CCNA project

“Enterprise Network Infrastructure Design Using VLANs, DHCP, EIGRP, and ACLs”

Information
Technology
Institute

:By

Abdalla Mohamed

Aboelfotouh

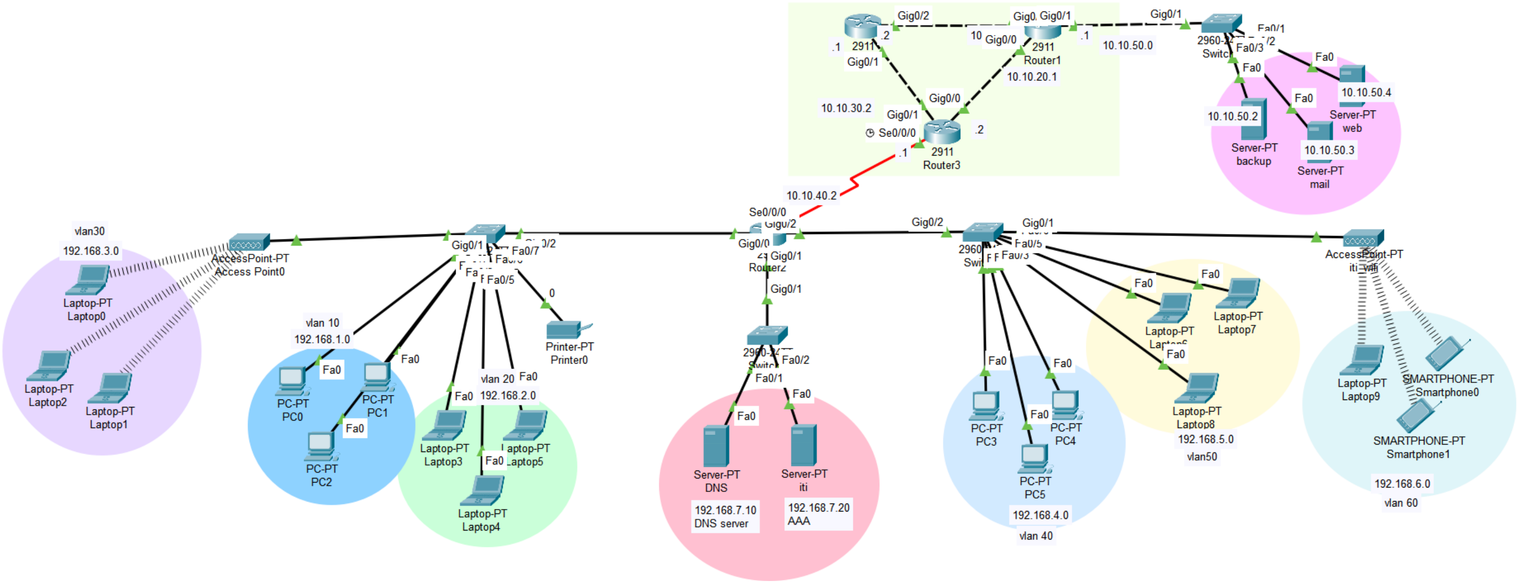
: Under Supervision

Eng. Saleh Mahmoud

1. Introduction

This project presents the design, implementation, and configuration of a complete enterprise network based on CCNA concepts. The network topology simulates a real-world organizational environment using multiple routers, switches, VLANs, servers, and end devices.

This project integrates core CCNA topics including VLANs, trunking, DHCP, dynamic routing, STP, SSH, AAA, and ACLs into a single functional network. It serves as a comprehensive hands-on practice project that reflects real enterprise networking scenarios and reinforces both configuration and troubleshooting skills.



2. Project Objectives

1. Design a scalable enterprise network topology using routers, switches, servers, wireless access points, and multiple end devices.

2. Implement VLAN segmentation to logically separate network departments, reduce broadcast traffic, and enhance network performance and security.

3. Configure inter-VLAN routing to enable communication between different VLANs while maintaining proper network isolation.

4. Deploy DHCP services to automatically distribute IP addresses, subnet masks, default gateways, and DNS server information to all end devices.

5. Implement dynamic routing using EIGRP to ensure efficient route exchange and reliable connectivity between routers.

6. Enable Rapid Spanning Tree Protocol (RSTP) on switches to prevent switching loops and ensure fast convergence.

7. Secure device management access by configuring hostnames, encrypted passwords, SSH-only remote access, and centralized authentication using a RADIUS server.

8. Apply Access Control Lists (ACLs) to control access to network services such as DNS, web, mail, and FTP/TFTP services based on host, network, and VLAN security policies.

9. Configure TFTP services to support network device configuration backup and restoration, simulating real enterprise network maintenance procedures.

10. Integrate enterprise network services including DNS, web, mail, DHCP, AAA (RADIUS), and TFTP to create a complete and functional network environment.

3. Basic Router and server Configuration and Secure Management

The router hostname:

Hostname: Abdalla Mohamed •

DomainName: ITI.com •

Password and Security Configuration:

- **Enable Secret:** Configured and encrypted
- **Service Password Encryption:** Enabled

Console Access Configuration:

The console line is secured with a password to prevent unauthorized local access.

- **Console Line:** line console 0
- **Authentication:** Password-based login

Remote Access Configuration (VTY Lines)

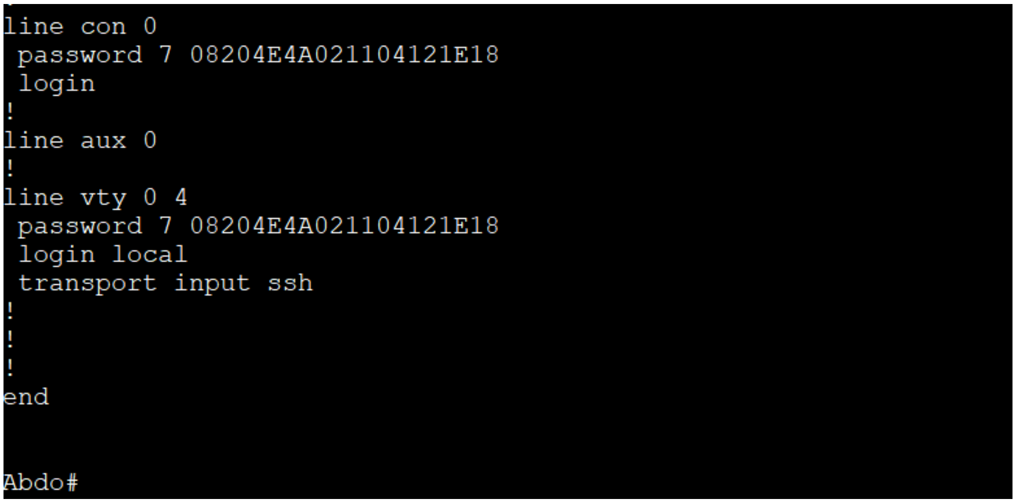
Virtual Terminal (VTY) lines are configured to allow secure remote management.

- **VTY Lines:** 0–15
- **Authentication Method:** Local username database
- **Allowed Protocol:** SSH only
- **RSA Key Generation:** Enabled
- **Remote Access Protocol:** SSH

Local User Account Configuration

A local user account is created to support SSH authentication. This user account is used for secure remote login to the router.

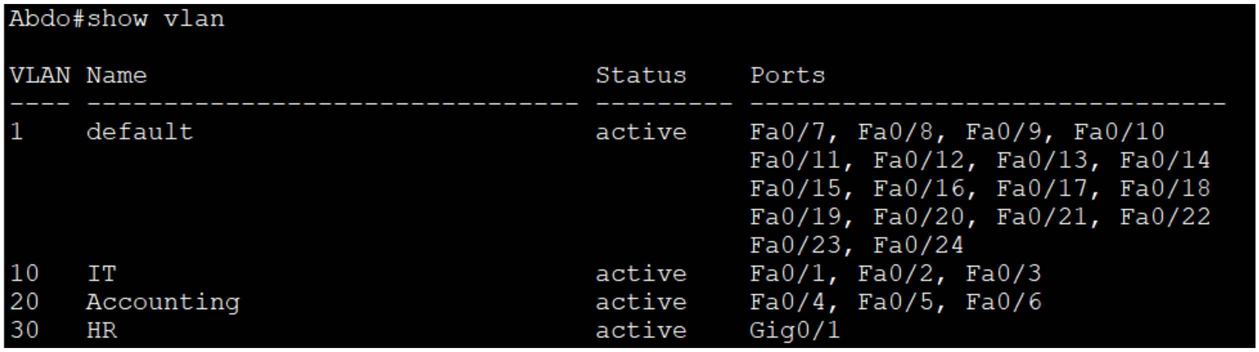
- **Username:** Elsayed
- **Password:** 123



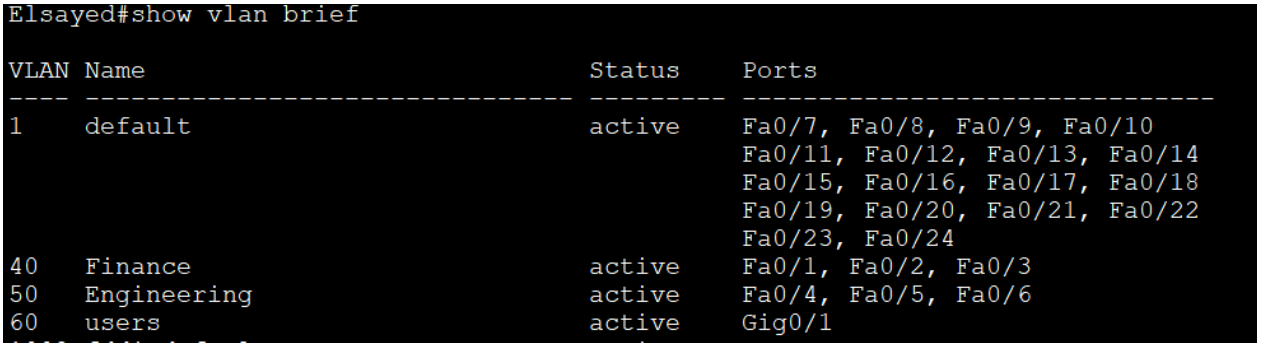
```
line con 0
 password 7 08204E4A021104121E18
 login
!
line aux 0
!
line vty 0 4
 password 7 08204E4A021104121E18
 login local
 transport input ssh
!
!
!
end


Abdo#
```

4. VLANs Table

VLAN ID	Department Name	IP Subnet Range	Default Gateway	Assigned Switch Ports
10	IT	192.168.1.0/24	192.168.1.1	Fa0/1, Fa0/2, Fa0/3
20	Accounting	192.168.2.0/24	192.168.2.1	Fa0/4, Fa0/5, Fa0/6
30	HR	192.168.3.0/24	192.168.3.1	Gig0/1
40	Finance	192.168.4.0/24	192.168.4.1	Fa0/1, Fa0/2, Fa0/3
50	Engineering	192.168.5.0/24	192.168.5.1	Fa0/4, Fa0/5, Fa0/6
60	Users	192.168.6.0/24	192.168.6.1	Gig0/1



```
Abdo#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
10   IT                               active    Fa0/1, Fa0/2, Fa0/3
20   Accounting                       active    Fa0/4, Fa0/5, Fa0/6
30   HR                               active    Gig0/1
```



```
Elsayed#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
40   Finance                          active    Fa0/1, Fa0/2, Fa0/3
50   Engineering                      active    Fa0/4, Fa0/5, Fa0/6
60   users                            active    Gig0/1
```

5. Access point

Two VLANs are extended through wireless access points to provide Wi-Fi access for different departments. Each wireless network is mapped to a specific VLAN, allowing wireless devices to obtain network access according to their assigned department.

