Information
Technology
Institute

Software Company Network Architecture

Authors

Ahmed Gamal Mohamed Ali

Yousef Mohamed Ahmed Aboelata

Adham Mamdouh ElSherbiny ElBadaway

Supervisor

ENG. Ekram Abdelwahed

System Administration

ITI Intake 46

Alexandria University

November 14, 2025

Contents

1 Introduction

1.1 Project Overview

This project presents the design and implementation of a comprehensive network infrastructure for a modern software development company that operates using Agile methodologies. The network is built and simulated using Cisco Packet Tracer to demonstrate real-world enterprise networking concepts and best practices.

The company requires a robust, secure, and scalable network infrastructure to support its daily operations and facilitate communication between multiple departments. The network must provide reliable connectivity, implement security measures, ensure high availability, and offer centralized management capabilities.

1.2 Company Structure and Requirements

The software company consists of several key departments, each with specific networking requirements:

- **Software Development:** The core department that works using the Agile system. This team consists of developers, testers, and Scrum Masters responsible for developing applications and websites.
- **Human Resources (HR):** Manages employee data and requires secure access to sensitive information
- **Information Technology (IT):** Responsible for network management and technical infrastructure
- **Marketing:** Handles digital marketing campaigns and requires internet access for online platforms
- **Accounting:** Manages financial data with strict security and privacy requirements
- **Technical Support:** Provides customer assistance and requires access to various network resources

1.3 Network Design Objectives

The primary objectives of this network design are:

1. **Segmentation:** Isolate each department using VLANs to improve security and reduce broadcast traffic
2. **Inter-Department Communication:** Enable controlled communication between departments through Inter-VLAN routing
3. **Dynamic IP Assignment:** Implement centralized DHCP services for efficient IP address management
4. **Scalability:** Use dynamic routing protocols (OSPF) to support network growth
5. **High Availability:** Implement redundant links using EtherChannel technology
6. **Internet Connectivity:** Provide secure internet access for all departments with NAT/PAT

7. **Centralized Authentication:** Use AAA server for secure user authentication and authorization

8. **File Sharing:** Deploy FTP server for centralized file storage and sharing

9. **Remote Management:** Configure SSH for secure remote administration

1.4 Implemented Technologies

To meet the company's networking requirements, the following technologies and protocols have been implemented:

Technology	Purpose
VLANs	Logical segmentation of the network by department to improve security and reduce broadcast domains
Router-on-a-Stick	Enable communication between different VLANs using a single router interface with sub-interfaces
OSPF	Dynamic routing protocol for efficient route calculation and network scalability
DHCP Server	Standalone server for automatic IP address assignment to all network devices
AAA Server	Centralized authentication, authorization, and accounting for network access control
Static NAT	Translate private IP addresses to public IP for specific servers requiring internet access
PAT	Port Address Translation for multiple internal devices to share a single public IP address for internet access
EtherChannel	Link aggregation between switches for increased bandwidth and redundancy
FTP Server	Centralized file storage and transfer service for company-wide file sharing
SSH	Secure Shell protocol for encrypted remote management of network devices

Table 1: Implemented Network Technologies

1.5 Network Topology Overview

The network topology consists of the following components designed to provide security, scalability, and efficient communication:

- **VLANs:** Four VLANs, one dedicated to each department (Software Development, HR, IT, Marketing, Accounting, and Technical Support) for network segmentation
- **Routers:** Six routers (R1_AYY through R6_AYY) running OSPF for dynamic routing and handling Inter-VLAN routing using Router-on-a-Stick configuration
- **Switches:** Seven switches (S1_AYY through S7_AYY) connecting end-user devices.
- **Servers:** Three dedicated servers - AAA Server for authentication, DHCP Server for IP address assignment, and FTP Server for file sharing
- **Gateway Router:** Edge router providing internet connectivity through ISP and handling NAT/PAT translations
- **IP Addressing:** Subnetting scheme implemented to efficiently allocate IP addresses for all devices across the network

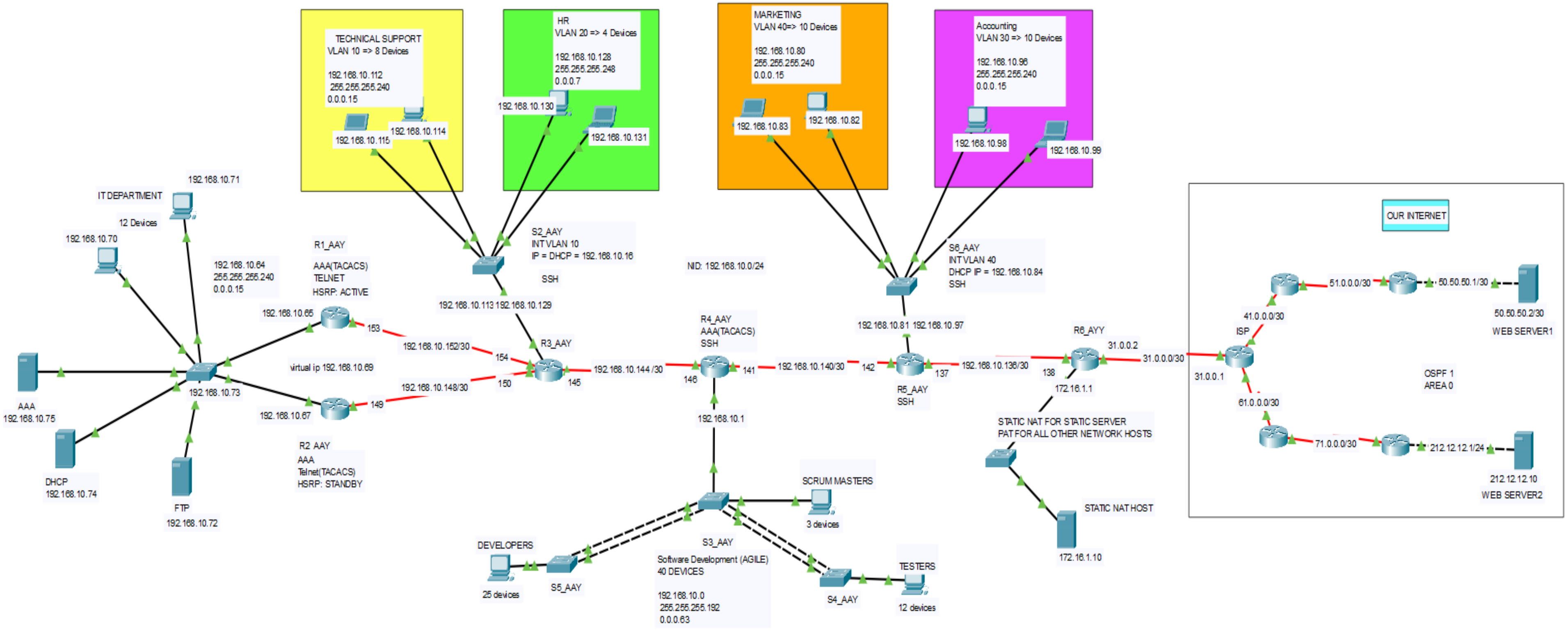


Figure 1: Network Topology Diagram

2 IP Addressing and Subnetting

2.1 IP Address Plan

The network uses a private IP address range 192.168.10.0/24 with Variable Length Subnet Masking (VLSM) to efficiently allocate IP addresses based on the number of devices in each department and network segment. The subnetting scheme is designed to minimize IP address waste while providing adequate address space for future growth.

Network Address	Subnet Mask	Wildcard Mask	Usable Hosts
192.168.10.0	255.255.255.192	0.0.0.63	62
192.168.10.64	255.255.255.240	0.0.0.15	14
192.168.10.80	255.255.255.240	0.0.0.15	14
192.168.10.96	255.255.255.240	0.0.0.15	14
192.168.10.112	255.255.255.240	0.0.0.15	14
192.168.10.128	255.255.255.248	0.0.0.7	6
192.168.10.136	255.255.255.252	0.0.0.3	2
192.168.10.140	255.255.255.252	0.0.0.3	2
192.168.10.144	255.255.255.252	0.0.0.3	2
192.168.10.148	255.255.255.252	0.0.0.3	2
192.168.10.152	255.255.255.252	0.0.0.3	2

Table 2: IP Address Subnetting Plan

The /30 subnets (255.255.255.252) are allocated for point-to-point connections between routers, providing exactly 2 usable IP addresses per link, which is optimal for router-to-router connections.

2.2 VLAN IP Assignment

The network is divided into multiple VLANs to separate departments and servers for security and traffic management. Each VLAN is assigned a dedicated subnet with a default gateway for Inter-VLAN routing.

VLAN ID	Department	Network Address	Gateway	Hosts
-	Software Development	192.168.10.0/26	192.168.10.1	32
-	IT & Servers	192.168.10.64/28	192.168.10.69 (VIP)	12
40	Marketing	192.168.10.80/28	192.168.10.81	10
30	Accounting	192.168.10.96/28	192.168.10.97	10
10	Technical Support	192.168.10.112/28	192.168.10.113	8
20	HR	192.168.10.128/29	192.168.10.129	4

Table 3: VLAN IP Address Assignment

Server Assignments within IT Department Network (192.168.10.64/28):

- **DHCP Server:** 192.168.10.74
- **AAA Server:** 192.168.10.75
- **FTP Server:** 192.168.10.72

Router-to-Router Point-to-Point Links (/30 networks):

Network Address	Router 1	Router 2
192.168.10.136/30	R5_AYY (.137)	R6_AYY (.138)
192.168.10.140/30	R4_AYY (.141)	R5_AYY (.142)
192.168.10.144/30	R3_AYY (.145)	R4_AYY (.146)
192.168.10.148/30	R2_AYY (.149)	R3_AYY (.150)
192.168.10.152/30	R1_AYY (.153)	R3_AYY (.154)

Table 4: Point-to-Point Router Links

3 VLAN Configuration

3.1 Overview

Virtual Local Area Networks (VLANs) are used to logically divide a physical network into separate broadcast domains. VLANs operate at Layer 2 and allow us to group devices by department regardless of their physical location.

