PROJECT REPORT

CS-3001 Computer Networks

Advanced Enterprise Network Design with Integrated Security and Dynamic Routing

Muhammad Rehan Tariq 22i-0965

National University
of computer and emerging sciences

FAST NUCES, Islamabad
Department of Computer Science

Objective:

The goal of this project is to design and implement a robust enterprise network using Cisco Packet Tracer. The network features **Enhanced Interior Gateway Routing Protocol (EIGRP)** for dynamic routing, **Network Address Translation (NAT)** for secure external communication, **Dynamic Host Configuration Protocol (DHCP)** for automated IP address allocation, and **Access Control Lists (ACLs)** for traffic filtering and enhanced security. This design ensures efficient communication, scalability, and secure data transmission across multiple departments.

Key Features of the Network Design

1. **Hierarchical Topology**:
   The network follows a hierarchical model with three layers:
   - **Core Layer**: Responsible for high-speed backbone connections.
   - **Distribution Layer**: Facilitates inter-VLAN routing and implements policies such as security filtering.
   - **Access Layer**: Connects end-user devices to the network.

2. **Dynamic Routing (EIGRP)**:
   - **Enhanced Interior Gateway Routing Protocol (EIGRP)** ensures fast convergence, load balancing, and loop-free operations, enabling real-time updates and optimized routing paths.

3. **Integrated Security**:
   - **Access Control Lists (ACLs)** are applied to restrict unauthorized traffic.
   - **Network Address Translation (NAT)** provides secure communication between private and public networks.

4. **Scalable IP Addressing**:
    - **Dynamic Host Configuration Protocol (DHCP)** automates IP address allocation, reducing administrative overhead.

Technologies Used: Cisco Packet Tracer Instructor Version

Network Design Overview

The network is divided into the following segments:

- **Finance Department (Orange Cluster)**:
  Hosts key financial servers and devices. Security policies are implemented to restrict sensitive data access.
- **IT Department (Red Cluster)**:
  Contains IT infrastructure, including critical servers and high-bandwidth connections.
- **Admin Department (Green Cluster)**:
  Hosts administrative devices and servers, ensuring secure communication with other departments.

How Cisco was used

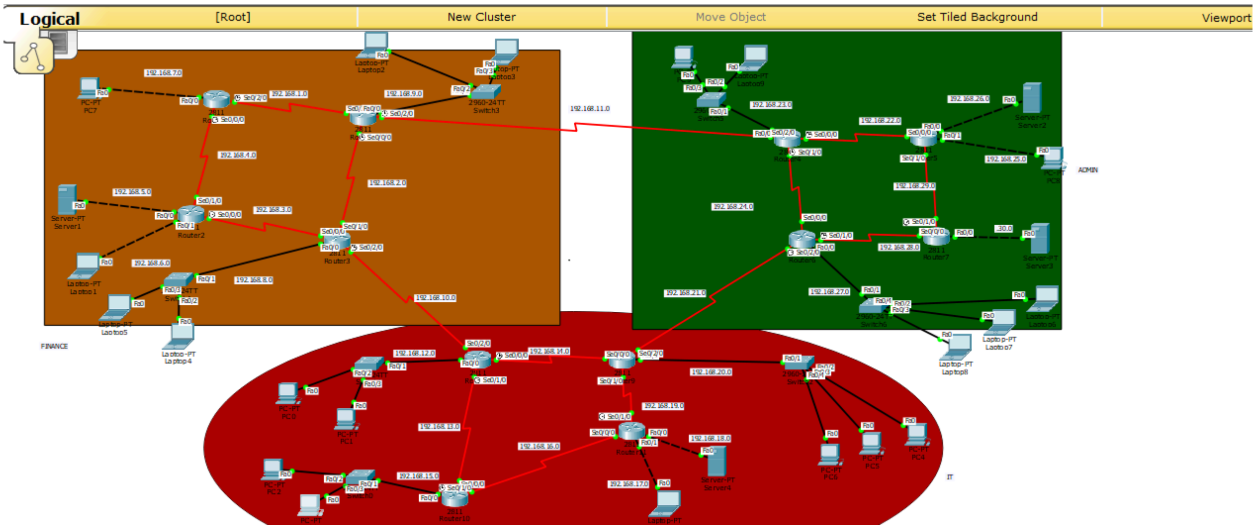
Cisco Packet Tracer was utilized to design, simulate, and implement the enterprise network. It provided a virtual environment for creating and configuring devices like routers, switches, and servers while testing their functionality. Key applications included:

