UNIVERSITI TEKNOLOGI PETRONAS

TFB2043/TEB2193/TEB2213: Information Assurance and Security- September 2025

Date: 18/11/2025

Group: Group 18

Name	Student ID	Course
Tan Yency	22010927	Information Technology
Low Rui Han	22011080	Information Technology
Muhammad Akil Mufid Bin Adam	22011338	Information Technology
Muhammad Azril Zuhairi Bin Azlan	22011040	Information Technology
Akmal Faiz bin Adam Kamal	22010864	Information Technology
Mohammad bilal afzal	24004510	Information Technology

GitHub link

https://github.com/Tanycy/IAS-Project-Sep-2025.git

Table of Contents

1.0 Introduction

The current digital world has necessitated a maintained and properly organised network infrastructure to help in facilitating the smooth running of business and safeguarding sensitive organizational information. The scope of this project is to plan and set up a functional network environment of a company made up of four major departments namely Information Technology (IT), Customer Service (CS), Human Resource (HR), Information Security (IS) and a centralized server room. Every department is provided with a suitable network topology depending on the operational requirements of that department and the inter departmental connection is made with the help of routers and switches.

Various practices have been implemented to enhance the security of the networks, these include encrypted router passwords, Secure Shell (SSH) remote access and Simple Network Management Protocol (SNMP) monitoring. Such designs aid in securing communication, remote intervention and gadget observing throughout the whole infrastructure.

This report describes network design, configuration process, IP addressing approach, labelling of devices and restrictions of firewall. Other than that, the testing process and the assessment of possible remaining vulnerabilities to cybersecurity are given. This project aims at showing how to establish a safe, scalable and effective network that meets the needs of the running of the organization which follows the best practices in network security.

1.1 Configuration

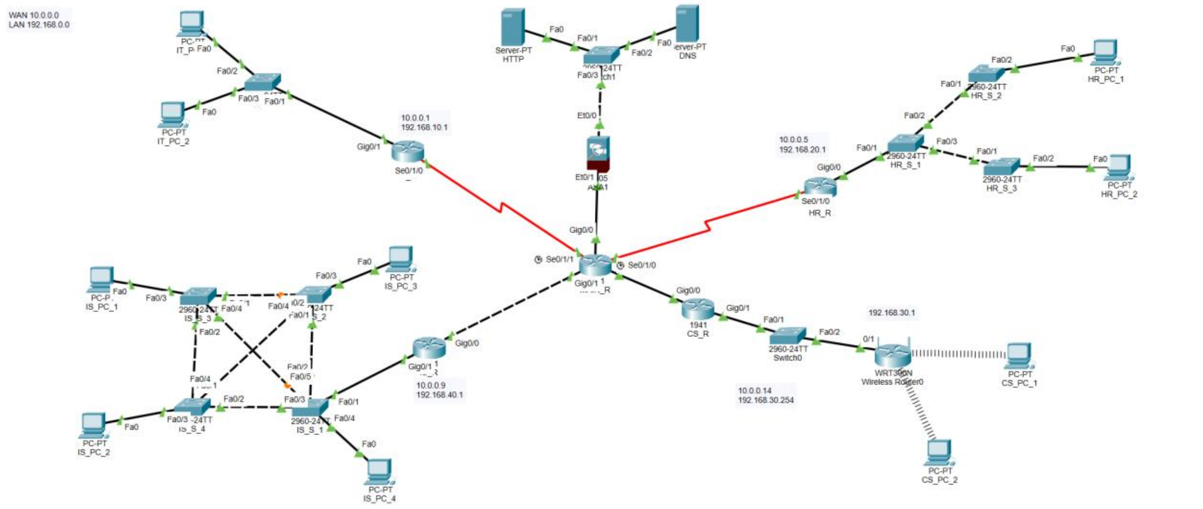
In this project, we start with IP addressing, then static routing, DHCP for PCs, enable password, do SSH, SNMP for management:

1. IP Addressing: We assign IP addresses to devices (routers, switches, PCs) so each device has a unique identity on the network. This ensures proper communication and reachability.
2. Static Routing: We manually configure routes on routers, specifying exactly how packets should travel between subnets. Static routing gives us full control over the routing paths and is simple to implement for small or stable topologies.
3. DHCP (Dynamic Host Configuration Protocol) : This protocol automatically allocates IP addresses, subnet masks, default gateways, and other parameters to the PCs. Instead

of manually configuring each PC, a DHCP server leases these parameters to clients dynamically.

4. Enable Password: This refers to setting a privileged (enable) password on network devices (like routers/switches) to restrict access to privileged EXEC mode. This is important for security only authorized users can make configuration changes.
5. SSH (Secure Shell): We enable SSH to allow secure, encrypted remote access to our network devices. Unlike Telnet, SSH encrypts the communication, protecting login credentials and command traffic.
6. SNMP (Simple Network Management Protocol): We implement SNMP for network management and monitoring. With SNMP, a central management station (network manager) can query devices (routers/switches) for status, performance metrics, or configuration.

2.0 Topology



3.0 IP routing table

Device	Interface	Purpose	IP address	Subnet
MAIN_R	GigabitEthernet0/0	Link to ASA	10.0.10.10	255.255.255.252
	Serial0/1/1	Link to IT_R	10.0.0.2	
	Serial0/1/0	Link to HR_R	10.0.0.6	
	GigabitEthernet0/1	Link to IS_R	10.0.0.10	
	Vlan 1	Link to CS_R	10.0.0.13	
IT_R	Serial0/1/0	Link to MAIN_R	10.0.0.1	255.255.255.252
	GigabitEthernet0/1.10	Link to IT_S	192.168.10.1	255.255.255.0
HR_R	Serial0/1/0	Link to MAIN_R	10.0.0.5	255.255.255.252
	GigabitEthernet0/0.20	Link to HR_S	192.168.20.1	255.255.255.0
IS_R	GigabitEthernet0/0	Link to MAIN_R	10.0.0.9	255.255.255.252
	GigabitEthernet0/1.30	Link to IS_S	192.168.40.1	255.255.255.0
CS_R	Serial0/1/0	Link to MAIN_R	10.0.0.14	255.255.255.252
	GigabitEthernet0/0	Link to CS_S	192.168.30.254	255.255.255.0

4.0 IP configuration

4.1 MAIN_R

```
hostname MAIN_R

//Link to ASA Firewall
interface GigabitEthernet0/0
 ip address 10.0.10.10 255.255.255.0
 no shutdown

//Link to IT_R
interface Serial0/1/1
ip address 10.0.0.2 255.255.255.252
 no shutdown

//Link to HR_R
interface Serial0/1/0
ip address 10.0.0.6 255.255.255.252
 no shutdown

//Link to IS_R
interface GigabitEthernet0/1
ip address 10.0.0.10 255.255.255.252
 no shutdown
```

```
//Link to CS_R

interface FastEthernet0/0/0

 ip address 10.0.0.13 255.255.255.252

 no shutdown


switchport mode access

switchport access vlan 1
```

4.2 IT_R

```
hostname IT_R

//Link to MAIN_R

interface Serial0/1/0

ip address 10.0.0.1 255.255.255.252

 no shutdown


//LAN link to Switch

interface GigabitEthernet0/1

 ip address 192.168.10.1 255.255.255.0

 no shutdown
```

4.3 HR_R

```
hostname HR_R
//Link to MAIN_R
interface Serial0/1/0
ip address 10.0.0.5 255.255.255.252
 no shutdown

//LAN link to Switch
interface GigabitEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 no shutdown
```

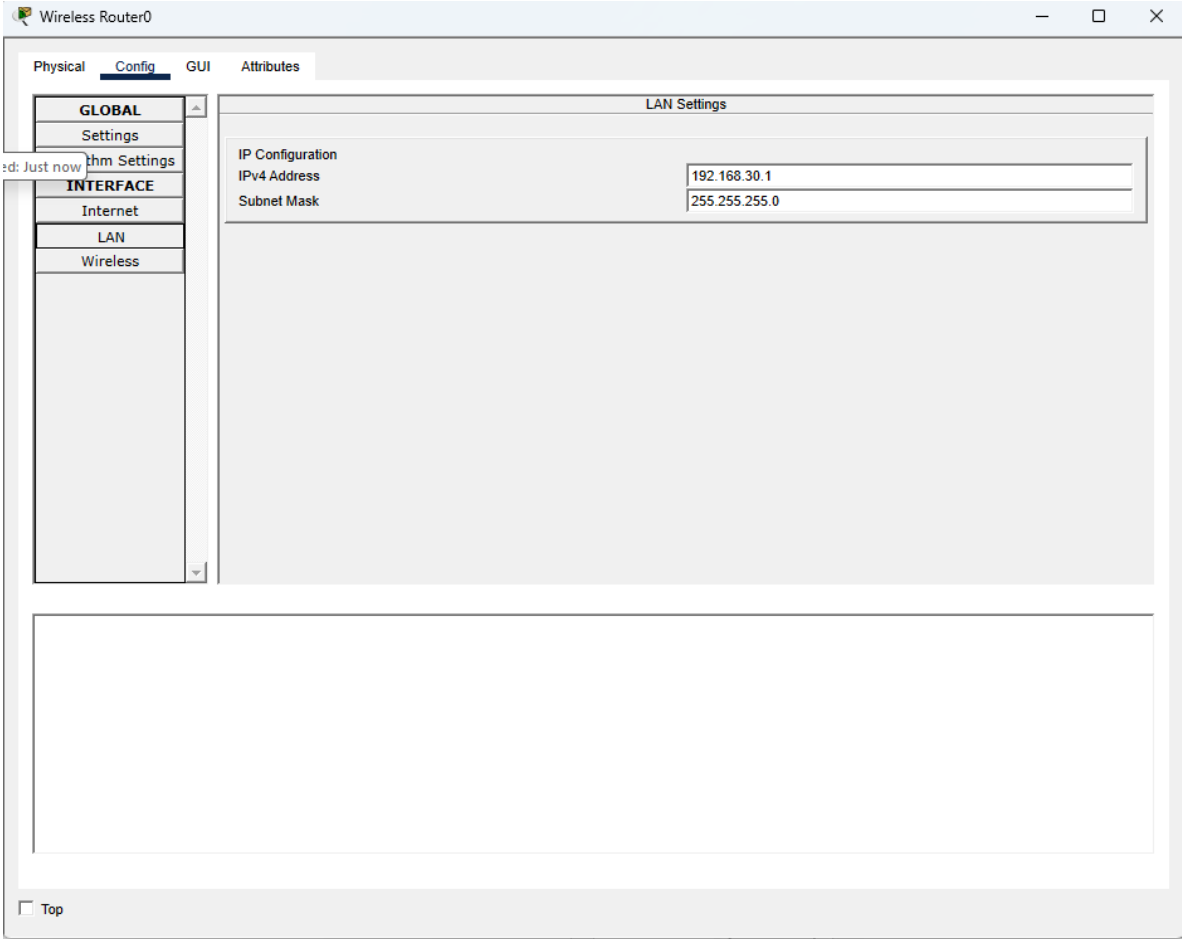
4.4 IS_R

```
hostname IS_R
//Link to MAIN_R
interface GigabitEthernet0/0
ip address 10.0.0.9 255.255.255.252
 no shutdown

//LAN link to Switch
interface GigabitEthernet0/0
 ip address 192.168.40.1 255.255.255.0
 no shutdown
```

4.5 CS_R

```
hostname CS_R

//WAN link to MAIN_R

interface Serial0/1/0

 ip address 10.0.0.14 255.255.255.252

 no shutdown



//LAN link to Switch

interface GigabitEthernet0/0

 ip address 192.168.30.254 255.255.255.0

 no shutdown
```