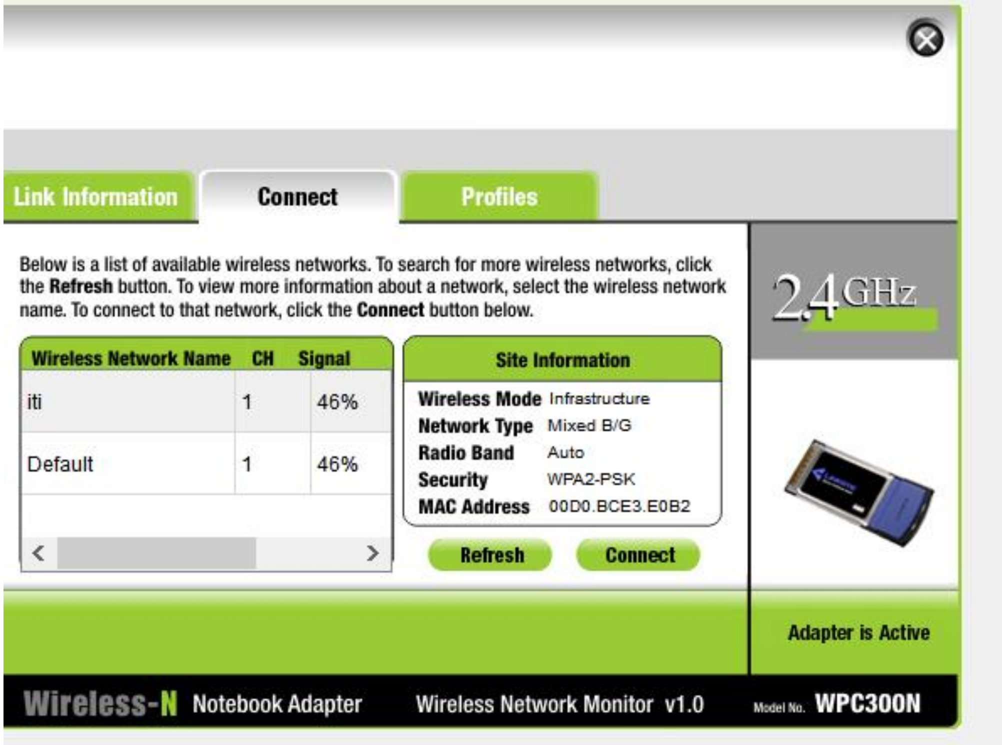
Connected Wireless Devices:

VLAN 30 (Default Wireless Network):

- VLAN ID: 30
- Department: Human Resources
- 3 Laptops
- Purpose: Provides wireless access for HR department users with controlled network access.

VLAN 60 (Wireless Network: ITI):

- Department: Users
- SSID Name: ITI
- 1 Laptop
- 2 Smartphones
- Purpose: Provides wireless access for general users and mobile devices.

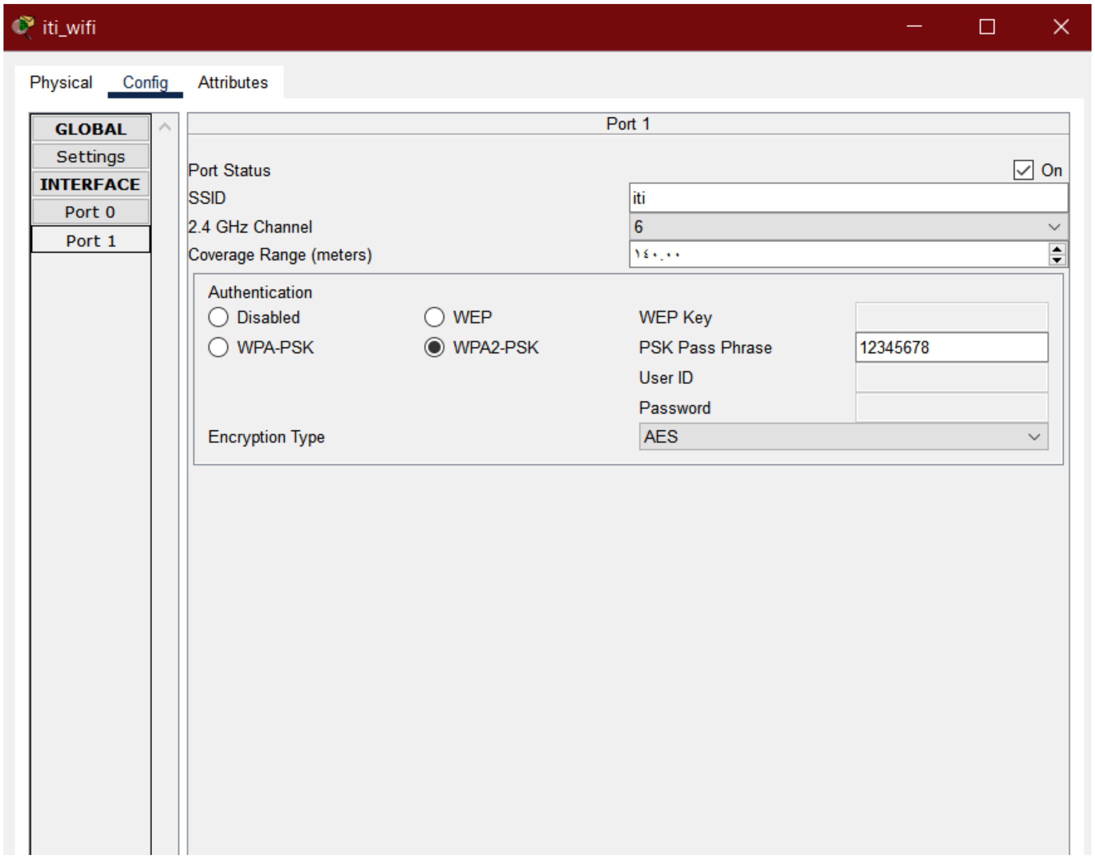


Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
iti	1	46%
Default	1	46%

Site Information

Wireless Mode Infrastructure
Network Type Mixed B/G
Radio Band Auto
Security WPA2-PSK
MAC Address 00D0.BCE3.E0B2



Port 1

Port Status ☑ On

SSID: iti

2.4 GHz Channel: 6

Coverage Range (meters): ١٤٠٫٠٠

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase: 12345678

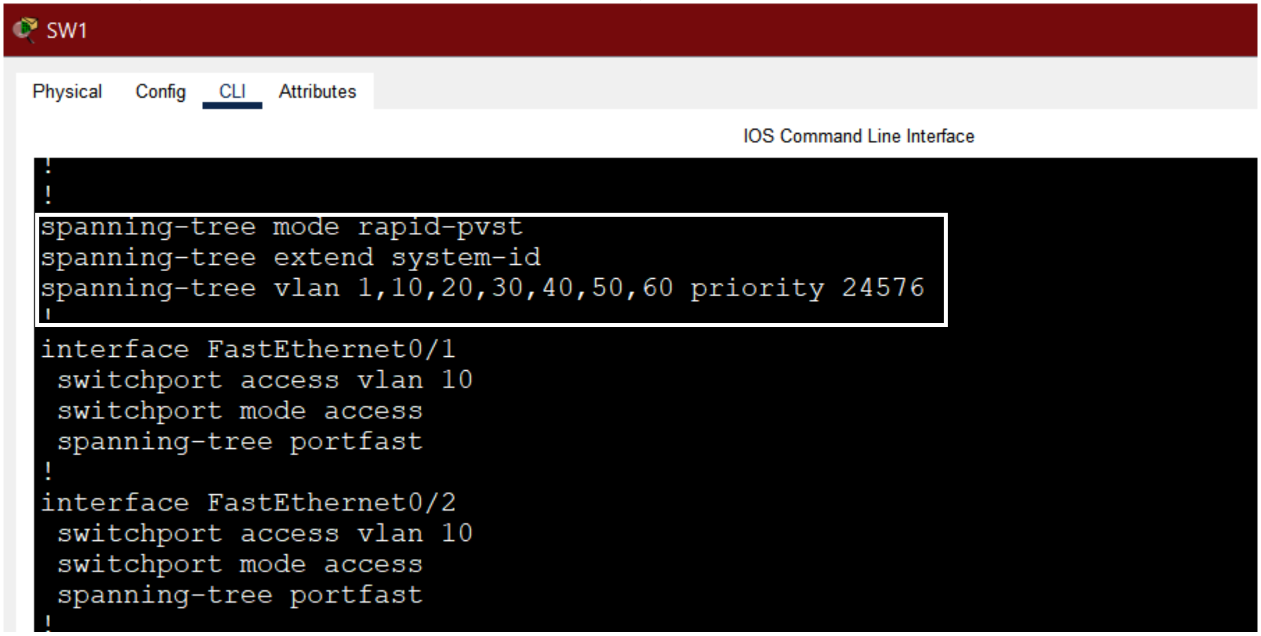
User ID

Password

Encryption Type: AES

6. Rapid Spanning Tree Protocol (RSTP)

Rapid Spanning Tree Protocol (RSTP) is enabled on all switches to prevent Layer 2 loops and provide fast network convergence. This ensures a stable, loop-free switching environment with quick recovery from link failures.

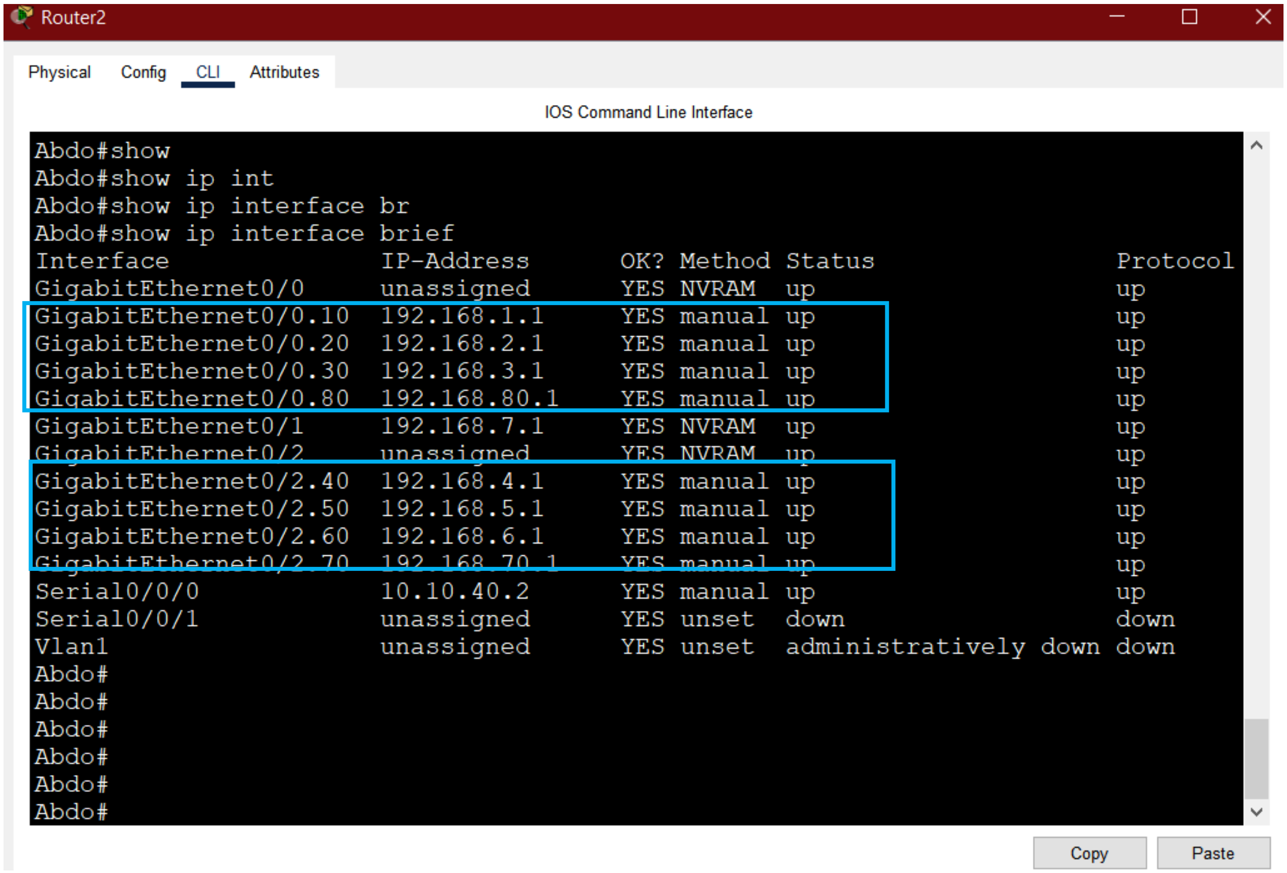


```
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1,10,20,30,40,50,60 priority 24576
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
```

7. VLAN and Router-On-A-Stick (ROAS) Implementation

Router-on-a-Stick is used in this project to enable inter-VLAN routing using a single physical router interface connected to the switch via an IEEE 802.1Q trunk.

In this design, the switch interface connected to the router is configured as a trunk port. On the router, sub interfaces are created on the physical interface, with each sub interface assigned to a specific VLAN and configured with its own IP address to act as the default gateway for that VLAN.

