CS556 - Advanced Netowork LAB Assignment 3 Network Configuration for NIT Meghalaya

Utsav Balar (t24cs003)

Contents

You are tasked with configuring a network for NIT Meghalaya consisting of 3 switches (S1, S2, S3), 3 PCs (PC1, PC2, PC3), and 2 routers (R1, R2). The network should be configured with VLANs, basic routing between subnets, port security, and management access. Your goal is to ensure devices in different VLANs can communicate while maintaining security.

1. Switch Configuration (S1, S2, S3):

- Set hostnames for each switch:
  - S1: Computer Science
    - **S1**: `hostname Computer_Science`
  - S2: Electrical Engineering
    - **S2**: `hostname Electrical_Engineering`
  - S3: Mechanical Engineering
    - **S3**: `hostname Mechanical_Engineering`
  - Create and assign the following VLANs on all switches:
    - VLAN 10: Computer Science
    - VLAN 20: Electrical Engineering
    - VLAN 30: Mechanical Engineering

```
vlan 10
name Computer_Science
vlan 20
name Electrical_Engineering
vlan 30
name Mechanical_Engineering
```

- Assign appropriate switch ports to each VLAN:
  - PC1 to VLAN 10 (Computer Science)
    - **S1**:
      - Fa0/1 (PC1): `plaintext interface fa0/1 switchport mode access switchport access vlan 10`
      - Fa0/2 (R1 Fa0/0): `plaintext interface fa0/2 switchport mode access switchport access vlan 10`
  - PC2 to VLAN 20 (Electrical Engineering)
    - **S2**:
    - Fa0/1 (PC2): `plaintext interface fa0/1 switchport mode access switchport access vlan 20`
    - Fa0/2 (R1 Fa0/1): `plaintext interface fa0/2 switchport mode access switchport access vlan 20`
  - PC3 to VLAN 30 (Mechanical Engineering)
    - **S3**:
    - Fa0/1 (PC3):
      ```
      interface fa0/1
      switchport mode access
      switchport access vlan 30
      ```
    - Fa0/2 (R2 Fa0/0):
      ```
      interface fa0/2
      switchport mode access
      switchport access vlan 30
      ```
  - Configure trunking between the switches to allow VLANs to propagate.
    - **S1**:

```
interface fa0/24
switchport mode trunk
```

    - **S2**:

```
interface fa0/24
switchport mode trunk
interface fa0/23
switchport mode trunk
```

    - **S3**:

```
interface fa0/23
switchport mode trunk
```

2. Router Configuration (R1, R2):

- Configure the router interfaces with the following IP addresses:
  - R1:
    - Fa0/0: 192.168.10.1/24 (for VLAN 10)
    - Fa0/1: 192.168.20.1/24 (for VLAN 20)

```
interface fa0/0
ip address 192.168.10.1 255.255.255.0
no shutdown
interface fa0/1
ip address 192.168.20.1 255.255.255.0
no shutdown
interface s0/0
ip address 10.0.0.1 255.255.255.252
no shutdown
```

  - R2:
    - Fa0/0: 192.168.30.1/24 (for VLAN 30)

```
interface fa0/0
```

```
ip address 192.168.30.1 255.255.255.0
no shutdown
interface s0/0
ip address 10.0.0.2 255.255.255.252
no shutdown
```

- Enable RIP Routing on both routers to allow communication between the different VLANs (via router-on-a-stick).
  - **R1**:

```
router rip
version 2
network 192.168.10.0
network 192.168.20.0
network 10.0.0.0
```

  - **R2**:

```
router rip
version 2
network 192.168.30.0
network 10.0.0.0
```

3. Port Security Configuration:

- Configure port security on each switch, limiting MAC addresses to 1 per port for each connected device (PC1, PC2, PC3).
  - **S1 (Fa0/1)**:

```
interface fa0/1
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
```

  - **S2 (Fa0/1)**:

```
interface fa0/1
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
```

  - **S3 (Fa0/1)**:

```
interface fa0/1
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
```

This limits each port to a single MAC address, shutting down the port if an unauthorized device attempts to connect.

4. Management VLAN and SSH Access:

- Configure VLAN 1 as the management VLAN and assign the following IP addresses to each switch:
  - S1 (CS Dept): 192.168.10.10

```
interface vlan 10
 ip address 192.168.10.10 255.255.255.0
```

- S2 (EE Dept): 192.168.20.10

```
interface vlan 20
 ip address 192.168.20.10 255.255.255.0
```

- S3 (ME Dept): 192.168.30.10

```
interface vlan 30
 ip address 192.168.30.10 255.255.255.0
```

- Set up SSH on each switch for secure remote access.

```
crypto key generate rsa
(1024 modulus)
ip ssh version 2
line vty 0 4
transport input ssh
login local
username admin password cisco
```

5. Basic Troubleshooting:

- Test the connectivity:
  - PC1 should only be able to communicate with devices in VLAN 10.
  - PC2 should only be able to communicate with devices in VLAN 20.
  - PC3 should only be able to communicate with devices in VLAN 30.
- Ensure that PC1, PC2, and PC3 can successfully ping devices in their respective VLANs.
- Troubleshoot and resolve any connectivity issues. Addressing Table:

```
Device Interface IP Address Subnet Mask
S1 VLAN 1 192.168.10.10 255.255.255.0
S2 VLAN 1 192.168.20.10 255.255.255.0
S3 VLAN 1 192.168.30.10 255.255.255.0
PC1 NIC 192.168.10.11 255.255.255.0
PC2 NIC 192.168.20.11 255.255.255.0
PC3 NIC 192.168.30.11 255.255.255.0
R1 Fa0/0 192.168.10.1 255.255.255.0
Fa0/1 192.168.20.1 255.255.255.0
R2 Fa0/0 192.168.30.1 255.255.255.0
Instructions:
```

6. Switch Configuration:

- Set the hostnames and configure the VLANs on S1, S2, and S3.
- Assign the switch ports to the correct VLANs and configure trunking between the switches.

7. Router Configuration:

- Configure R1 and R2 with the given IP addresses and enable RIP routing to ensure communication between all VLANs.

8. Port Security:

- Apply port security on all switch ports connected to the PCs, restricting each port to only allow the MAC address of the connected device.

9. Management VLAN and SSH:

- Configure the management VLAN on each switch and enable SSH for remote management.

10. Basic Troubleshooting:

- Test the connectivity between the PCs within their VLANs.
- Troubleshoot and resolve any issues related to VLAN configurations, port security, and routing. Completion Requirements:
  - PC1, PC2, and PC3 should only communicate with devices in their assigned VLAN.
  - SSH should be configured for secure management on the switches.
  - Routing between the VLANs should be functional via RIP.
  - Port security should be applied to restrict access to the network.