4.6 Wireless router

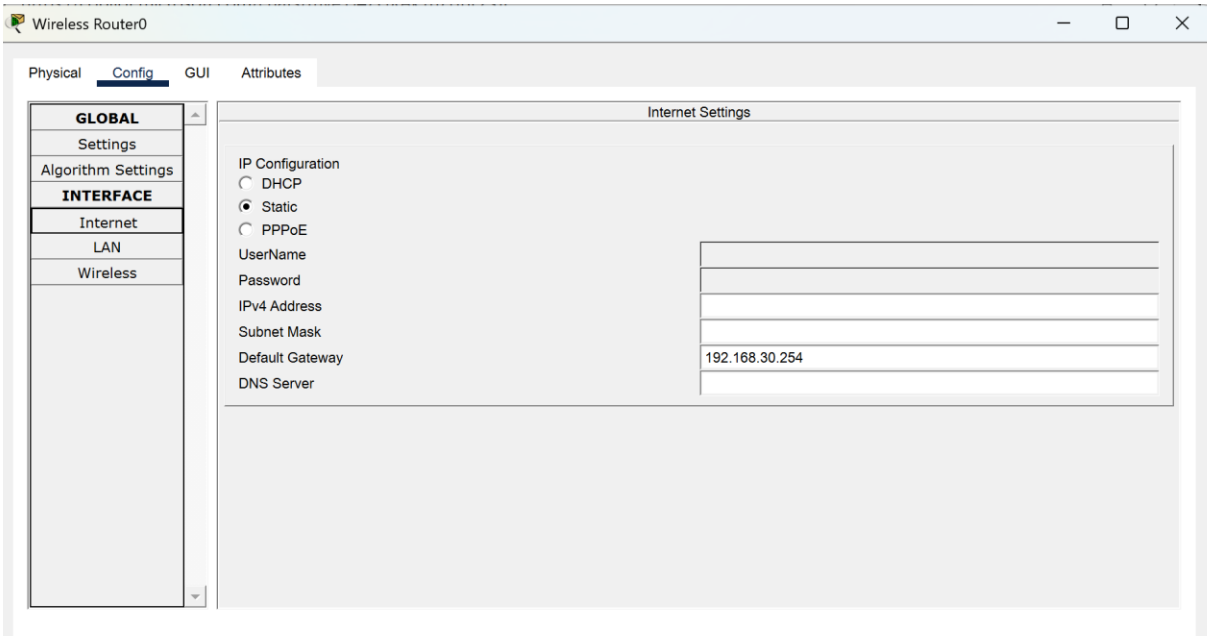


LAN Settings

IP Configuration

IPv4 Address 192.168.30.1

Subnet Mask 255.255.255.0



Internet Settings

IP Configuration

○ DHCP

● Static

○ PPPoE

UserName

Password

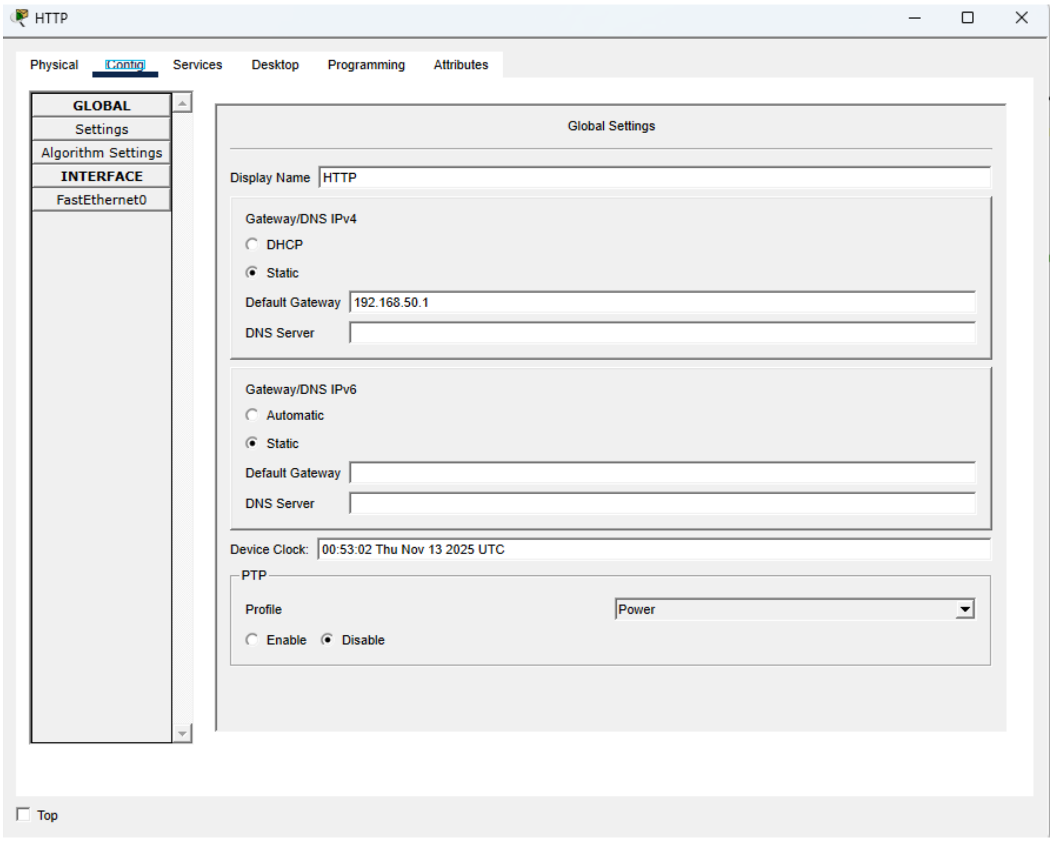
IPv4 Address

Subnet Mask

Default Gateway 192.168.30.254

DNS Server

4.7 HTTP server



Global Settings

Display Name HTTP

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway 192.168.50.1

DNS Server

Gateway/DNS IPv6

○ Automatic

● Static

Default Gateway

DNS Server

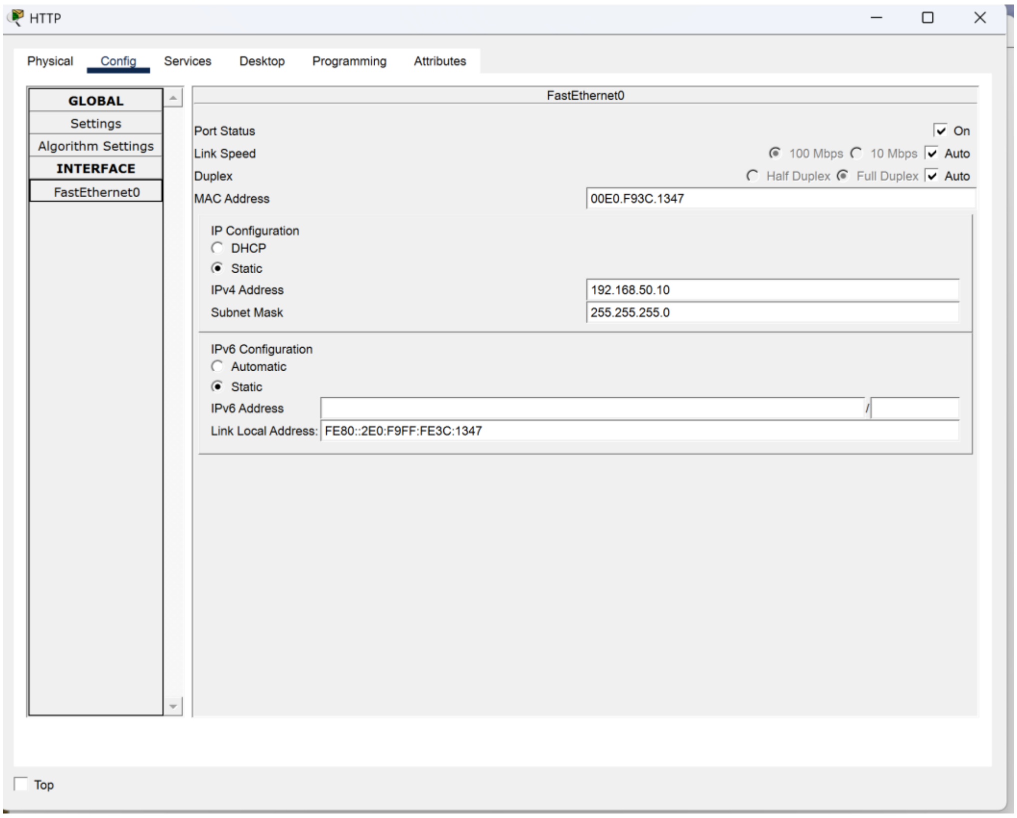
Device Clock: 00:53:02 Thu Nov 13 2025 UTC

