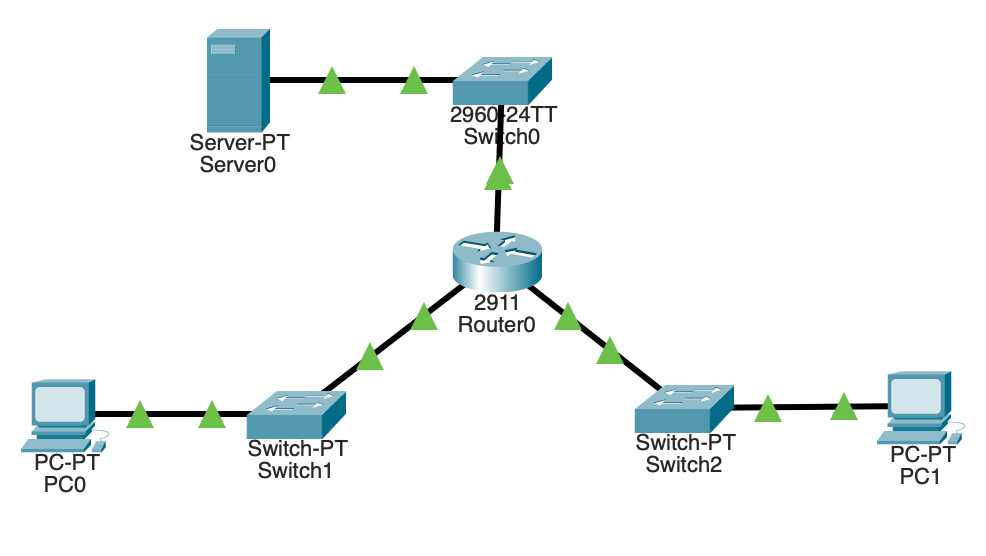
21BDS0340

Abhinav Dinesh Srivatsa

Information Security Management

Digital Assignment – II

**Network Configuration for Standard/Extended ACL**



**Pinging before ACL Implementation**

A screen shot of a computer

Description automatically generatedA computer screen with white text

Description automatically generated

**Implementing Standard ACL**

A screenshot of a computer

Description automatically generated

**Explaining the Commands**

1. Creating a standard access list called block20
2. Adding a rule to deny any packet from the network 20.0.0.0/8
3. Adding a rule to permit any other packets
4. Applying the rule as an out rule to the gigabit interface 0/0, where the server is connected.
5. The makes sure devices on the network 20.0.0.0/8 cannot access the server.

**Pinging after Standard ACL Implementation**

**A computer screen with white text

Description automatically generated**

**A computer screen with white text

Description automatically generated**

**Implementing Extended ACL**

A computer screen shot of a computer code

Description automatically generated

**Explaining the Commands**

1. Adding a rule to the extended ACL list 101 to deny any ICMP echo packets originating from the network 20.0.0.0/8 that are sent to any device in 10.0.0.0/8
2. Adding a rule to the extended ACL list 101 the permit any packet otherwise.
3. Applying the rule as an in rule to the gigabit interface 0/1, where the network 20.0.0.0/8 is connected to the router.
4. This enables any device on the 20.0.0.0/8 network to not access the server via ICMP echoes but can still view the HTTP page.

**Pinging after Extended ACL Implementation**

**A screen shot of a computer

Description automatically generated**

**HTTP Request after Extended ACL Implementation**

**A screenshot of a computer

Description automatically generated**