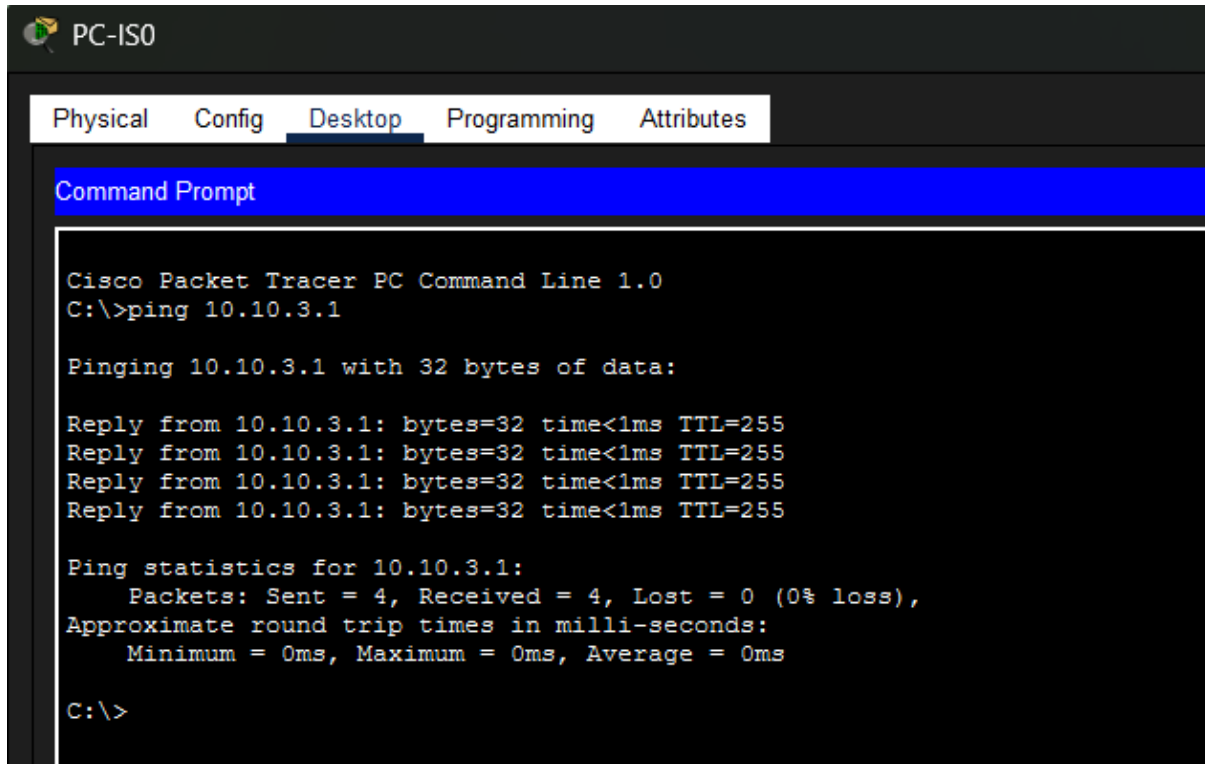
Pinging 10.10.2.1 with 32 bytes of data:

Reply from 10.10.2.1: bytes=32 time=13ms TTL=255
Reply from 10.10.2.1: bytes=32 time=17ms TTL=255
Reply from 10.10.2.1: bytes=32 time=6ms TTL=255
Reply from 10.10.2.1: bytes=32 time=23ms TTL=255

Ping statistics for 10.10.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 23ms, Average = 14ms

C:\>
```

2.3 ping from PC-IS1 to its gateway



The screenshot shows the 'PC-IS0' window in Cisco Packet Tracer. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command to 10.10.3.1, resulting in four successful replies with 0% loss.

