Contents

Table of Figures:

1. Network Overview

Project Title:

Enterprise Multi-Floor VLAN Network with Centralized Services and Security

Objective:

To design and implement a secure, scalable and segmented network for a multi-floor organization using VLANS for departmental separation, centralized DHCP, TFTP, Syslog and AAA services, and ensure Inter-VLAN communication through Router-on-a-Stick (ROAS) configuration.

Organizational Layout:

The network covers 4 floors, with each floor containing different departments:

- **Floor1**: Cashier and Reception
- **Floor 2**: Manager and HR
- **Floor 3**: IT and Admin
- **Floor 4**: Network services (DHCP, TDTP, Syslog, AAA)

2. Basic configuration

In this network setup, I configured the hostname on each switch to reflect its role and location. The distribution switch was named **Core_SW**, serving as the central point for all VLAN trunk connections. The access switches were named according to their floor levels for easy identification. for example, **F1_SW, F2_SW**, and so on, with numbers increasing on each floor. To enhance local security, a console password was set on all switches, along with an **enable secret** password to restrict access to privileged EXEC mode. To ensure that all stored passwords were protected, the command **service password-encryption** was applied, which encrypts all plaintext passwords in the configuration file.

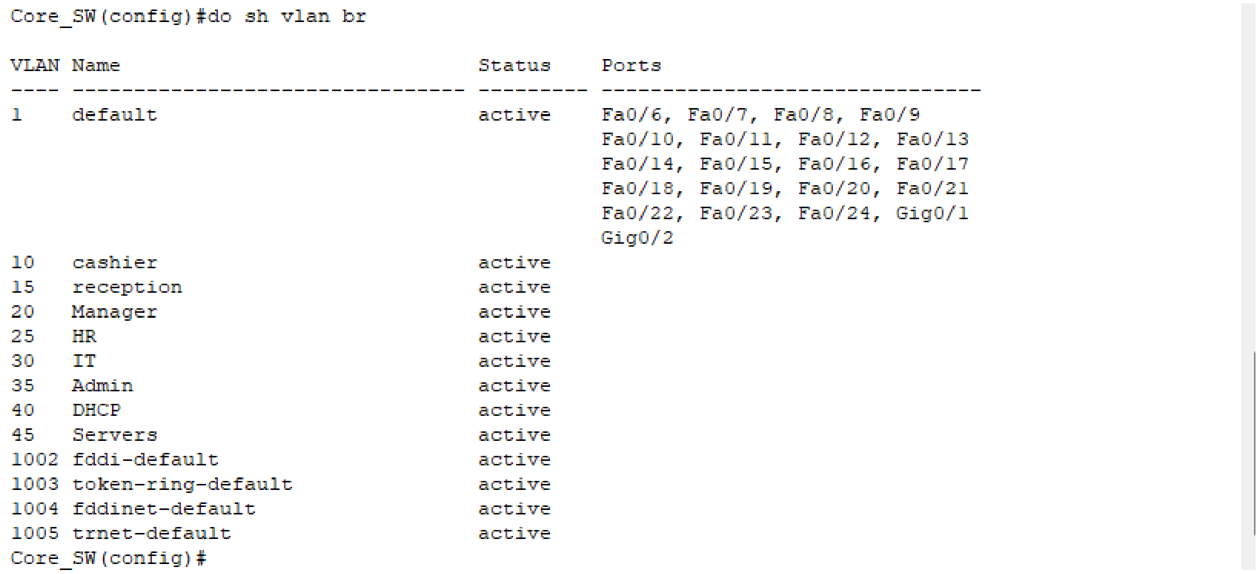
Additionally, SSH (Secure Shell) was configured on the router to allow secure remote access, replacing Telnet which is insecure due to its lack of encryption. This helps maintain confidentiality during remote administrative sessions. Furthermore, the command **no ip domain-lookup** was used to prevent the router from trying to resolve mistyped commands as hostnames, which would otherwise result in unnecessary DNS queries and delay in the command-line interface. This improves the efficiency of command-line operations, especially when errors are made during manual configuration.

3. Features that are implemented

3.1. VLAN Implementation:

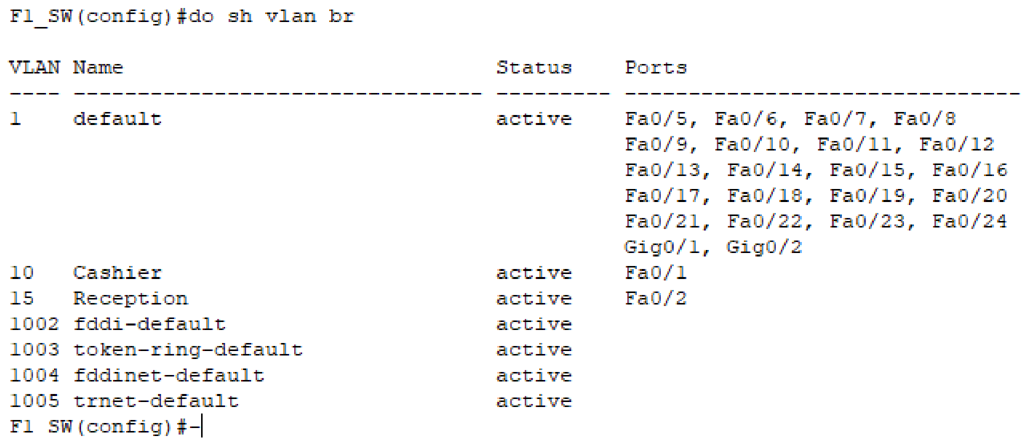
Each department is assigned an unique VLAN ID to logically separate traffic and reduce broadcast domain.

- VLANS are assigned in given way:
- VLAN 10: Cashier
- VLAN 15: Reception
- VLAN 20: Manager
- VLAN 25: HR
- VLAN 30: IT
- VLAN 35: Admin
- VLAN 40: DHCP
- VLAN 45: TFTP, Syslog and AAA



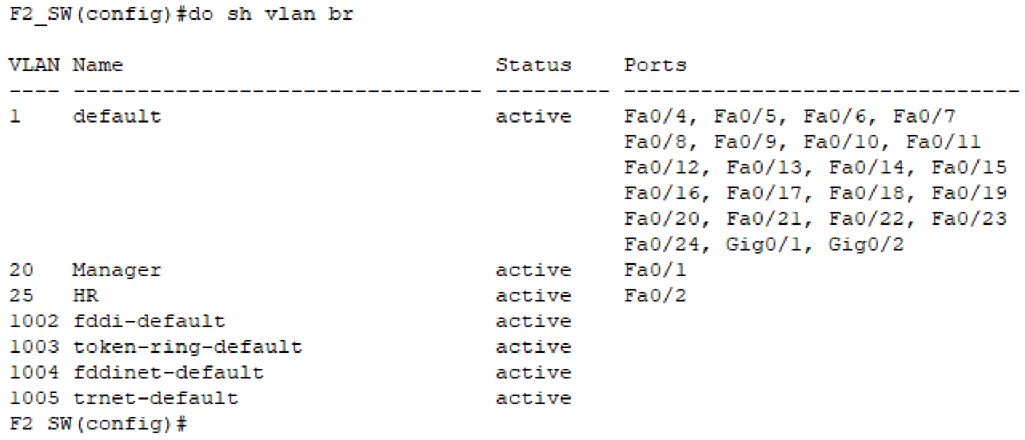
```
Core_SW(config)#do sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/6, 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, Gig0/1
                                                Gig0/2
10   cashier                          active
15   reception                        active
20   Manager                          active
25   HR                               active
30   IT                               active
35   Admin                            active
40   DHCP                             active
45   Servers                          active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Core_SW(config)#
```

Figure 1: Screenshot of the VLANs in Core_SW.



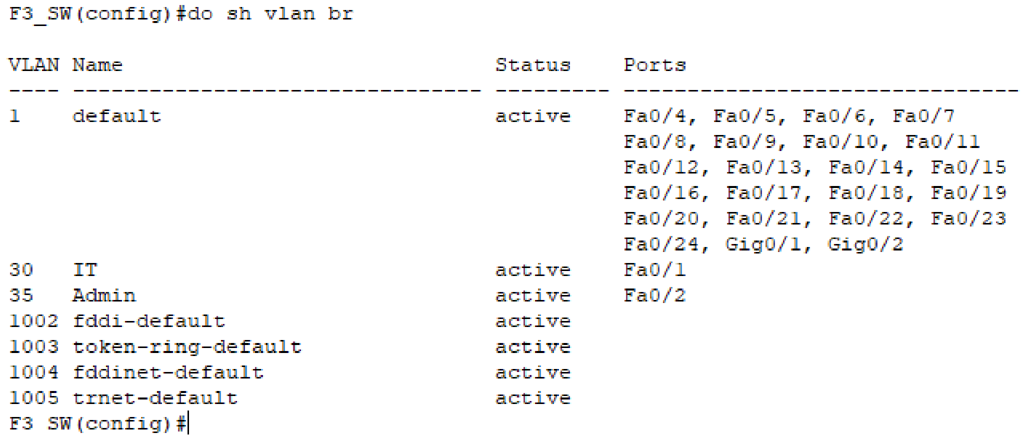
```
F1_SW(config)#do sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, 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
                                                Gig0/1, Gig0/2
10   Cashier                          active    Fa0/1
15   Reception                        active    Fa0/2
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
F1 SW(config)#-
```