- **Network Design**: Created a logical topology with clusters for Finance, IT, and Admin departments.
- **Dynamic Routing (EIGRP)**: Configured routers for efficient routing and verified using commands like `show ip eigrp neighbors`.
- **NAT Implementation**: Enabled secure communication between private and public networks through dynamic IP translation.

- **DHCP Configuration**: Automated IP assignment to devices using subnet-specific pools.
- **ACL Application**: Enforced security by filtering traffic and blocking unauthorized access.
- **End-to-End Testing**: Validated communication, security, and routing efficiency using ICMP and Packet Tracer's simulation tools.

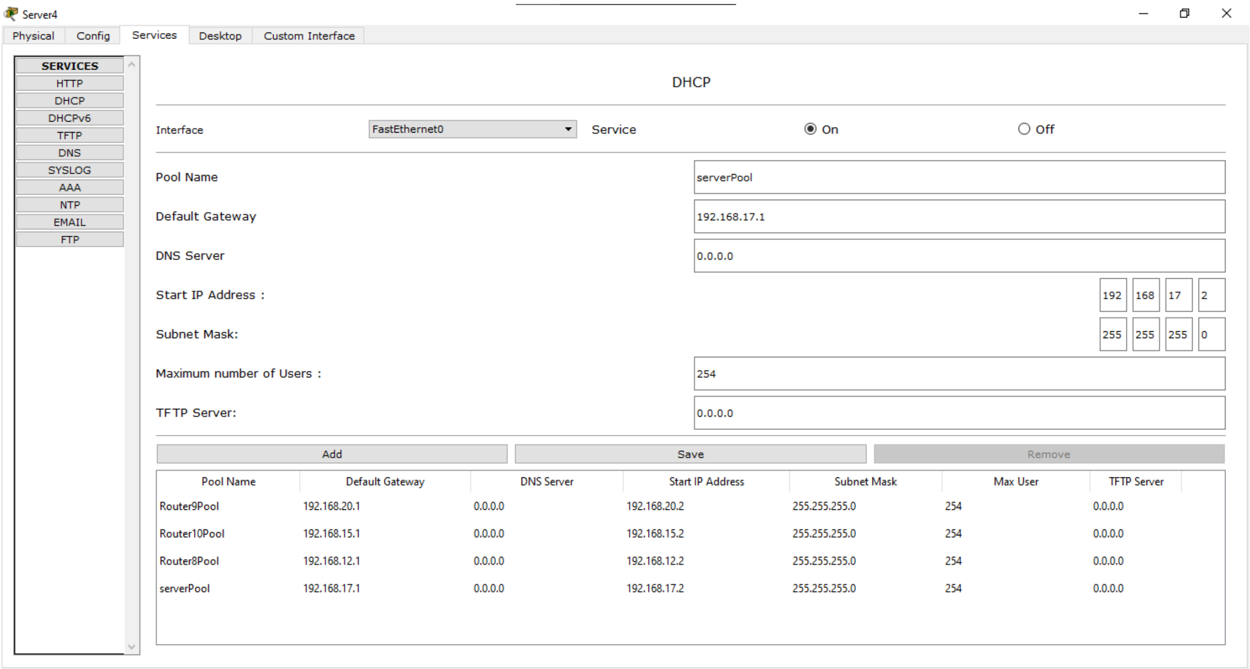
This ensured a scalable, secure, and functional network design.