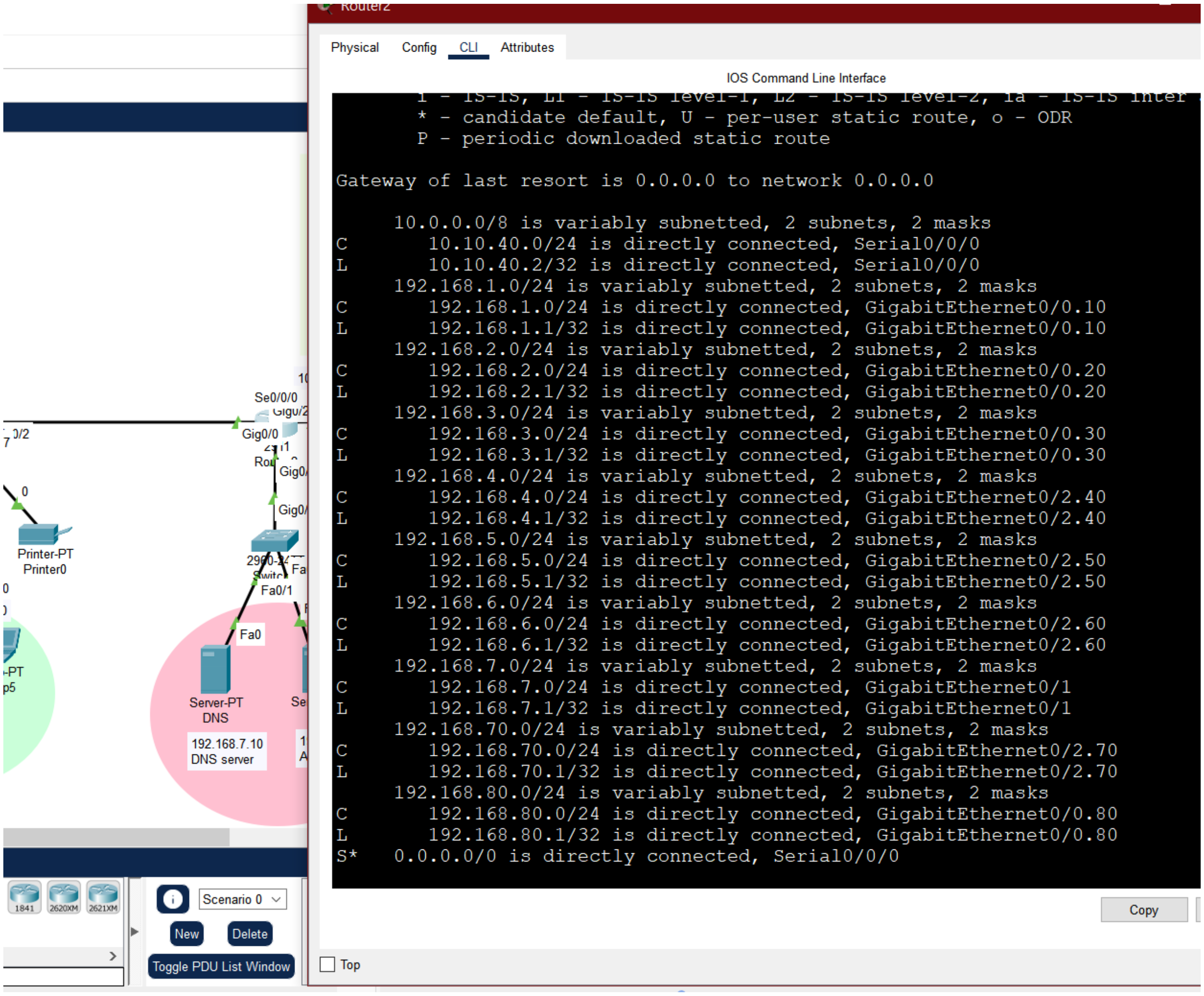


```
Abdo#show
Abdo#show ip int
Abdo#show ip interface br
Abdo#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES NVRAM  up                    up
GigabitEthernet0/0.10  192.168.1.1     YES manual up                    up
GigabitEthernet0/0.20  192.168.2.1     YES manual up                    up
GigabitEthernet0/0.30  192.168.3.1     YES manual up                    up
GigabitEthernet0/0.80  192.168.80.1    YES manual up                    up
GigabitEthernet0/1     192.168.7.1     YES NVRAM  up                    up
GigabitEthernet0/2     unassigned      YES NVRAM  up                    up
GigabitEthernet0/2.40  192.168.4.1     YES manual up                    up
GigabitEthernet0/2.50  192.168.5.1     YES manual up                    up
GigabitEthernet0/2.60  192.168.6.1     YES manual up                    up
GigabitEthernet0/2.70  192.168.70.1    YES manual up                    up
Serial0/0/0            10.10.40.2      YES manual up                    up
Serial0/0/1            unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  administratively down down
Abdo#
Abdo#
Abdo#
Abdo#
Abdo#
Abdo#
```

8. Routing

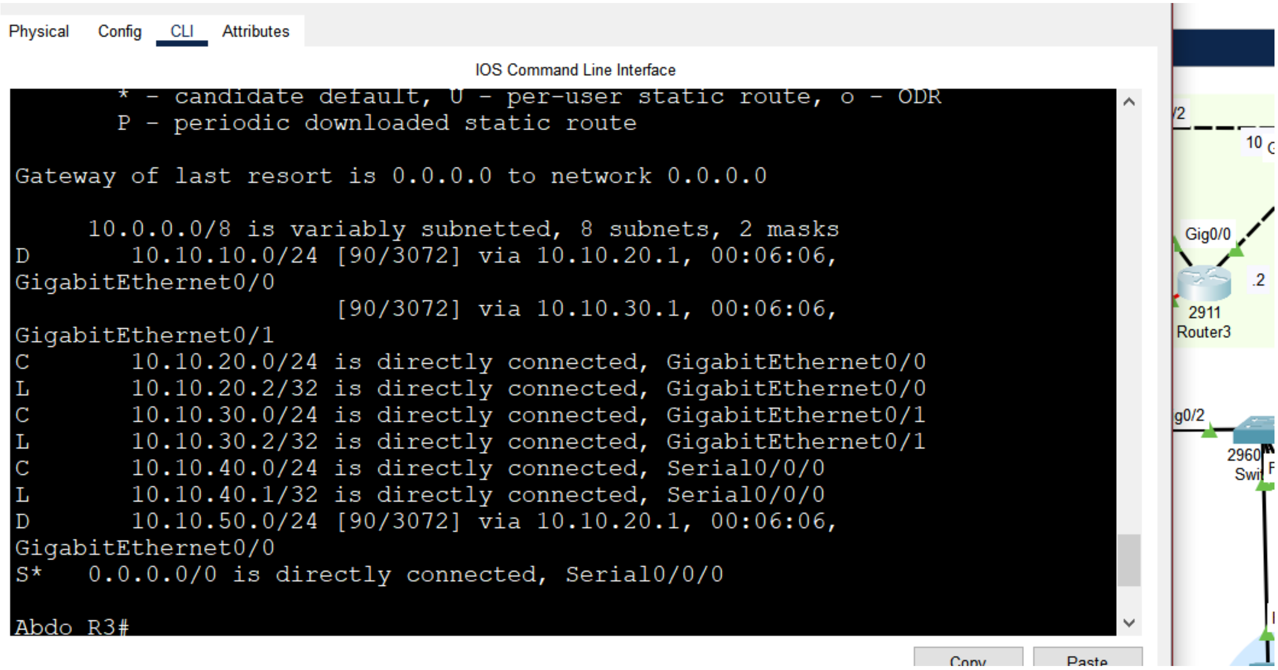
Routing is implemented in this project to enable communication between different VLANs, network segments, and routers. Both Static Routing and Dynamic Routing (EIGRP) are used

Default routing is configured on selected routers to define a gateway of last resort. This allows routers to forward packets destined for unknown networks to a predefined next-hop router.

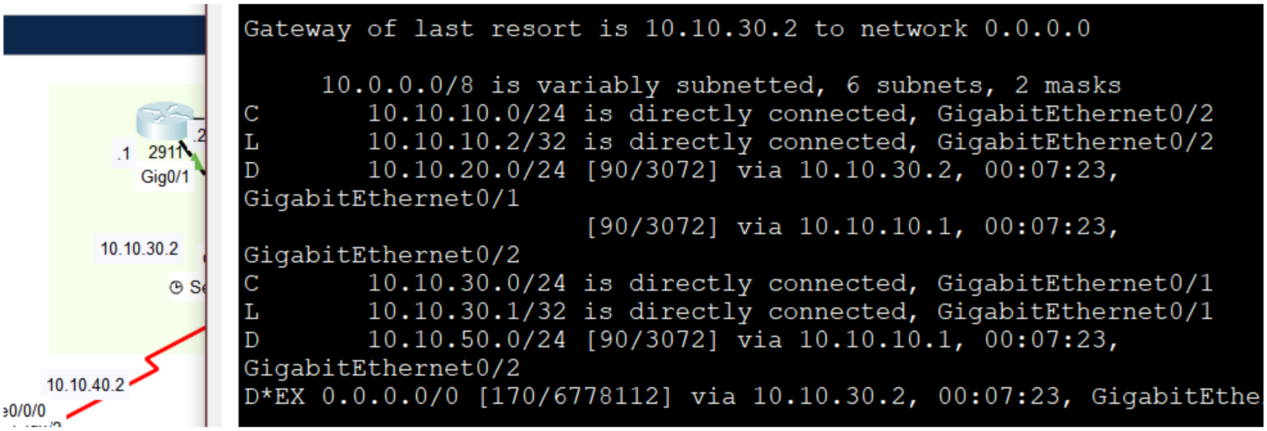


```
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.40.0/24 is directly connected, Serial0/0/0
L       10.10.40.2/32 is directly connected, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0.10
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0.10
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0.20
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0.20
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0.30
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0.30
     192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.4.0/24 is directly connected, GigabitEthernet0/2.40
L       192.168.4.1/32 is directly connected, GigabitEthernet0/2.40
     192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.5.0/24 is directly connected, GigabitEthernet0/2.50
L       192.168.5.1/32 is directly connected, GigabitEthernet0/2.50
     192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.6.0/24 is directly connected, GigabitEthernet0/2.60
L       192.168.6.1/32 is directly connected, GigabitEthernet0/2.60
     192.168.7.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.7.0/24 is directly connected, GigabitEthernet0/1
L       192.168.7.1/32 is directly connected, GigabitEthernet0/1
     192.168.70.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.70.0/24 is directly connected, GigabitEthernet0/2.70
L       192.168.70.1/32 is directly connected, GigabitEthernet0/2.70
     192.168.80.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.80.0/24 is directly connected, GigabitEthernet0/0.80
L       192.168.80.1/32 is directly connected, GigabitEthernet0/0.80
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

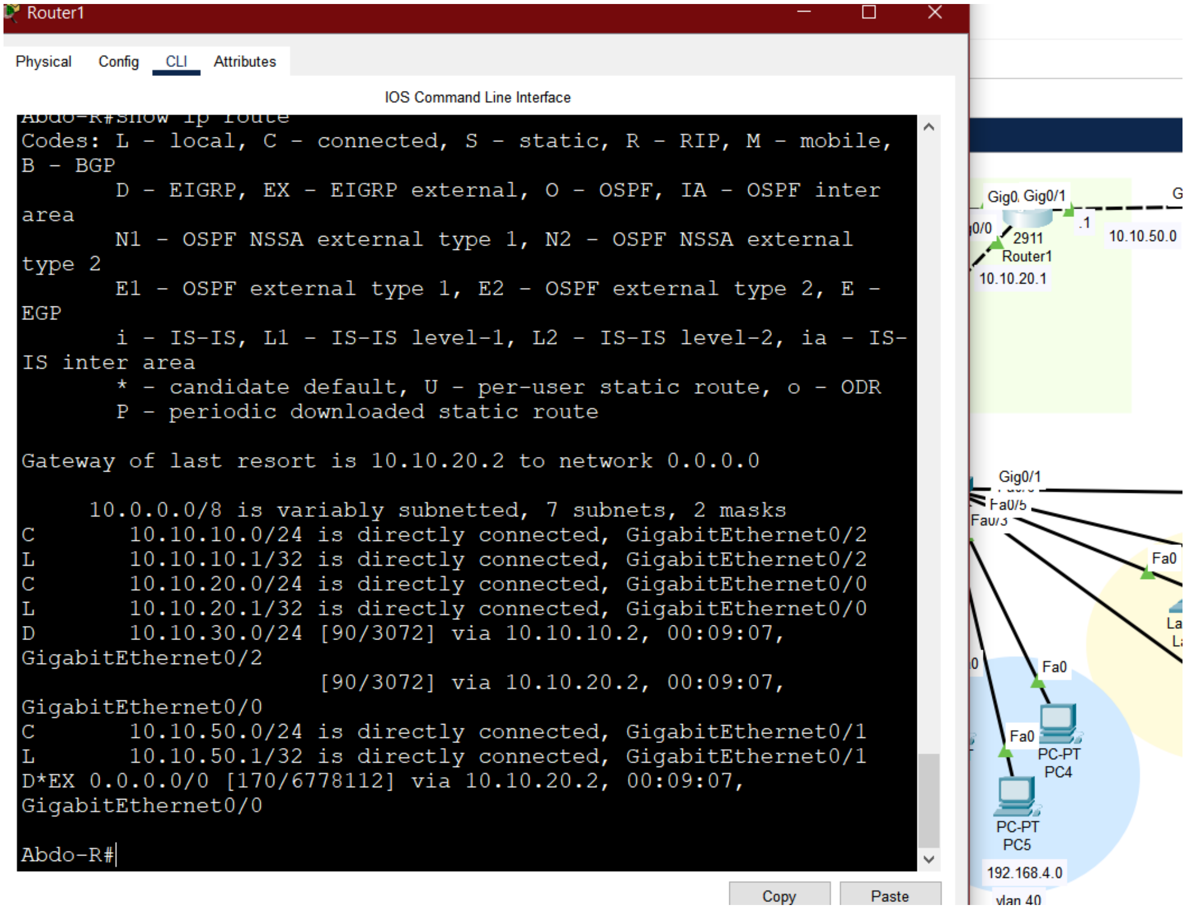
Enhanced Interior Gateway Routing Protocol (EIGRP) is deployed as the dynamic routing protocol between routers in the network. EIGRP enables routers to automatically exchange routing information and dynamically update their routing tables when network changes occur.