Figure 2: Screenshot of the VLANs in F1_SW



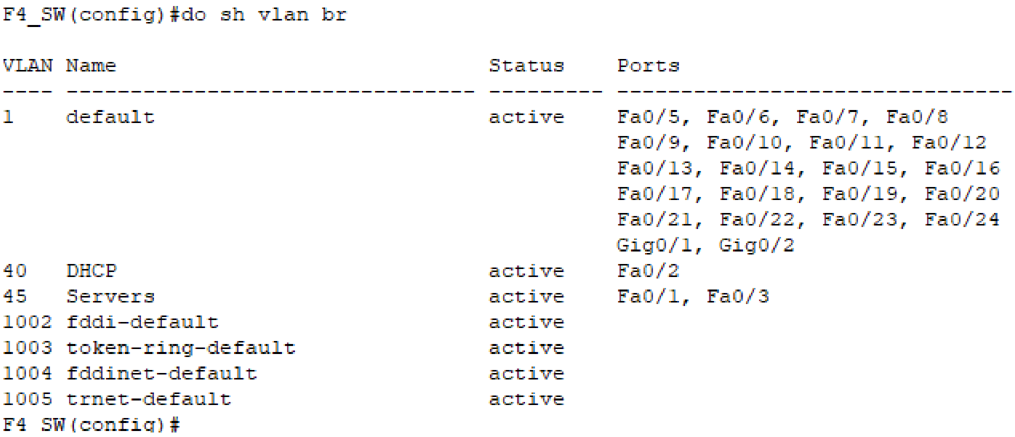
```
F2_SW(config)#do sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, 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, Gig0/1, Gig0/2
20   Manager                          active    Fa0/1
25   HR                               active    Fa0/2
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
F2 SW(config)#
```

Figure 3: Screenshot of the VLANs in F2_SW



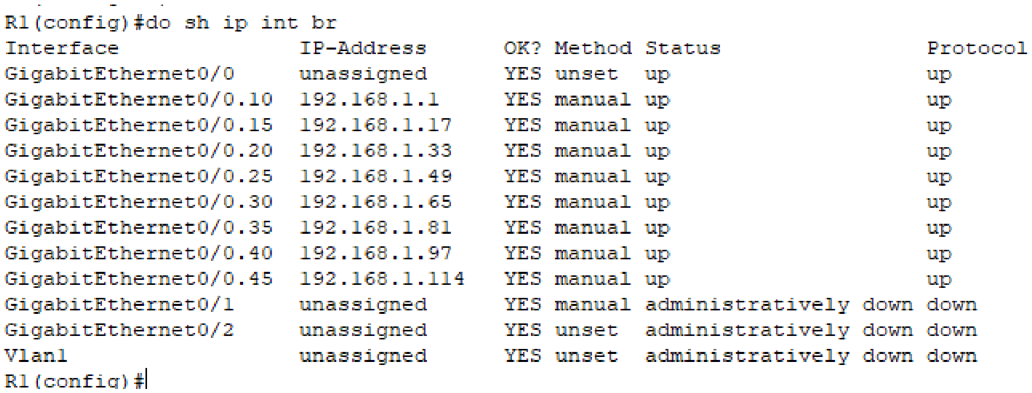
```
F3_SW(config)#do sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, 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, Gig0/1, Gig0/2
30   IT                               active    Fa0/1
35   Admin                            active    Fa0/2
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
F3 SW(config)#
```

Figure 4: Screenshot of the VLANs in F3_SW



```
F4_SW(config)#do sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, 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
                                                Gig0/1, Gig0/2
40   DHCP                             active    Fa0/2
45   Servers                          active    Fa0/1, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
F4_SW(config)#
```

Figure 5: Screenshot of the VLANs in F4_SW



```
R1(config)#do sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.1.1     YES manual up                    up
GigabitEthernet0/0.15  192.168.1.17    YES manual up                    up
GigabitEthernet0/0.20  192.168.1.33    YES manual up                    up
GigabitEthernet0/0.25  192.168.1.49    YES manual up                    up
GigabitEthernet0/0.30  192.168.1.65    YES manual up                    up
GigabitEthernet0/0.35  192.168.1.81    YES manual up                    up
GigabitEthernet0/0.40  192.168.1.97    YES manual up                    up
GigabitEthernet0/0.45  192.168.1.114   YES manual up                    up
GigabitEthernet0/1     unassigned      YES manual administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
R1(config)#
```

Figure 6: IP of the Sub interfaces in the router.

3.2. Subnetting and Inter-VLAN routing

Next the network 192.168.1.0/24 was divided to make sure that every department has the capacity of 14 usable hosts.

Floor	VLANS	Network	Subnet	Default Gateway
1	Cashier (10)	192.168.1.0	255.255.255.240	192.168.1.1
	RECEPTION (15)	192.168.1.15	255.255.255.240	192.168.1.16
2	Manager (20)	192.168.1.32	255.255.255.240	192.168.1.33
	HR (25)	192.168.1.48	255.255.255.240	192.168.1.49
3	IT (30)	192.168.1.64	255.255.255.240	192.168.1.65
	Admin (35)	192.168.1.80	255.255.255.240	192.168.1.81
4	DHCP (40)	192.168.1.96	255.255.255.240	192.168.1.97
	TFTP (45)	192.168.1.112	255.255.255.240	192.168.1.113
	Syslog and AAA(45)			

Static IP of DHCP server = 192.168.1.99

Static IP of TFTP server = 192.168.1.115

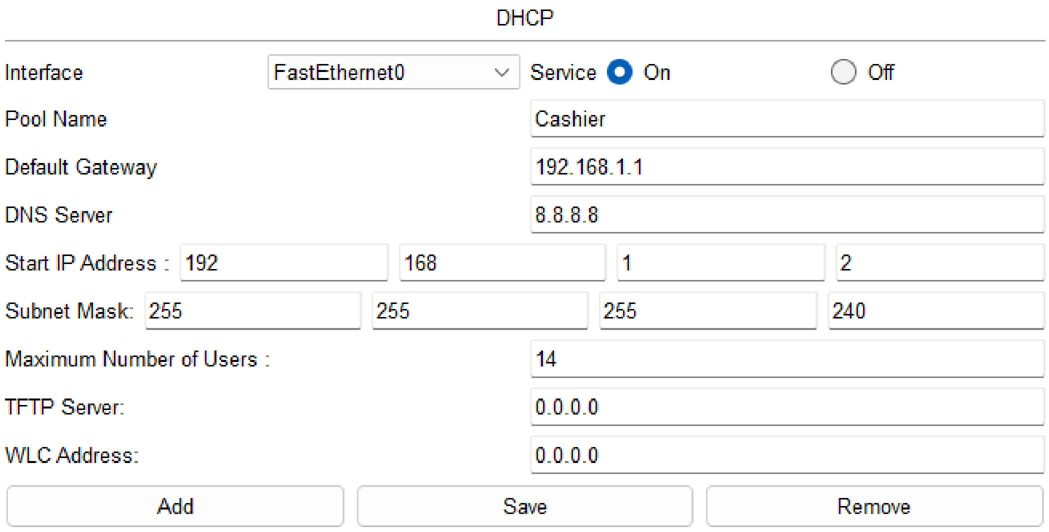
Static IP of Syslog and AAA server = 192.168.1.116

Now Router-on-a-Stick was used for inter-VLAN routing.

- A single physical interface on the router is subdivided into sub interfaces.
  Before assigning IP address the command **encapsulation dot1q <VLAN number>** was entered to enable 802.1q VLAN tagging in the sub interfaces which is essential for ROAS.
- Each sub interface is assigned to a VLAN and configured with the corresponding gateway IP.

3.3. DHCP Server configuration

Now the DHCP server is configured for each VLAN which is placed in the fourth floor.


DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name Cashier

Default Gateway 192.168.1.1

DNS Server 8.8.8.8

Start IP Address : 192 168 1 2

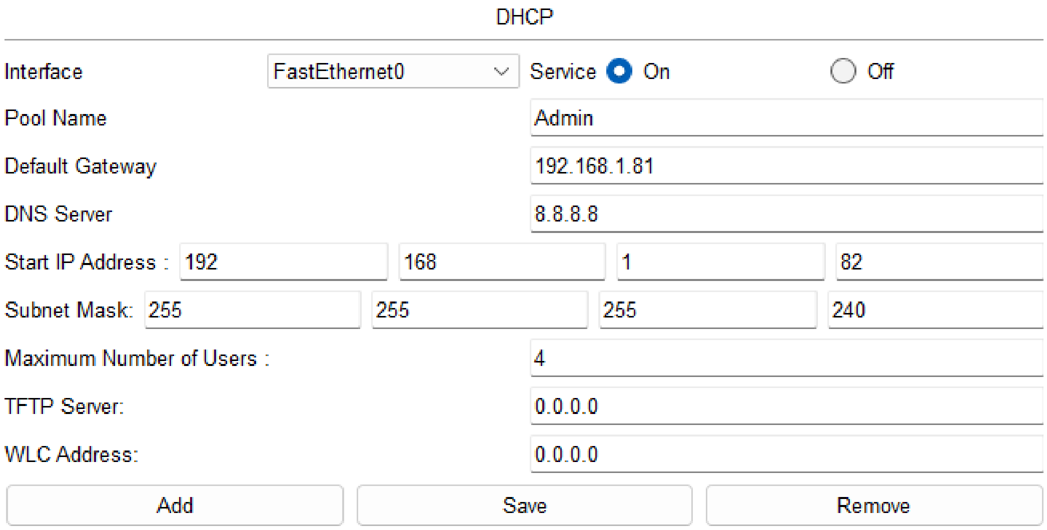
Subnet Mask: 255 255 255 240

Maximum Number of Users : 14

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Figure 7: DHCP configuration for Cashier VLAN.


DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name Admin

Default Gateway 192.168.1.81

DNS Server 8.8.8.8

Start IP Address : 192 168 1 82

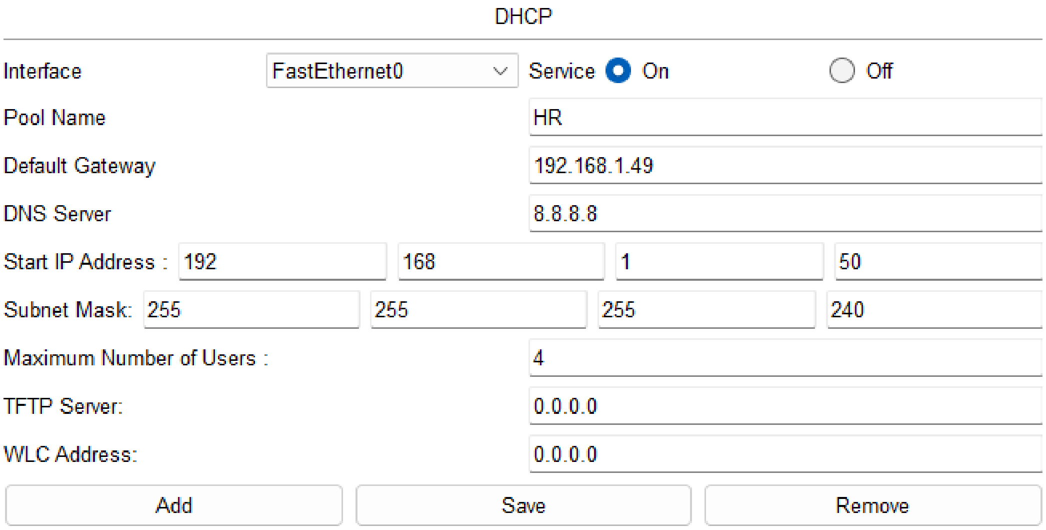
Subnet Mask: 255 255 255 240

Maximum Number of Users : 4

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Figure 8: DHCP configuration for Admin VLAN.


DHCP

Interface: FastEthernet0 — Service ● On ○ Off

Pool Name: HR

Default Gateway: 192.168.1.49

DNS Server: 8.8.8.8

Start IP Address : 192 168 1 50

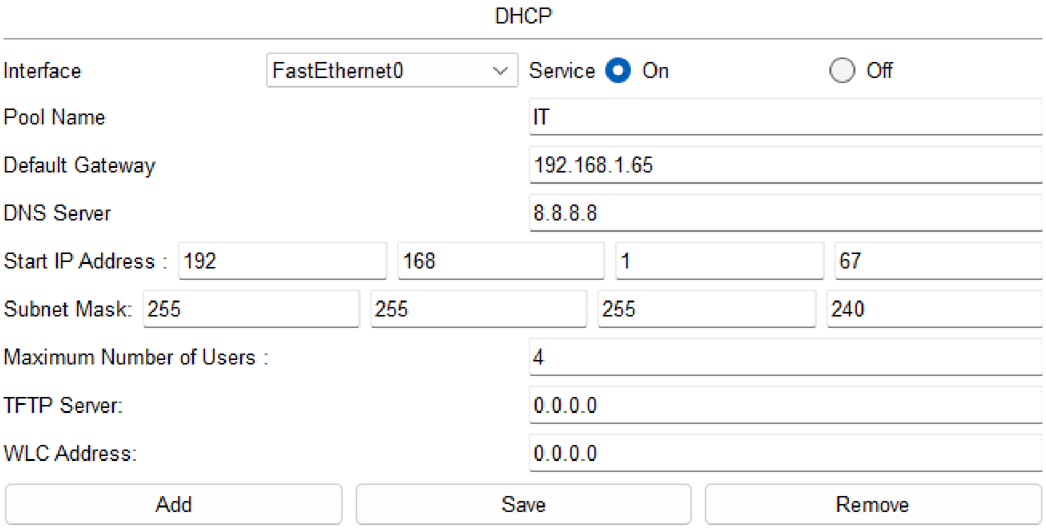
Subnet Mask: 255 255 255 240

Maximum Number of Users : 4

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Figure 9: DHCP configuration for HR VLAN.


DHCP

Interface: FastEthernet0 — Service ● On ○ Off

Pool Name: IT

Default Gateway: 192.168.1.65

DNS Server: 8.8.8.8

Start IP Address : 192 168 1 67

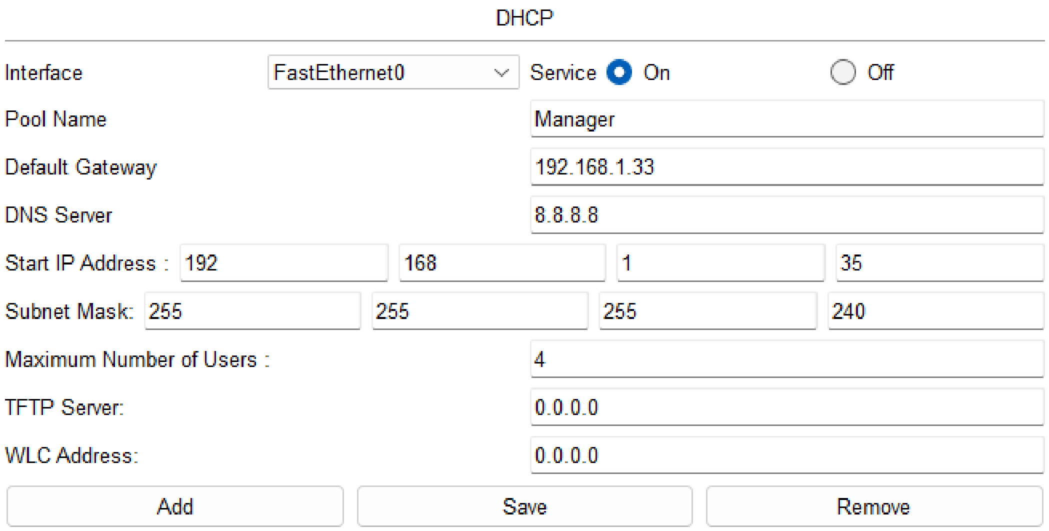
Subnet Mask: 255 255 255 240

Maximum Number of Users : 4

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Figure 10: DHCP configuration for IT VLAN.


DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: Manager

Default Gateway: 192.168.1.33

DNS Server: 8.8.8.8

Start IP Address : 192 168 1 35

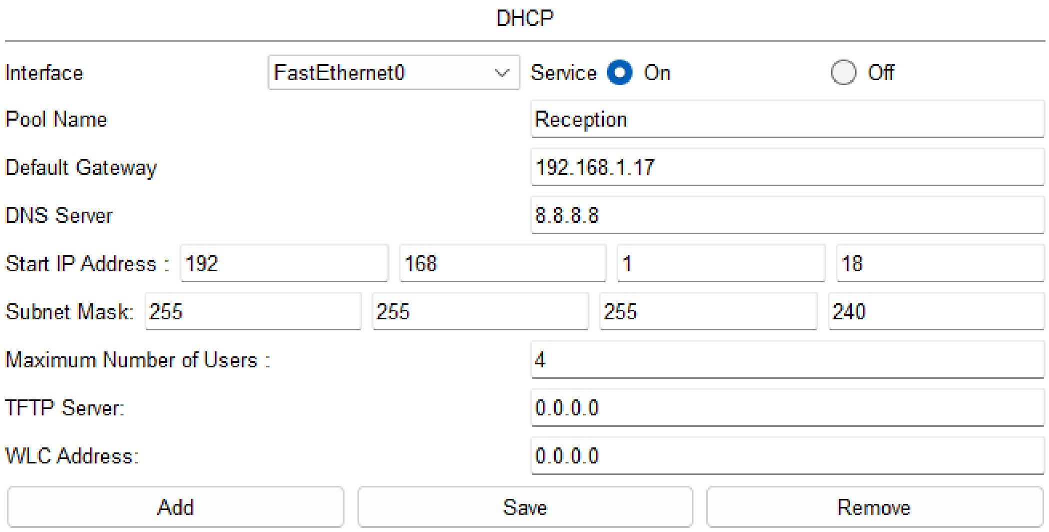
Subnet Mask: 255 255 255 240

Maximum Number of Users : 4

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Figure 11: DHCP configuration for Manager VLAN.


DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: Reception

Default Gateway: 192.168.1.17

DNS Server: 8.8.8.8

Start IP Address : 192 168 1 18

Subnet Mask: 255 255 255 240

Maximum Number of Users : 4

TFTP Server: 0.0.0.0

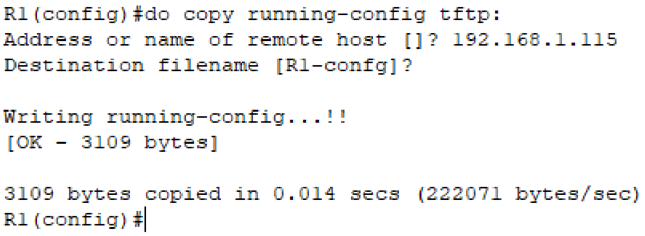
WLC Address: 0.0.0.0

Figure 12: DHCP configuration for Reception VLAN.

Router Sub interfaces were configured with **ip helper-address 192.168.1.99** (except DHCP and Servers VLANs) to configure the interfaces as relay agent to forward DHCP requests.