Benefits of using VLANs in our network:

- Improve security by isolating department traffic
- Reduce broadcast traffic and improve performance
- Simplify network management
- Provide flexibility for network changes

3.2 VLAN Design

We created four VLANs for the network, one for each department. Technical Support and HR are connected to switch S2_AAY, while Marketing and Accounting are connected to switch S3_AAY.

VLAN ID	VLAN Name	Department	Network
10	TECHNICAL_SUPPORT	Technical Support	192.168.10.112/28
20	HR	Human Resources	192.168.10.128/29
40	MARKETING	Marketing	192.168.10.80/28
30	ACCOUNTING	Accounting	192.168.10.96/28

Table 5: VLAN Design and Assignment

3.3 Configuration

3.3.1 Creating VLANs

First, we create the VLANs on the switch:

Listing 1: Creating VLANs on Switch S2_AAY

```
S2_AAY(config)# vlan 10
S2_AAY(config-vlan)# name technical_support
S2_AAY(config-vlan)# exit

S2_AAY(config)# vlan 20
S2_AAY(config-vlan)# name HR
S2_AAY(config-vlan)# exit
```

3.3.2 Configuring Access Ports

Access ports connect end devices to their assigned VLANs:

Listing 2: Access Port Configuration

```
S2_AAY(config)# interface FastEthernet0/1
S2_AAY(config-if)# switchport access vlan 10
S2_AAY(config-if)# switchport mode access
S2_AAY(config-if)# exit

S2_AAY(config)# interface FastEthernet0/2
S2_AAY(config-if)# switchport access vlan 20
S2_AAY(config-if)# switchport mode access
S2_AAY(config-if)# exit

S2_AAY(config)# interface FastEthernet0/3
S2_AAY(config-if)# switchport access vlan 10
S2_AAY(config-if)# switchport mode access
S2_AAY(config-if)# exit

S2_AAY(config)# interface FastEthernet0/4
S2_AAY(config-if)# switchport access vlan 20
S2_AAY(config-if)# switchport mode access
S2_AAY(config-if)# exit
```

3.4 Verification

3.4.1 VLAN Topology

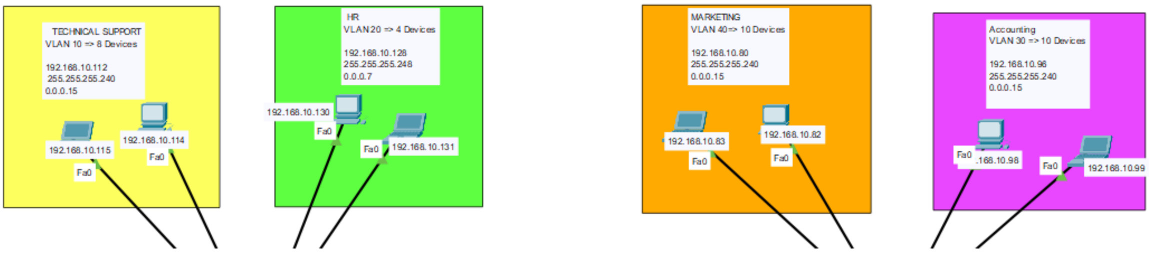
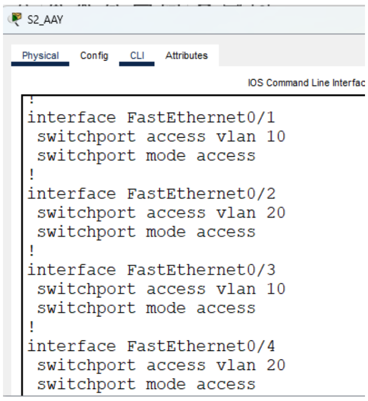


Figure 2: VLAN Topology - Four VLANs for different departments

3.4.2 Access Port Verification



```
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
```

Figure 3: Access Port Configuration showing VLAN assignments

The configuration shows:

- FastEthernet0/1 and Fa0/3: VLAN 10 (Technical Support)
- FastEthernet0/2 and Fa0/4: VLAN 20 (HR)

4 Inter-VLAN Routing

4.1 Overview

Inter-VLAN routing is required to allow communication between devices in different VLANs. By default, VLANs are isolated from each other at Layer 2, so a Layer 3 device (router) is needed to route traffic between them.

We implemented Inter-VLAN routing using the **Router-on-a-Stick (ROAS)** method. This approach uses a single physical router interface with multiple logical sub-interfaces, one for each VLAN. Each sub-interface acts as the default gateway for its respective VLAN.

The ROAS protocol was applied to every switch that has more than one VLAN and the router connected to it. This allows all VLANs to communicate with each other through the router while maintaining logical separation.

4.2 Configuration

4.2.1 Router Sub-Interface Configuration

To implement ROAS, we configure sub-interfaces on the router's physical interface. Each sub-interface is assigned to a specific VLAN using 802.1Q encapsulation and given an IP address that serves as the default gateway for that VLAN.

Example: Router R3_AAY Interface GigabitEthernet0/0/0 Configuration

Listing 3: Router Sub-Interface Configuration for VLAN 10 and VLAN 20

```
R3_AAY(config)# interface GigabitEthernet0/0/0.10
R3_AAY(config-subif)# encapsulation dot1Q 10
R3_AAY(config-subif)# ip address 192.168.10.113 255.255.255.240
R3_AAY(config-subif)# ip helper-address 192.168.10.74
R3_AAY(config-subif)# exit

R3_AAY(config)# interface GigabitEthernet0/0/0.20
```

```
R3_AAY(config-subif)# encapsulation dot1Q 20
R3_AAY(config-subif)# ip address 192.168.10.129 255.255.255.248
R3_AAY(config-subif)# exit
```

Configuration Explanation:

- **Sub-interface naming:** G0/0/0.10 and G0/0/0.20 (physical interface.VLAN_ID)
- **Encapsulation dot1Q:** Specifies 802.1Q VLAN tagging with the VLAN ID
- **IP address:** The gateway IP for each VLAN
  - VLAN 10: 192.168.10.113 (Technical Support)
  - VLAN 20: 192.168.10.129 (HR)

4.2.2 Physical Interface Activation

The physical interface must be enabled (no shutdown) for the sub-interfaces to work:

Listing 4: Enabling Physical Interface

```
R3_AAY(config)# interface GigabitEthernet0/0/0
R3_AAY(config-if)# no shutdown
R3_AAY(config-if)# exit
```

4.2.3 Configuring Trunk Ports

Trunk ports carry traffic for multiple VLANs between switches and routers:

Listing 5: Trunk Port Configuration

```
S2_AAY(config)# interface GigabitEthernet0/1
S2_AAY(config-if)# switchport mode trunk
S2_AAY(config-if)# exit
```

4.3 Verification

4.3.1 Topology Verification

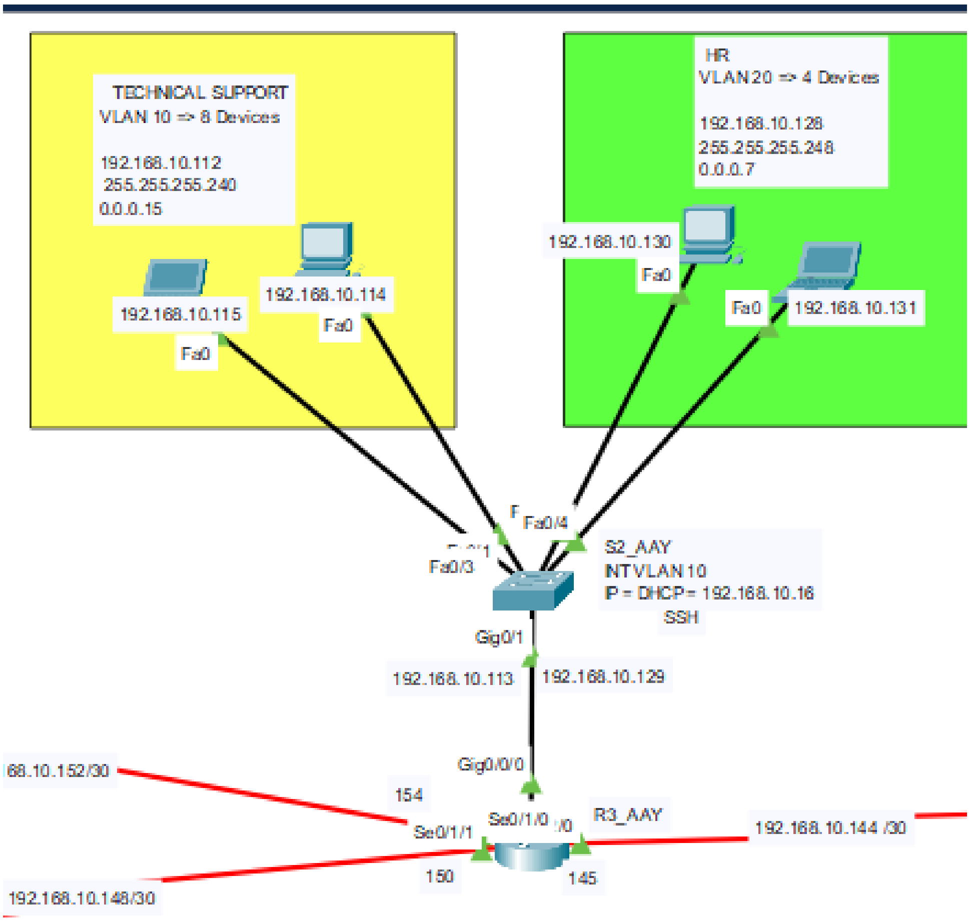
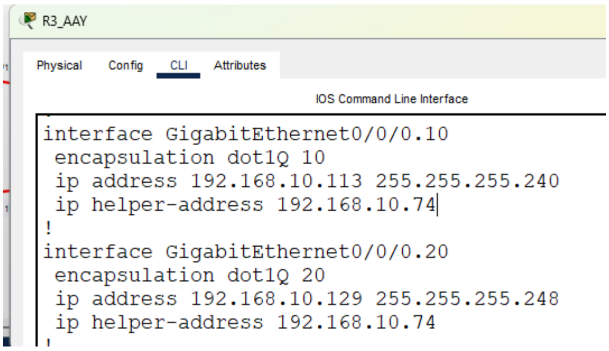