PTP

Profile Power

○ Enable ● Disable

□ Top



FastEthernet0

Port Status ☑ On

Link Speed ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 00E0.F93C.1347

IP Configuration

○ DHCP

● Static

IPv4 Address 192.168.50.10

Subnet Mask 255.255.255.0

IPv6 Configuration

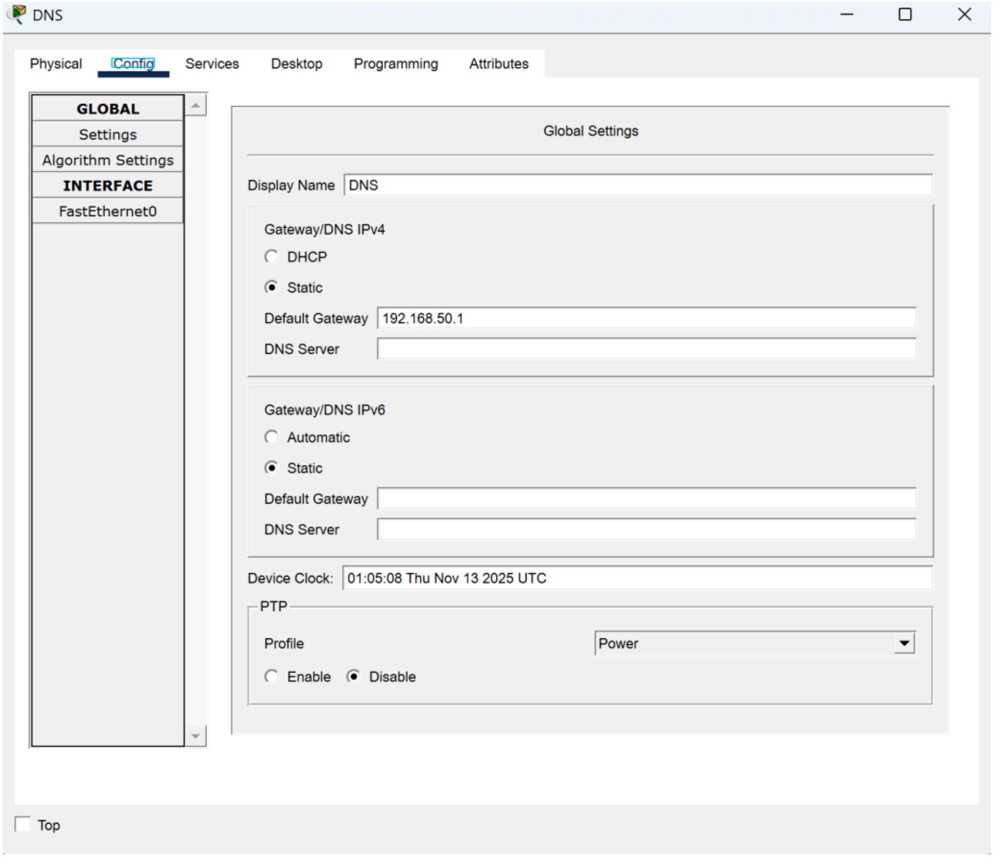
○ Automatic

● Static

IPv6 Address /

Link Local Address: FE80::2E0:F9FF:FE3C:1347

4.8 DNS server



Global Settings

Display Name DNS

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway 192.168.50.1

DNS Server

Gateway/DNS IPv6

○ Automatic

● Static

Default Gateway

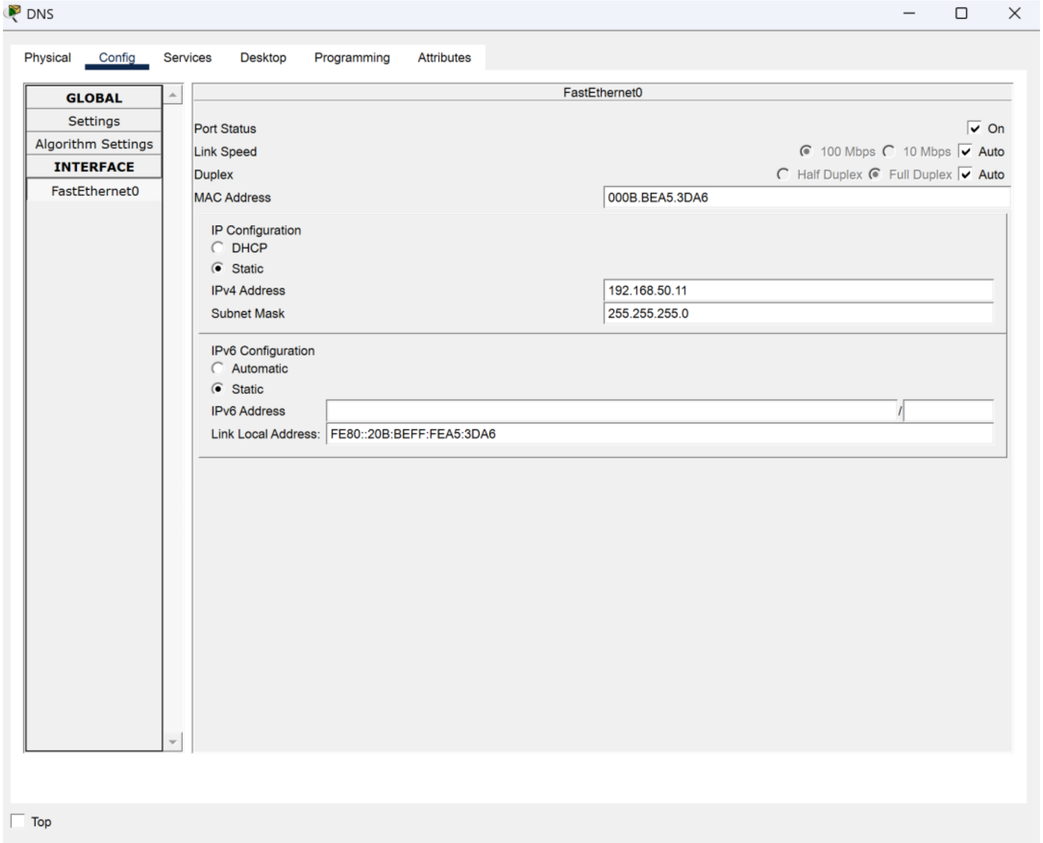
DNS Server

Device Clock: 01:05:08 Thu Nov 13 2025 UTC

PTP

Profile Power

○ Enable ● Disable



FastEthernet0

Port Status ☑ On

Link Speed ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 000B.BEA5.3DA6

IP Configuration

○ DHCP

● Static

IPv4 Address 192.168.50.11

Subnet Mask 255.255.255.0

IPv6 Configuration

○ Automatic

● Static

IPv6 Address /

Link Local Address: FE80::20B:BEFF:FEA5:3DA6

□ Top

5.0 Enable ASA Firewall

5.1 MAIN_S

```
vlan 2

 name SERVER_VLAN



//Assign VLAN 2 to active ports

interface range Fa0/1 - 3

 switchport mode access

 switchport access vlan 2

 no shutdown
```

5.2 ASA Firewall

```
//Bind physical interfaces to VLANs

interface Ethernet0/0

 switchport access vlan 1

 no shutdown


interface Ethernet0/1

 switchport access vlan 2

 no shutdown


//Configure VLAN interfaces

interface vlan 1

 nameif inside

 security-level 100

 ip address 10.0.10.1 255.255.255.0

 no shutdown


interface vlan 2

 nameif outside

 security-level 0

 ip address 192.168.50.1 255.255.255.0

 no shutdown
```

//NAT for outbound access

object network INSIDE-NET

 subnet 10.0.10.0 255.255.255.0

 nat (inside,outside) dynamic interface

//Default route to router

route outside 0.0.0.0 0.0.0.0 192.168.50.10

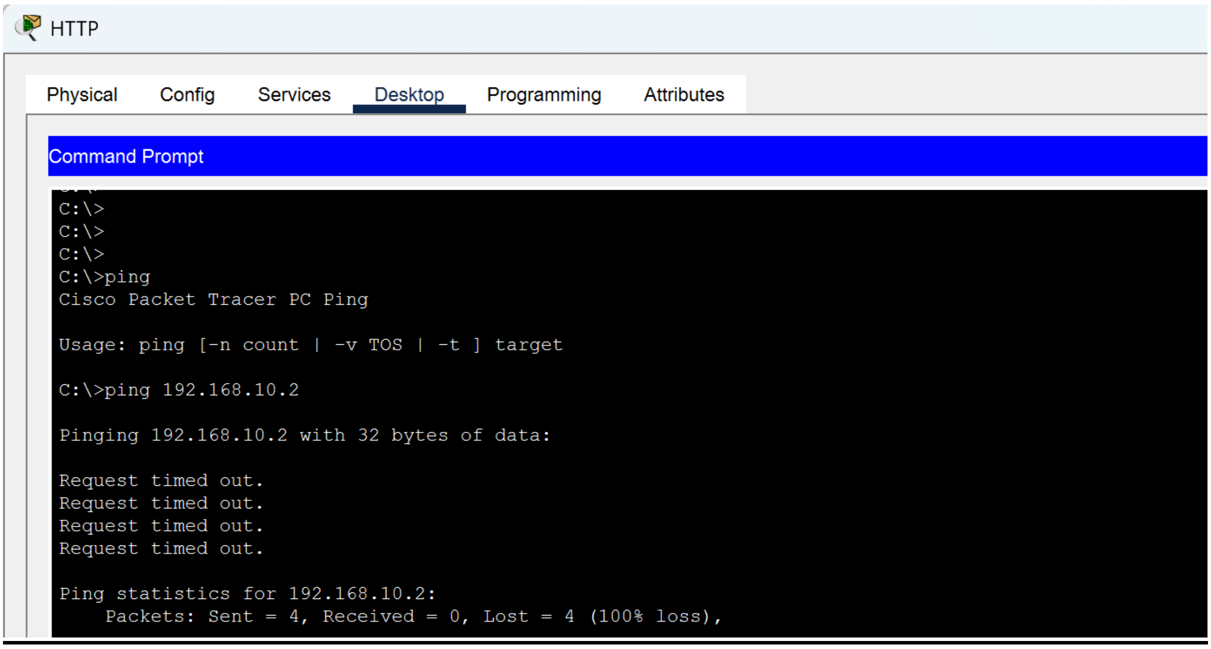
//access list

access-list OUTSIDE-IN extended deny ip host 192.168.50.10 10.0.10.0 255.255.255.0

access-list OUTSIDE-IN extended deny ip host 192.168.50.20 10.0.10.0 255.255.255.0

access-group OUTSIDE-IN in interface outside

outside server cannot ping to inside PC so firewall effective



```
C:\>
C:\>
C:\>
C:\>ping
Cisco Packet Tracer PC Ping

Usage: ping [-n count | -v TOS | -t ] target

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

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

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

6.0 Static routing

6.1 Main _R

ip route 192.168.10.0 255.255.255.0 10.0.0.1

ip route 192.168.20.0 255.255.255.0 10.0.0.5

ip route 192.168.40.0 255.255.255.0 10.0.0.9

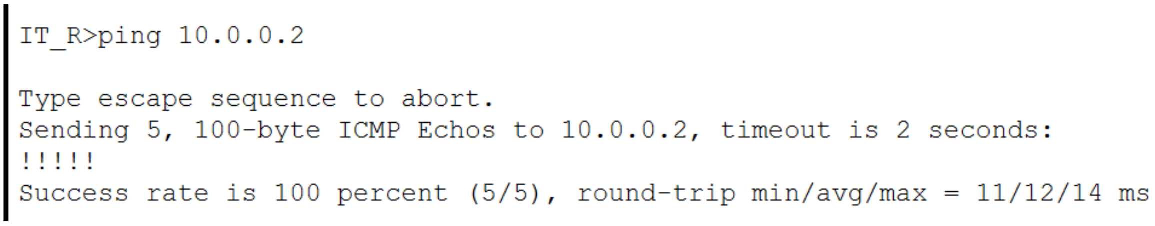
ip route 192.168.30.0 255.255.255.0 10.0.0.14

ip route 10.0.10.0 255.255.255.0 192.168.50.1

6.2 IT_R

ip route 0.0.0.0 0.0.0.0 10.0.0.2

IT_R to MAIN_R

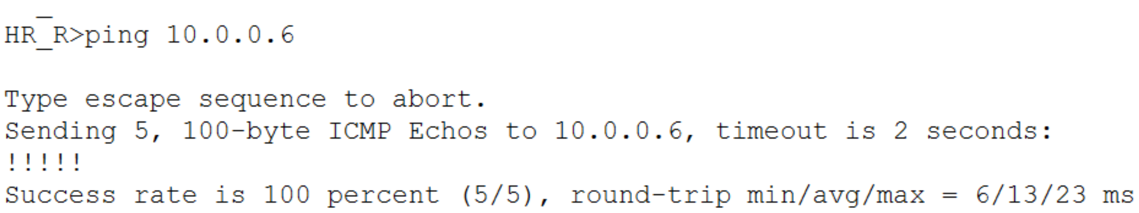


```
IT_R>ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/12/14 ms
```

6.3 HR_R

ip route 0.0.0.0 0.0.0.0 10.0.0.6

HR_R to MAIN_R

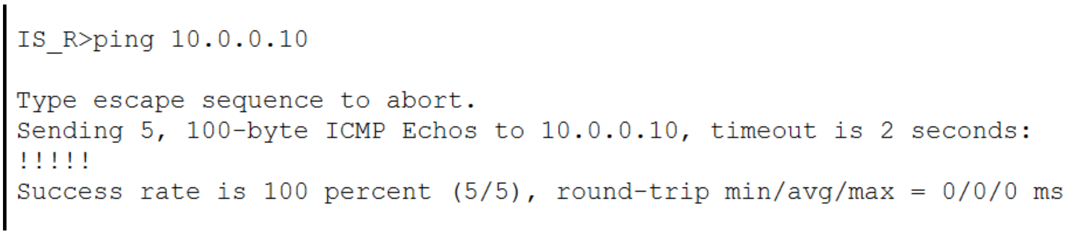


```
HR_R>ping 10.0.0.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/13/23 ms
```

6.4 IS_R

ip route 0.0.0.0 0.0.0.0 10.0.0.10

IS_R to MAIN_R

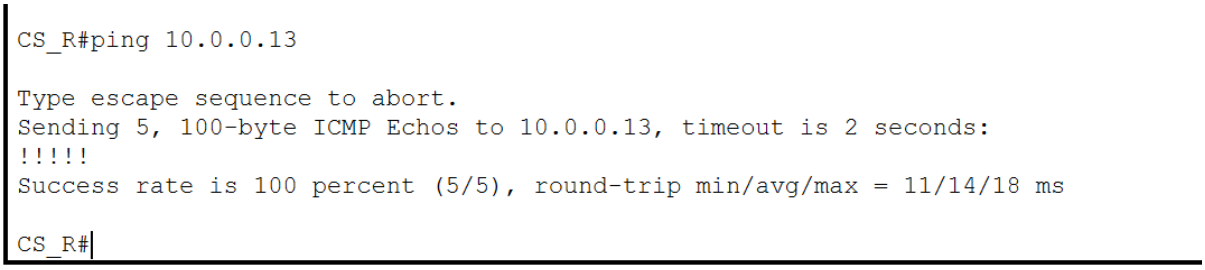


```
IS_R>ping 10.0.0.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

6.5 CS_R

ip route 0.0.0.0 0.0.0.0 10.0.0.13

CS_R to MAIN_R



```
CS_R#ping 10.0.0.13

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/14/18 ms

CS_R#
```

7.0 DHCP

7.1 DHCP FOR IT PC

7.1.1 IT_R

```
//Link to IT_S
//Subinterface for VLAN 10
interface gigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 no shutdown

//DHCP pool for IT
ip dhcp pool IT_POOL
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.50.20
```

7.1.2 IT_S

```
//Create vlan 10
vlan 10

//Assign IT_PC_1 to VLAN 10
interface fastEthernet0/2
 switchport mode access
 switchport access vlan 10
```