TOPOLOGY:



CONFIGURATIONS AND RESULTS:

DHCP:

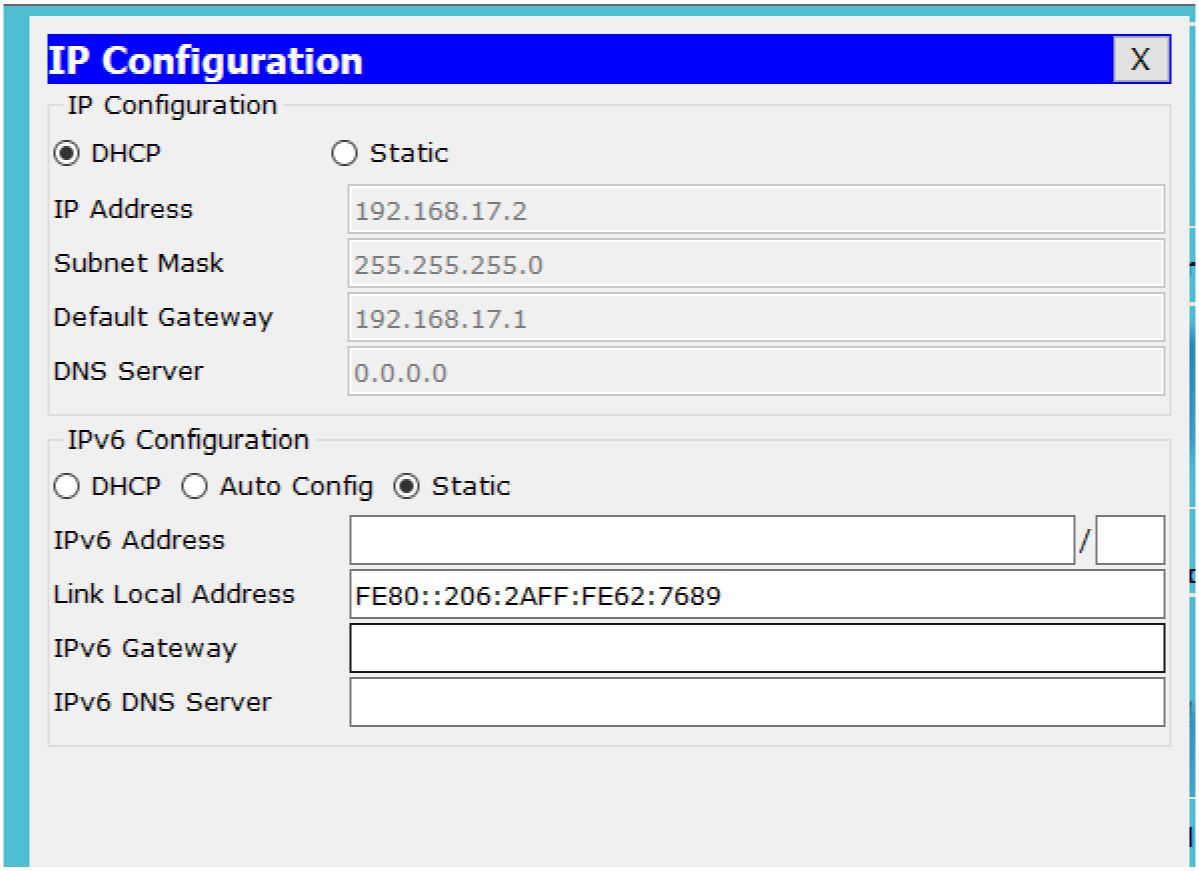


DHCP

Interface: FastEthernet0   Service: ● On ○ Off

Pool Name	serverPool
Default Gateway	192.168.17.1
DNS Server	0.0.0.0
Start IP Address :	192 168 17 2
Subnet Mask:	255 255 255 0
Maximum number of Users :	254
TFTP Server:	0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
Router9Pool	192.168.20.1	0.0.0.0	192.168.20.2	255.255.255.0	254	0.0.0.0
Router10Pool	192.168.15.1	0.0.0.0	192.168.15.2	255.255.255.0	254	0.0.0.0
Router8Pool	192.168.12.1	0.0.0.0	192.168.12.2	255.255.255.0	254	0.0.0.0
serverPool	192.168.17.1	0.0.0.0	192.168.17.2	255.255.255.0	254	0.0.0.0