Figure 4: ROAS Topology showing Router R3_AAY connected to Switch S2_AAY with VLANs 10 and 20

The topology shows:

- **VLAN 10 (Technical Support):** Yellow section with network 192.168.10.112/28
- **VLAN 20 (HR):** Green section with network 192.168.10.128/29
- **Switch S2_AAY:** Connects both VLANs through trunk link to router
- **Router R3_AAY:** Performs Inter-VLAN routing using sub-interfaces

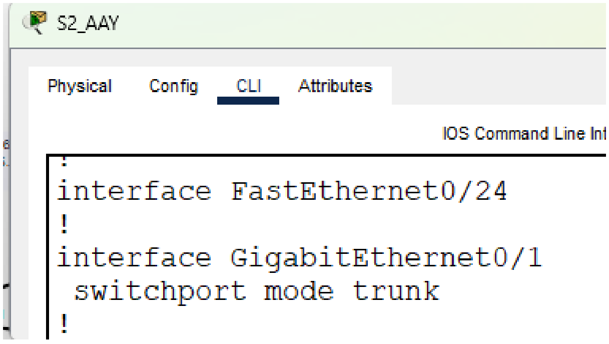
4.3.2 Router Configuration Verification



```
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.113 255.255.255.240
 ip helper-address 192.168.10.74
!
interface GigabitEthernet0/0/0.20
 encapsulation dot1Q 20
 ip address 192.168.10.129 255.255.255.248
 ip helper-address 192.168.10.74
```

Figure 5: Router R3_AAY Sub-Interface Configuration for VLANs 10 and 20

4.3.3 Trunk Port Verification



```
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
 switchport mode trunk
!
```

Figure 6: Trunk Port Configuration on GigabitEthernet0/1

5 DHCP Server

5.1 Overview

Dynamic Host Configuration Protocol (DHCP) is used to automatically assign IP addresses and network configuration to devices on the network. Instead of manually configuring each device, DHCP provides IP addresses, subnet masks, default gateways, and DNS servers dynamically.

Benefits of using DHCP in our network:

- Automatic IP address assignment reduces configuration errors
- Centralized management of IP addresses
- Efficient use of IP address space
- Easy to add new devices to the network

We implemented a standalone DHCP server to provide IP configuration to all departments. Five DHCP pools were created to cover all networks except the IT department and Internet gateway, which use static IP addresses.

Note: Due to Packet Tracer limitations, the DHCP server can only handle 5 pools maximum. When adding a sixth pool, it removes the first pool, so IT department devices are configured with static IPs.

5.2 Configuration

5.2.1 DHCP Server Pool Configuration

The DHCP server is configured with five pools, one for each department network:

Pool Name	Network	Default Gateway	DNS Server	Max Users
SD_Agile_P5	192.168.10.0/26	192.168.10.1	8.8.8.8	60
AC_P4	192.168.10.96/28	192.168.10.97	8.8.8.8	12
MR_P3	192.168.10.80/28	192.168.10.81	8.8.8.8	12
HR_P2	192.168.10.128/29	192.168.10.129	8.8.8.8	5
TS_P1	192.168.10.112/28	192.168.10.113	8.8.8.8	12

Table 6: DHCP Pool Configuration

Pool Assignments:

- **SD_Agile_P5:** Software Development department (60 devices)
- **AC_P4:** Accounting department (12 devices)
- **MR_P3:** Marketing department (12 devices)
- **HR_P2:** Human Resources department (5 devices)
- **TS_P1:** Technical Support department (12 devices)

5.2.2 IP Helper-Address Configuration

For routers not directly connected to the DHCP server, we configured the `ip helper-address` command on the sub-interfaces. This command forwards DHCP broadcast requests from clients to the DHCP server, allowing devices on different VLANs to receive IP configurations.

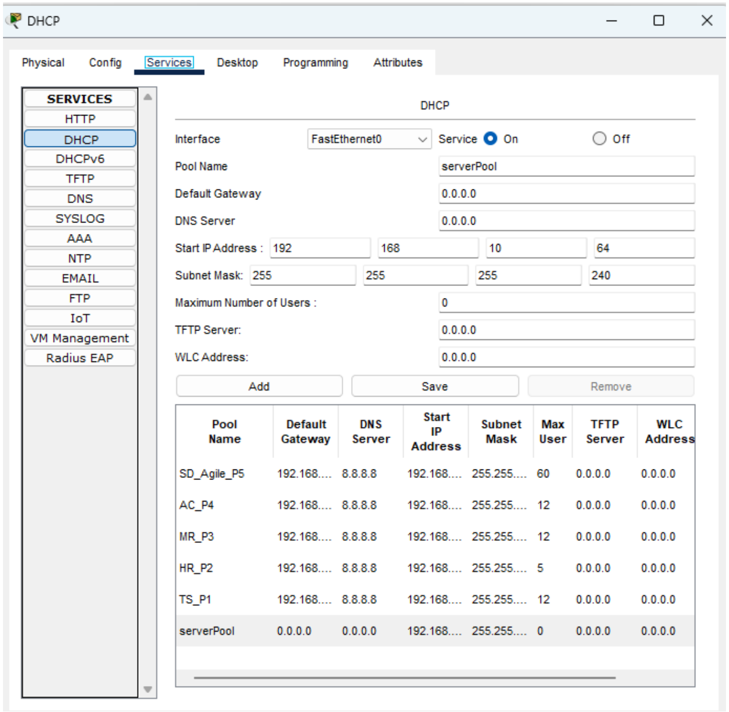
Example Configuration:

Listing 6: IP Helper-Address Configuration on Router

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.192
Router(config-if)# ip helper-address 192.168.10.74
Router(config-if)# exit
```

5.3 Verification

5.3.1 DHCP Pool Status



DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address : 192 168 10 64

Subnet Mask: 255 255 255 240

Maximum Number of Users : 0

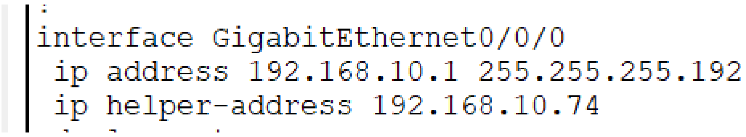
TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
SD_Agile_P5	192.168....	8.8.8.8	192.168....	255.255....	60	0.0.0.0	0.0.0.0
AC_P4	192.168....	8.8.8.8	192.168....	255.255....	12	0.0.0.0	0.0.0.0
MR_P3	192.168....	8.8.8.8	192.168....	255.255....	12	0.0.0.0	0.0.0.0
HR_P2	192.168....	8.8.8.8	192.168....	255.255....	5	0.0.0.0	0.0.0.0
TS_P1	192.168....	8.8.8.8	192.168....	255.255....	12	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168....	255.255....	0	0.0.0.0	0.0.0.0

Figure 7: DHCP Server Configuration showing all five pools

5.3.2 IP Helper-Address Verification

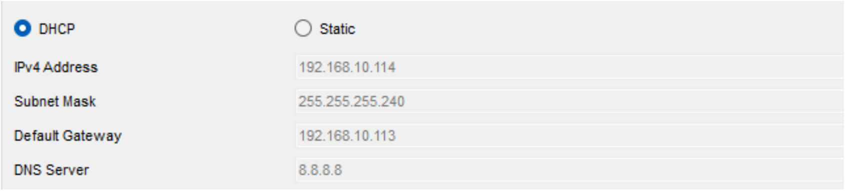


