Advanced Network ACL Configuration – Project Report

1. Introduction

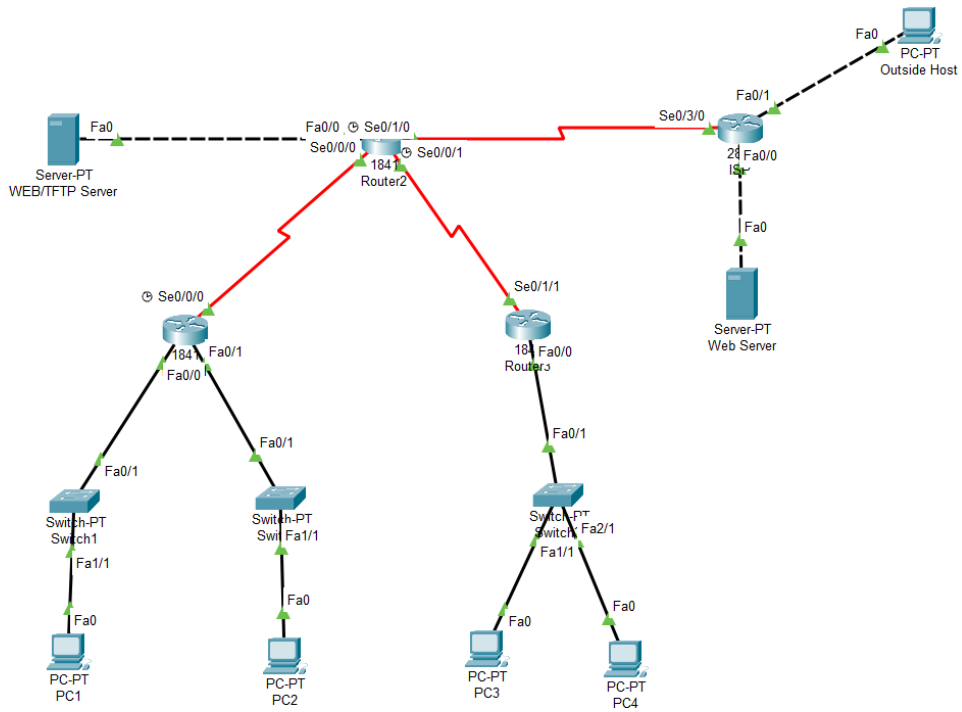
This project demonstrates the implementation of Extended Access Control Lists (ACLs) using Cisco Packet Tracer. A simulated enterprise-grade network was built using multiple routers and segments to enforce packet filtering policies for specific hosts and services. The scenario showcases how ACLs can be applied to improve security at the network level by selectively allowing or denying traffic based on protocol, IP, and direction.

2. Network Topology

The network consists of the following components:

- Routers: R1, R2, R3, ISP
- End devices: PC1–PC4, Outside Host, Servers
- Services: WEB, TFTP
- Protocols: OSPF or EIGRP for dynamic routing

Refer to the diagram below for a visual overview of the network topology:



3. IP Addressing Table

Each network component is assigned IP addresses as follows (sample entries):

- R1 Fa0/0: 192.168.10.1/24
- R2 Fa0/0: 192.168.20.1/24
- R3 Fa0/0: 192.168.30.1/24
- PC1: 192.168.10.10/24
- WEB Server: 209.165.201.30/27
- Outside Host: 209.165.202.158/27

(Full addressing provided in scenario details.)

4. Tasks and Configuration Summary

Task 1: Network Implementation and Routing

The network was successfully implemented in Cisco Packet Tracer. Connectivity between all segments was verified using ping commands. Routing was configured using EIGRP to enable communication across all routers. All devices received full routing table entries, and connectivity was established end-to-end.

Task 2: ACL for 192.168.10.0/24 – Block Telnet

An extended ACL was applied to block Telnet (TCP port 23) from the 192.168.10.0/24 network to any destination. All other traffic was permitted.
Example configuration:

```
access-list 100 deny tcp 192.168.10.0 0.0.0.255 any eq 23
access-list 100 permit ip any any
```

This ACL was applied to the outbound interface on R1 facing the network core.

Task 3: ACL for 192.168.30.0/24 – Allow TFTP and Web Only

To restrict 192.168.30.0/24 users to only TFTP and Web services, the following ACL was configured:

```
access-list 110 permit udp 192.168.30.0 0.0.0.255 host 192.168.20.254 eq 69
access-list 110 permit tcp 192.168.30.0 0.0.0.255 host 209.165.201.30 eq 80
access-list 110 deny ip 192.168.30.0 0.0.0.255 any
```

Applied on the outbound interface of R3 toward the WAN core.

Task 4: ACL for Outside Host (209.165.202.156)

Only access to the Web Server (209.165.201.30) was permitted from the outside host. ACL configuration:

```
access-list 120 permit tcp host 209.165.202.156 host 209.165.201.30 eq 80
access-list 120 deny ip host 209.165.202.156 any
```

This was applied on the inbound interface of the ISP router.

5. Conclusion

The project successfully demonstrates real-world ACL deployment in a simulated environment. Each ACL applied aligns with security policies typically found in enterprise networks. The configuration enforces access restriction based on IP, service type, and traffic direction to protect sensitive internal resources from unauthorized access.