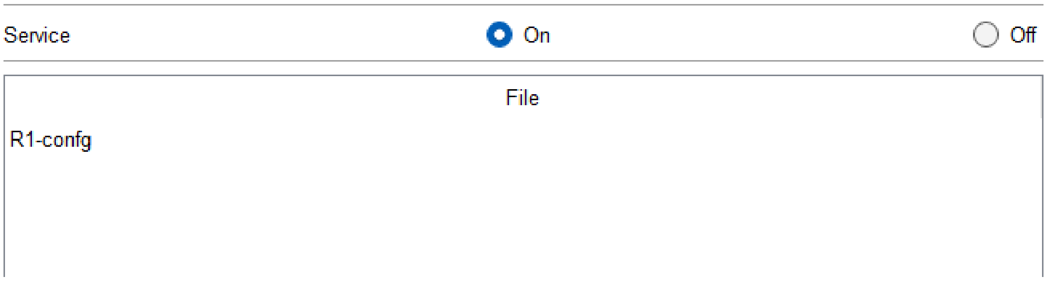
3.4. TFTP Server

It was Used to store and backup configurations of router.



```
R1(config)#do copy running-config tftp:
Address or name of remote host []? 192.168.1.115
Destination filename [R1-confg]?

Writing running-config...!!
[OK - 3109 bytes]

3109 bytes copied in 0.014 secs (222071 bytes/sec)
R1(config)#
```

Figure 13: Copying the configuration file to the TFTP server.



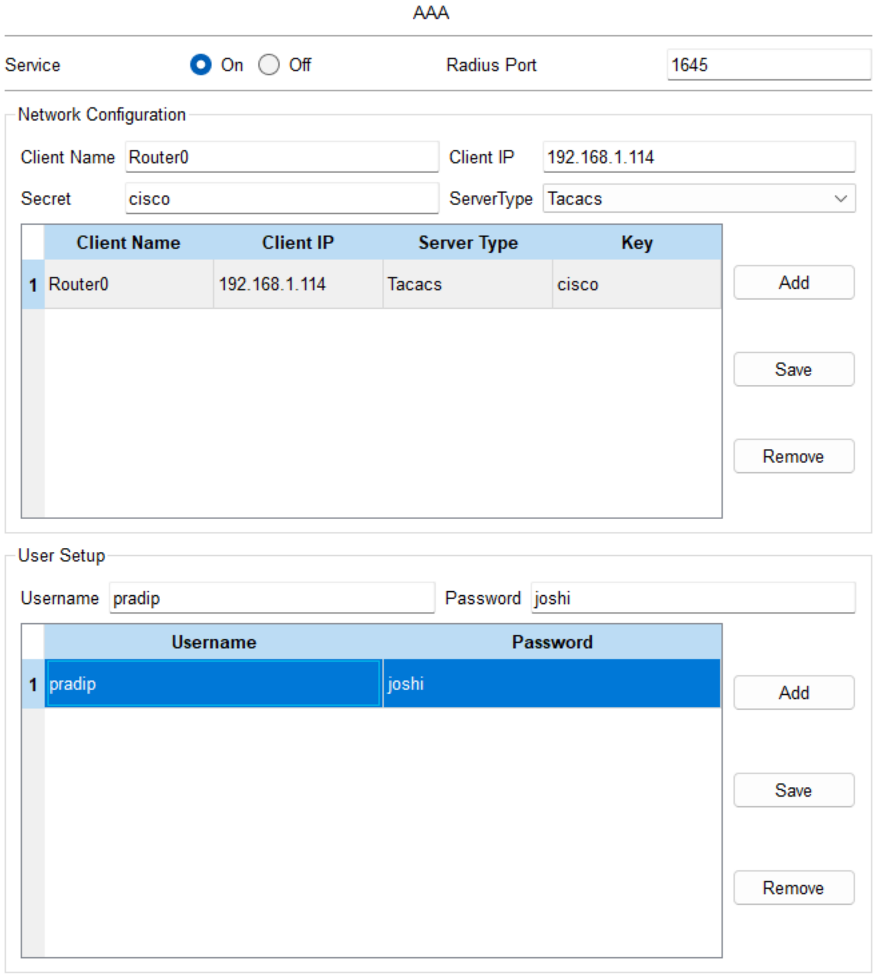
Service ● On ○ Off

File

R1-confg

Figure 14: Configuration file of Router stored in TFTP server.

3.5. AAA Server



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Router0 Client IP 192.168.1.114

Secret cisco ServerType Tacacs

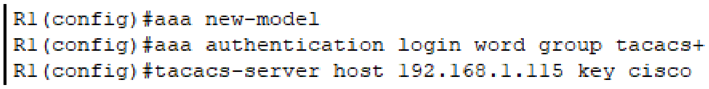
	Client Name	Client IP	Server Type	Key
1	Router0	192.168.1.114	Tacacs	cisco

User Setup

Username pradip Password joshi

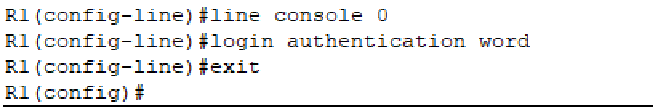
	Username	Password
1	pradip	joshi

Figure 15: After configuring AAA server.



```
R1(config)#aaa new-model
R1(config)#aaa authentication login word group tacacs+
R1(config)#tacacs-server host 192.168.1.115 key cisco
```

Figure 16: Configuration of AAA in router.



```
R1(config-line)#line console 0
R1(config-line)#login authentication word
R1(config-line)#exit
R1(config)#
```

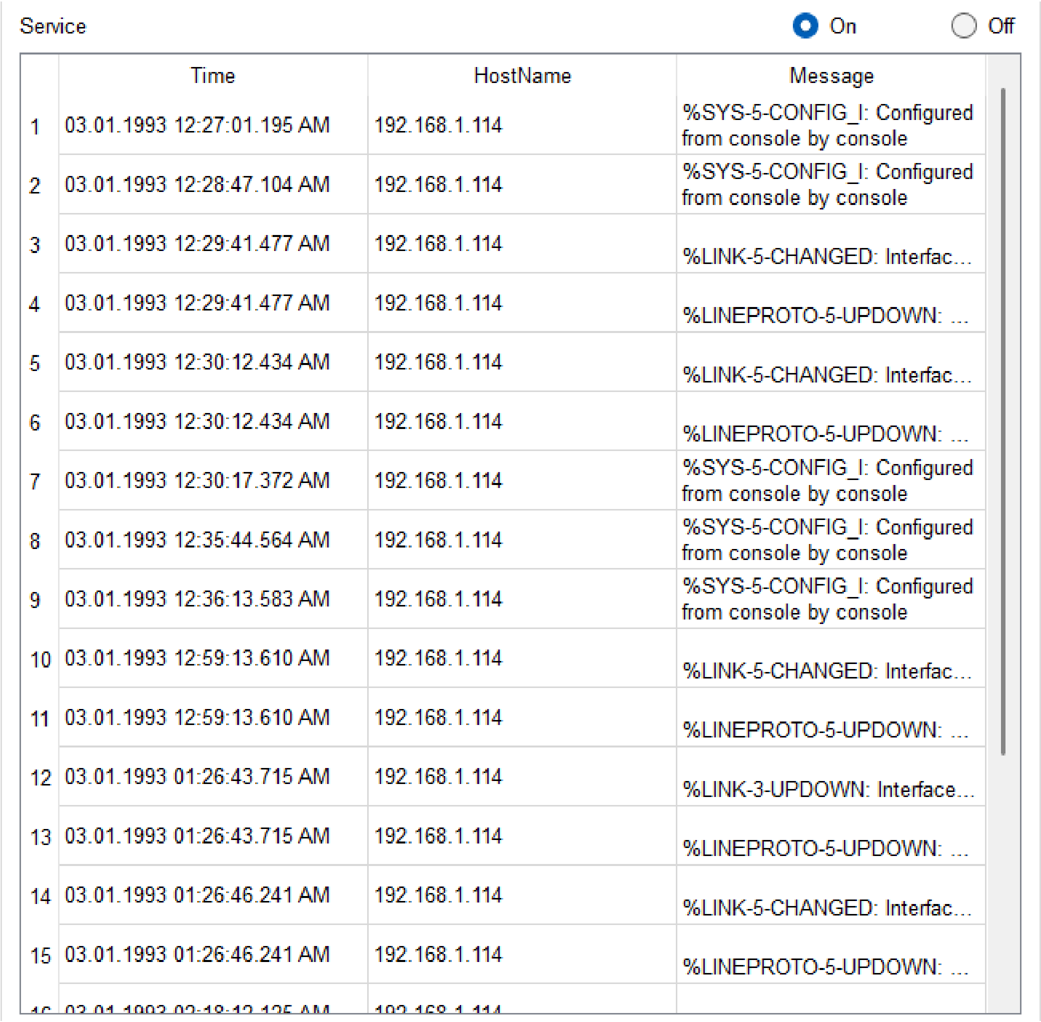
Figure 17: Implementing AAA in console of router.

3.6. Syslog Server

It is used for Centralized logging of all router/switch events.

The following commands were entered to configure the router to send log messages to the syslog server.