```
interface GigabitEthernet0/0/0
 ip address 192.168.10.1 255.255.255.192
 ip helper-address 192.168.10.74
```

Figure 8: IP Helper-Address Configuration on Router Interface

The `ip helper-address 192.168.10.74` command is configured on each router interface connected to client VLANs. This ensures that DHCP requests are forwarded to the DHCP server at 192.168.10.74, even when the server is on a different subnet.

5.3.3 Client IP Assignment Verification



● DHCP ○ Static

IPv4 Address	192.168.10.114
Subnet Mask	255.255.255.240
Default Gateway	192.168.10.113
DNS Server	8.8.8.8

Figure 9: Verification of DHCP Operation showing successful IP address assignment to the client

6 EtherChannel

6.1 Overview

EtherChannel is a link aggregation technology that combines multiple physical Ethernet links into a single logical link. This provides increased bandwidth and redundancy between network devices.

In our software development company, the Agile methodology requires high-speed data transfer between developers, testers, and Scrum Masters. Team members need to share large files, access version control systems, and collaborate on projects simultaneously. To meet these requirements, we implemented EtherChannel technology between the switches connecting these teams.

EtherChannel Protocols:

There are two main protocols for configuring EtherChannel:

- **PAgP (Port Aggregation Protocol):** Cisco proprietary protocol that negotiates EtherChannel formation between Cisco devices
- **LACP (Link Aggregation Control Protocol):** IEEE 802.3ad standard protocol that works with multi-vendor devices

In our network, we use **LACP** because it is an open standard.

Benefits of EtherChannel in our network:

- **Increased Bandwidth:** Multiple physical links combine to provide higher throughput
- **Redundancy:** If one link fails, traffic continues on remaining links
- **Load Balancing:** Traffic is distributed across all available links
- **Fast Convergence:** Link failures are detected quickly without waiting for STP
- **Efficient Resource Use:** All links are active simultaneously (no blocked ports)

6.2 Configuration

We configured EtherChannel using **Link Aggregation Control Protocol (LACP)**, which is an IEEE standard protocol (802.3ad) for negotiating link aggregation. LACP provides automatic configuration and better interoperability compared to Cisco's proprietary PAgP protocol.

6.2.1 EtherChannel Topology

The EtherChannel configuration connects three switches in the Software Development department:

- **S3_AAY (Scrum Masters):** 3 devices - LACP Active mode
- **S4_AAY (Developers):** 25 devices - LACP Passive mode
- **S5_AAY (Testers):** 12 devices - LACP Passive mode

LACP Mode Explanation:

- **Active Mode (S3_AAY):** Actively sends LACP packets to initiate negotiation
- **Passive Mode (S4_AAY & S5_AAY):** Waits for LACP packets before responding

This configuration ensures that the Scrum Masters' switch (Active) initiates the EtherChannel formation with both the Developers' and Testers' switches (Passive).

6.2.2 Switch S3_AAY Configuration (Active - Scrum Masters)

Listing 7: EtherChannel Configuration on S3_AAY (Active Mode)

```
S3_AAY(config)# interface range FastEthernet0/4, FastEthernet0/6
S3_AAY(config-if-range)# channel-group 1 mode active
S3_AAY(config-if-range)# exit

S3_AAY(config)# interface range FastEthernet0/2, FastEthernet0/5
S3_AAY(config-if-range)# channel-group 2 mode active
S3_AAY(config-if-range)# exit

S3_AAY(config)# interface Port-channel 1
S3_AAY(config-if)# switchport mode trunk
S3_AAY(config-if)# exit

S3_AAY(config)# interface Port-channel 2
S3_AAY(config-if)# switchport mode trunk
S3_AAY(config-if)# exit
```

6.2.3 Switch S4_AAY Configuration (Passive - Developers)

Listing 8: EtherChannel Configuration on S4_AAY (Passive Mode)

```
S4_AAY(config)# interface range FastEthernet0/1, FastEthernet0/4
S4_AAY(config-if-range)# channel-group 1 mode passive
S4_AAY(config-if-range)# exit

S4_AAY(config)# interface Port-channel 1
S4_AAY(config-if)# switchport mode trunk
S4_AAY(config-if)# exit
```

6.2.4 Switch S5_AAY Configuration (Passive - Testers)

Listing 9: EtherChannel Configuration on S5_AAY (Passive Mode)

```
S5_AAY(config)# interface range FastEthernet0/1, FastEthernet0/4
S5_AAY(config-if-range)# channel-group 2 mode passive
S5_AAY(config-if-range)# exit

S5_AAY(config)# interface Port-channel 2
S5_AAY(config-if)# switchport mode trunk
S5_AAY(config-if)# exit
```

Configuration Explanation:

- **channel-group 1/2:** Creates logical Port-channel interface
- **mode active:** Switch actively initiates LACP negotiation
- **mode passive:** Switch waits for LACP packets
- **switchport mode trunk:** Allows multiple VLANs across the EtherChannel

6.3 Verification

6.3.1 EtherChannel Topology Verification

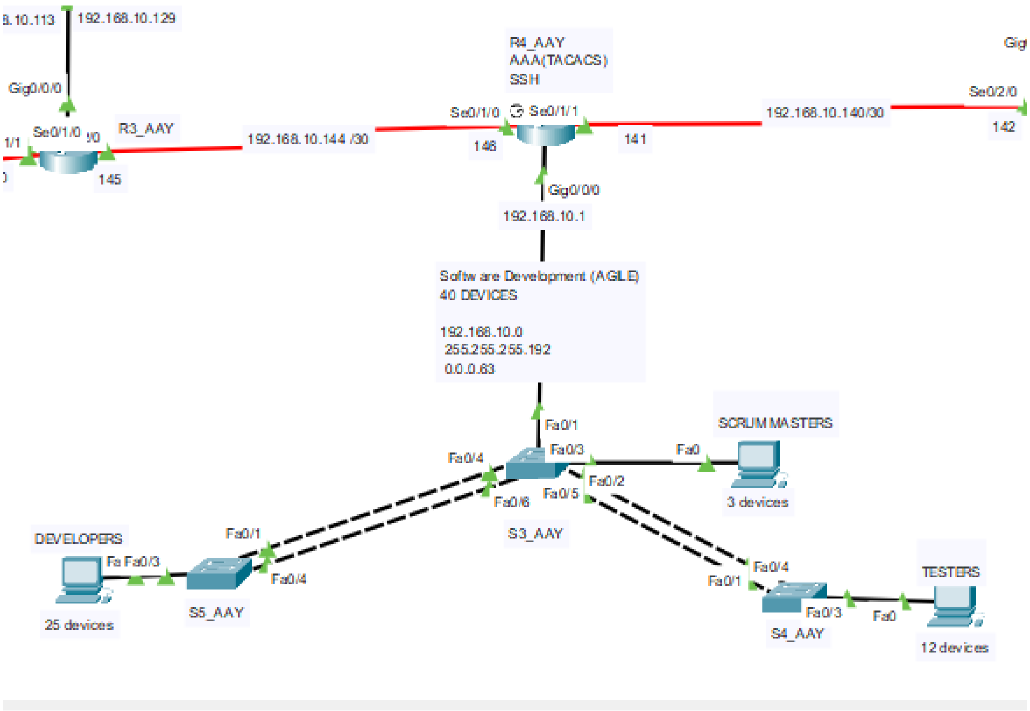
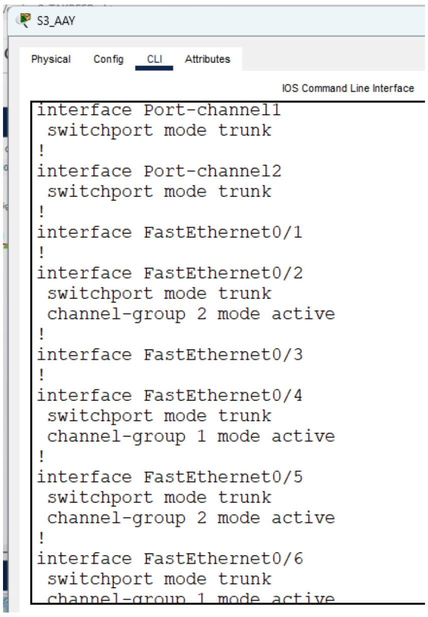


Figure 10: EtherChannel Links showing redundant connections between S3_AAY, S4_AAY, and S5_AAY

6.3.2 EtherChannel Configuration Verification



```
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/3
!
interface FastEthernet0/4
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/5
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/6
 switchport mode trunk
 channel-group 1 mode active
```

Figure 11: EtherChannel Configuration - Developers (25 devices), Scrum Masters (3 devices), and Testers (12 devices)

7 OSPF Routing

7.1 Overview

Open Shortest Path First (OSPF) is a dynamic interior gateway routing protocol that uses link-state technology to calculate the best path through a network. OSPF is classified as an Interior Gateway Protocol (IGP), designed for use within a single autonomous system.

Why OSPF is used in our network:

- **Fast Convergence:** Quickly adapts to network topology changes
- **Scalability:** Supports large and complex networks efficiently
- **Loop-Free Routing:** Uses Dijkstra's algorithm to calculate loop-free paths
- **Efficient Bandwidth Use:** Sends updates only when topology changes occur
- **Support for VLSM:** Works with Variable Length Subnet Masking and CIDR
- **Industry Standard:** Open standard protocol (not vendor-specific)

We implemented **OSPFv2** with a single-area design using **Area 0 (Backbone Area)** for all networks. This simplifies configuration and management while providing efficient routing across all departments and connections.

7.2 Configuration

7.2.1 OSPF Configuration on Router R3_AAY

The OSPF configuration includes all networks directly connected to the router. Each network is advertised in Area 0 to ensure all routers can communicate and share routing information.

Listing 10: OSPF Configuration on Router R3_AAY