```
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
D       10.10.10.0/24 [90/3072] via 10.10.20.1, 00:06:06,
GigabitEthernet0/0
                      [90/3072] via 10.10.30.1, 00:06:06,
GigabitEthernet0/1
C       10.10.20.0/24 is directly connected, GigabitEthernet0/0
L       10.10.20.2/32 is directly connected, GigabitEthernet0/0
C       10.10.30.0/24 is directly connected, GigabitEthernet0/1
L       10.10.30.2/32 is directly connected, GigabitEthernet0/1
C       10.10.40.0/24 is directly connected, Serial0/0/0
L       10.10.40.1/32 is directly connected, Serial0/0/0
D       10.10.50.0/24 [90/3072] via 10.10.20.1, 00:06:06,
GigabitEthernet0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0

Abdo_R3#
```

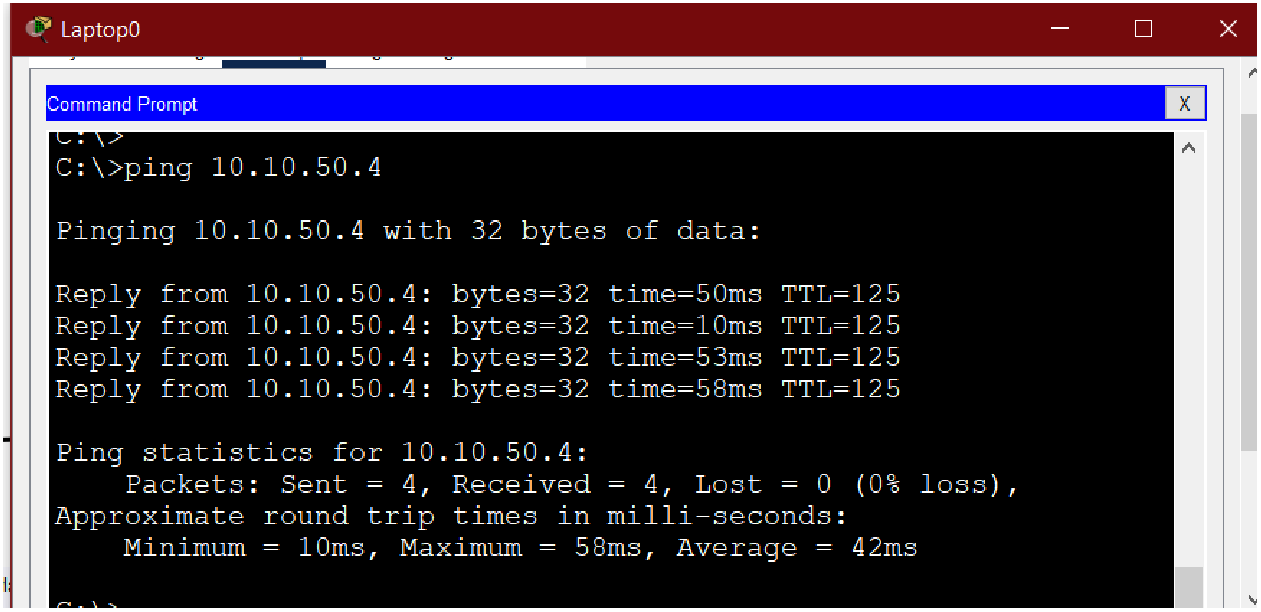


```
Gateway of last resort is 10.10.30.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.10.10.0/24 is directly connected, GigabitEthernet0/2
L       10.10.10.2/32 is directly connected, GigabitEthernet0/2
D       10.10.20.0/24 [90/3072] via 10.10.30.2, 00:07:23,
GigabitEthernet0/1
                      [90/3072] via 10.10.10.1, 00:07:23,
GigabitEthernet0/2
C       10.10.30.0/24 is directly connected, GigabitEthernet0/1
L       10.10.30.1/32 is directly connected, GigabitEthernet0/1
D       10.10.50.0/24 [90/3072] via 10.10.10.1, 00:07:23,
GigabitEthernet0/2
D*EX 0.0.0.0/0 [170/6778112] via 10.10.30.2, 00:07:23, GigabitEthe
```



```
Abdo-R#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.20.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.10.10.0/24 is directly connected, GigabitEthernet0/2
L       10.10.10.1/32 is directly connected, GigabitEthernet0/2
C       10.10.20.0/24 is directly connected, GigabitEthernet0/0
L       10.10.20.1/32 is directly connected, GigabitEthernet0/0
D       10.10.30.0/24 [90/3072] via 10.10.10.2, 00:09:07,
GigabitEthernet0/2
                      [90/3072] via 10.10.20.2, 00:09:07,
GigabitEthernet0/0
C       10.10.50.0/24 is directly connected, GigabitEthernet0/1
L       10.10.50.1/32 is directly connected, GigabitEthernet0/1
D*EX 0.0.0.0/0 [170/6778112] via 10.10.20.2, 00:09:07,
GigabitEthernet0/0

Abdo-R#
```

Routing was verified by performing a ping test from VLAN 30 to the remote network 10.10.50.4. The ping was successful, confirming that default static routing and EIGRP are correctly configured and that inter-network communication is working properly.

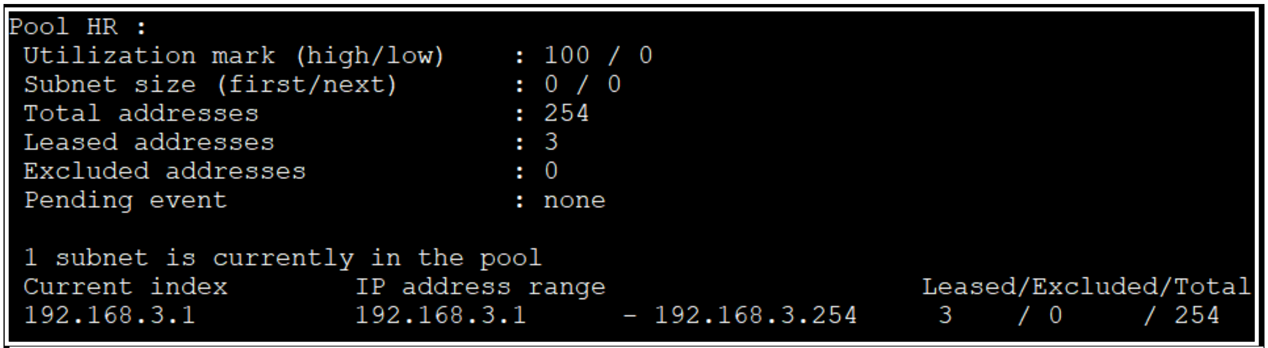


```
C:\>
C:\>ping 10.10.50.4

Pinging 10.10.50.4 with 32 bytes of data:

Reply from 10.10.50.4: bytes=32 time=50ms TTL=125
Reply from 10.10.50.4: bytes=32 time=10ms TTL=125
Reply from 10.10.50.4: bytes=32 time=53ms TTL=125
Reply from 10.10.50.4: bytes=32 time=58ms TTL=125

Ping statistics for 10.10.50.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 58ms, Average = 42ms

C:\>
```

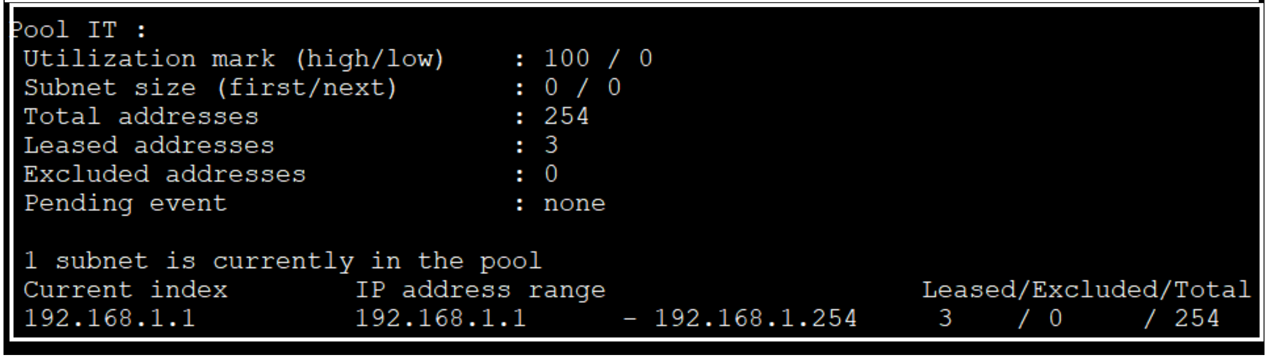
9. DHCP Configuration

Dynamic Host Configuration Protocol (DHCP) is implemented on the router to automatically assign IP addresses to all end devices in the network. The DHCP service provides IP address, subnet mask, default gateway, and DNS server information, reducing manual configuration and administrative overhead.

Pool Name	**Network / Range**	**Subnet Mask**	**Leased IPs**
IT (VLAN 10)	192.168.1.0 – 192.168.1.254	/24	3
Accounting (VLAN 20)	192.168.2.0 – 192.168.2.254	/24	3
HR (VLAN 30)	192.168.3.0 – 192.168.3.254	/24	3
Finance (VLAN 40)	192.168.4.0 – 192.168.4.254	/24	3
Engineering (VLAN 50)	192.168.5.0 – 192.168.5.254	/24	3
Users (VLAN 60)	192.168.6.0 – 192.168.6.254	/24	3
Native VLAN	192.168.80.0 – 192.168.80.254	/24	1
Servers (SW4)	10.10.50.0 – 10.10.50.254	/24	3

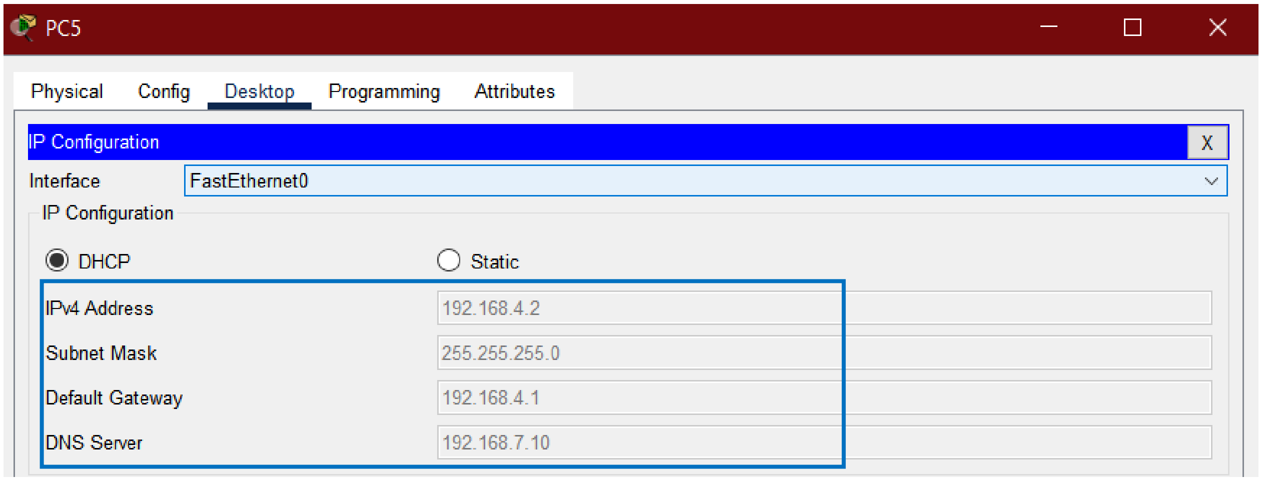