//Assign IT_PC_2 to VLAN 10

interface fastEthernet0/3

 switchport mode access

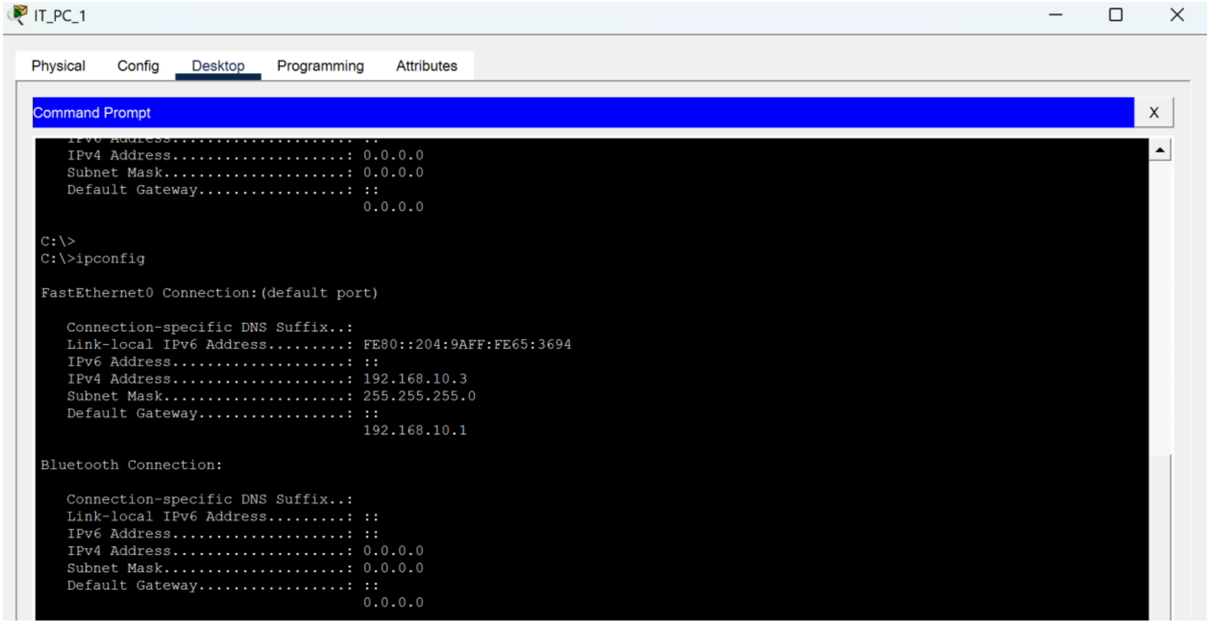
 switchport access vlan 10

//Trunk uplink to IT_R

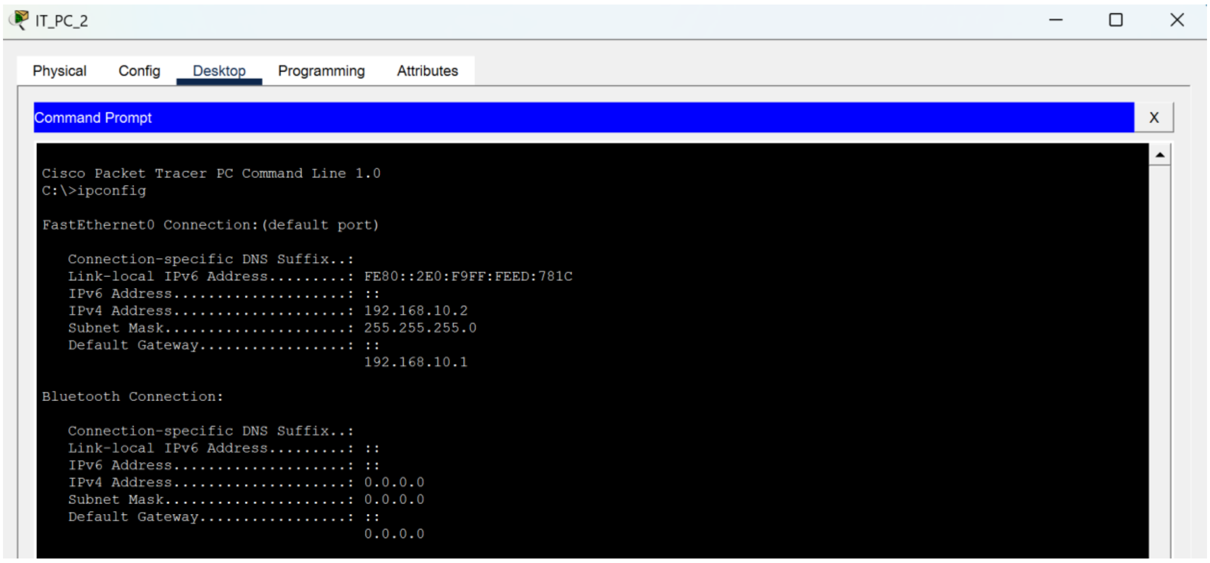
interface fastEthernet0/1

 switchport mode trunk

 switchport trunk allowed vlan 10



```
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::204:9AFF:FE65:3694
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.10.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.10.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```



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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::2E0:F9FF:FEED:781C
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.10.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.10.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```

7.2DHCP FOR HR PC

7.2.1 HR_R

```
//Link to HR_S

//Subinterface for VLAN 20

interface gigabitEthernet0/0.20

 encapsulation dot1Q 20

 ip address 192.168.20.1 255.255.255.0

 no shutdown


// DHCP pool for HR

ip dhcp pool HR_POOL

 network 192.168.20.0 255.255.255.0

 default-router 192.168.20.1

 dns-server 192.168.50.20
```

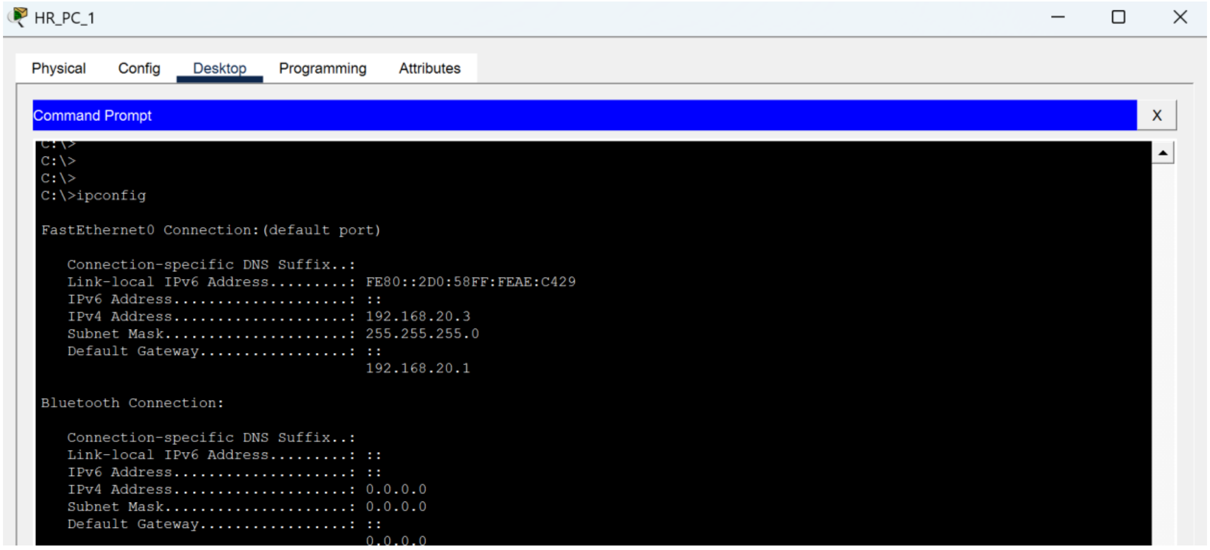
7.2.2 HR_S_1

```
// Create VLAN 20

vlan 20


//Trunk to HR_R

interface fastEthernet0/1

 switchport mode trunk

 switchport trunk allowed vlan 20
```

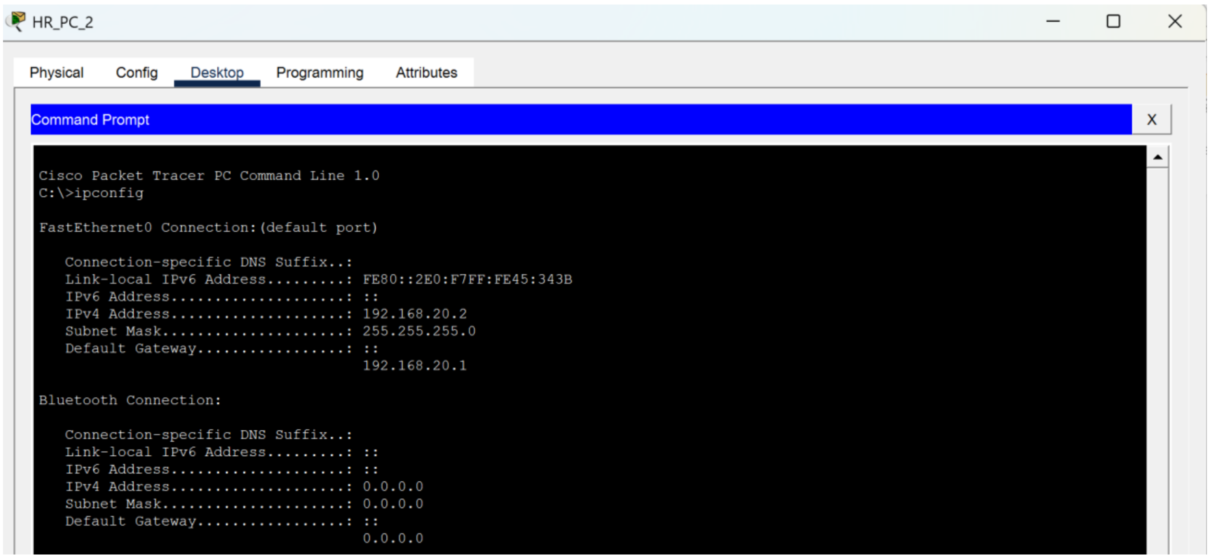
```
// Trunk to HR_S_2
interface fastEthernet0/2
 switchport mode trunk
 switchport trunk allowed vlan 20
// Trunk to HR_S_3
interface fastEthernet0/3
 switchport mode trunk
 switchport trunk allowed vlan 20
```

7.2.3 HR_S_2

```
//Create VLAN 20
vlan 20

//Trunk to HR_S_1
interface fastEthernet0/1
 switchport mode trunk
 switchport trunk allowed vlan 20

// Access port for HR_PC_1
interface fastEthernet0/2
 switchport mode access
 switchport access vlan 20
```



```
C:\>
C:\>
C:\>
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: 
   Link-local IPv6 Address.........: FE80::2D0:58FF:FEAE:C429
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.20.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.20.1

Bluetooth Connection:

   Connection-specific DNS Suffix..: 
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```



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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: 
   Link-local IPv6 Address.........: FE80::2E0:F7FF:FE45:343B
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.20.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.20.1

Bluetooth Connection:

   Connection-specific DNS Suffix..: 
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```