IP Configuration

IP Configuration

● DHCP ○ Static

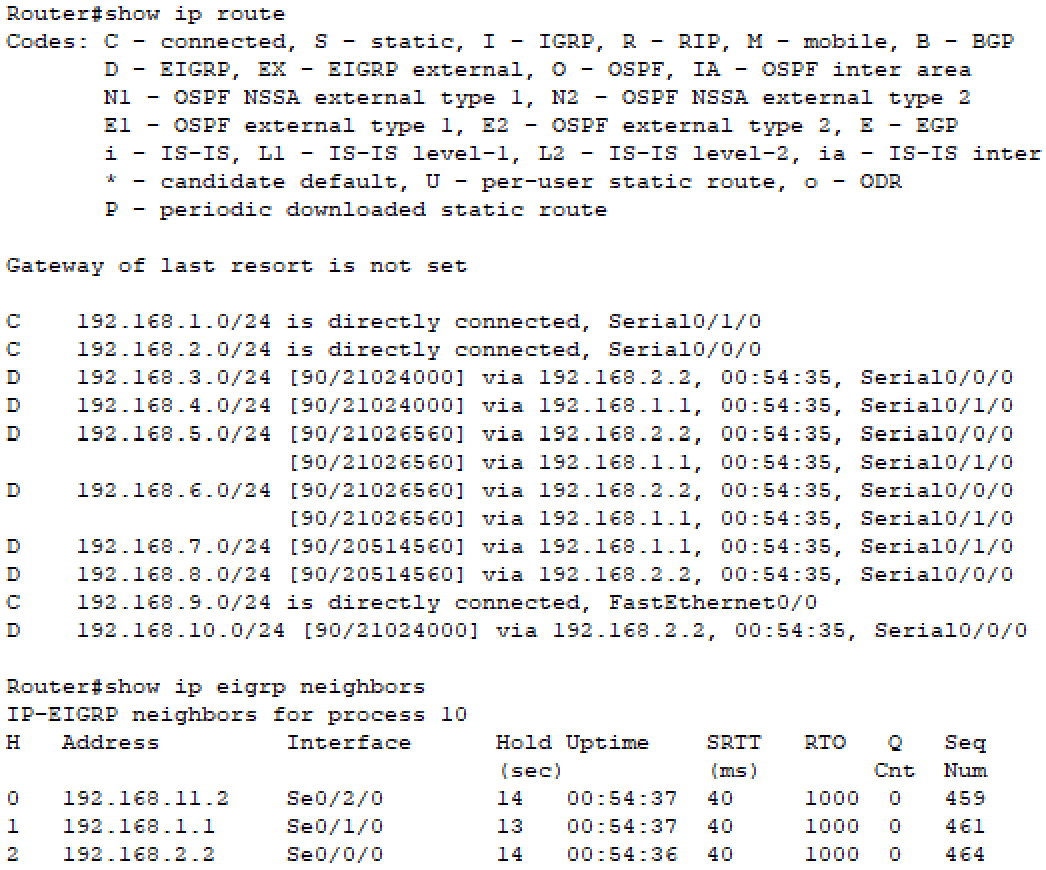
IP Address	192.168.17.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.17.1
DNS Server	0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