```
R3_AAY(config)# router ospf 1
R3_AAY(config-router)# network 192.168.10.128 0.0.0.7 area 0
R3_AAY(config-router)# network 192.168.10.112 0.0.0.15 area 0
R3_AAY(config-router)# network 192.168.10.144 0.0.0.3 area 0
R3_AAY(config-router)# network 192.168.10.152 0.0.0.3 area 0
R3_AAY(config-router)# network 192.168.10.148 0.0.0.3 area 0
R3_AAY(config-router)# exit
```

Configuration Explanation:

- **router ospf 1:** Enables OSPF routing process with process ID 1
- **network [address] [wildcard-mask] area 0:** Advertises networks in OSPF Area 0
  - 192.168.10.128/29 - HR department VLAN 20
  - 192.168.10.112/28 - Technical Support department VLAN 10
  - 192.168.10.144/30 - Point-to-point router link
  - 192.168.10.152/30 - Point-to-point router link
  - 192.168.10.148/30 - Point-to-point router link

7.2.2 OSPF Configuration Process

The same OSPF configuration process is applied to all routers (R1_AAY through R6_AAY):

1. Enable OSPF with a process ID (typically 1)
2. Configure network statements for all directly connected networks
3. Use wildcard masks to specify the network range
4. Assign all networks to Area 0 for single-area OSPF design

7.3 Verification

7.3.1 OSPF Topology Verification

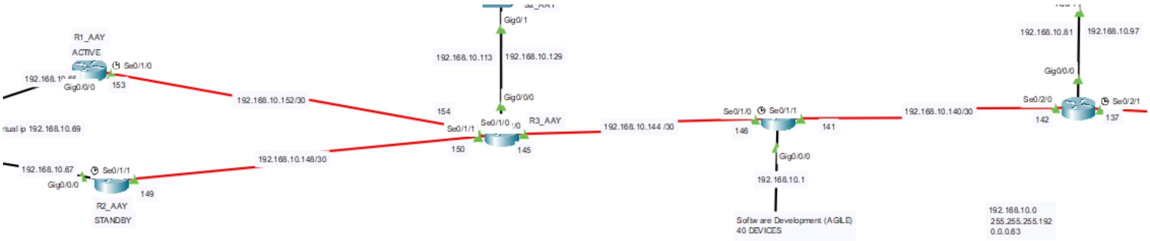
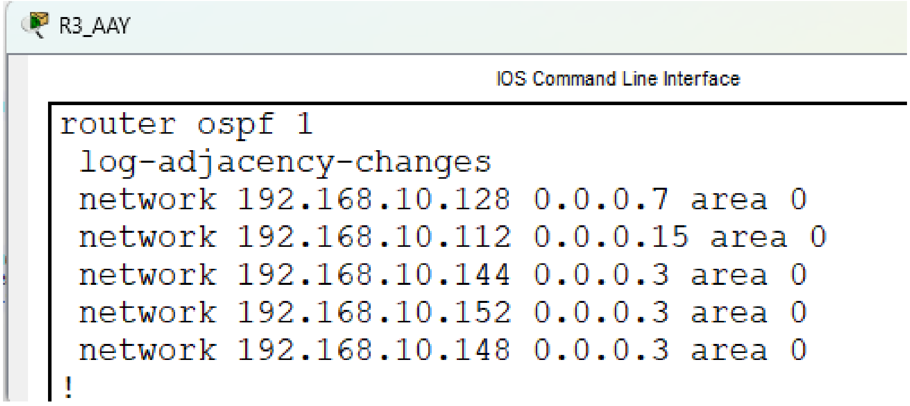


Figure 12: OSPF Network Topology showing router connections and OSPF Area 0

7.3.2 OSPF Configuration Verification

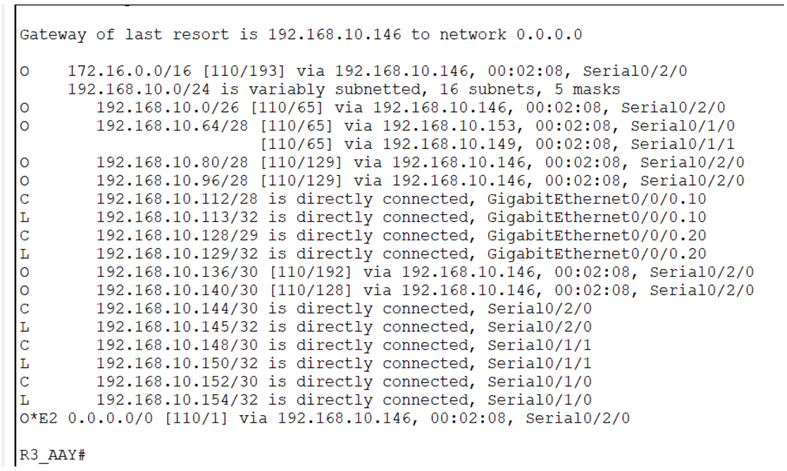


```
router ospf 1
 log-adjacency-changes
 network 192.168.10.128 0.0.0.7 area 0
 network 192.168.10.112 0.0.0.15 area 0
 network 192.168.10.144 0.0.0.3 area 0
 network 192.168.10.152 0.0.0.3 area 0
 network 192.168.10.148 0.0.0.3 area 0
!
```

Figure 13: OSPF Configuration on Router R3_AAY showing network statements and Area 0 assignment

The configuration shows that Router R3_AAY advertises five networks in OSPF Area 0, including both VLAN subnets and point-to-point router links.

7.3.3 OSPF Routing Verification



```
Gateway of last resort is 192.168.10.146 to network 0.0.0.0

O    172.16.0.0/16 [110/193] via 192.168.10.146, 00:02:08, Serial0/2/0
     192.168.10.0/24 is variably subnetted, 16 subnets, 5 masks
O       192.168.10.0/26 [110/65] via 192.168.10.146, 00:02:08, Serial0/2/0
O       192.168.10.64/28 [110/65] via 192.168.10.153, 00:02:08, Serial0/1/0
                         [110/65] via 192.168.10.149, 00:02:08, Serial0/1/1
O       192.168.10.80/28 [110/129] via 192.168.10.146, 00:02:08, Serial0/2/0
O       192.168.10.96/28 [110/129] via 192.168.10.146, 00:02:08, Serial0/2/0
C       192.168.10.112/28 is directly connected, GigabitEthernet0/0/0.10
L       192.168.10.113/32 is directly connected, GigabitEthernet0/0/0.10
C       192.168.10.128/29 is directly connected, GigabitEthernet0/0/0.20
L       192.168.10.129/32 is directly connected, GigabitEthernet0/0/0.20
O       192.168.10.136/30 [110/192] via 192.168.10.146, 00:02:08, Serial0/2/0
O       192.168.10.140/30 [110/128] via 192.168.10.146, 00:02:08, Serial0/2/0
C       192.168.10.144/30 is directly connected, Serial0/2/0
L       192.168.10.145/32 is directly connected, Serial0/2/0
C       192.168.10.148/30 is directly connected, Serial0/1/1
L       192.168.10.150/32 is directly connected, Serial0/1/1
C       192.168.10.152/30 is directly connected, Serial0/1/0
L       192.168.10.154/32 is directly connected, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 192.168.10.146, 00:02:08, Serial0/2/0

R3_AAY#
```

Figure 14: Routing Table Verification using `show ip route` confirming correct network learning and route installation

8 HSRP

8.1 Overview

Hot Standby Router Protocol (HSRP) is a Cisco redundancy protocol that provides backup routing and automatic failover. HSRP allows two routers to work together as a single virtual router for network devices.

We implemented HSRP to provide backup between the IT department and the rest of the network. If the active router fails, the standby router automatically takes over, ensuring the network continues to operate without interruption.

Benefits of HSRP:

- Automatic failover if active router fails
- No device reconfiguration needed during failover
- Eliminates single point of failure
- Minimizes network downtime

HSRP Configuration in Our Network:

- **Virtual IP Address:** 192.168.10.69
- **Active Router:** R1_AAY (Priority 110)
- **Standby Router:** R2_AAY (Priority 100 - default)
- **HSRP Group:** 1

8.2 Configuration

8.2.1 Active Router Configuration (R1_AAY)

Router R1_AAY is configured as the active router with a higher priority (110) to ensure it becomes the active gateway under normal conditions.

Listing 11: HSRP Configuration on R1_AAY (Active Router)

```
R1_AAY(config)# interface GigabitEthernet0/0/0
R1_AAY(config-if)# ip address 192.168.10.65 255.255.255.240
R1_AAY(config-if)# standby 1 ip 192.168.10.69
R1_AAY(config-if)# standby 1 priority 110
R1_AAY(config-if)# standby 1 preempt
R1_AAY(config-if)# exit
```

R1_AAY Configuration Explanation:

- **ip address 192.168.10.65:** Physical IP address of R1_AAY
- **standby 1 ip 192.168.10.69:** Virtual IP address shared between routers
- **standby 1 priority 110:** Higher priority makes this router active (default is 100)
- **standby 1 preempt:** Allows this router to reclaim active role if it recovers from failure

8.2.2 Standby Router Configuration (R2_AAY)

Router R2_AAY is configured as the standby router with default priority (100), making it the backup router.

Listing 12: HSRP Configuration on R2_AAY (Standby Router)

```
R2_AAY(config)# interface GigabitEthernet0/0/0
R2_AAY(config-if)# ip address 192.168.10.67 255.255.255.240
R2_AAY(config-if)# standby 1 ip 192.168.10.69
R2_AAY(config-if)# standby 1 preempt
R2_AAY(config-if)# exit
```

8.3 Verification

8.3.1 HSRP Topology Verification

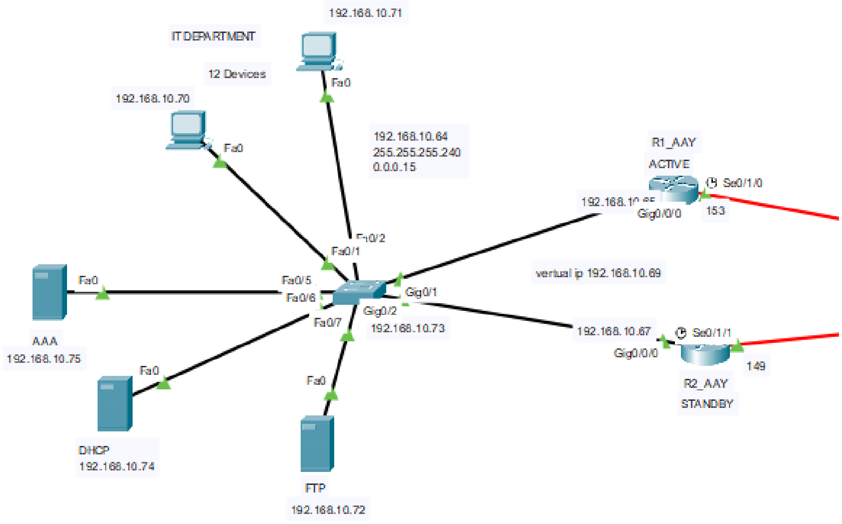
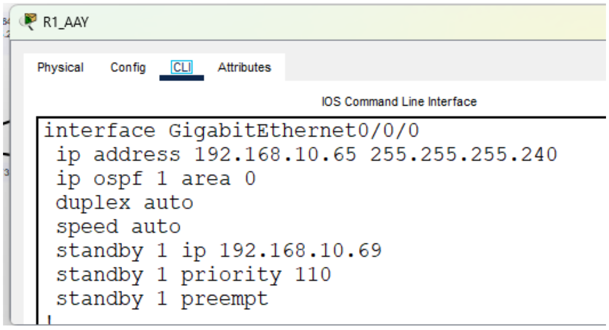


Figure 15: HSRP Configuration between R1_AAY (Active) and R2_AAY (Standby)

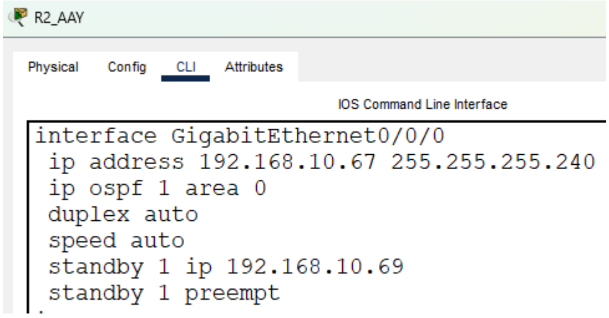
8.3.2 Active Router Configuration Verification