```
Pool HR :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 3
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.3.1          192.168.3.1      - 192.168.3.254     3     / 0       / 254
```



```
Pool IT :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 3
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.1          192.168.1.1      - 192.168.1.254     3     / 0       / 254
```

DHCP verification



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.4.2

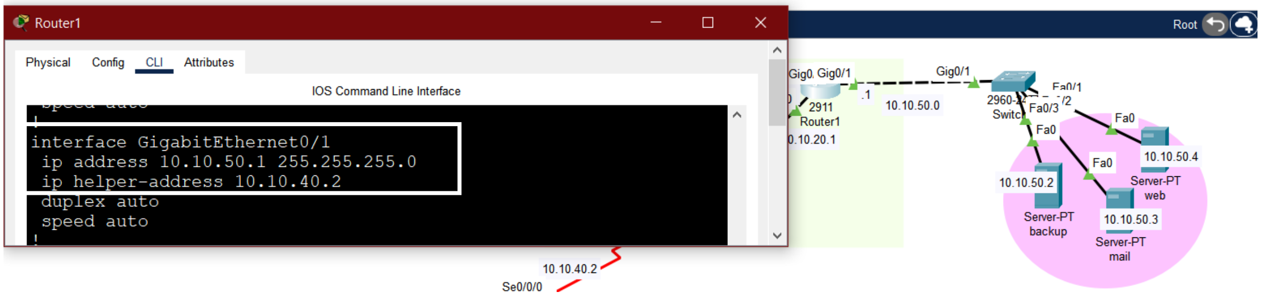
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.4.1

DNS Server: 192.168.7.10

DHCP relay agent configuration

DHCP relay is configured on router using the ip helper-address command to forward client requests to the DHCP server:

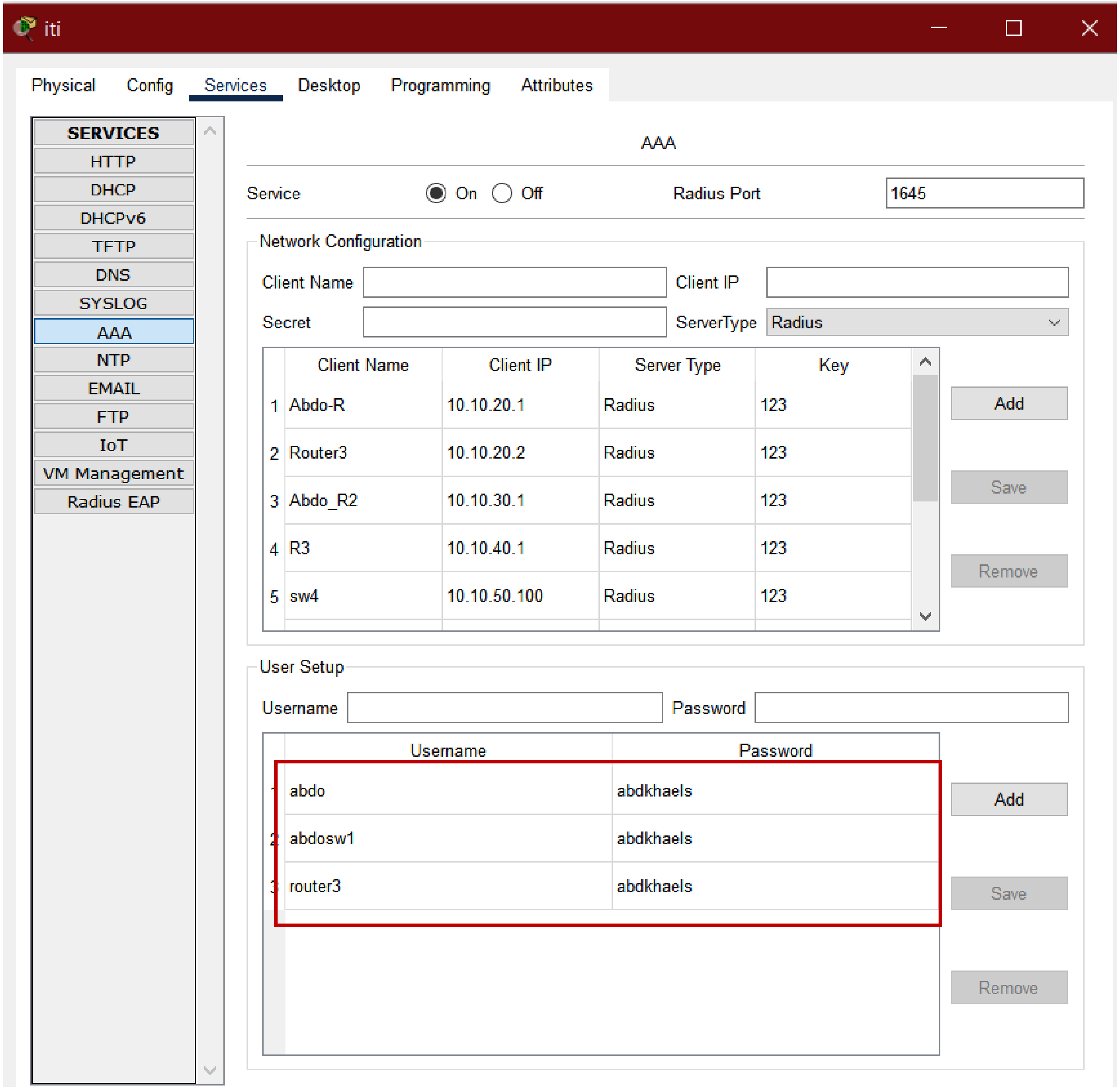


```
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.10.50.1 255.255.255.0
 ip helper-address 10.10.40.2
 duplex auto
 speed auto
!
```

10. AAA (Authentication, Authorization, Accounting)

AAA (Authentication, Authorization, Accounting) is a security framework used to control and monitor access to network resources. It is natively supported on networking platforms from Cisco and commonly integrated with centralized identity solutions like RADIUS or TACACS+.

AAA server configuration



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Client IP

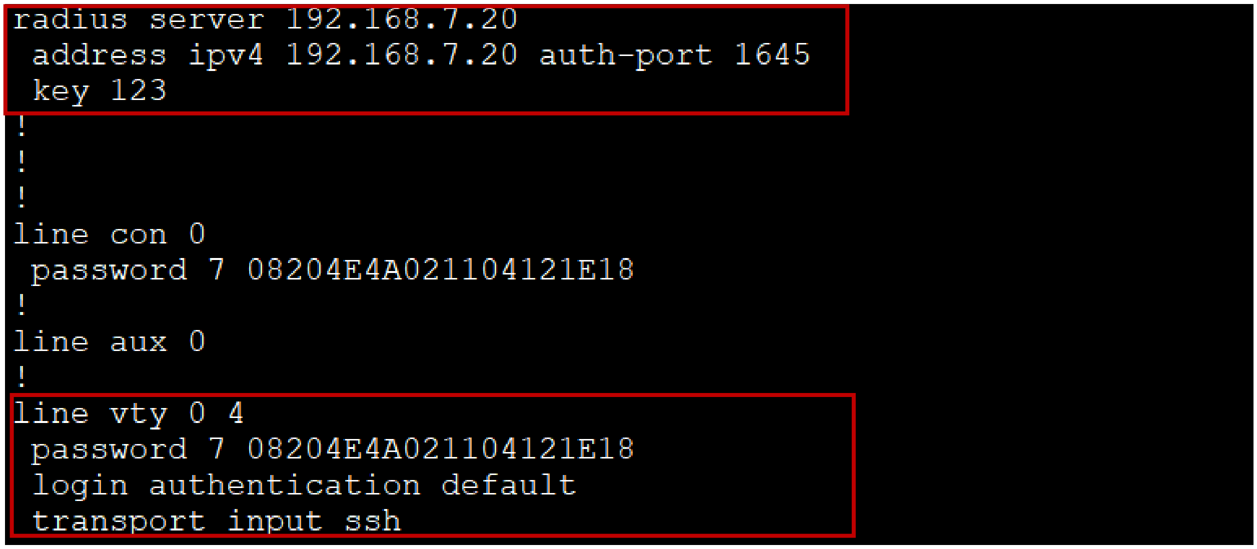
Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	Abdo-R	10.10.20.1	Radius	123
2	Router3	10.10.20.2	Radius	123
3	Abdo_R2	10.10.30.1	Radius	123
4	R3	10.10.40.1	Radius	123
5	sw4	10.10.50.100	Radius	123

User Setup

Username Password

	Username	Password
1	abdo	abdkhaels
2	abdosw1	abdkhaels
3	router3	abdkhaels



```
radius server 192.168.7.20
 address ipv4 192.168.7.20 auth-port 1645
 key 123
!
!
!
line con 0
 password 7 08204E4A021104121E18
!
line aux 0
!
line vty 0 4
 password 7 08204E4A021104121E18
 login authentication default
 transport input ssh
```

11. SSH Access Configuration

The network is configured to prioritize centralized security while maintaining a local "safety net." This is achieved through the following logic:

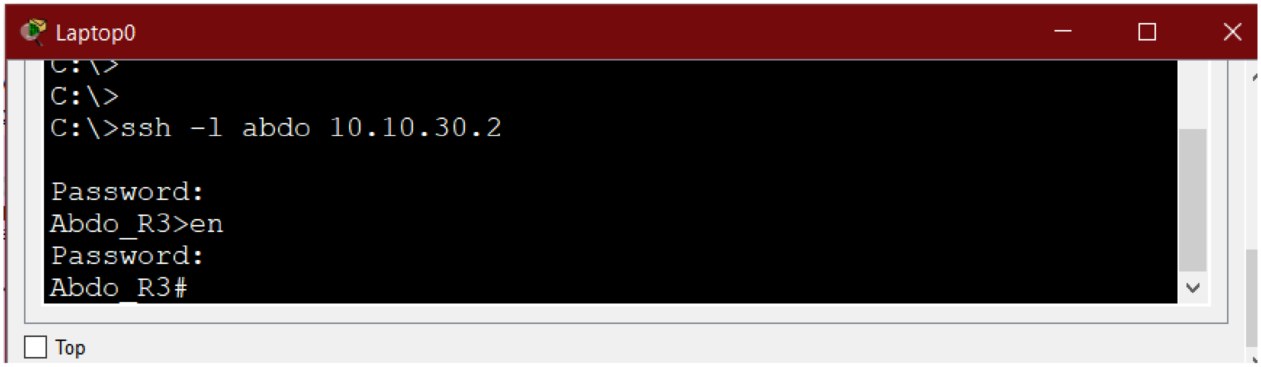
- **Primary Method (RADIUS):** When an administrator attempts to SSH into any router or switch, the device first queries the **AAA (RADIUS) Server** (192.168.7.20) for the credentials stored there (e.g., username abdo).
- **Secondary Method (Local):** If the AAA Server is unreachable (offline or network failure), the device automatically falls back to its **Local Database**.

Verification of Fallback Access:

The implementation ensures 100% uptime for administrative access under two scenarios:

Scenario A: AAA Server is Online (Standard Operation)

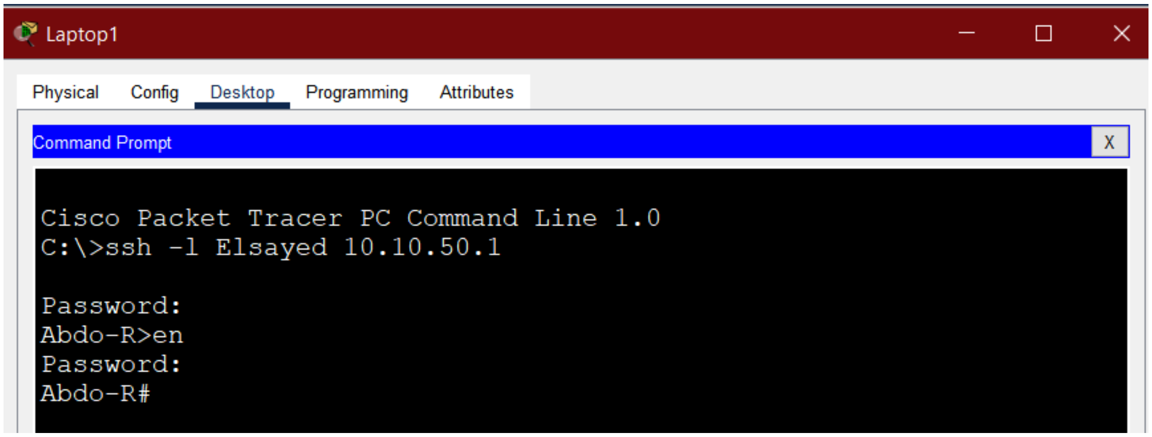
- **Username:** abdo (or any user defined in the AAA server).
- **Password:** abdkhaels.