7.3 DHCP FOR IS_PC

7.3.1 IS_R

//Link to IS_R

//Subinterface for VLAN 40

interface gigabitEthernet0/1.40

 encapsulation dot1Q 40

 ip address 192.168.40.1 255.255.255.0

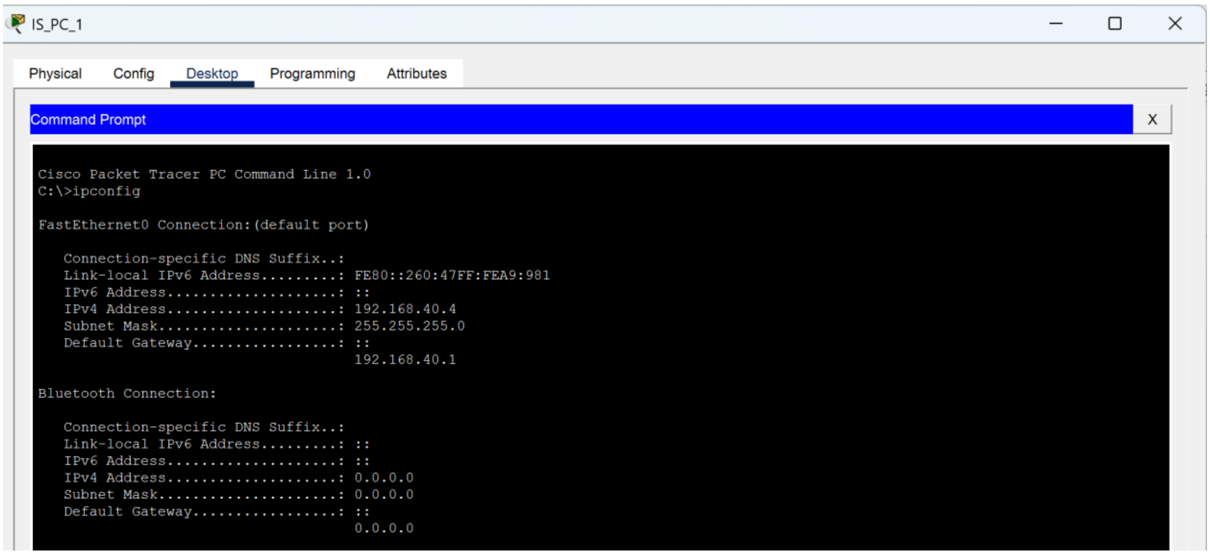
```
 no shutdown

// DHCP pool for IS
ip dhcp pool IS_POOL
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 192.168.50.11
```

7.3.2 IS_S_1

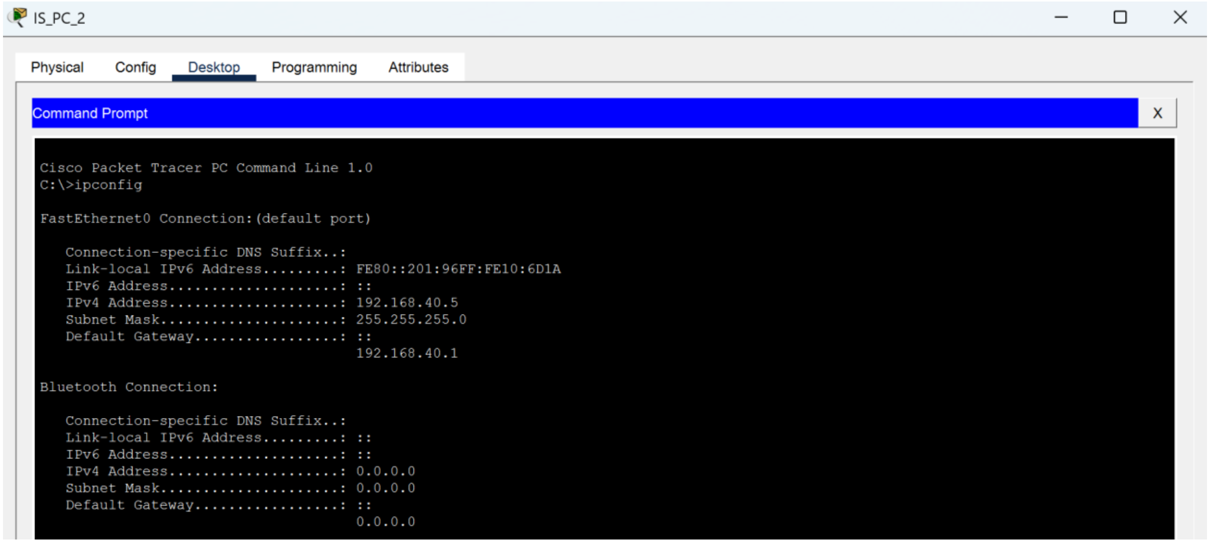
```
// Create VLAN 40
vlan 40

//Trunk to IS_S_2, IS_S_4, IS_R
interface range FastEthernet0/1 -3
 switchport mode trunk
 switchport trunk allowed vlan 40

interface fastEthernet0/5
switchport mode trunk
 switchport trunk allowed vlan 40

// Access port for HR_PC_4
interface fastEthernet0/4
 switchport mode access
 switchport access vlan 40
```

7.3.3 IS_S_2 & IS_S_3 & IS_S_4

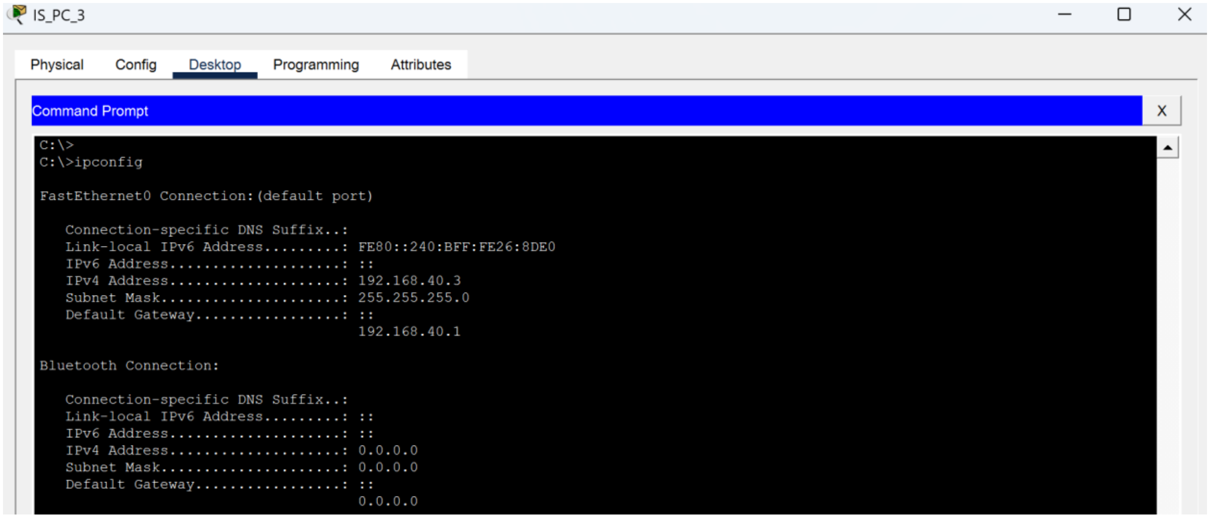
```
// Create VLAN 40

vlan 40







//Trunk to switchers

interface range FastEthernet0/1 - 2

 switchport mode trunk

 switchport trunk allowed vlan 40


interface fastEthernet0/4

switchport mode trunk

 switchport trunk allowed vlan 40


// Access port for PC

interface fastEthernet0/3

 switchport mode access

 switchport access vlan 40
```



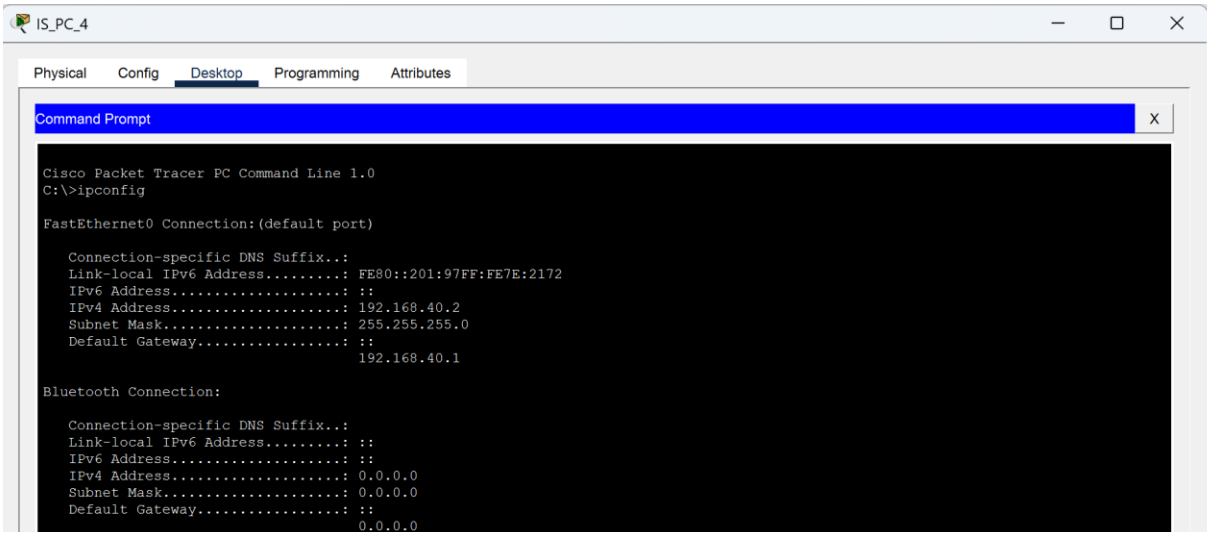
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: 
   Link-local IPv6 Address.........: FE80::260:47FF:FEA9:981
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.40.4
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.40.1

Bluetooth Connection:

   Connection-specific DNS Suffix..: 
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```



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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: 
   Link-local IPv6 Address.........: FE80::201:96FF:FE10:6D1A
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.40.5
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.40.1

Bluetooth Connection:

   Connection-specific DNS Suffix..: 
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```