```
interface GigabitEthernet0/0/0
 ip address 192.168.10.65 255.255.255.240
 ip ospf 1 area 0
 duplex auto
 speed auto
 standby 1 ip 192.168.10.69
 standby 1 priority 110
 standby 1 preempt
```

Figure 16: HSRP Configuration on R1_AAY (Active) with priority 110

8.3.3 Standby Router Configuration Verification



```
interface GigabitEthernet0/0/0
 ip address 192.168.10.67 255.255.255.240
 ip ospf 1 area 0
 duplex auto
 speed auto
 standby 1 ip 192.168.10.69
 standby 1 preempt
```

Figure 17: HSRP Configuration on R2_AAY (Standby) with default priority 100

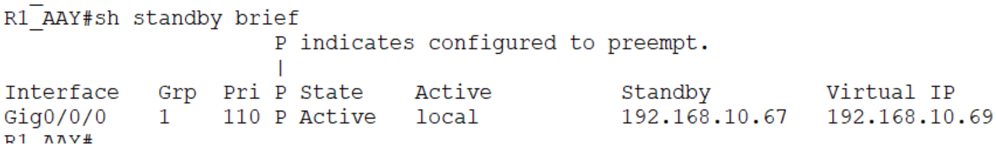
8.3.4 HSRP Status Verification

Use the following command to verify HSRP operation:

Listing 13: HSRP Verification Command

```
R1_AAY# show standby brief
R2_AAY# show standby brief
```

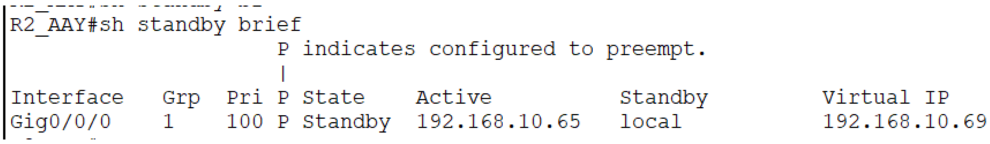
Active Router (R1_AAY) Status:



```
R1_AAY#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0/0    1    110 P Active   local           192.168.10.67   192.168.10.69
R1_AAY#
```

Figure 18: show standby brief output on R1_AAY showing Active state with priority 110

Standby Router (R2_AAY) Status:



```
R2_AAY#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0/0    1    100 P Standby  192.168.10.65   local           192.168.10.69
```

Figure 19: show standby brief output on R2_AAY showing Standby state with priority 100

9 FTP Server

9.1 Overview

File Transfer Protocol (FTP) is a standard network protocol used to transfer files between a client and server over a TCP/IP network. FTP provides a reliable method for uploading, downloading, and managing files on a remote server.

Purpose of FTP Server in our network:

We implemented an FTP server to store and manage network device configurations as backup files. This allows network administrators to:

- Save router and switch configurations centrally
- Restore configurations quickly in case of device failure
- Maintain version history of configuration changes
- Share configuration files between network devices
- Provide secure access to network documentation

The FTP server stores configuration backups from all routers (R1_AAY through R6_AAY) and switches (S1_AAY through S7_AAY), ensuring that network configurations are preserved and can be restored when needed.

9.2 Configuration

9.2.1 FTP Server Setup

The FTP server is configured with the following parameters:

- **Server IP Address:** 192.168.10.72
- **Location:** IT Department network (192.168.10.64/28)
- **Service Status:** Enabled (On)

9.2.2 User Account Configuration

Two user accounts are created on the FTP server with full access permissions:

Username	Password	Permissions
admin	123	RWDNL (Read, Write, Delete, Rename, List)
cisco	123	RWDNL (Read, Write, Delete, Rename, List)

Table 7: FTP Server User Accounts

9.2.3 Backing Up Device Configuration to FTP

Example: Backing up Switch S2_AAY Configuration

Listing 14: FTP Configuration and Backup on Switch S2_AAY

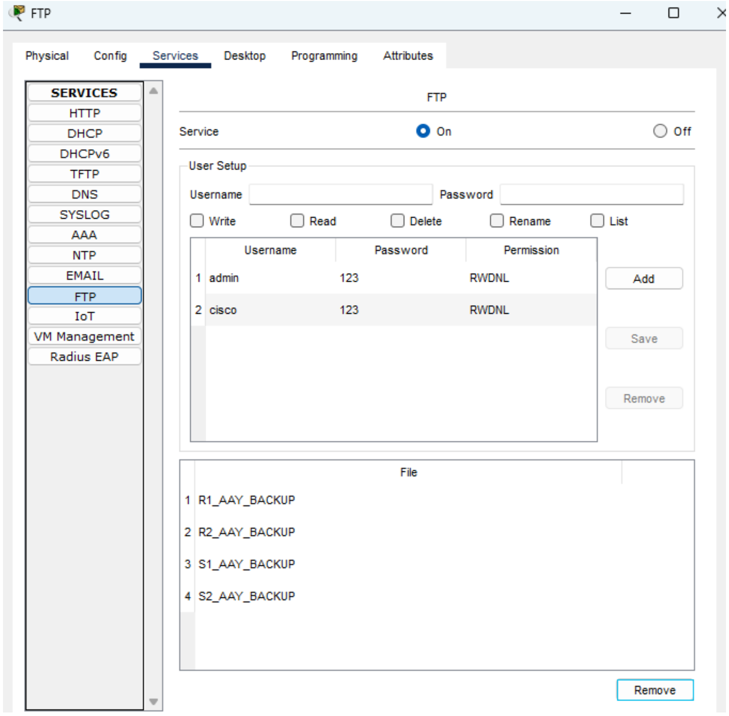
```
! Configure FTP credentials on the device
S2_AAY(config)# ip ftp username cisco
S2_AAY(config)# ip ftp password 123
S2_AAY# copy running-config ftp:
Address or name of remote host []? 192.168.10.72
Destination filename [S2_AAY-config]? S2_AAY_BACKUP
```

Command Explanation:

- **ip ftp username cisco:** Sets FTP username for authentication
- **ip ftp password 123:** Sets FTP password
- **copy running-config ftp:** Initiates FTP transfer from running configuration
- **192.168.10.72:** FTP server IP address
- **S2_AAY_BACKUP:** Filename for the backup file on FTP server

9.3 Verification

9.3.1 FTP Server Configuration Verification



FTP

Service ● On ○ Off

Username Password

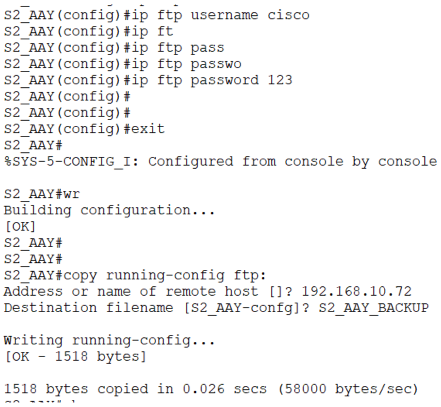
□ Write □ Read □ Delete □ Rename □ List

	Username	Password	Permission
1	admin	123	RWDNL
2	cisco	123	RWDNL

	File
1	R1_AAY_BACKUP
2	R2_AAY_BACKUP
3	S1_AAY_BACKUP
4	S2_AAY_BACKUP

Figure 20: FTP Server Configuration showing user accounts and stored backup files

9.3.2 FTP Backup Process Verification



```
S2_AAY(config)#ip ftp username cisco
S2_AAY(config)#ip ft
S2_AAY(config)#ip ftp pass
S2_AAY(config)#ip ftp passwo
S2_AAY(config)#ip ftp password 123
S2_AAY(config)#
S2_AAY(config)#
S2_AAY(config)#exit
S2_AAY#
%SYS-5-CONFIG_I: Configured from console by console

S2_AAY#wr
Building configuration...
[OK]
S2_AAY#
S2_AAY#
S2_AAY#copy running-config ftp:
Address or name of remote host []? 192.168.10.72
Destination filename [S2_AAY-confg]? S2_AAY_BACKUP

Writing running-config...
[OK - 1518 bytes]

