**NPS Lab Experiment 10**

**Network Configuration and Access Control Setup in Cisco Packet Tracer**

**Step 1: Network Setup**

1. Launch **Cisco Packet Tracer**.
2. From the device list, add the following:
   * **4 PCs**: PC0, PC1, PC2, PC3.
   * **2 Switches**.
   * **1 Router**.
   * **2 Servers**.

**Step 2: Configure IP Addresses on PCs**

1. **PC0**: Set IP address to 192.168.10.10.
2. **PC1**: Set IP address to 192.168.10.20.
3. **PC2**: Set IP address to 192.168.10.30.
4. **PC3**: Set IP address to 192.168.10.40.

**Step 3: Connect Devices Using Automatic Cabling**

1. Use **automatic cabling** to connect:
   * Each PC to the respective switch.
   * Switches to the router using **GigabitEthernet0/1** and **GigabitEthernet0/2**.

**Step 4: Router Configuration for Standard Access List**

1. Enter privileged mode (enable) and global configuration mode (configure terminal).
2. Assign IP address 192.168.10.10 with subnet mask 255.255.255.0 to the router.
3. Create a **standard access list**:
   * Permit all IPs except 192.168.10.20.
4. Apply the access list to **interface fa0/1**.

**Step 5: Router Configuration for Extended Access List**

1. Create an **extended access list** to deny TCP traffic from 192.168.10.10 to 192.168.10.20 on port 80.
2. Permit all other IP traffic.
3. Apply this extended access list to **interface fa0/1**.
4. Exit configuration mode and verify the configuration by displaying the access lists.

**Step 6: Testing the Network**

1. Go to the **Command Prompt** on **PC0** and **PC1**.
2. Test connectivity using the following:
   * Ping 192.168.10.20 to verify connectivity.
3. Verify access restrictions by attempting to access resources blocked by the access list.

