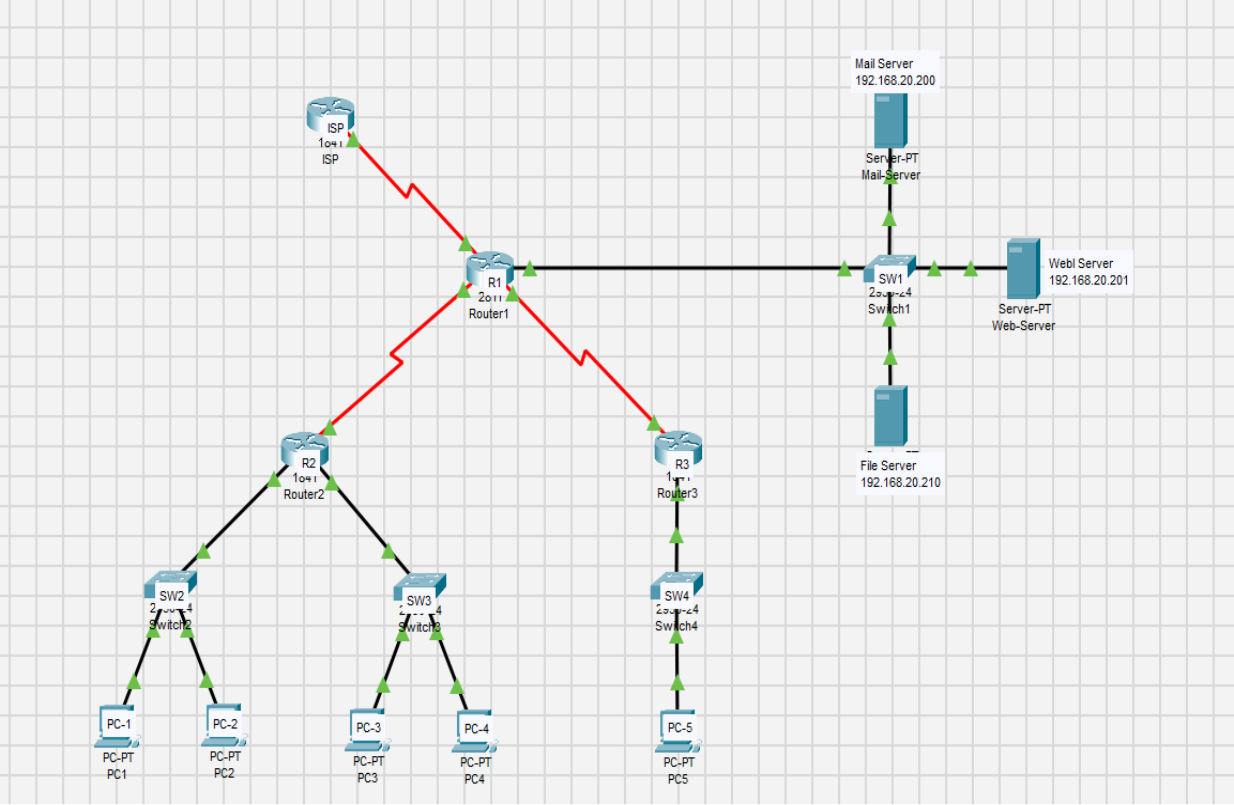

Objectives

Configure a **Standard ACL** to block traffic from a specific network.

Configure an **Extended ACL** to restrict internet access based on source and destination IP.

Implement a **VTY ACL** to control remote access to a router.

Verify ACL functionality through ping and Telnet tests.

Configurations

Standard ACL: Block 192.168.11.0/24 from Local Networks on R3

R3(config)# ip access-list standard STND-1

R3(config-std-nacl)# deny 192.168.11.0 0.0.0.255

R3(config-std-nacl)# permit any

R3(config)# interface Serial 0/0/0

R3(config-if)# ip access-group STND-1 in

PC3 (192.168.11.10) cannot reach PC5 (192.168.30.10).

Extended ACL: Block Internet Access for 192.168.10.0/24

R2(config)# ip access-list extended EXTEND-1

R2(config-ext-nacl)# deny ip 192.168.10.0 0.0.0.255 host 200.200.200.1

R2(config-ext-nacl)# permit ip any any

R2(config)# interface Serial 0/0/0

R2(config-if)# ip access-group EXTEND-1 out

PC1 (192.168.10.x) cannot reach 200.200.200.1 (ISP) but can reach internal networks.

VTY ACL: Restrict Remote Access to R1

R1(config)# ip access-list standard STND-2

R1(config-std-nacl)# permit 10.2.2.0 0.0.0.3

R1(config-std-nacl)# permit 192.168.30.0 0.0.0.255

R1(config-std-nacl)# deny any

R1(config)# line vty 0 4

R1(config-line)# access-class STND-2 in

R3 can Telnet to R1, but R2 cannot.

Verification Commands

show access-lists

show ip interface Serial 0/0/0

show ip nat translations

Summary

Standard ACLs filter traffic by source IP.

Extended ACLs filter traffic by source and destination IP, protocol, and ports.

VTY ACLs restrict remote router access for security.

ACL placement is critical for proper network security.