```
C:\>
C:\>
C:\>ssh -l abdo 10.10.30.2

Password:
Abdo_R3>en
Password:
Abdo_R3#
```

Scenario B: AAA Server is Offline (Emergency Access)

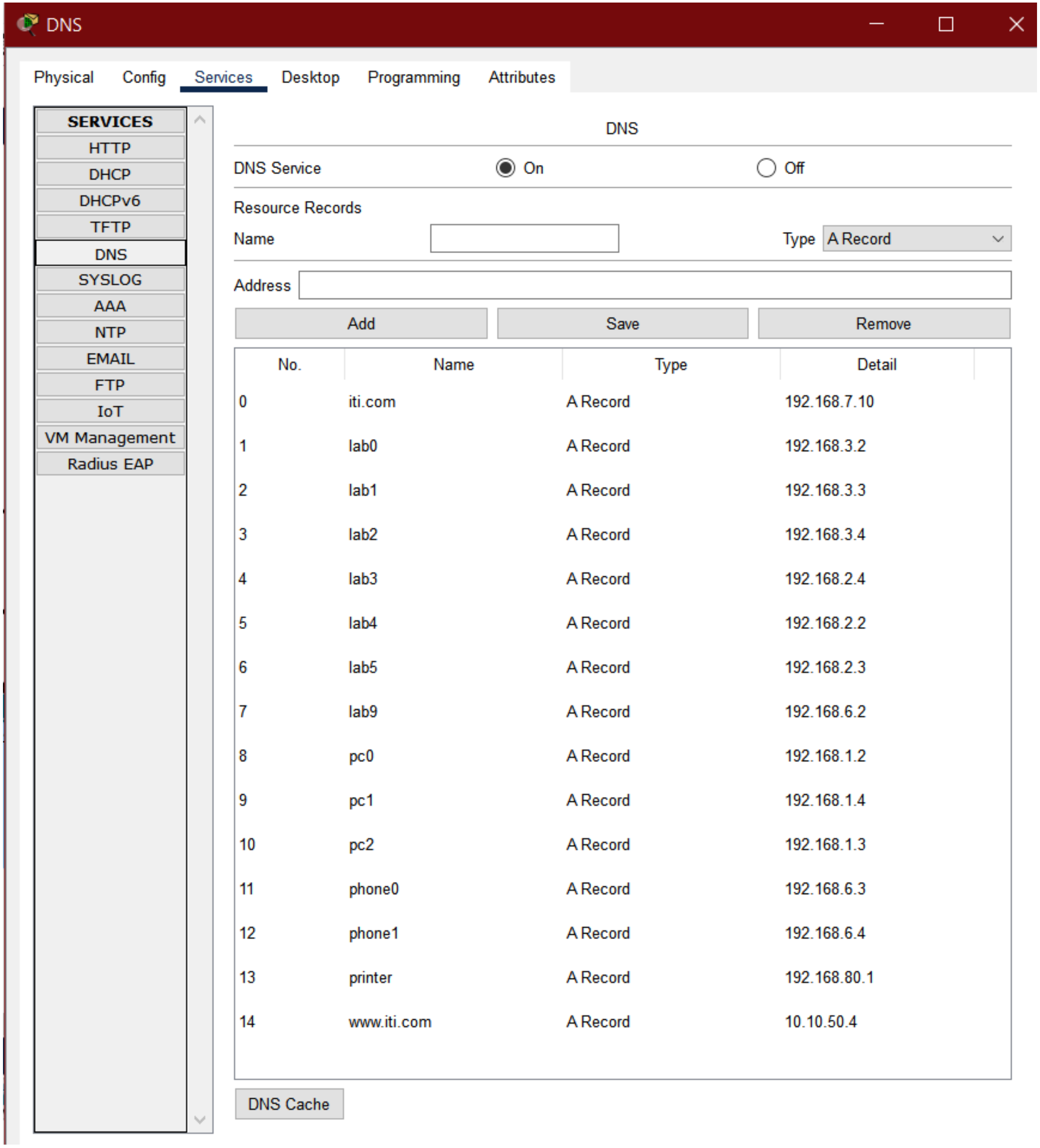
- **Username:** Elsayed.
- **Password:** 123.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Elsayed 10.10.50.1

Password:
Abdo-R>en
Password:
Abdo-R#
```

12. DNS Server

The DNS Server (192.168.7.10) acts as the central directory for the network, mapping hostnames to IP addresses to simplify user access.



DNS Service ● On ○ Off

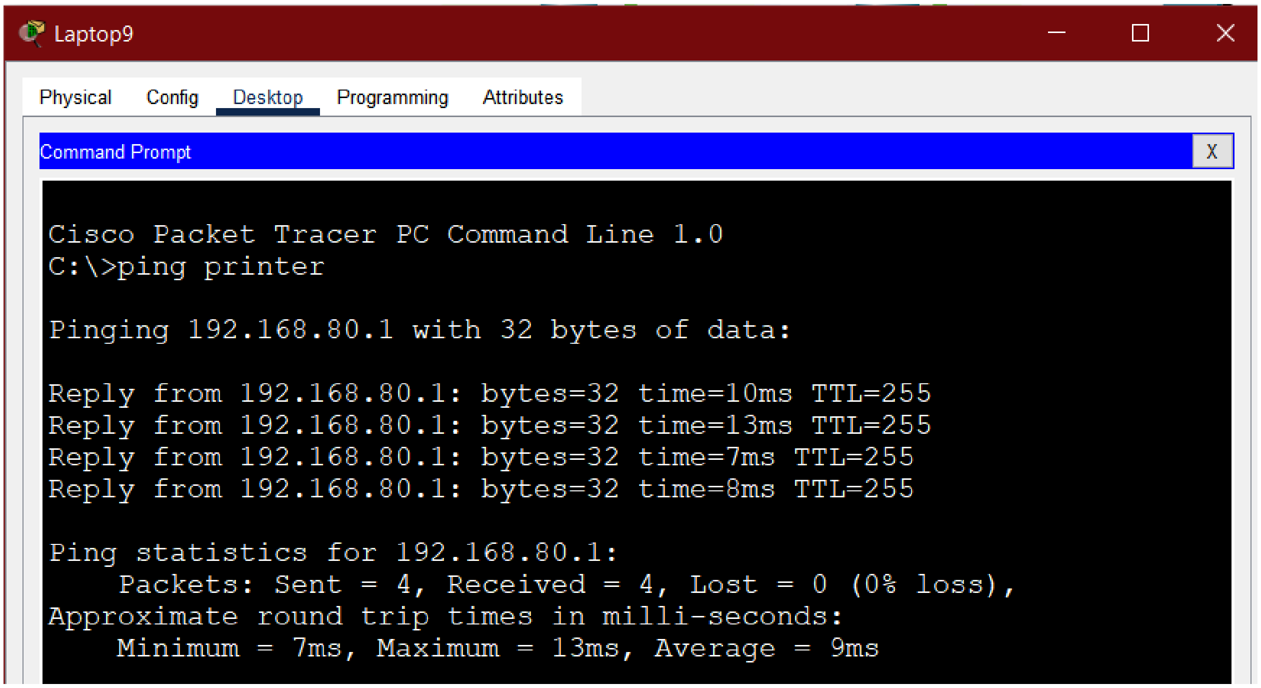
Name

Type A Record

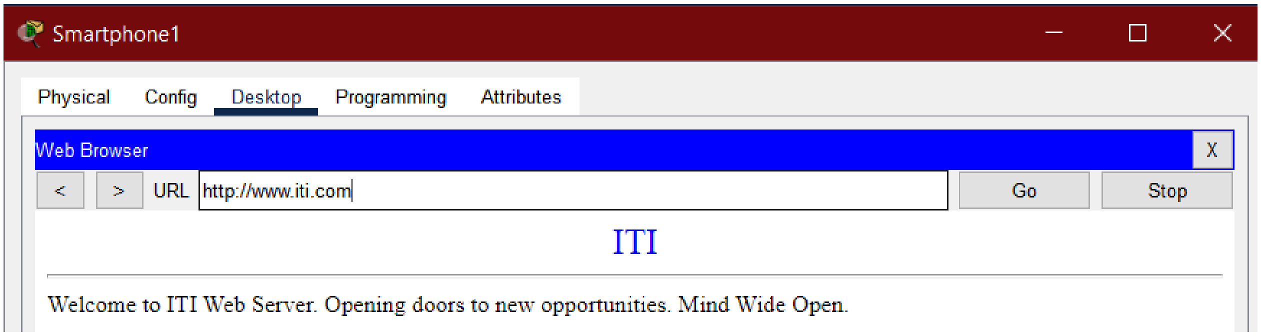
Address

No.	Name	Type	Detail
0	iti.com	A Record	192.168.7.10
1	lab0	A Record	192.168.3.2
2	lab1	A Record	192.168.3.3
3	lab2	A Record	192.168.3.4
4	lab3	A Record	192.168.2.4
5	lab4	A Record	192.168.2.2
6	lab5	A Record	192.168.2.3
7	lab9	A Record	192.168.6.2
8	pc0	A Record	192.168.1.2
9	pc1	A Record	192.168.1.4
10	pc2	A Record	192.168.1.3
11	phone0	A Record	192.168.6.3
12	phone1	A Record	192.168.6.4
13	printer	A Record	192.168.80.1
14	www.iti.com	A Record	10.10.50.4

DNS Verification:



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

Pinging 192.168.80.1 with 32 bytes of data:

Reply from 192.168.80.1: bytes=32 time=10ms TTL=255
Reply from 192.168.80.1: bytes=32 time=13ms TTL=255
Reply from 192.168.80.1: bytes=32 time=7ms TTL=255
Reply from 192.168.80.1: bytes=32 time=8ms TTL=255