```
PC-IS0
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.3.1

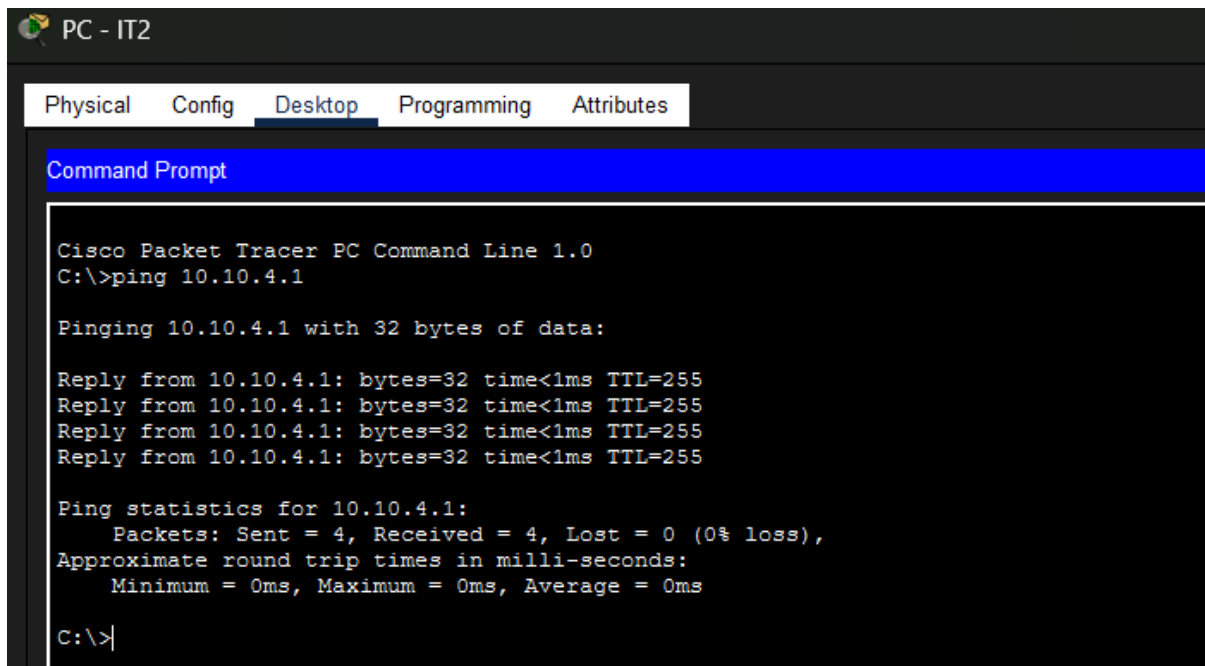
Pinging 10.10.3.1 with 32 bytes of data:

Reply from 10.10.3.1: bytes=32 time<1ms TTL=255
Reply from 10.10.3.1: bytes=32 time<1ms TTL=255
Reply from 10.10.3.1: bytes=32 time<1ms TTL=255
Reply from 10.10.3.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

2.4 ping PC-IT1 to its gateway



The screenshot shows the 'PC - IT2' window in Cisco Packet Tracer. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command to 10.10.4.1, resulting in four successful replies with 0% loss.

```
PC - IT2
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.4.1

Pinging 10.10.4.1 with 32 bytes of data:

Reply from 10.10.4.1: bytes=32 time<1ms TTL=255
Reply from 10.10.4.1: bytes=32 time<1ms TTL=255
Reply from 10.10.4.1: bytes=32 time<1ms TTL=255
Reply from 10.10.4.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

3. Ping between departments

3.1 Ping Router-IT to Router-Server

```
Router-IT#ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router-IT#ping 10.10.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

3.2 Ping Router-IT to IS-Server

```
Router-IT#ping 192.168.0.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

Router-IT#ping 10.10.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

3.3 Ping Router-IT to CS-Server