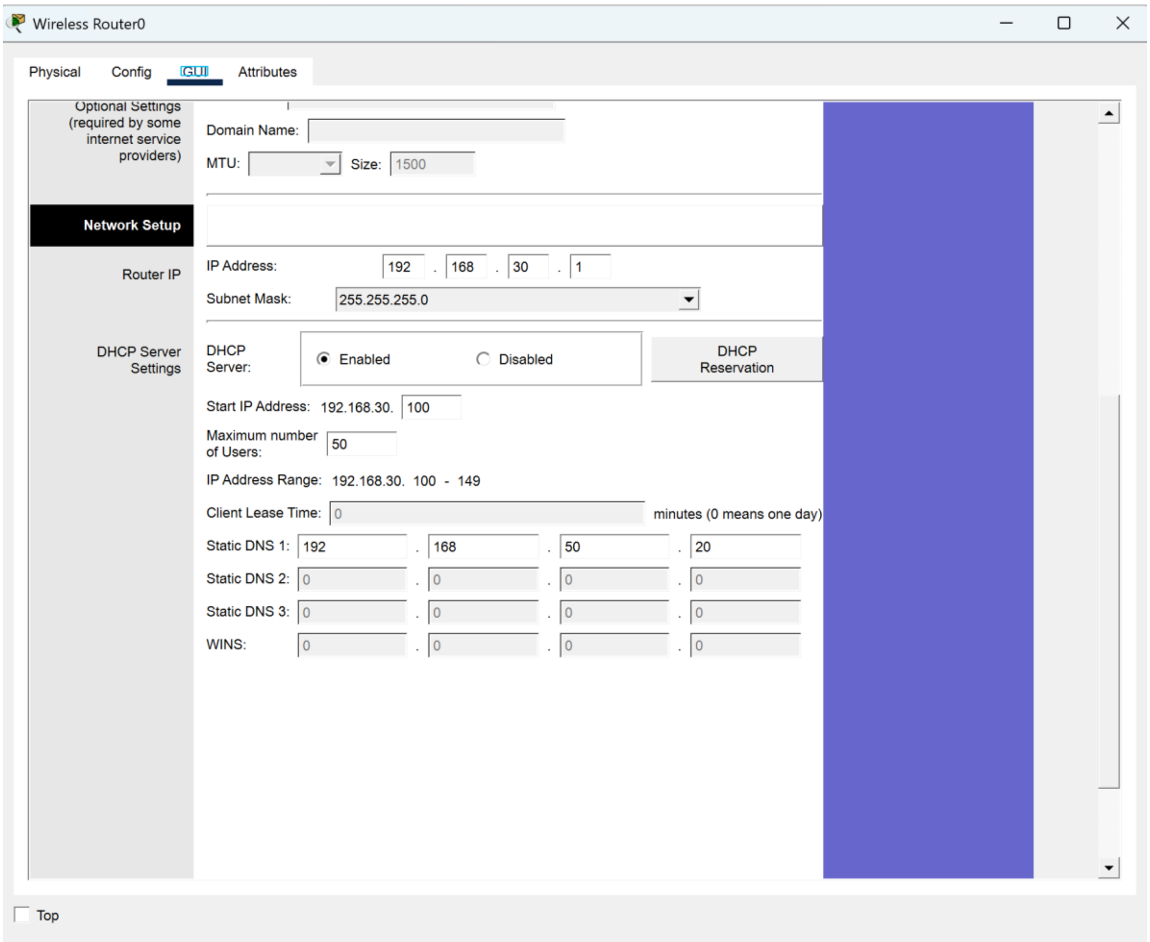


```
C:\>
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::240:BFF:FE26:8DE0
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.40.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.40.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```



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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::201:97FF:FE7E:2172
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.40.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.40.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```

7.4 DHCP FOR CS_PC



Optional Settings (required by some internet service providers)

Domain Name:

MTU: Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 30 . 1

Subnet Mask: 255.255.255.0

DHCP Server Settings

DHCP Server: ● Enabled ○ Disabled

DHCP Reservation

Start IP Address: 192.168.30. 100

Maximum number of Users: 50

IP Address Range: 192.168.30. 100 - 149

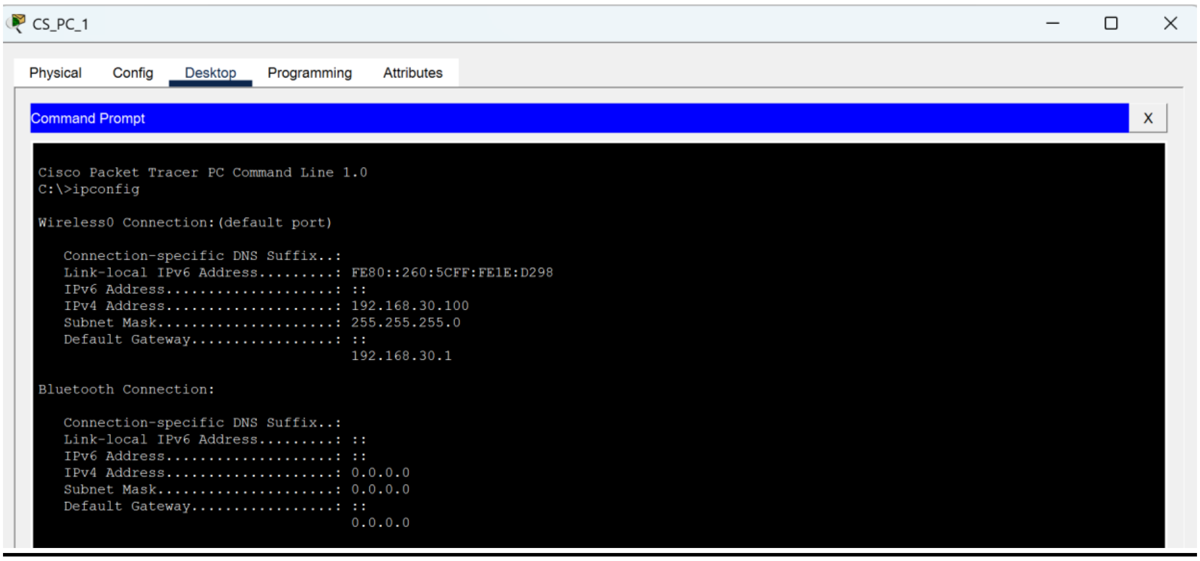
Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 192 . 168 . 50 . 20

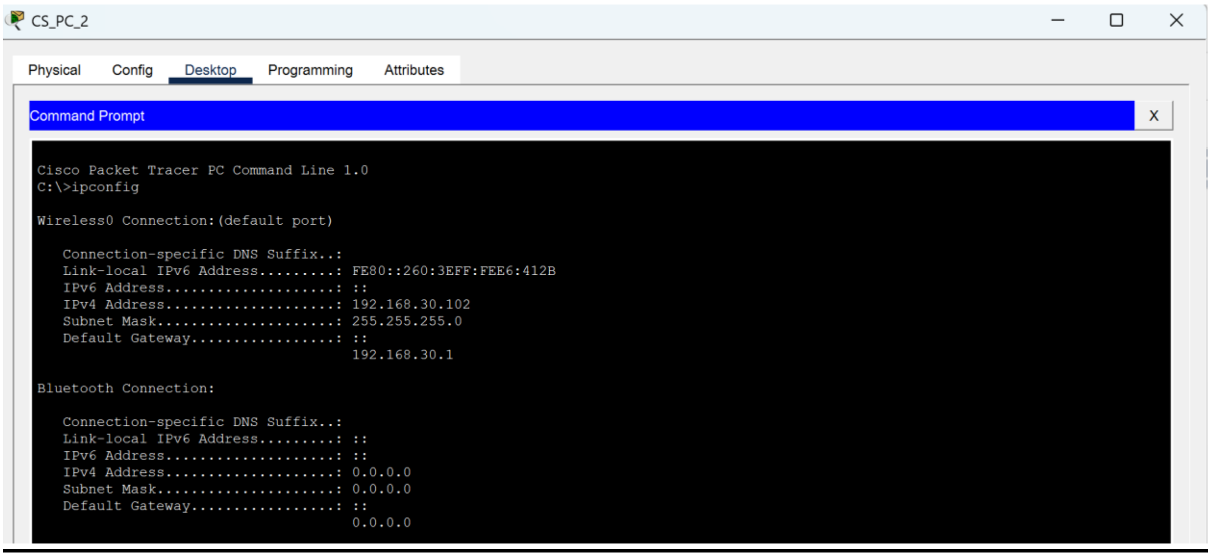
Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0



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

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::260:5CFF:FE1E:D298
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.30.100
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.30.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```



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

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::260:3EFF:FEE6:412B
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.30.102
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.30.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```

7.5 PC IP address after DHCP configuration and static IP addressing

Device	IP Address	IP type
IT_PC_1	192.168.10.3	DHCP
IT_PC_2	192.168.10.2	DHCP
HR_PC_1	192.168.20.3	DHCP
HR_PC_2	192.168.20.2	DHCP
IS_PC_1	192.168.40.4	DHCP
IS_PC_2	192.168.40.5	DHCP
IS_PC_3	192.168.40.3	DHCP
IS_PC_4	192.168.40.2	DHCP
CS_PC_1	192.168.30.100	DHCP
CS_PC_2	192.168.30.102	DHCP
HTTP server	192.168.50.10	Static
DNS server	192.168.50.11	Static

8.0 Password &SSH setup

8.1 MAIN_R

```
// Set encrypted enable password
enable secret cisco123


// Create local admin account
username guest privilege 1 secret guest123


// Secure console accessenable
line console 0
 login local
 exec-timeout 5 0
 logging synchronous


// Secure remote access (VTY lines)
line vty 0 4
 login local
 transport input ssh
 exec-timeout 10 0


// Encrypt all plaintext passwords
service password-encryption
```

// Add a legal warning banner

banner motd #

Unauthorized access prohibited. Activity may be monitored.

#

hostname MAIN_R

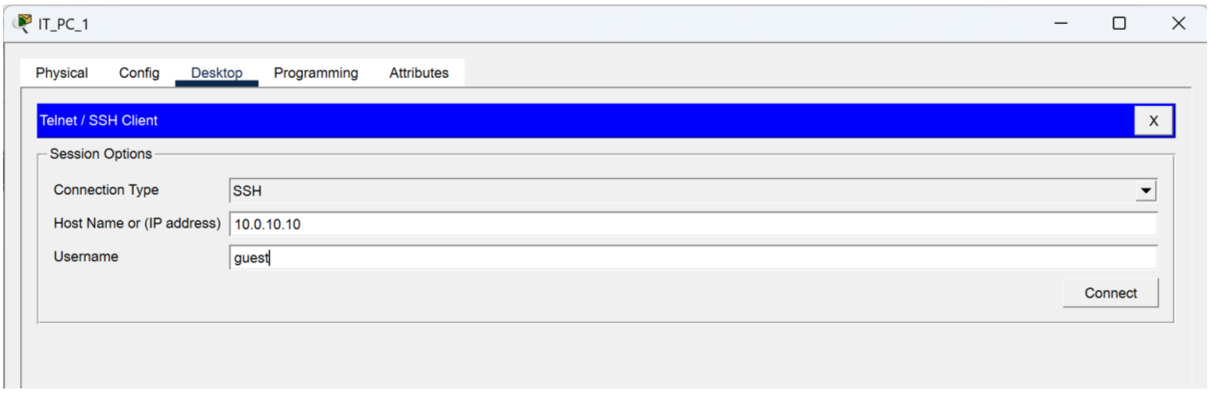
ip domain-name corp.local

crypto key generate rsa

How many bits in the modulus [512]: 1024

ip ssh version 2

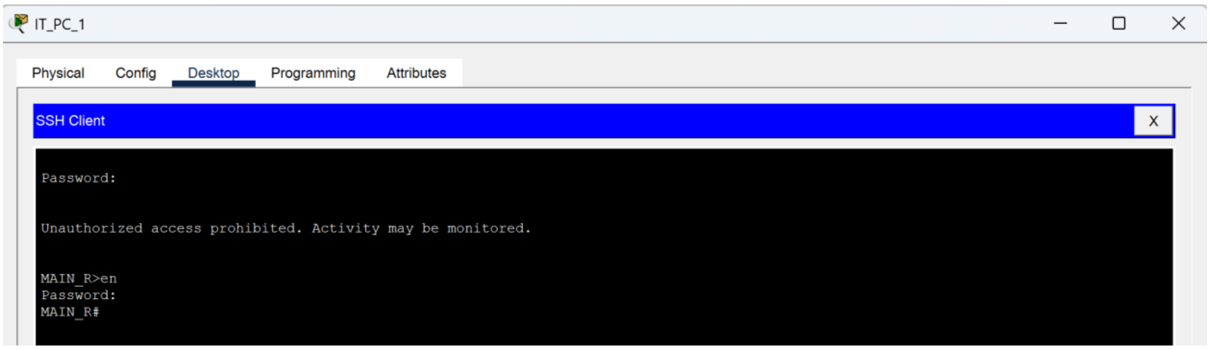
8.1.1 IT_PC_1 to MAIN_R



Connection Type: SSH

Host Name or (IP address): 10.0.10.10

Username: guest



```
Password:

Unauthorized access prohibited. Activity may be monitored.

MAIN_R>en
Password:
MAIN_R#
```

8.2 ASA SSH Setup

```
hostname ASA

domain-name corp.local

crypto key generate rsa modulus 1024

username admin password admin123

aaa authentication ssh console LOCAL

ssh 192.168.50.0 255.255.255.0 inside

ssh timeout 10

enable password cisco123
```

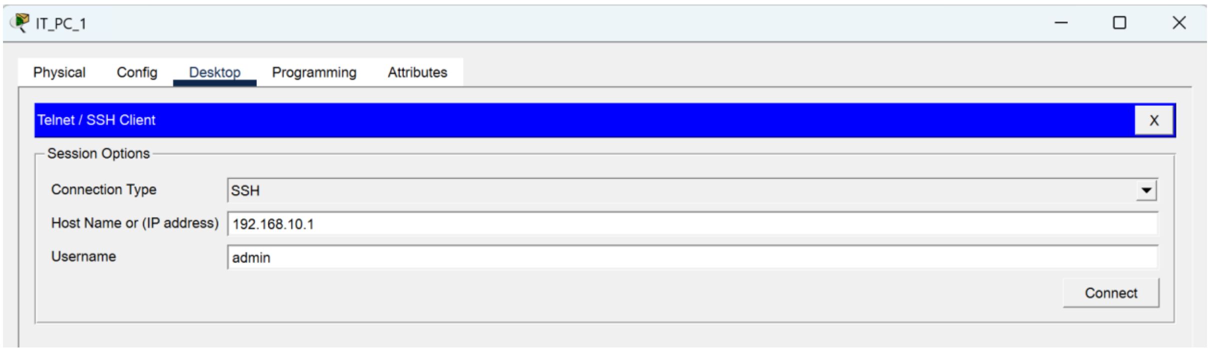
8.3 IT_R& IS_R& HR_R& CS_R