- **configure terminal**
- **logging 192.168.1.116**
- **logging trap informational**
- **service timestamps log datetime**



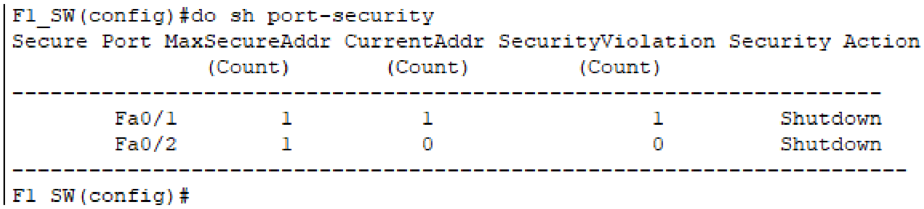
Service ● On ○ Off

	Time	HostName	Message
1	03.01.1993 12:27:01.195 AM	192.168.1.114	%SYS-5-CONFIG_I: Configured from console by console
2	03.01.1993 12:28:47.104 AM	192.168.1.114	%SYS-5-CONFIG_I: Configured from console by console
3	03.01.1993 12:29:41.477 AM	192.168.1.114	%LINK-5-CHANGED: Interfac...
4	03.01.1993 12:29:41.477 AM	192.168.1.114	%LINEPROTO-5-UPDOWN: ...
5	03.01.1993 12:30:12.434 AM	192.168.1.114	%LINK-5-CHANGED: Interfac...
6	03.01.1993 12:30:12.434 AM	192.168.1.114	%LINEPROTO-5-UPDOWN: ...
7	03.01.1993 12:30:17.372 AM	192.168.1.114	%SYS-5-CONFIG_I: Configured from console by console
8	03.01.1993 12:35:44.564 AM	192.168.1.114	%SYS-5-CONFIG_I: Configured from console by console
9	03.01.1993 12:36:13.583 AM	192.168.1.114	%SYS-5-CONFIG_I: Configured from console by console
10	03.01.1993 12:59:13.610 AM	192.168.1.114	%LINK-5-CHANGED: Interfac...
11	03.01.1993 12:59:13.610 AM	192.168.1.114	%LINEPROTO-5-UPDOWN: ...
12	03.01.1993 01:26:43.715 AM	192.168.1.114	%LINK-3-UPDOWN: Interface...
13	03.01.1993 01:26:43.715 AM	192.168.1.114	%LINEPROTO-5-UPDOWN: ...
14	03.01.1993 01:26:46.241 AM	192.168.1.114	%LINK-5-CHANGED: Interfac...
15	03.01.1993 01:26:46.241 AM	192.168.1.114	%LINEPROTO-5-UPDOWN: ...
16	03.01.1993 02:18:12.125 AM	192.168.1.114	

Figure 18: Screenshot of the log being captured in syslog server.

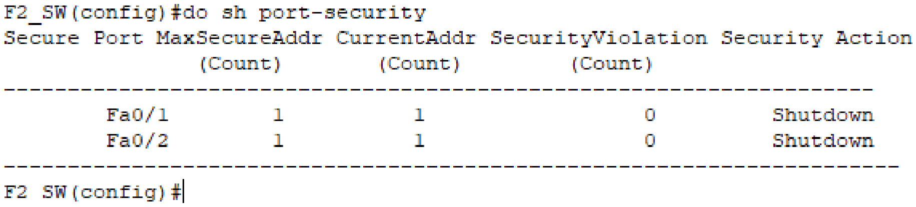
3.7. Port-Security

- Applied to all access ports of all the switches.
- Only one device (MAC address) is allowed per port.
- Violations cause ports to shut down for security enforcement.



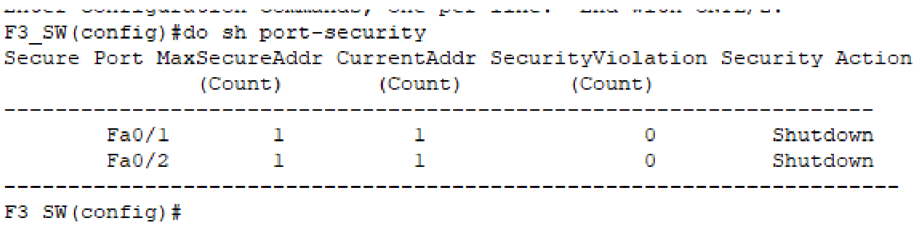
```
F1_SW(config)#do sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/1        1          1                 1         Shutdown
        Fa0/2        1          0                 0         Shutdown
----------------------------------------------------------------------
F1 SW(config)#
```

Figure 19: Port-Security in floor 1 switch.



```
F2_SW(config)#do sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/1        1          1                 0         Shutdown
        Fa0/2        1          1                 0         Shutdown
----------------------------------------------------------------------
F2 SW(config)#
```

Figure 20: Port-Security in floor 2 switch.



```
F3_SW(config)#do sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/1        1          1                 0         Shutdown
        Fa0/2        1          1                 0         Shutdown
----------------------------------------------------------------------
F3 SW(config)#
```

Figure 21: Port-Security in floor 3 switch.

3.8. Extended ACL

To enforce strict inter-departmental access policies and protect sensitive resources, an Extended ACL was configured on the router. This ACL controls which VLANs (departments) can initiate communication with others, based on IP addresses and applied directionally on the router's sub interfaces.

Access Policy Overview:

1. Cashier (VLAN 10):

- It cannot access any VLAN except the DHCP server.
- Strictly isolated to reduce exposure and maintain transactional integrity.

2. Reception (VLAN 15):

- It has full access to all other departments.
- It acts as a central communication point or public access zone.

3. Manager (VLAN 20):

- It has full access to all departments.
- As a high-level administrative role, it needs visibility across the network.

4. HR (VLAN 25):

- It has access to Reception, Manager, and HR.
- It is blocked from accessing Cashier, IT, and Admin for confidentiality reasons.

5. IT (VLAN 30):

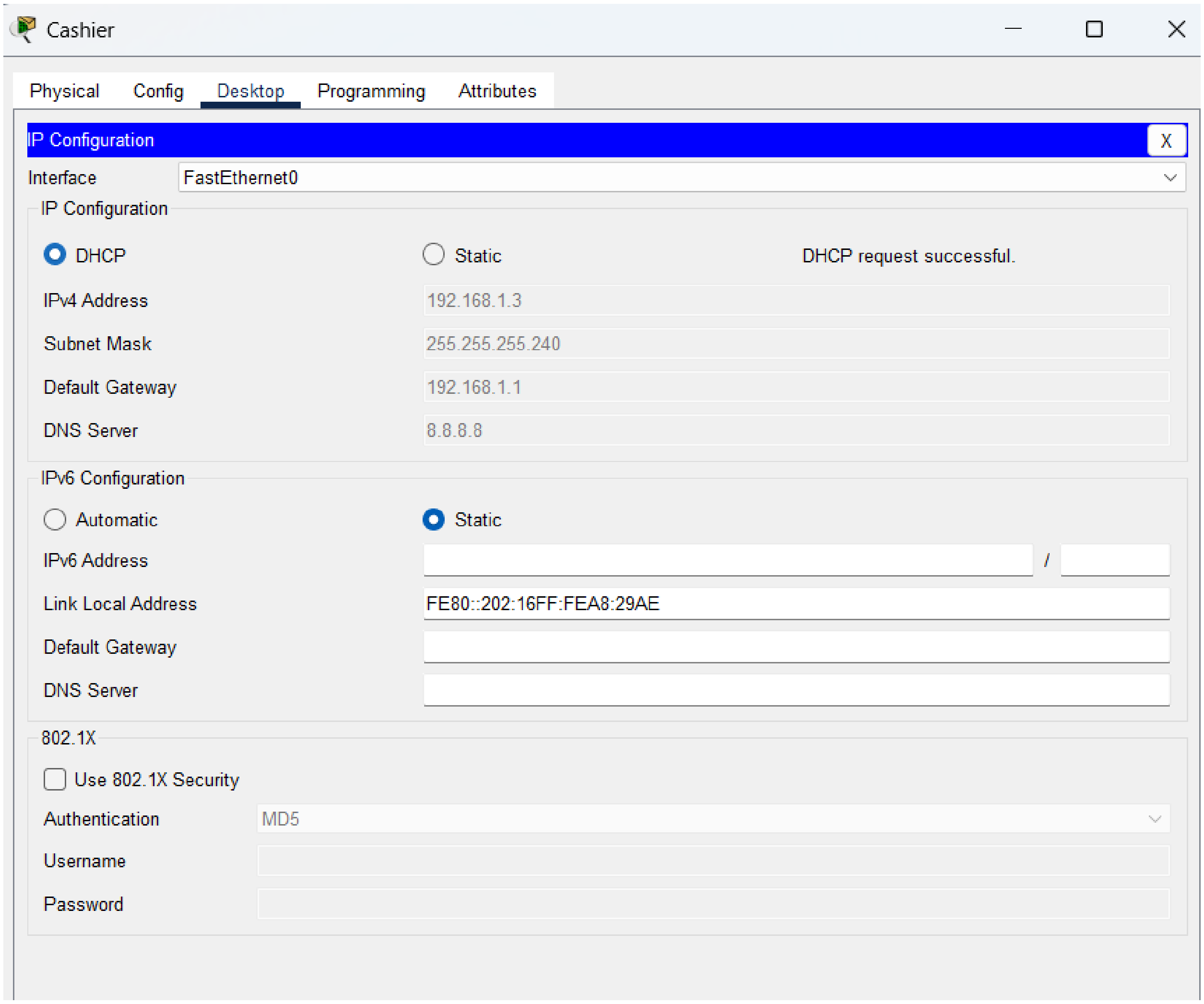
- It has full access to all VLANs, required for network maintenance and monitoring.
- It is considered as trusted.

6. Admin (VLAN 35):

- It has access to Reception, Manager, and Admin.
- It cannot access Cashier, HR, or IT which reflects the departmental isolation.