```
Router-IT#ping 192.168.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

Router-IT#ping 10.10.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

3.4 Ping Router-IT to HR-Server

```
Router-IT#ping 192.168.0.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

```
Router-IT#ping 10.10.1.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.10.1.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
Router-IT#
```

Activity 3

Identify and explain three potential cybersecurity vulnerabilities that could still exist in this infrastructure. For each vulnerability, propose a realistic mitigation strategy that aligns with best practices in network security.

Vulnerability 1: Weak or Outdated Wi-Fi Security

The Customer Service department relies entirely on Wi-Fi through three access points, however the security level of these APs is not specified. If the access points are configured using older security protocols such as WPA2-PSK or have weak pre-shared keys, attackers can capture wireless traffic and attempt password cracking. This could allow unauthorized access to internal network resources which leads to data theft or injection of malicious traffic.

To protect the CS department's wireless network, the organization should upgrade all access points to support WPA3-Enterprise or, if its unavailable, WPA2-Enterprise with 802.1X authentication could be used. This replaces simple shared passwords with secure individual user authentication through a RADIUS server. Strong passwords and regular key rotation should also be enforced to reduce the effectiveness of brute-force attacks.

Vulnerability 2: SNMPv2c Uses Plaintext Community Strings

Although SNMP is enabled for network monitoring, many organizations use SNMPv1 or SNMPv2c by default. These versions transmit community strings which is similar to passwords in plaintext, making it easy to intercept during packet sniffing. With the "public" or "private" community string, an attacker can access device information, monitor network activity or even change configurations. This exposes the entire network infrastructure to remote manipulation without the attacker needing full device access.

The most effective mitigation is to use SNMPv3 instead of SNMPv2c which provides encrypted communication, user-based authentication and stricter access control. Only authorized monitoring servers should be allowed to communicate with network devices using SNMP which is being enforced through Access Control Lists (ACLs). Default community strings must be removed and SNMP polling should be restricted to specific interfaces. These steps will prevent attackers from intercepting or abusing SNMP traffic.

Vulnerability 3: Lack of Segmentation and VLAN Isolation

The four department, IT, CS, HR and IS appear to be interconnected through routers and switches, it remains unclear whether proper segmentation has been implemented. If all devices operate within the same broadcast domain or if traffic between the four departments are not restricted, an attacker who compromise even one host can easily move across the network. This allows access to sensitive systems in HR, IT or IS department which will increase the risk of data breaches, credential theft or malware spreading across departments. Without segmentation, the entire organization becomes vulnerable once a single point is comprised.

Creating separate VLANs for each department will ensure it will operate in its own isolated network segment. Using inter-VLAN routing with strict ACLs to ensure each department can only access the resources they are authorized to reach. For highly sensitive areas such as the HR department or the server room, deploying a firewall between VLANs will provide deeper traffic inspection and filtering. Additionally, by enabling switch port-security to restrict which devices can connect to each port will prevent rogue or unauthorized devices from entering the network.

Conclusion

This project has successfully demonstrated the design and implementation of a secure and efficient network infrastructure which is tailored to the needs of a multi-department organisation. By applying appropriate topology types such as the star, tree, ring and mesh topology, each department's operational requirements were supported while ensuring reliable connectivity. The integration of security mechanisms which include encrypted router passwords, SSH for secure remote administration and SNMP for monitoring has reinforced the importance of protecting network devices and data from unauthorized access.

Through the use of Cisco Packet Tracer, this project bridges theoretical concepts with practical application which allow hands-on configuration of devices, protocols and security settings. The structured arrangement of departments supported by a centralized server room, further highlights the importance of proper network segmentation and manageable infrastructure design. Overall, the project provides a comprehensive understanding of information assurance and security principles which showcase how secure network architecture is essential in safeguarding organizational operations.

References

GeeksforGeeks. (2025, July 23). *Basic firewall configuration in Cisco Packet Tracer*

GeeksforGeeks. <https://www.geeksforgeeks.org/computer-networks/basic-firewall-configuration-in-cisco-packet-tracer/>

GeeksforGeeks. (2025b, July 23). *Implementation of static routing in Cisco 2 router*

connections. GeeksforGeeks. <https://www.geeksforgeeks.org/computer-networks/implementation-of-static-routing-in-cisco-2-router-connections/>

Receponer. (2016, November 24). *Configure SNMP Protocol on Cisco Packet Tracer*. BT

BLOG. <https://receponer.wordpress.com/2016/11/24/configure-snmp-protocol-on-cisco-packet-tracer/>

Kimanzi, S. (2020, February 10). *DNS server configuration in Packet Tracer*. Computer

Networking Tips. <https://computernetworking747640215.wordpress.com/2018/07/05/dns-server-configuration-in-packet-tracer/>

Scarfone, K., & Mullins, J. (2020). *Guide to Bluetooth and Wireless LAN Security (NIST SP 800-153)*. National Institute of Standards and Technology.

<https://doi.org/10.6028/NIST.SP.800-153>

Petryschuk, S. (2024, October 24). *SNMPv2 vs. SNMPv3: An SNMP Versions Comparison*

Table. Auvik. <https://www.auvik.com/franklyit/blog/difference-between-snmp-v2-v3/>

Wickramasinghe, S. (2025). *What is network segmentation? A complete guide*. Splunk.

https://www.splunk.com/en_us/blog/learn/network-segmentation.html

Cisco Press. (n.d.). *Inter-VLAN routing*. Cisco Press.

<https://www.ciscopress.com/articles/article.asp?p=3089357&seqNum=4>

ASUS. (n.d.). *What is WPA3? What are the advantages ...* ASUS Support.

<https://www.asus.com/my/support/faq/1042478/>