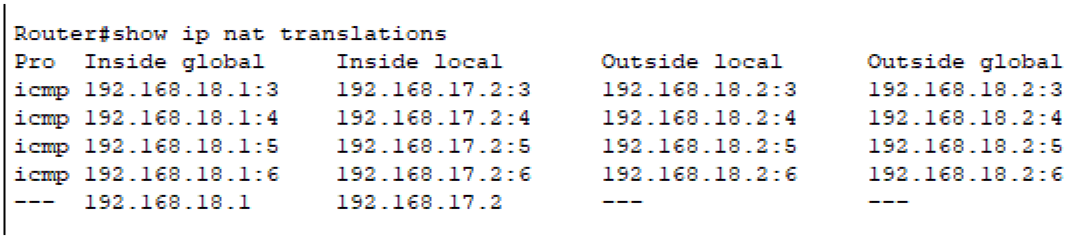
IPv6 Address	/
Link Local Address	FE80::206:2AFF:FE62:7689
IPv6 Gateway	
IPv6 DNS Server	

EIGRP:

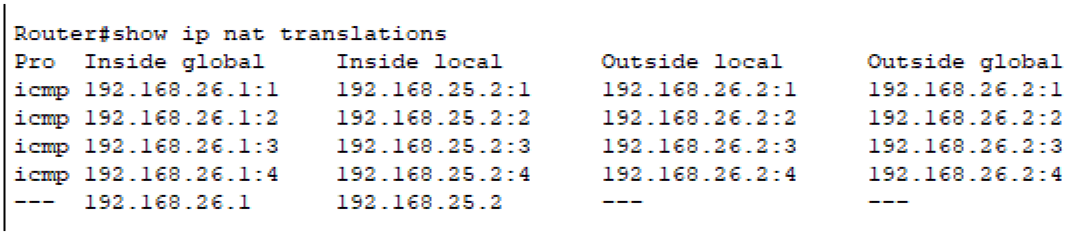


```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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 not set

C    192.168.1.0/24 is directly connected, Serial0/1/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
D    192.168.3.0/24 [90/21024000] via 192.168.2.2, 00:54:35, Serial0/0/0
D    192.168.4.0/24 [90/21024000] via 192.168.1.1, 00:54:35, Serial0/1/0
D    192.168.5.0/24 [90/21026560] via 192.168.2.2, 00:54:35, Serial0/0/0
                    [90/21026560] via 192.168.1.1, 00:54:35, Serial0/1/0
D    192.168.6.0/24 [90/21026560] via 192.168.2.2, 00:54:35, Serial0/0/0
                    [90/21026560] via 192.168.1.1, 00:54:35, Serial0/1/0
D    192.168.7.0/24 [90/20514560] via 192.168.1.1, 00:54:35, Serial0/1/0
D    192.168.8.0/24 [90/20514560] via 192.168.2.2, 00:54:35, Serial0/0/0
C    192.168.9.0/24 is directly connected, FastEthernet0/0
D    192.168.10.0/24 [90/21024000] via 192.168.2.2, 00:54:35, Serial0/0/0

Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)        Cnt  Num
0   192.168.11.2    Se0/2/0        14   00:54:37  40     1000  0   459
1   192.168.1.1     Se0/1/0        13   00:54:37  40     1000  0   461
2   192.168.2.2     Se0/0/0        14   00:54:36  40     1000  0   464
```

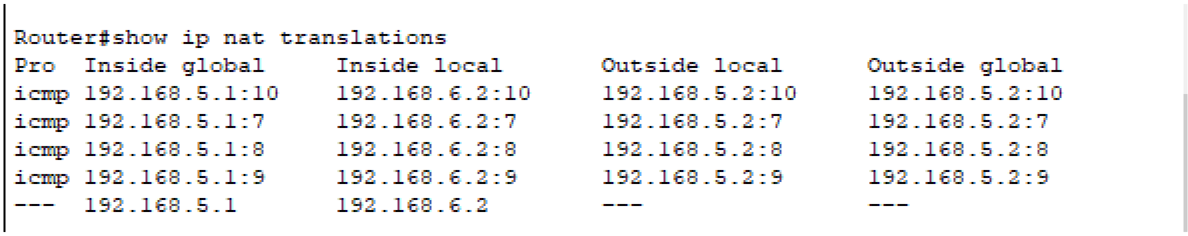
NAT :



```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 192.168.18.1:3    192.168.17.2:3     192.168.18.2:3     192.168.18.2:3
icmp 192.168.18.1:4    192.168.17.2:4     192.168.18.2:4     192.168.18.2:4
icmp 192.168.18.1:5    192.168.17.2:5     192.168.18.2:5     192.168.18.2:5
icmp 192.168.18.1:6    192.168.17.2:6     192.168.18.2:6     192.168.18.2:6
---  192.168.18.1      192.168.17.2       ---                ---
```