1518 bytes copied in 0.026 secs (58000 bytes/sec)
```

Figure 21: FTP backup process on Switch S2_AAY showing successful configuration upload

10 AAA and SSH Authentication

10.1 Overview

Authentication, Authorization, and Accounting (AAA) is a security framework that controls access to network devices. AAA provides centralized user authentication, ensuring that only authorized personnel can access and manage network infrastructure.

Secure Shell (SSH) is a secure protocol for remote access to network devices. Unlike Telnet, which sends data in plaintext, SSH encrypts all communication to protect passwords and commands.

AAA Protocols:

There are two main protocols for AAA:

- **TACACS+:** Cisco protocol that separates authentication, authorization, and accounting. Uses TCP port 49
- **RADIUS:** Standard protocol that combines authentication and authorization. Uses UDP ports 1812/1813

In our network, we use **TACACS+** protocol for device authentication. We implemented an AAA server for authentication when using remote login on routers and switches. Some devices are configured with **SSH** for secure encrypted access, while others use **Telnet** for testing purposes.

Remote Access Methods:

- **AAA-SSH (Secure):** Used on some routers and switches (e.g., R4_AAY) - Encrypted
- **AAA-Telnet:** Used on some routers (e.g., R1_AAY) with AAA authentication - Not encrypted
- **SSH** Some Devices use SSH with local local only (e.g., R6_AAY)

10.2 Configuration

10.2.1 AAA Server Configuration

The AAA server is configured with the following parameters:

- **Server IP Address:** 192.168.10.75
- **Location:** IT Department network (192.168.10.64/28)
- **Radius Port:** 1645

10.2.2 AAA Server Setup

The AAA server is configured with TACACS+ protocol for device authentication. Three network devices are registered as clients:

Client Name	Client IP	Server Type	Key
R4_AAY	192.168.10.146	Tacacs	123
R1_AAY	192.168.10.65	Tacacs	123
R2_AAY	192.168.10.67	Tacacs	123

Table 8: AAA Server Client Configuration

User Account:

- **Username:** admin
- **Password:** 123

10.2.3 SSH Configuration on Network Devices

SSH must be configured on each network device to provide secure remote access. The configuration includes domain name, RSA key generation, and AAA authentication.

Example: SSH Configuration on Switch S2_AAY

Listing 15: SSH Configuration on Switch S2_AAY

```
S2_AAY(config)# line vty 0 4
S2_AAY(config-line)# login local
S2_AAY(config-line)# transport input ssh
S2_AAY(config-line)# exit

S2_AAY(config)# enable secret 123
S2_AAY(config)# username admin secret 123

S2_AAY(config)# ip domain-name it1
S2_AAY(config)# crypto key generate rsa
The name for the keys will be: S2_AAY.it1
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S2_AAY(config)#
```

10.2.4 AAA Authentication Configuration on Router

For devices using AAA server authentication, the following configuration is applied:

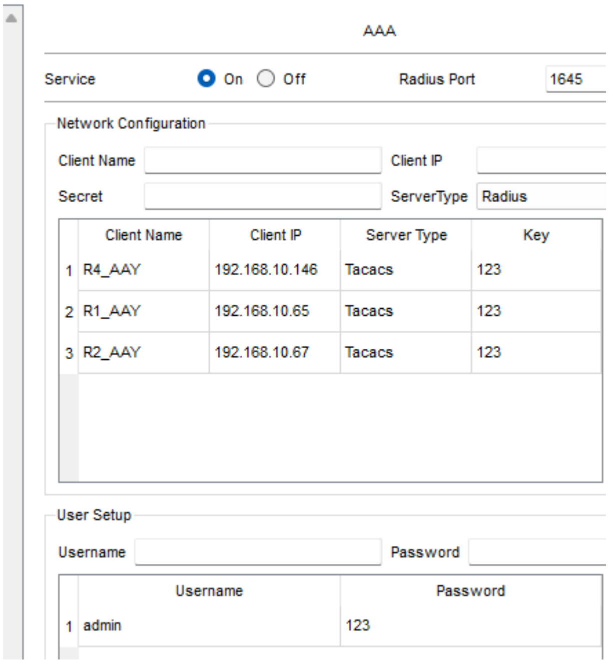
Example: AAA Configuration on Router R1_AAY

Listing 16: AAA Configuration on Router R1_AAY

```
R1_AAY(config)# aaa new-model
R1_AAY(config)# aaa authentication login jimmy group tacacs+ local

R1_AAY(config)# tacacs-server host 192.168.10.75 key 123

R1_AAY(config)# line vty 0 4
R1_AAY(config-line)# login authentication jimmy
R1_AAY(config-line)# transport input telnet
R1_AAY(config-line)# exit
```

10.3 Verification

10.3.1 AAA Server Configuration Verification



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	R4_AAY	192.168.10.146	Tacacs	123
2	R1_AAY	192.168.10.65	Tacacs	123
3	R2_AAY	192.168.10.67	Tacacs	123

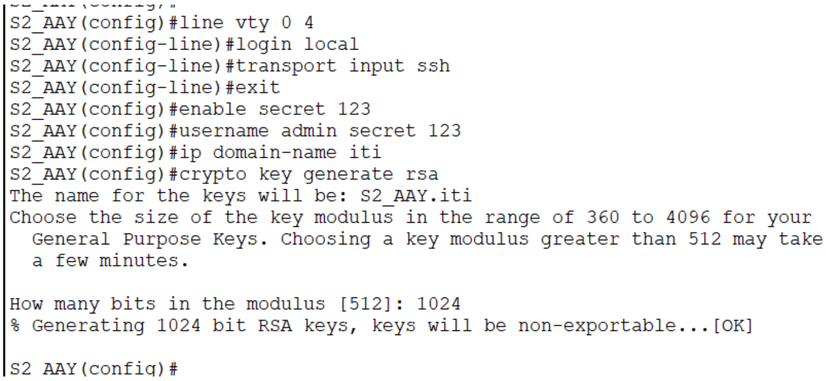
User Setup

Username Password

	Username	Password
1	admin	123

Figure 22: AAA Server Configuration showing client devices and user accounts

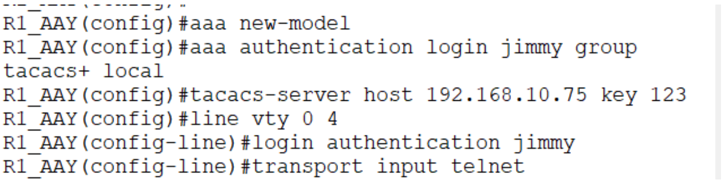
10.3.2 SSH Configuration Verification



```
S2_AAY(config)#line vty 0 4
S2_AAY(config-line)#login local
S2_AAY(config-line)#transport input ssh
S2_AAY(config-line)#exit
S2_AAY(config)#enable secret 123
S2_AAY(config)#username admin secret 123
S2_AAY(config)#ip domain-name iti
S2_AAY(config)#crypto key generate rsa
The name for the keys will be: S2_AAY.iti
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S2_AAY(config)#
```

Figure 23: SSH Configuration on Switch S2_AAY with RSA key generation

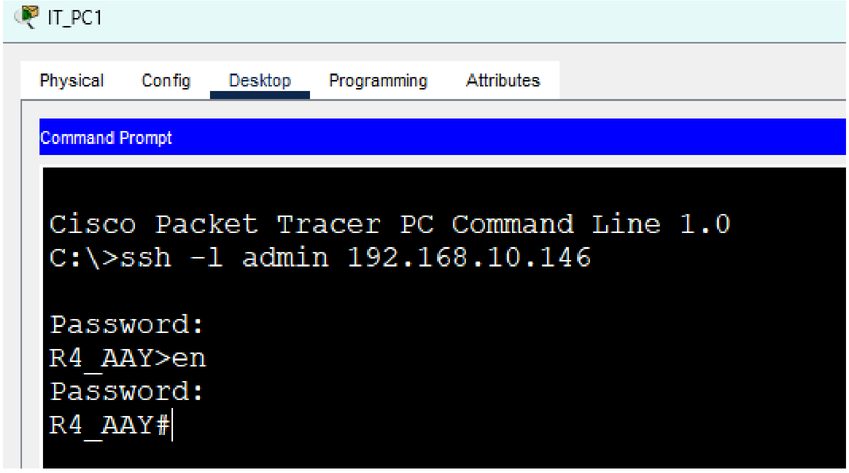
10.3.3 AAA Authentication Configuration Verification



```
R1_AAY(config)#aaa new-model
R1_AAY(config)#aaa authentication login jimmy group
tacacs+ local
R1_AAY(config)#tacacs-server host 192.168.10.75 key 123
R1_AAY(config)#line vty 0 4
R1_AAY(config-line)#login authentication jimmy
R1_AAY(config-line)#transport input telnet
```

Figure 24: AAA Configuration on Router R1_AAY with TACACS+ server settings

10.3.4 AAA Authentication via SSH Verification



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.10.146

Password:
R4_AAY>en
Password:
R4_AAY#
```

Figure 25: AAA Authentication test using SSH from PC - successful login

11 NAT

11.1 Overview

Network Address Translation (NAT) is a method of mapping private IP addresses to public IP addresses, enabling internal network devices to communicate with external networks like the Internet. NAT provides security by hiding internal network structure and conserves public IP addresses.

Types of NAT:

- **Static NAT:** One-to-one mapping between a private IP address and a public IP address. Used for servers that need to be accessible from the Internet (e.g., FTP server)
- **Dynamic NAT:** Maps private IP addresses to a pool of public IP addresses on a first-come, first-served basis
- **PAT (Port Address Translation):** Also called NAT Overload, maps multiple private IP addresses to a single public IP address using different port numbers. Most commonly used for Internet access

We implemented a simple Internet connection to test connectivity between internal and external networks. The configuration includes both Static NAT and PAT:

- **Static NAT:** For the static server (172.16.1.10 mapped to 31.0.0.2) to allow external access
- **PAT:** For all internal network devices (192.168.10.0/24) to access the Internet using a single public IP

11.2 NAT Configuration

11.2.1 Static NAT Configuration

Static NAT is configured to map the static server's private IP address to a public IP address, allowing it to be accessible from the Internet.