Ping statistics for 192.168.80.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 13ms, Average = 9ms
```



URL http://www.iti.com

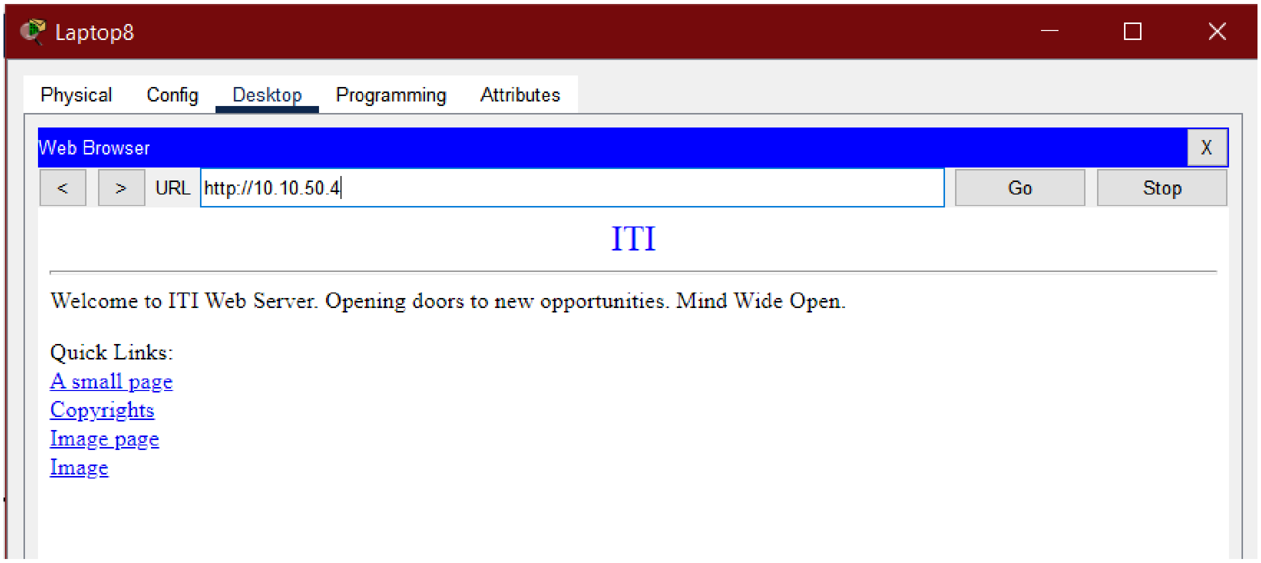
ITI

Welcome to ITI Web Server. Opening doors to new opportunities. Mind Wide Open.

13. Web Server

A web server is a dedicated system that hosts and delivers web content and web-based services to clients over the network using the HTTP/HTTPS application protocol.

Web server Verification:



http://10.10.50.4

ITI

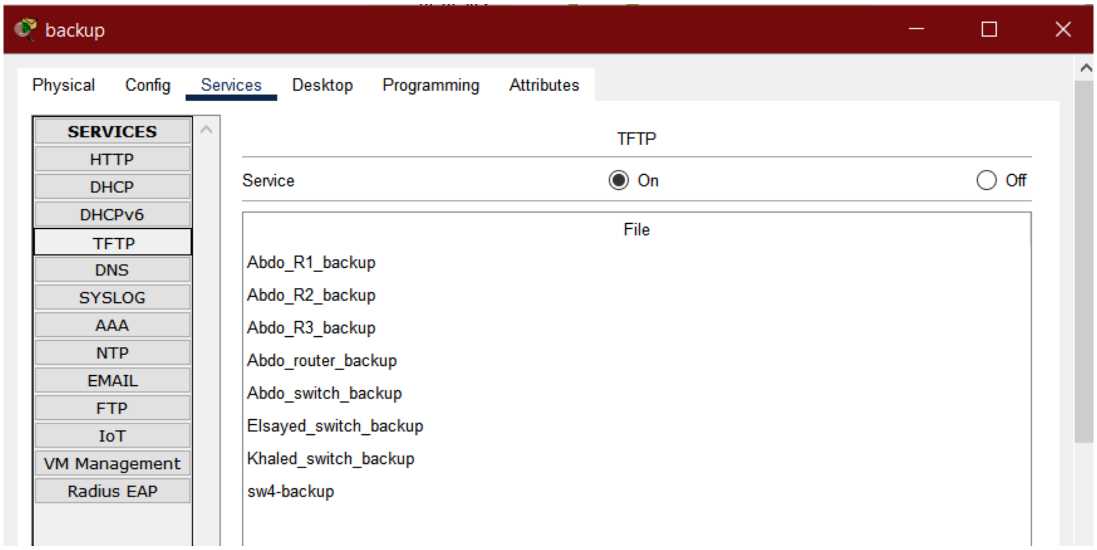
Welcome to ITI Web Server. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

14. TFTP Server

The Backup server (10.10.50.2) acts as a central repository for device configurations.

TFTP server Verification:



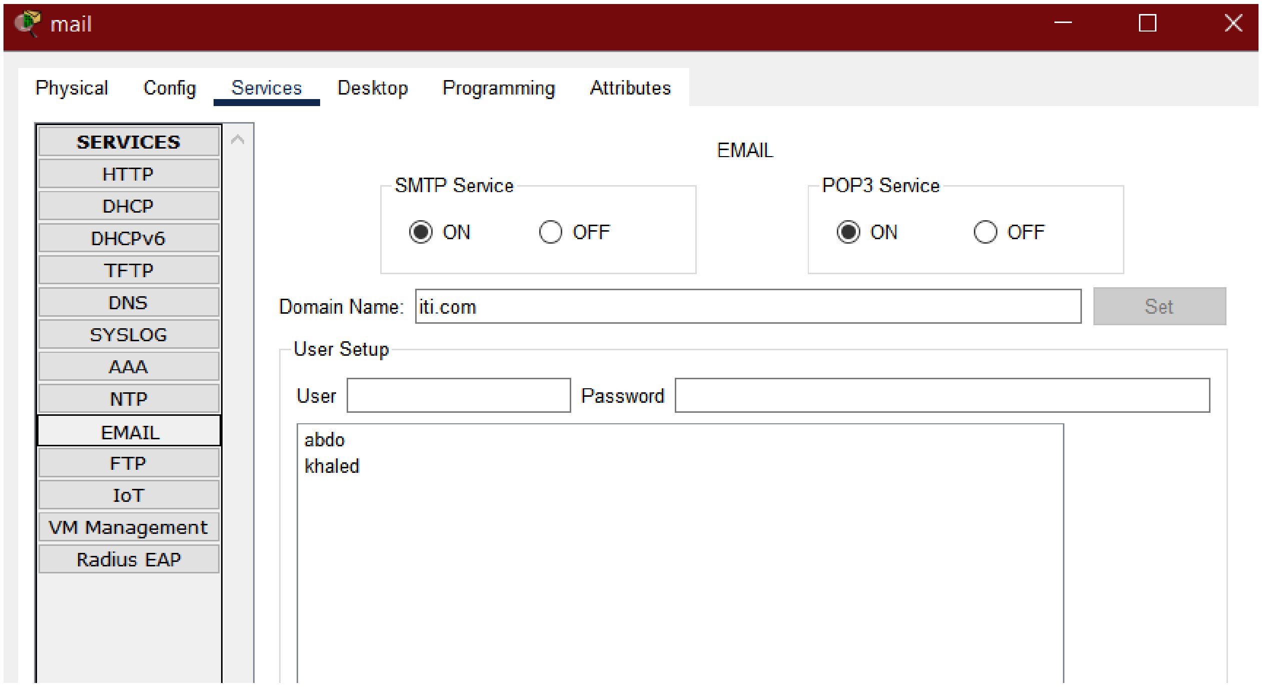
TFTP

Service ● On ○ Off

File
Abdo_R1_backup
Abdo_R2_backup
Abdo_R3_backup
Abdo_router_backup
Abdo_switch_backup
Elsayed_switch_backup
Khaled_switch_backup
sw4-backup

15. Email Server

The enterprise network utilizes a centralized **Mail Server** located at IP address **10.10.50.3** to manage organizational communications. To ensure secure access, user accounts such as **"abdo"** and **"khaled"** have been established with specific credentials.



EMAIL

SMTP Service: ● ON ○ OFF

POP3 Service: ● ON ○ OFF

Domain Name: iti.com

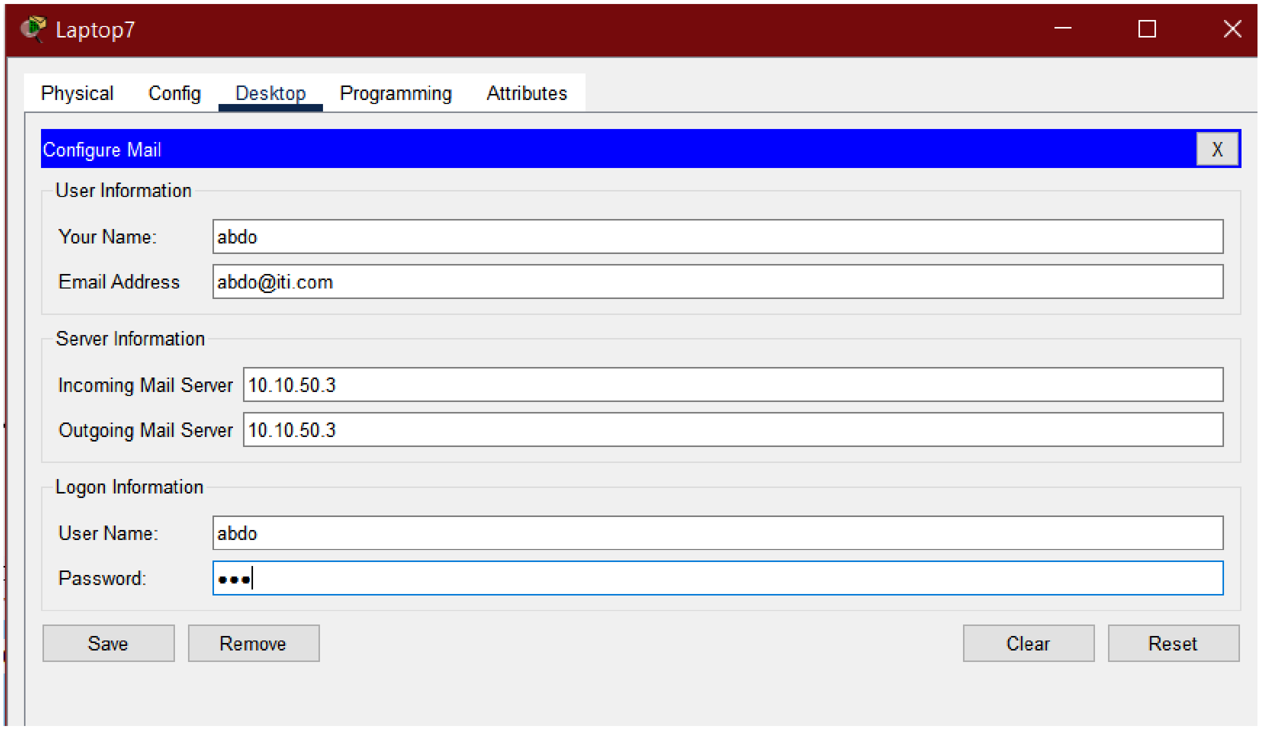
User Setup

User

Password

abdo
khaled

Email server Verification:



Configure Mail

User Information

Your Name: abdo

Email Address: abdo@iti.com

Server Information

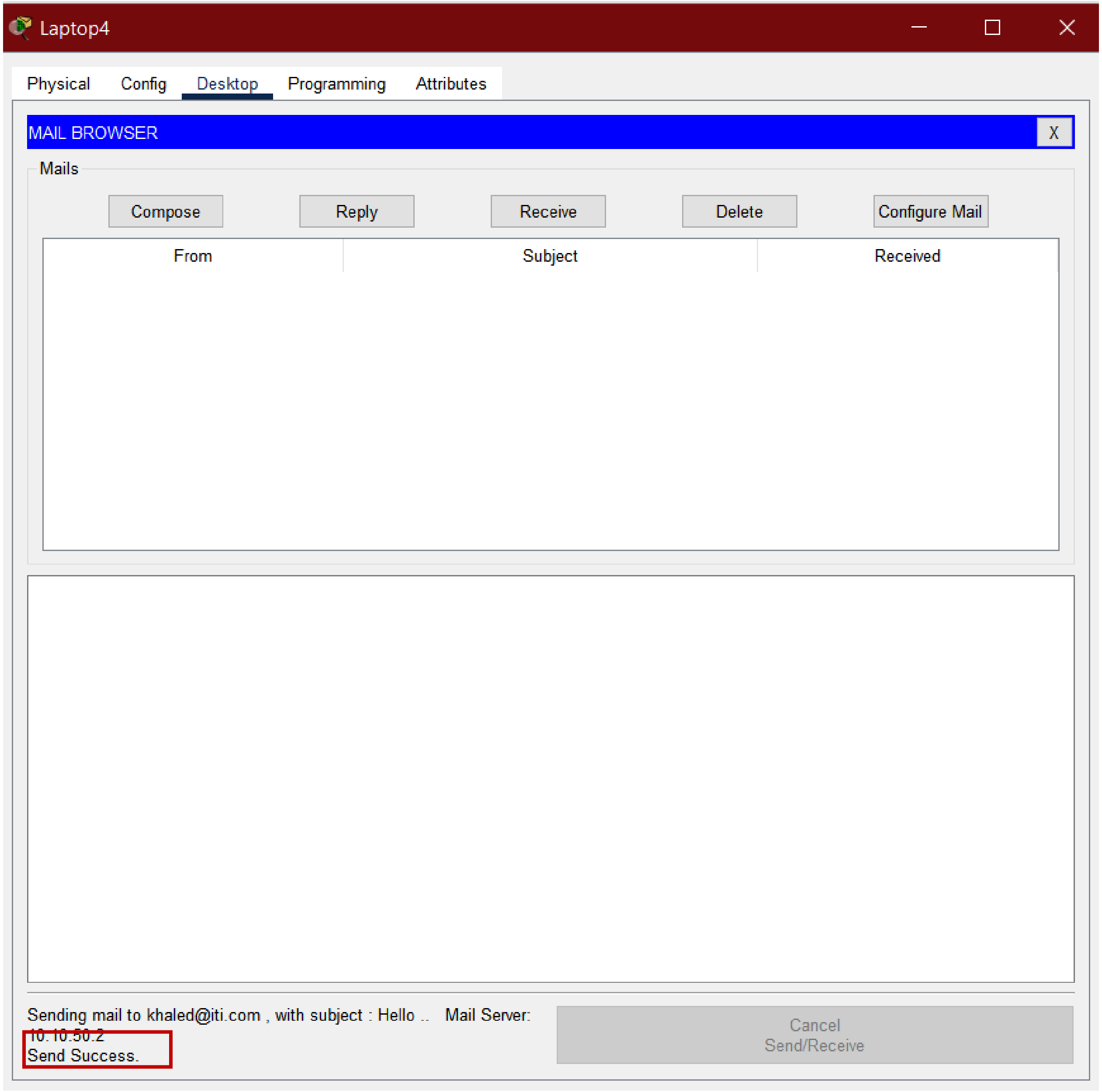
Incoming Mail Server: 10.10.50.3

Outgoing Mail Server: 10.10.50.3

Logon Information

User Name: abdo

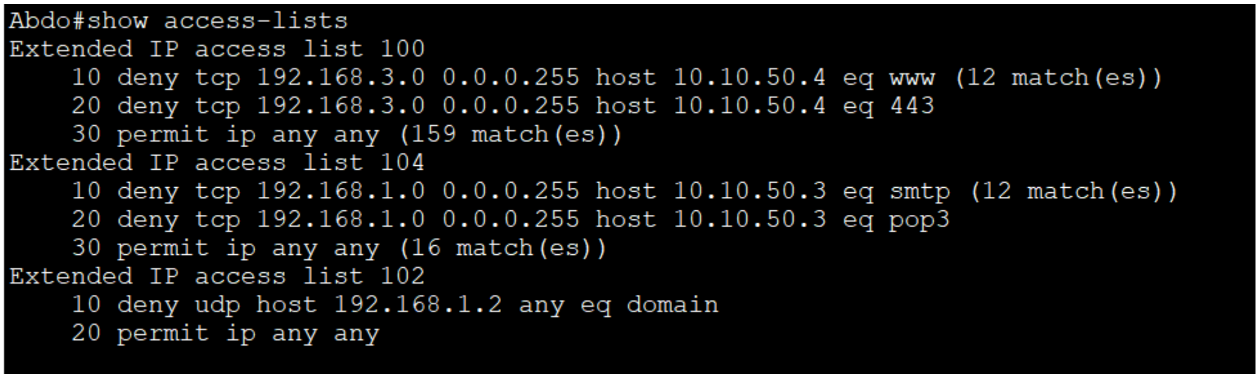
Password: •••



Sending mail to khaled@iti.com , with subject : Hello .. Mail Server: 10.10.50.2
Send Success.

16. Access List

To secure the network and control traffic flow, Extended Access Control Lists (ACLs) were implemented on the routing infrastructure. These rules ensure that critical services like DNS, Web, and Mail are only accessible by authorized hosts and networks.

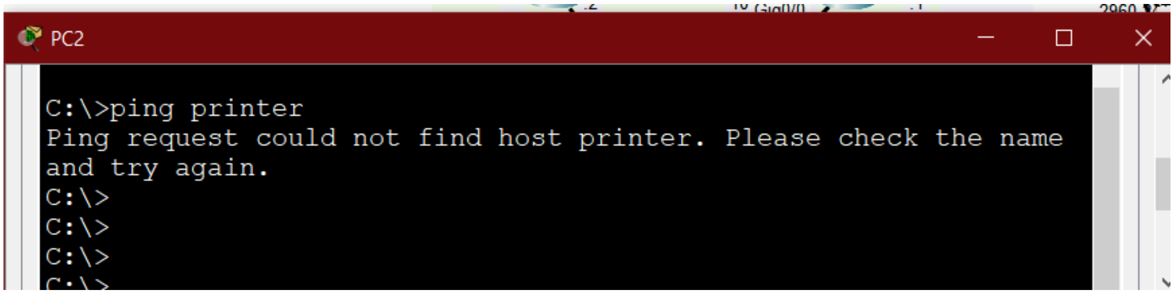