```
// Set encrypted enable password

enable secret cisco123


// Create local admin account

username admin privilege 15 secret admin123


// Secure console accessenable

line console 0

 login local

 exec-timeout 5 0

 logging synchronous
```

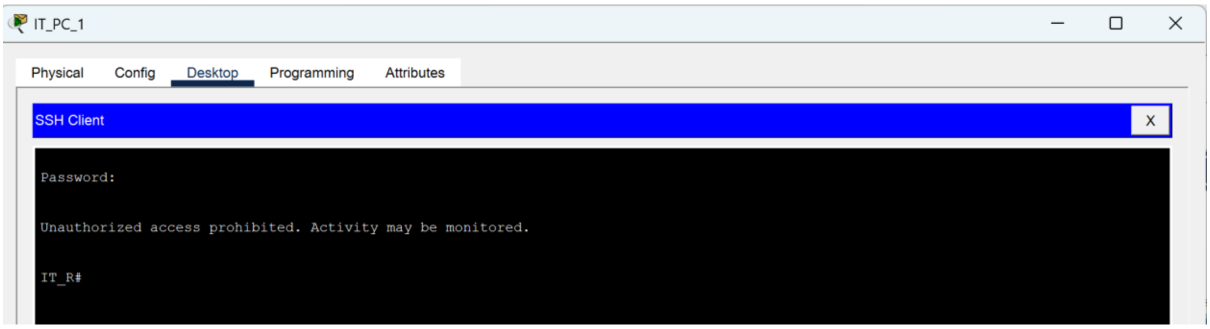
```
// Secure remote access (VTY lines)
line vty 0 4
 login local
 transport input ssh
 exec-timeout 10 0

// Encrypt all plaintext passwords
service password-encryption

// Add a legal warning banner
banner motd #
Unauthorized access prohibited. Activity may be monitored.
#
hostname IT_R/HR_R/IS_R/CS_R
ip domain-name corp.local

crypto key generate rsa
How many bits in the modulus [512]: 1024
ip ssh version 2
```

8.3.1 From IT_PC_1 ssh to router

SSH to IT_R

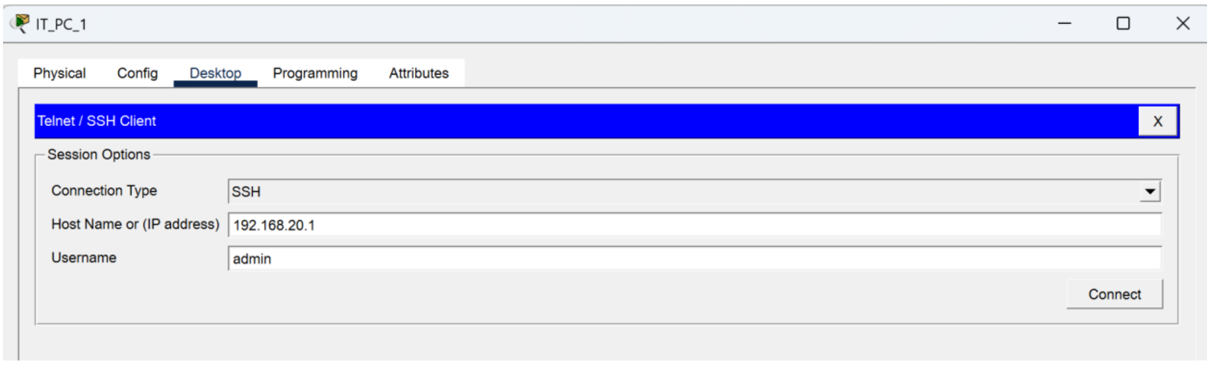


Connection Type: SSH
Host Name or (IP address): 192.168.10.1
Username: admin

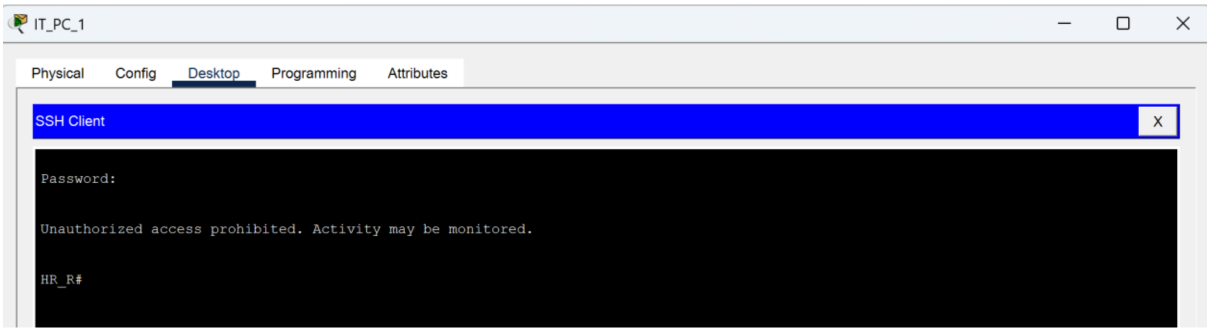


```
Password:

Unauthorized access prohibited. Activity may be monitored.

IT_R#
```

SSH to HR_

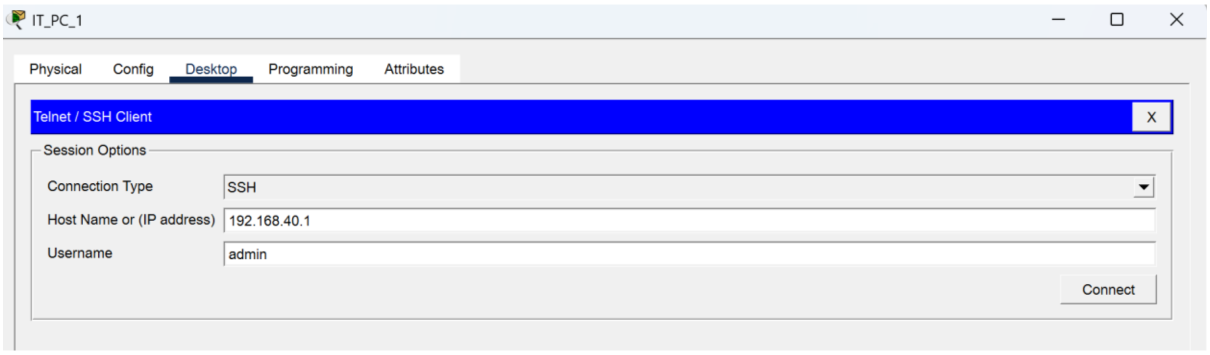


Connection Type: SSH
Host Name or (IP address): 192.168.20.1
Username: admin

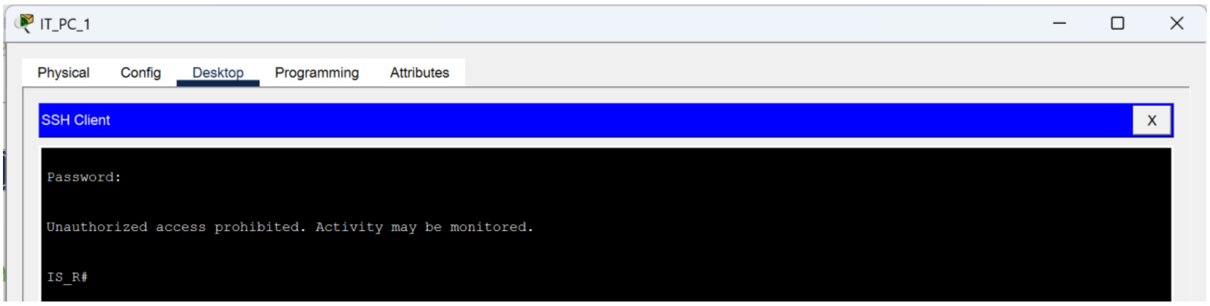


```
Password:

Unauthorized access prohibited. Activity may be monitored.

HR_R#
```

SSH to IS_R

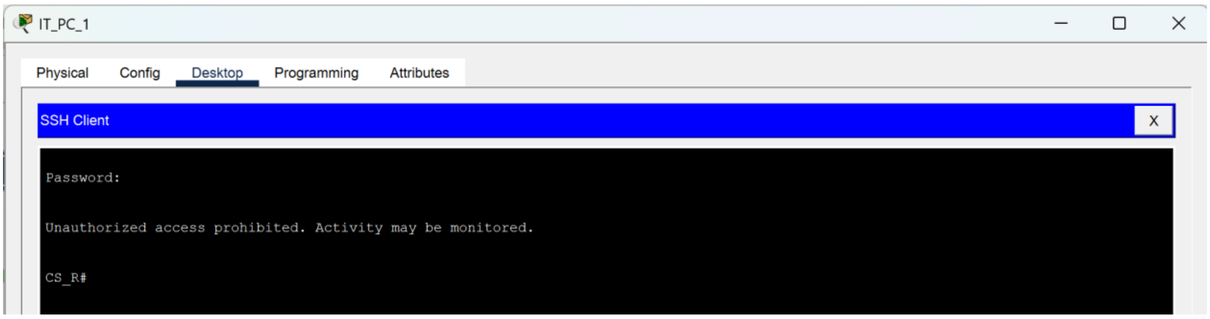


Connection Type: SSH
Host Name or (IP address): 192.168.40.1
Username: admin

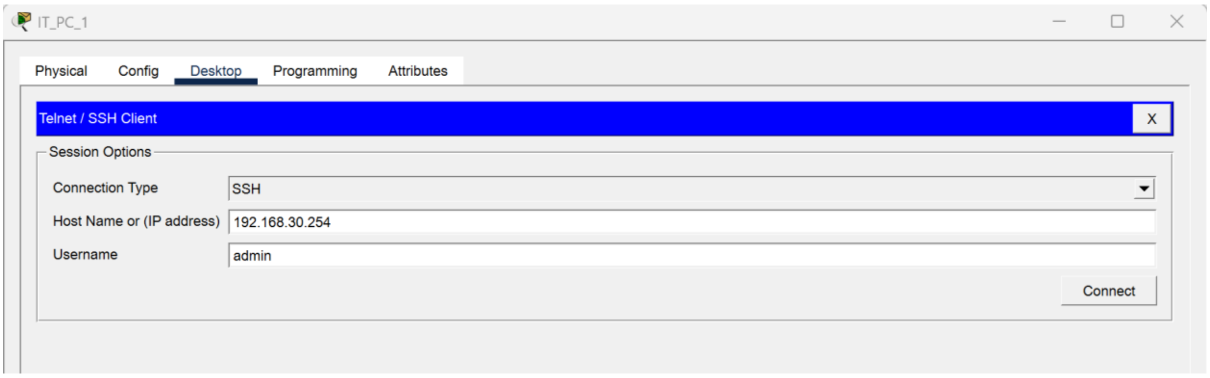


```
Password:

Unauthorized access prohibited. Activity may be monitored.

IS_R#
```

SSH to CS_R



```
Password:

Unauthorized access prohibited. Activity may be monitored.