Static NAT Mapping:

- **Inside Local:** 172.16.1.10 (Private IP of static server)
- **Inside Global:** 31.0.0.2 (Public IP for static server)

Configuration on Router R6_AAY:

Listing 17: Static NAT Configuration

```
R6_AAY(config)# ip nat inside source static 172.16.1.10 31.0.0.2
```

Interface Configuration:

Listing 18: NAT Inside and Outside Interface Configuration

```
R6_AAY(config)# interface GigabitEthernet0/0/0
R6_AAY(config-if)# ip nat inside
R6_AAY(config-if)# exit
R6_AAY(config)# interface Serial0/2/1
R6_AAY(config-if)# ip nat outside
R6_AAY(config-if)# exit
```

11.2.2 PAT Configuration

PAT Configuration on Router R6_AAY:

Listing 19: PAT (NAT Overload) Configuration

```
R6_AAY(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R6_AAY(config)# ip nat inside source list 1 interface Serial0/2/1 overload
R6_AAY(config)# interface GigabitEthernet0/0/0
R6_AAY(config-if)# ip nat inside
R6_AAY(config-if)# exit
R6_AAY(config)# interface Serial0/2/1
R6_AAY(config-if)# ip nat outside
R6_AAY(config-if)# exit
```

PAT Configuration Explanation:

- **access-list 1 permit 192.168.10.0 0.0.0.255:** Defines which internal addresses can be translated (entire 192.168.10.0/24 network)
- **ip nat inside source list 1:** Uses access list 1 to identify internal addresses
- **interface Serial0/2/1:** Specifies the outside interface whose IP will be used for translation
- **overload:** Enables PAT, allowing multiple internal devices to share one public IP using different port numbers

11.3 Verification

11.3.1 Simple ISP Topology

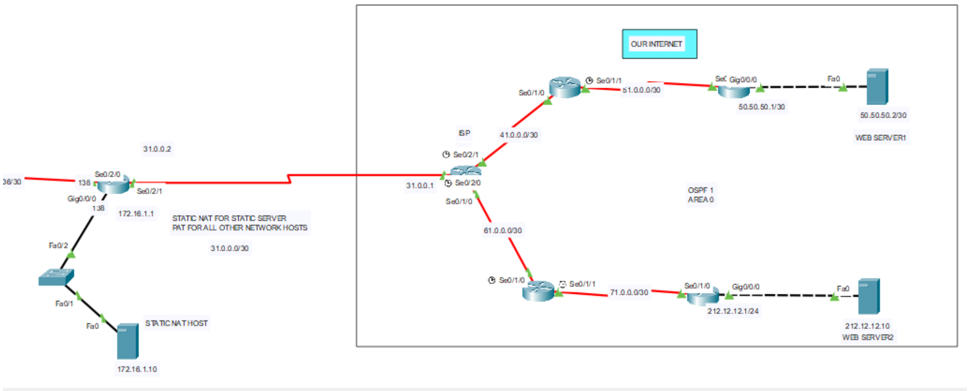
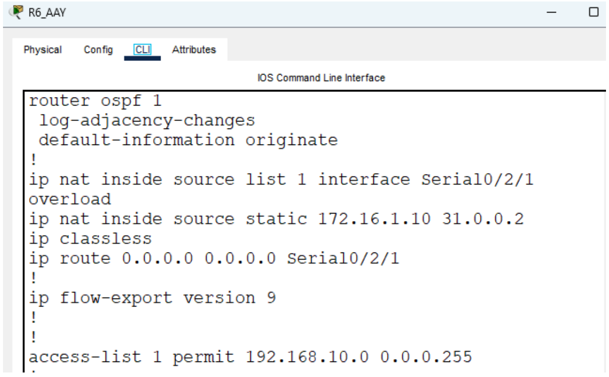


Figure 26: Simple Internet Circuit for testing NAT

The topology shows:

- **Static NAT Host:** 172.16.1.10 mapped to public IP 31.0.0.2
- **Internal Network:** 192.168.10.0/24 using PAT
- **ISP Connection:** Simple ISP circuit routed using OSPFv2.
- **Internet Connectivity:** Access to web servers (50.50.50.2/30 and 212.12.121.0)

11.3.2 NAT Configuration Verification



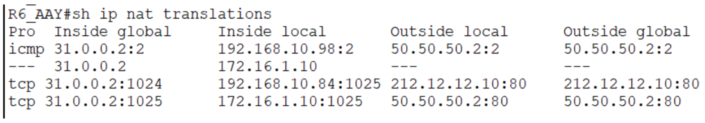
```
router ospf 1
 log-adjacency-changes
 default-information originate
!
ip nat inside source list 1 interface Serial0/2/1
overload
ip nat inside source static 172.16.1.10 31.0.0.2
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/2/1
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.10.0 0.0.0.255
```

Figure 27: NAT Configuration on Router R6_AAY

The configuration shows:

- OSPF routing enabled
- Static NAT , PAT with its access list configuration.
- Default route pointing to ISP (0.0.0.0/0 via Serial0/2/1)

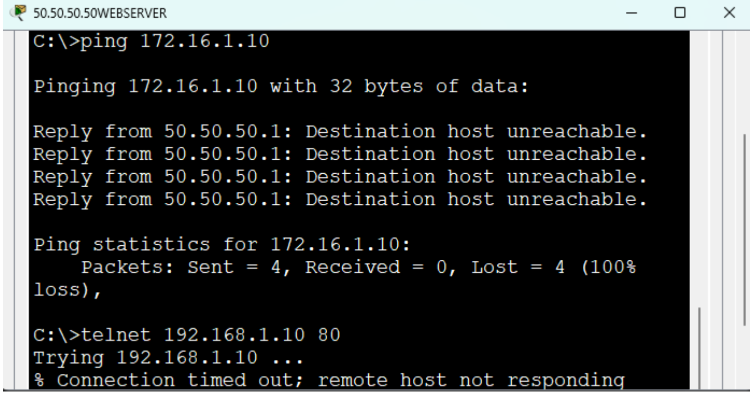
11.3.3 NAT Translation Table Verification



```
R6_AAY#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 31.0.0.2:2        192.168.10.98:2    50.50.50.2:2       50.50.50.2:2
---  31.0.0.2          172.16.1.10        ---                ---
tcp 31.0.0.2:1024      192.168.10.84:1025 212.12.12.10:80    212.12.12.10:80
tcp 31.0.0.2:1025      172.16.1.10:1025   50.50.50.2:80      50.50.50.2:80
```

Figure 28: NAT translation table showing active Static NAT and PAT translations

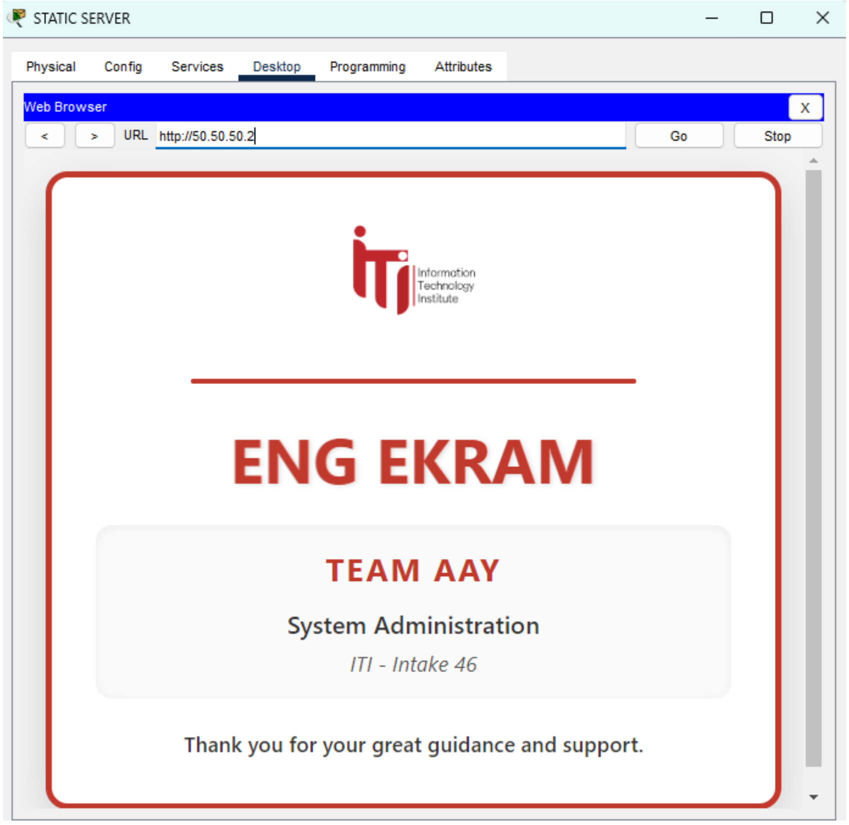
11.3.4 External Access to Static NAT Host Verification



```
C:\>ping 172.16.1.10

Pinging 172.16.1.10 with 32 bytes of data:

Reply from 50.50.50.1: Destination host unreachable.
Reply from 50.50.50.1: Destination host unreachable.
Reply from 50.50.50.1: Destination host unreachable.
Reply from 50.50.50.1: Destination host unreachable.

Ping statistics for 172.16.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100%
loss),

C:\>telnet 192.168.1.10 80
Trying 192.168.1.10 ...
% Connection timed out; remote host not responding
```

Figure 29: Failure ping and HTTP access from Internet server to Static NAT Server

11.3.5 Verify Connectivity



URL http://50.50.50.2

ENG EKRAM

TEAM AAY

System Administration

ITI - Intake 46

Thank you for your great guidance and support.

Figure 30: Test HTTP Connectivity