```
Abdo#show access-lists
Extended IP access list 100
    10 deny tcp 192.168.3.0 0.0.0.255 host 10.10.50.4 eq www (12 match(es))
    20 deny tcp 192.168.3.0 0.0.0.255 host 10.10.50.4 eq 443
    30 permit ip any any (159 match(es))
Extended IP access list 104
    10 deny tcp 192.168.1.0 0.0.0.255 host 10.10.50.3 eq smtp (12 match(es))
    20 deny tcp 192.168.1.0 0.0.0.255 host 10.10.50.3 eq pop3
    30 permit ip any any (16 match(es))
Extended IP access list 102
    10 deny udp host 192.168.1.2 any eq domain
    20 permit ip any any
```

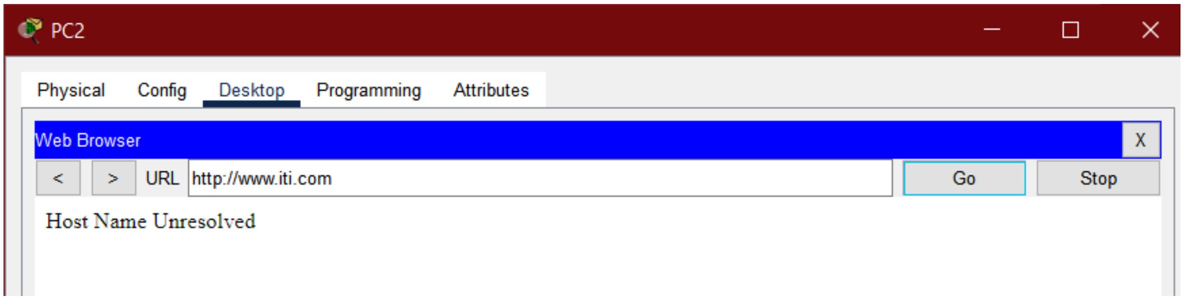
1. DNS Service Restriction (Host Level)

A specific security rule was applied to prevent a single host from performing name resolution queries.

- **Target Host:** 192.168.1.2 (VLAN 10 IT Department).
- **Action:** Deny UDP traffic on port 53 (DNS).
- **Objective:** To restrict this specific host from using the central DNS server (192.168.7.10) while allowing all other network devices to continue name resolution.



```
C:\>ping printer
Ping request could not find host printer. Please check the name
and try again.
C:\>
C:\>
C:\>
C:\>
```



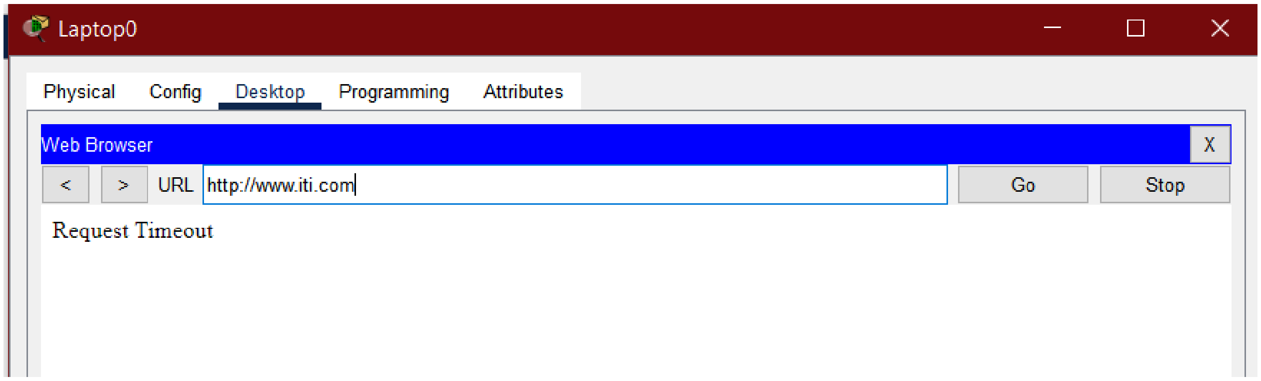
URL: http://www.iti.com

Host Name Unresolved

2. Web Server Access Control (Network Level)

Access to the internal organization website was restricted for the HR and Wireless department to optimize bandwidth and security.

- **Source Network:** 192.168.3.0/24 (VLAN 30).
- **Destination:** Web Server (10.10.50.4).
- **Action:** Deny TCP traffic on port 80 (HTTP) and port 443 (HTTPS).
- **Objective:** To block the entire HR/Wireless segment from accessing the web server while maintaining their connectivity to other network resources.



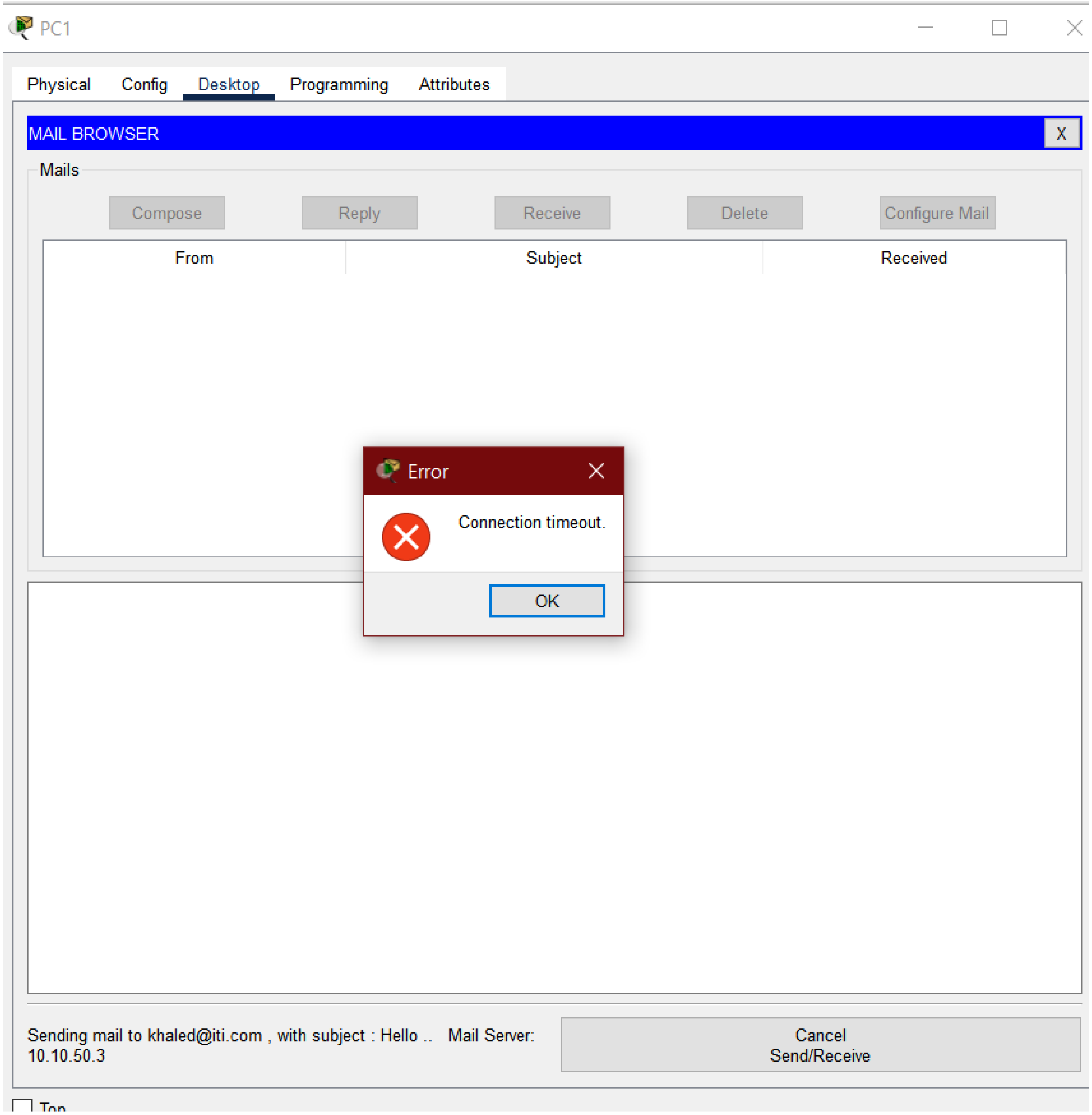
http://www.iti.com

Request Timeout

3. Mail Server Security (VLAN Level)

A dedicated **Mail Server** was integrated at IP 10.10.50.3 to handle **SMTP** and **POP3** services. A security policy was then enforced to isolate VLAN 10 from email communication.

- **Blocked Segment:** VLAN 10 (192.168.1.0/24).
- **Service Protocols:** SMTP (Port 25) and POP3 (Port 110).
- **Implementation:** An ACL was applied to the router interface to drop any mail-related packets originating from the IT department (VLAN 10).
- **Objective:** To prevent VLAN 10 users from sending or receiving emails via the central mail server for departmental security compliance.



Connection timeout.

Sending mail to khaled@iti.com , with subject : Hello .. Mail Server: 10.10.50.3