4. Testing

4.1. DHCP Test



Cashier

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 192.168.1.3

Subnet Mask: 255.255.255.240

Default Gateway: 192.168.1.1

DNS Server: 8.8.8.8

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::202:16FF:FEA8:29AE

Default Gateway:

DNS Server:

802.1X

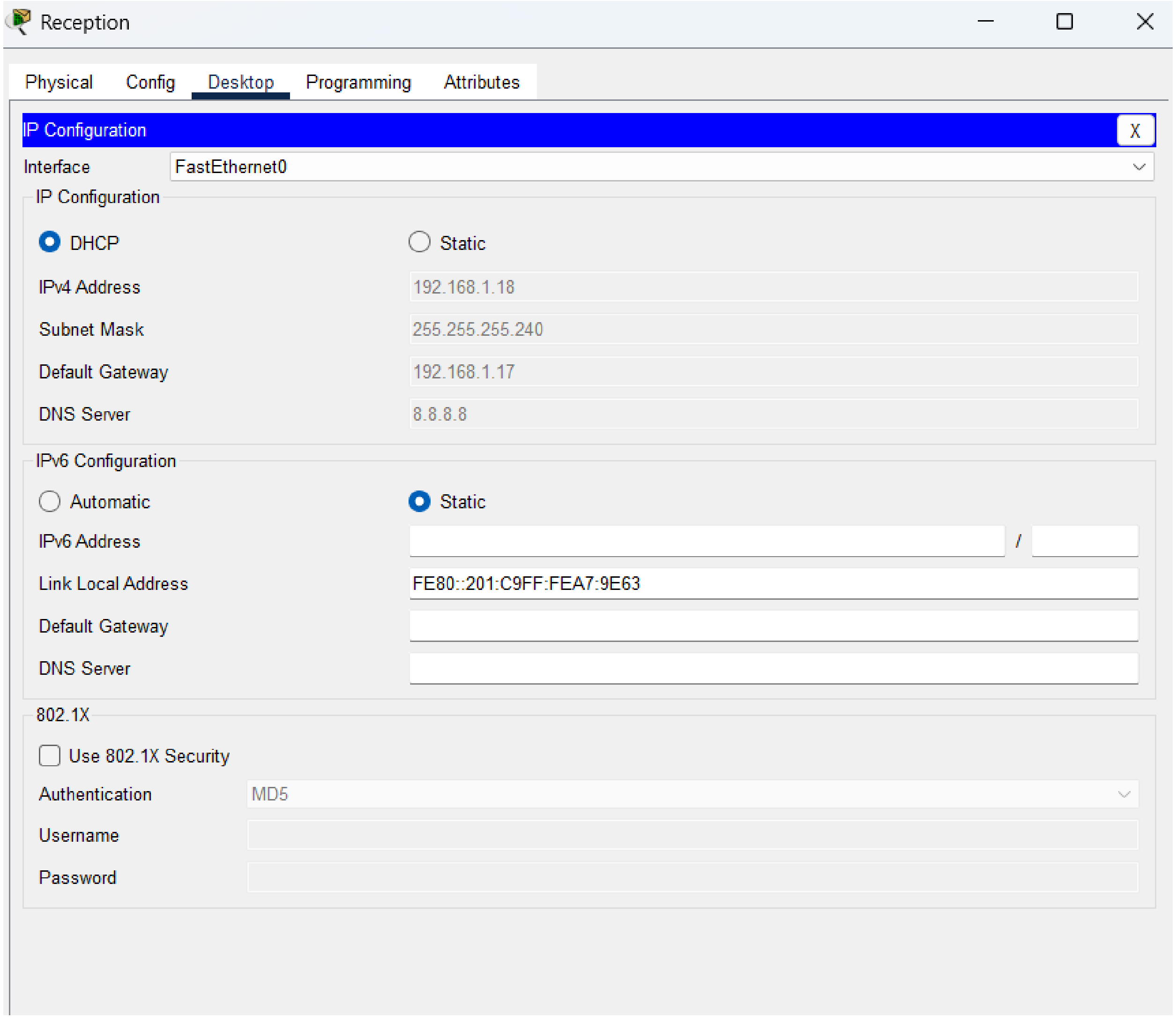
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Figure 22: IP configuration of Cashier PC using DHCP.



IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.1.18

Subnet Mask 255.255.255.240

Default Gateway 192.168.1.17

DNS Server 8.8.8.8

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::201:C9FF:FEA7:9E63

Default Gateway

DNS Server

802.1X

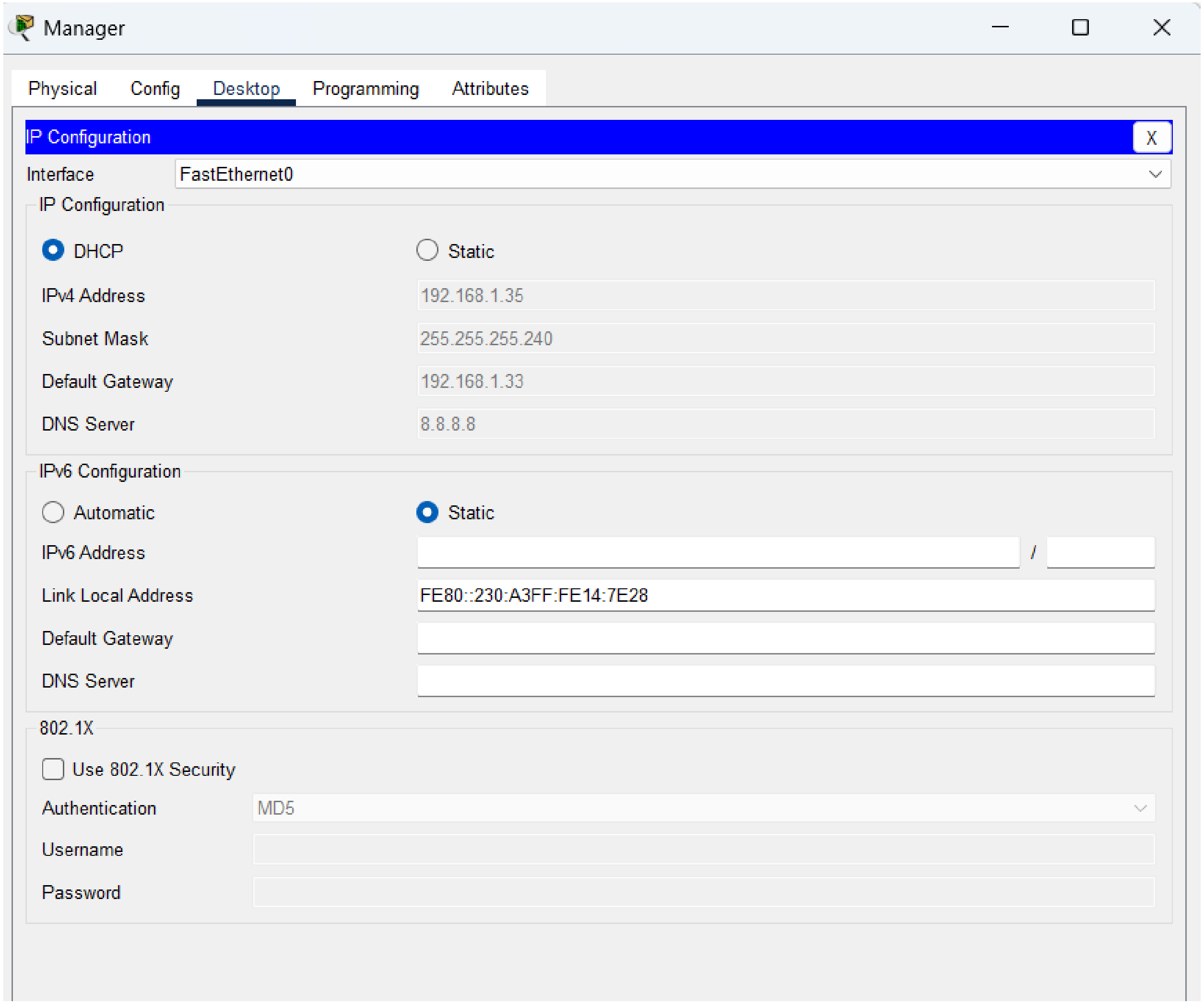
□ Use 802.1X Security

Authentication MD5

Username

Password

Figure 23: IP configuration of Reception PC using DHCP.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.1.35

Subnet Mask: 255.255.255.240

Default Gateway: 192.168.1.33

DNS Server: 8.8.8.8

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::230:A3FF:FE14:7E28

Default Gateway:

DNS Server:

802.1X

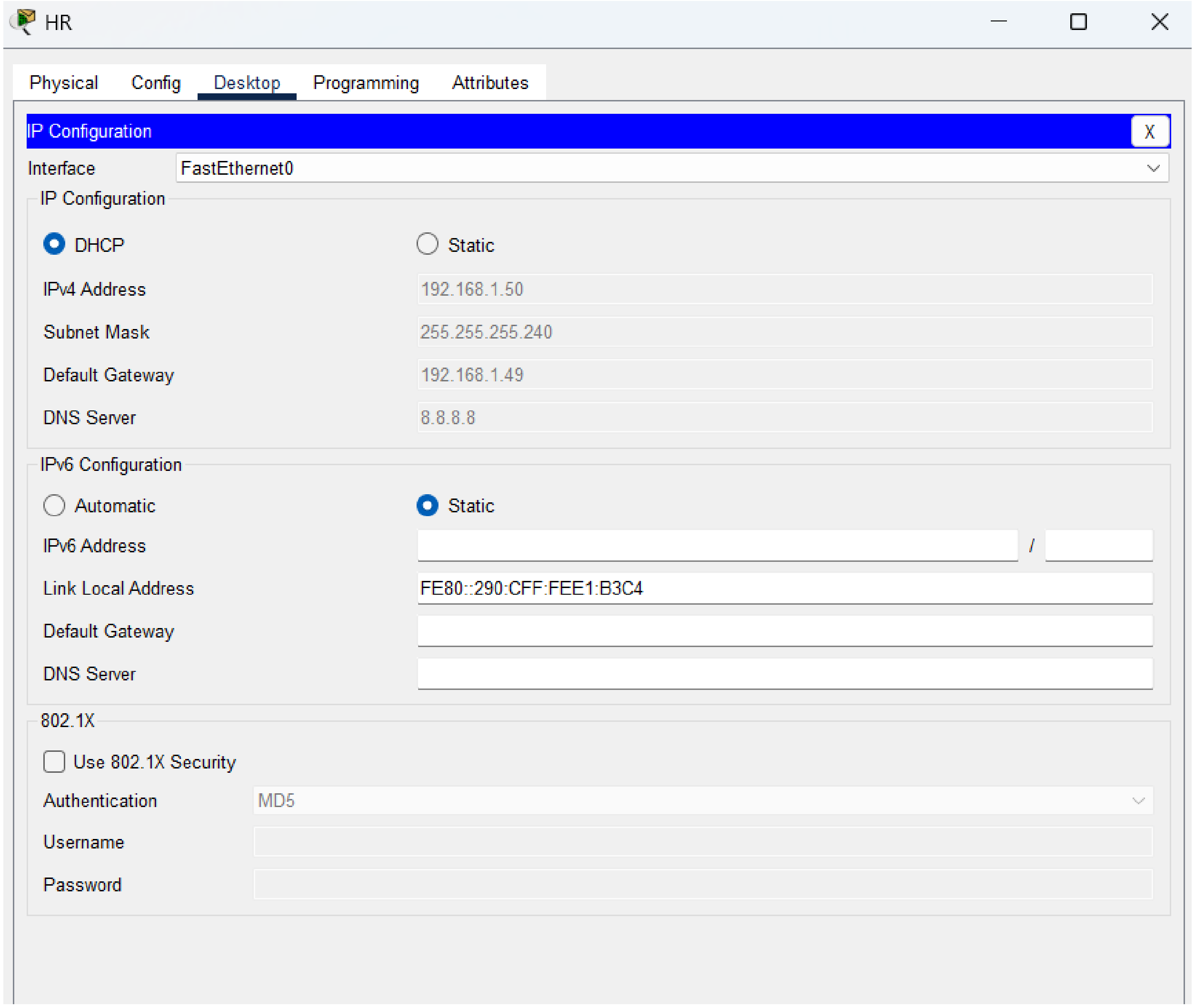
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Figure 24: IP configuration of Manager PC using DHCP.



Interface FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.1.50

Subnet Mask 255.255.255.240

Default Gateway 192.168.1.49

DNS Server 8.8.8.8

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::290:CFF:FEE1:B3C4

Default Gateway

DNS Server

802.1X

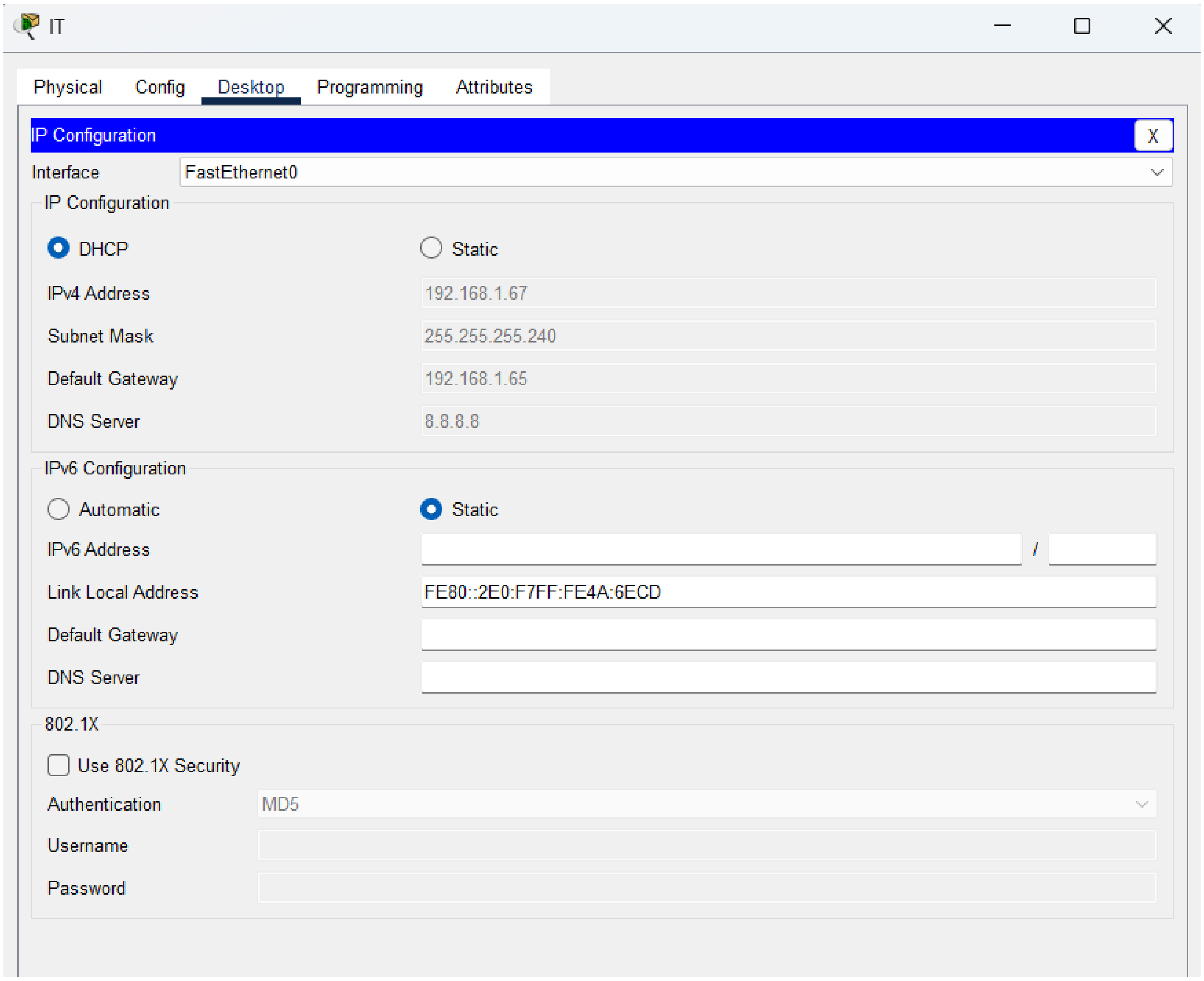
□ Use 802.1X Security

Authentication MD5

Username

Password

Figure 25: IP configuration of HR PC using DHCP.



IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.1.67

Subnet Mask: 255.255.255.240

Default Gateway: 192.168.1.65

DNS Server: 8.8.8.8

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2E0:F7FF:FE4A:6ECD

Default Gateway:

DNS Server:

802.1X

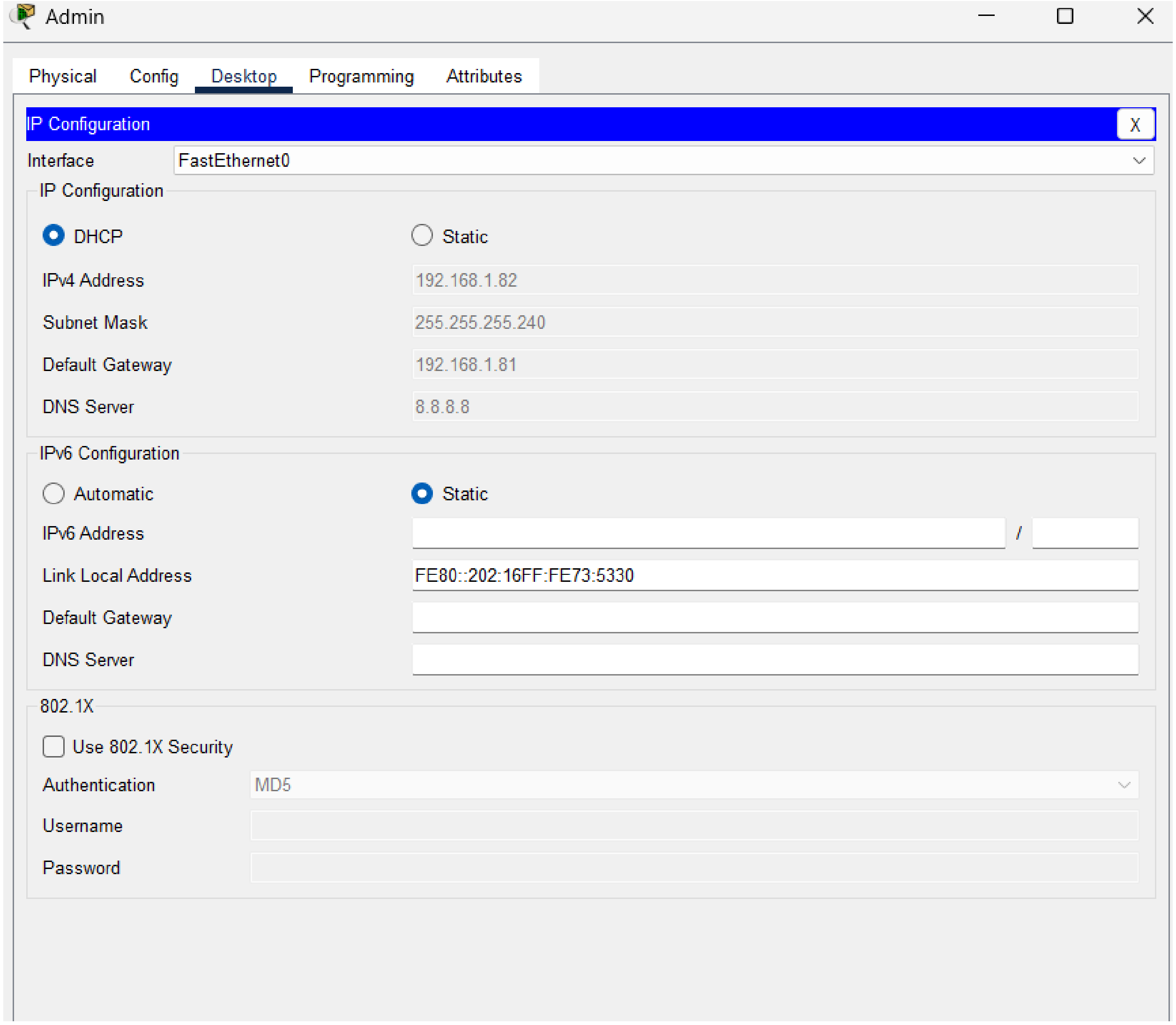
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Figure 26: IP configuration of IT PC using DHCP.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.1.82