CS_R#
```



Connection Type: SSH
Host Name or (IP address): 192.168.30.254
Username: admin

9.0 SNMP

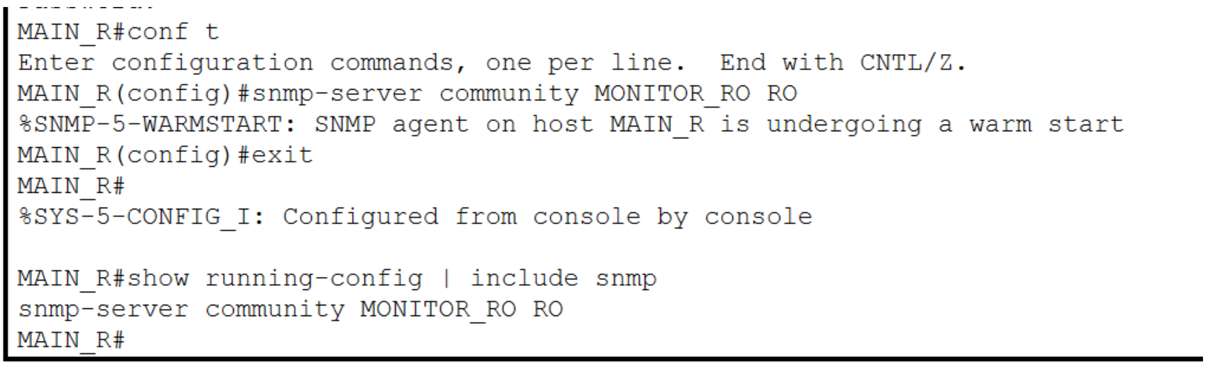
//Enables SNMP

snmp-server community MONITOR_RO RO

//check

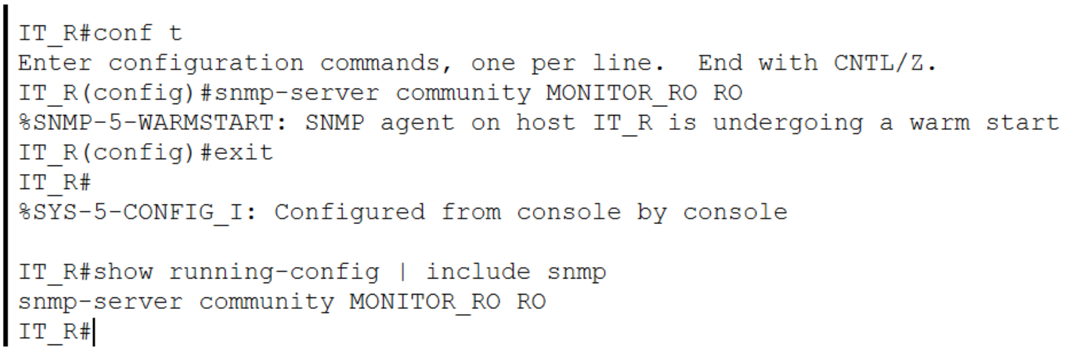
show running-config | include snmp

MAIN_R



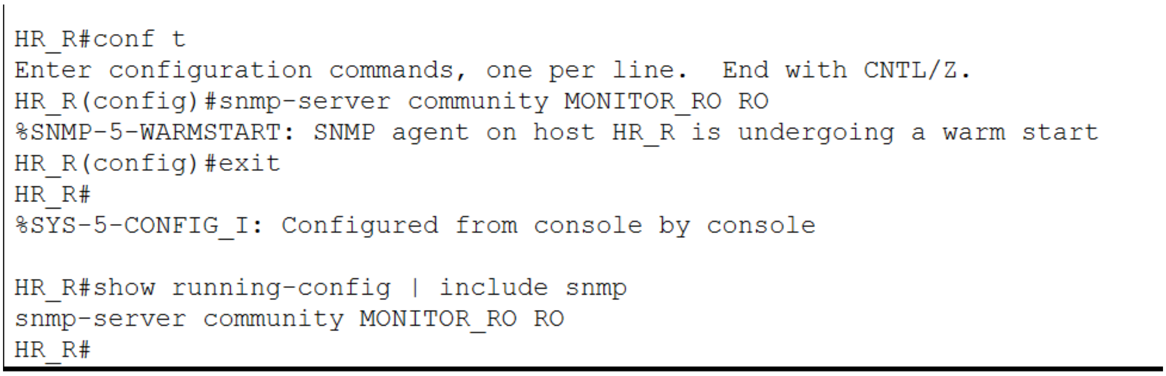
```
MAIN_R#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MAIN_R(config)#snmp-server community MONITOR_RO RO
%SNMP-5-WARMSTART: SNMP agent on host MAIN_R is undergoing a warm start
MAIN_R(config)#exit
MAIN_R#
%SYS-5-CONFIG_I: Configured from console by console

MAIN_R#show running-config | include snmp
snmp-server community MONITOR_RO RO
MAIN_R#
```

IT_R



```
IT_R#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IT_R(config)#snmp-server community MONITOR_RO RO
%SNMP-5-WARMSTART: SNMP agent on host IT_R is undergoing a warm start
IT_R(config)#exit
IT_R#
%SYS-5-CONFIG_I: Configured from console by console

IT_R#show running-config | include snmp
snmp-server community MONITOR_RO RO
IT_R#
```

HR_R



```
HR_R#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HR_R(config)#snmp-server community MONITOR_RO RO
%SNMP-5-WARMSTART: SNMP agent on host HR_R is undergoing a warm start
HR_R(config)#exit
HR_R#
%SYS-5-CONFIG_I: Configured from console by console

HR_R#show running-config | include snmp
snmp-server community MONITOR_RO RO
HR_R#
```

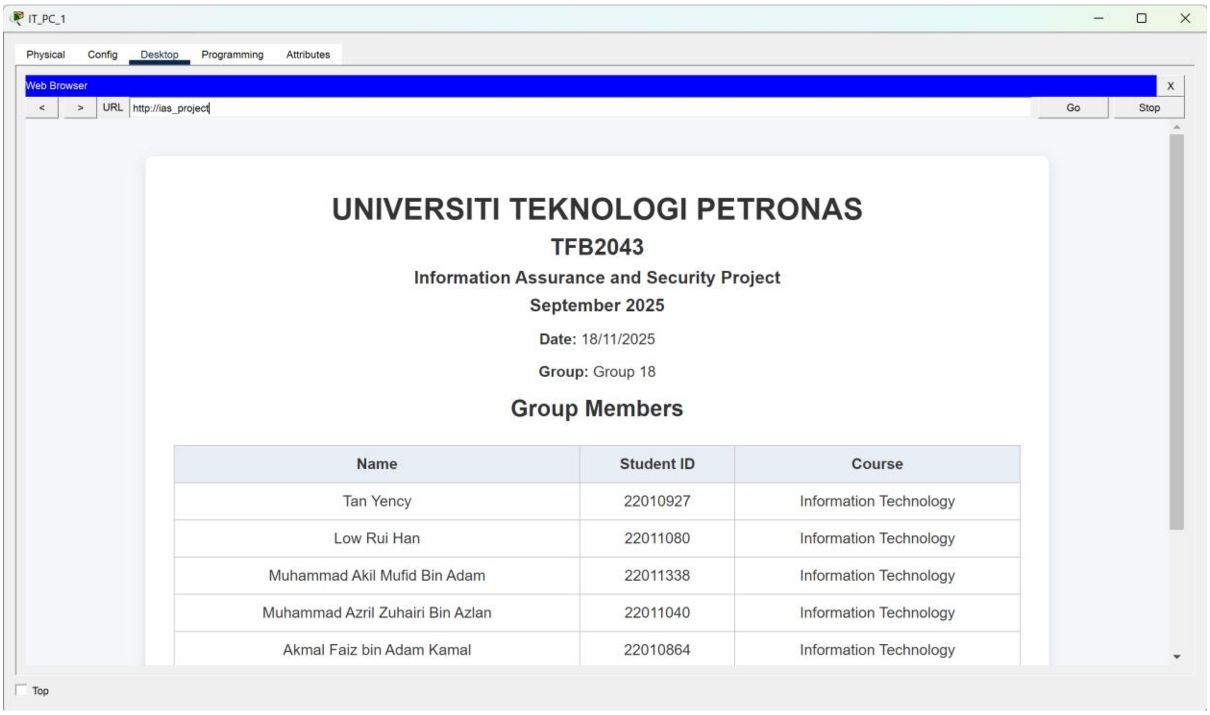
IS_R

```
IS_R#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IS_R(config)#snmp-server community MONITOR_RO RO
%SNMP-5-WARMSTART: SNMP agent on host IS_R is undergoing a warm start
IS_R(config)#exit
IS_R#
%SYS-5-CONFIG_I: Configured from console by console

IS_R#show running-config | include snmp
snmp-server community MONITOR_RO RO
IS_R#
```

CS_R

```
CS_R#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CS_R(config)#snmp-server community MONITOR_RO RO
%SNMP-5-WARMSTART: SNMP agent on host CS_R is undergoing a warm start
CS_R(config)#exit
CS_R#
%SYS-5-CONFIG_I: Configured from console by console

CS_R#show running-config | include snmp
snmp-server community MONITOR_RO RO
CS_R#
```

10.0 PC reach to the website



URL http://ias_project

UNIVERSITI TEKNOLOGI PETRONAS

TFB2043

Information Assurance and Security Project

September 2025

Date: 18/11/2025

Group: Group 18

Group Members

Name	Student ID	Course
Tan Yency	22010927	Information Technology
Low Rui Han	22011080	Information Technology
Muhammad Akil Mufid Bin Adam	22011338	Information Technology
Muhammad Azril Zuhairi Bin Azlan	22011040	Information Technology
Akmal Faiz bin Adam Kamal	22010864	Information Technology

11.0 SECURITY ANALYSIS

1. Unsecured Wireless Network Access

a) Vulnerability

The wireless router on the CS Subnet, which is a critical entry point, currently only has DHCP settings, but does not specify any wireless security measures such as WPA, WPA2, WPA3 or PSK. An attacker could easily gain access to the 192.168.30.0 network and pivot to other internal segments via the MAIN_R router.

b) Mitigation

A potential solution is configuring WPA2 or WPA3 with a strong Pre-Shared Key (PSK) alongside a robust password complexity policy. Furthermore, implementing MAC Adress filtering could be an additional layer of control.

2. Internal Spanning Tree Protocol (STP) Manipulation

a) Vulnerability

The current setup utilises multiple interconnected Cisco Switches in the IT, HR, and IS departments, which means the network is relying on STP to prevent loops. An attacker can infiltrate an unsecured access port by inserting superior BPDU frames, forcing their device to become the Root Bridge. This enables the attacker to reroute traffic for sniffing across VLANs.

b) Mitigation

A feasible approach is enabling BPDU Guard using the "spanning-tree bpdguard enable" command on all access ports that are connected to user devices such as PCs. This immediately shuts down any port receiving a BPDU and keeps the access port secure. Additionally, a Root Guard can be used on trunk ports to protect the root bridge selection.

3. Weak Password Policy on Routers

a) Vulnerability

The current setup has security measures such as secured remote access with SSH and utilisation of the “enable secret” command for encryption. However, the local user account passwords are simple and predictable. For example, guest123 for guest on MAIN_R and admin123 for admin on IT_R, HR_R, and IS_R. Additionally, the ASA enable password is Cisco123. Passwords like ‘cisco123’, ‘guest123’ and ‘admin123’ can be easily guessed or quickly cracked by dictionary or brute-force attacks. This is worsened by the standard usernames such as ‘guest’ and ‘admin’. The use of standard, common usernames further lower the bar for a successful dictionary or brute-force attack. This exposes the device to unauthorised access even with SSH enabled, as an attacker only needs to crack the weak password.

b) Mitigation

The simplest effective solution is to enforce a strong, complex password policy across all network devices. For example, passwords should be minimum 12 characters, contain a mix of upper and lower case letters, numbers, and symbols. It also should not be based on common words or sequences. All local user passwords should be changed according to the newly set requirements. Additionally, the routers can be configured to detect and prevent brute-force arracks by limiting failed login attempts using the “login block-for X attempts Y” command.

12.0 Conclusion

The project has completed the designed, implemented, and secured the companies network infrastructure for a company containing four distinct departments such as Information Technology (IT), Customer Service (CS), Human Resource (HR), and Information Security (IS), along with a centralized server room. The main goal was to create a functional, efficient, and secure network environment that facilitates a smooth communication while safeguarding sensitive organizational data.

The Implementation began with a logical IP addressing scheme and static routing to ensure controlled data flow across the network's hybrid topology, which included star, tree, ring, and mesh configurations. Key security measures were rigorously applied, including the configuration of encrypted enable passwords and SSH access on all routers to prevent unauthorized access and ensure encrypted remote management. Furthermore, the activation of the ASA firewall, configured with specific security levels, access control lists (ACLS), and Network Address Translation (NAT), established a robust defensive perimeter, effectively isolating the internal network from external threats.

The use of DHCP streamlined network management by dynamically assigning IP configurations to PC while SNMP was enabled to provide a foundation for ongoing network monitoring and management. A thorough security analysis to find any potential vulnerabilities, such as an unsecured wireless access point, risks of STP manipulation, and a weak password policy. For each identified risk, practical and industry-aligned mitigation strategies were proposed demonstrating a proactive approach to risk management.

In summary, this project has achieved its goal of showcasing the practical application of network design and security principles using Cisco Packet Tracer. The resulting network is not only functional and scalable to support organizational growth but also embodies core information assurance principles-confidentiality, Integrity, and availability-by Integrating multiple layers of security controls.