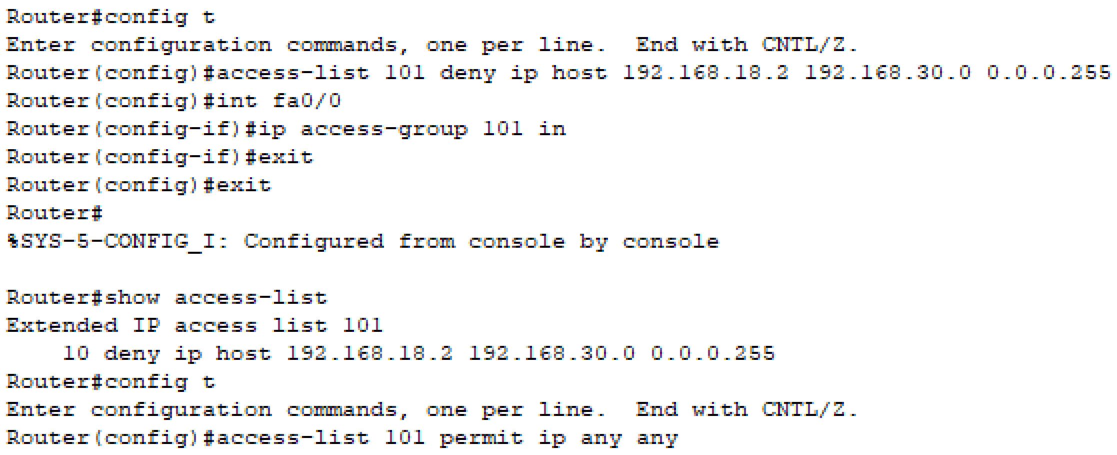


```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 192.168.26.1:1    192.168.25.2:1     192.168.26.2:1     192.168.26.2:1
icmp 192.168.26.1:2    192.168.25.2:2     192.168.26.2:2     192.168.26.2:2
icmp 192.168.26.1:3    192.168.25.2:3     192.168.26.2:3     192.168.26.2:3
icmp 192.168.26.1:4    192.168.25.2:4     192.168.26.2:4     192.168.26.2:4
---  192.168.26.1      192.168.25.2       ---                ---
```

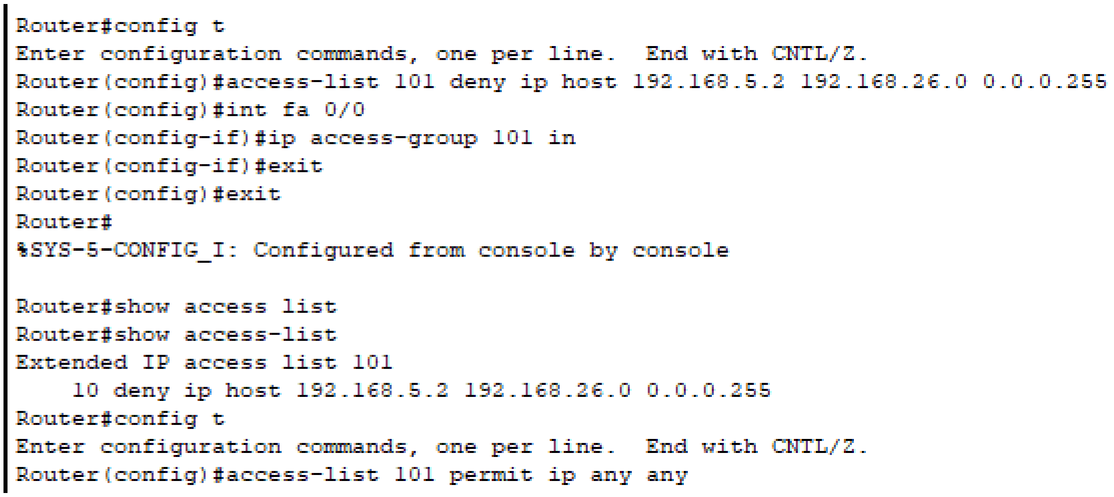


```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 192.168.5.1:10    192.168.6.2:10     192.168.5.2:10     192.168.5.2:10
icmp 192.168.5.1:7     192.168.6.2:7      192.168.5.2:7      192.168.5.2:7
icmp 192.168.5.1:8     192.168.6.2:8      192.168.5.2:8      192.168.5.2:8
icmp 192.168.5.1:9     192.168.6.2:9      192.168.5.2:9      192.168.5.2:9
---  192.168.5.1       192.168.6.2        ---                ---
```