Subnet Mask: 255.255.255.240

Default Gateway: 192.168.1.81

DNS Server: 8.8.8.8

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::202:16FF:FE73:5330

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

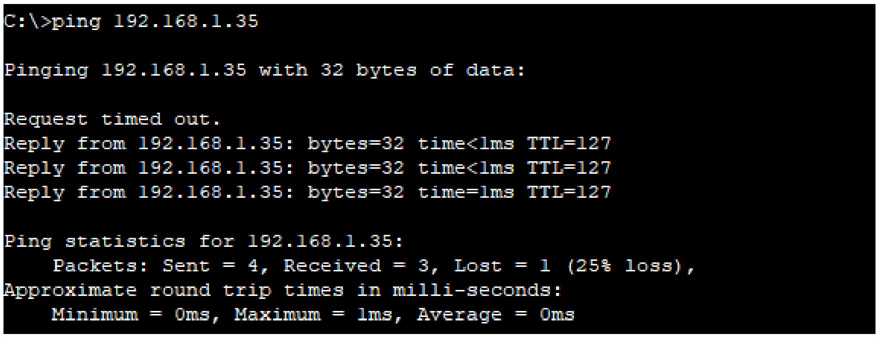
Username:

Password:

Figure 27: IP configuration of Admin PC using DHCP.

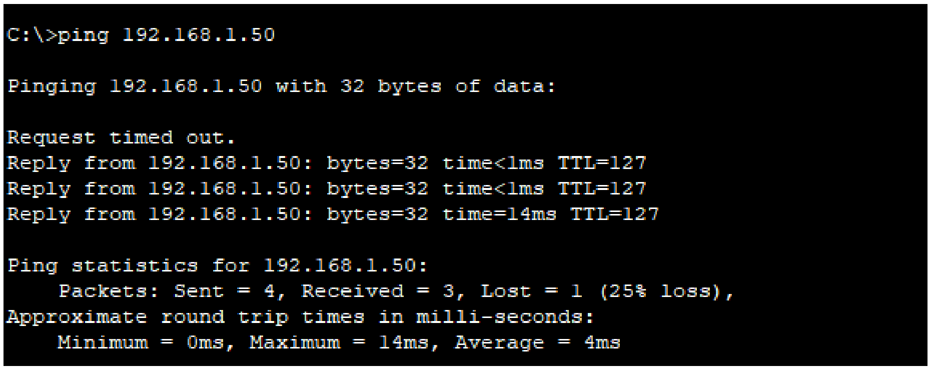
4.2. Inter VLAN Routing Test

1. Ping Reception to Manager



```
C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.35: bytes=32 time<1ms TTL=127
Reply from 192.168.1.35: bytes=32 time<1ms TTL=127
Reply from 192.168.1.35: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

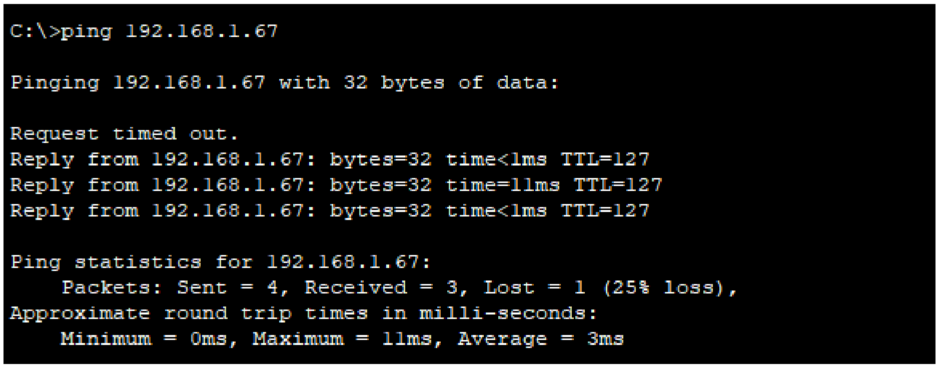
2. Ping Reception to HR



```
C:\>ping 192.168.1.50

Pinging 192.168.1.50 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.50: bytes=32 time<1ms TTL=127
Reply from 192.168.1.50: bytes=32 time<1ms TTL=127
Reply from 192.168.1.50: bytes=32 time=14ms TTL=127

Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 4ms
```

Ping was successful.

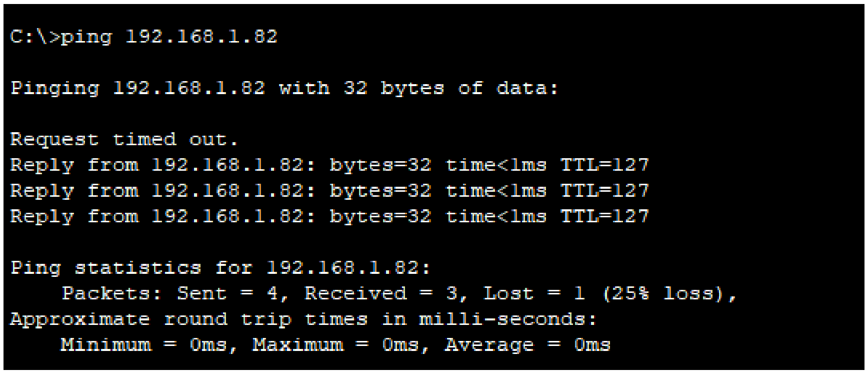
3. Ping Reception to IT



```
C:\>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.67: bytes=32 time<1ms TTL=127
Reply from 192.168.1.67: bytes=32 time=11ms TTL=127
Reply from 192.168.1.67: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

Ping was successful.

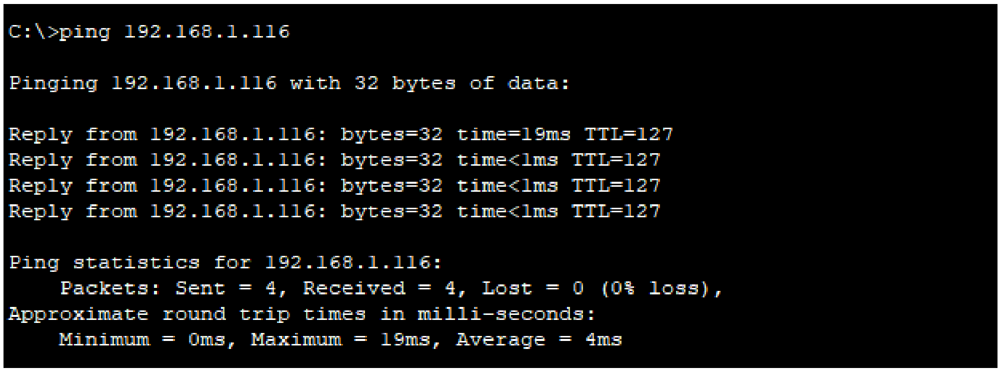
4. Ping Reception to Admin



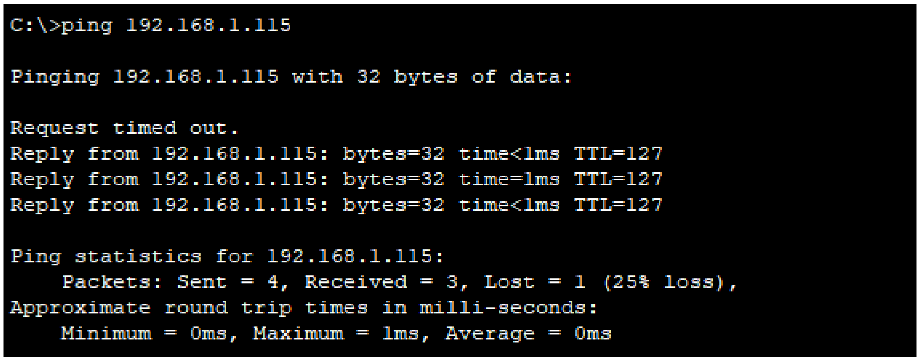
```
C:\>ping 192.168.1.82

Pinging 192.168.1.82 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.82: bytes=32 time<1ms TTL=127
Reply from 192.168.1.82: bytes=32 time<1ms TTL=127
Reply from 192.168.1.82: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.82:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping was successful.

5. Ping Reception to Servers



```
C:\>ping 192.168.1.116

Pinging 192.168.1.116 with 32 bytes of data:

Reply from 192.168.1.116: bytes=32 time=19ms TTL=127
Reply from 192.168.1.116: bytes=32 time<1ms TTL=127
Reply from 192.168.1.116: bytes=32 time<1ms TTL=127
Reply from 192.168.1.116: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.116:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 4ms
```



```
C:\>ping 192.168.1.115

Pinging 192.168.1.115 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.115: bytes=32 time<1ms TTL=127
Reply from 192.168.1.115: bytes=32 time=1ms TTL=127
Reply from 192.168.1.115: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.115:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Pings were successful.