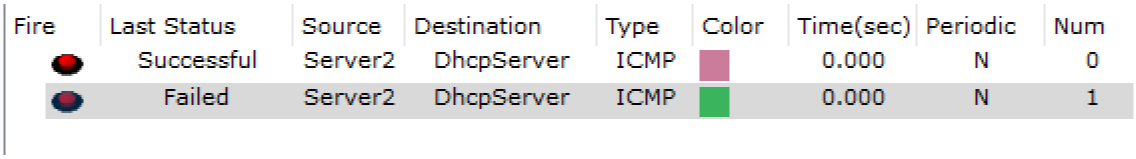
ACL:



```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 deny ip host 192.168.18.2 192.168.30.0 0.0.0.255
Router(config)#int fa0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
Extended IP access list 101
    10 deny ip host 192.168.18.2 192.168.30.0 0.0.0.255
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 permit ip any any
```



```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 deny ip host 192.168.5.2 192.168.26.0 0.0.0.255
Router(config)#int fa 0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access list
Router#show access-list
Extended IP access list 101
    10 deny ip host 192.168.5.2 192.168.26.0 0.0.0.255
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 permit ip any any
```



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Successful	Server2	DhcpServer	ICMP	🟥	0.000	N	0
●	Failed	Server2	DhcpServer	ICMP	🟩	0.000	N	1

Challenges and Solutions

Challenges Faced

1. **EIGRP Misconfigurations:**
   Misconfigured network IDs initially caused routing issues.
   Solution: Careful debugging and use of the `show ip route` and `show ip eigrp neighbors` commands.
2. **ACL Complexity:**
   Balancing access restrictions without blocking legitimate traffic.
   Solution: Thorough testing and iterative refinement of ACL rules.
3. **Device Connectivity Issues:**
   Incorrect interface assignments led to communication failures.
   Solution: Step-by-step verification using Packet Tracer's simulation mode.

Testing and Validation:

1. **Ping Tests:**
   Successfully tested interdepartmental communication and external internet connectivity using ICMP echo requests.
2. **Routing Verification:**
   Verified EIGRP routing tables to ensure accurate path selection.
3. **Security Validation:**
   Confirmed that ACLs effectively blocked unauthorized access while permitting legitimate traffic.

Conclusion

The network design successfully meets the objectives of scalability, security, and efficient communication. EIGRP's dynamic routing capabilities ensure optimal performance, while integrated security measures such as ACLs and NAT safeguard sensitive data and resources.

Future Recommendations:

1. **Implement VPN:**
   Secure remote access to the network.
2. **Upgrade to IPv6:**
   Future-proof the network by transitioning to IPv6.
3. **Incorporate Redundancy:**
   Add backup links and hardware to improve fault tolerance.
4. **Expand Security:**
   Use firewalls and intrusion detection/prevention systems for enhanced protection.