Practical 5: Network Segmentation with Switches and Routers

Practical Title: Use switches and routers to segment networks.

Aim: To understand and implement network segmentation using switches and routers to improve network performance and security.

Objective:

- To distinguish between collision and broadcast domains.
- To use a switch to create separate collision domains.
- To use a router to create separate broadcast domains.
- To understand the role of VLANs (Virtual LANs) in network segmentation.

Theory: **Network segmentation** is the process of dividing a computer network into smaller sub-networks. This reduces network traffic, improves security, and simplifies management. A **switch** segments a network into **collision domains**, meaning that devices connected to different switch ports do not compete for the same network medium, thereby reducing collisions. A **router** segments a network into **broadcast domains**, preventing broadcast traffic from one network from reaching another.

Steps:

1. **Create the Network Topology:**
    - Open Cisco Packet Tracer.
    - Create a simple topology with two PCs connected to a switch.
    - Add another switch and two more PCs, and connect this new switch to a different port on the first switch.
    - Add a router and connect the first switch to the router. The topology should demonstrate how switches and routers create different domains.
2. **Observe Collision and Broadcast Domains:**
    - On the initial topology (two PCs connected to a single switch), send a broadcast packet from one PC (using the "Add Simple PDU" tool). Observe that the broadcast packet is sent to all other devices connected to the same switch.

- Now, connect the router to the switch. The router will prevent broadcast packets from passing through to other networks, showing that the router is the boundary of the broadcast domain.
- Similarly, any data sent from one PC to another via the switch will be a unicast, not a collision, demonstrating how the switch has created separate collision domains for each connected device.

3. **Implement VLANs (Optional, but recommended):**
   - On the switch, go to the **CLI** tab and configure two VLANs, for example, VLAN 10 for "Sales" and VLAN 20 for "Marketing".
   - Assign specific switch ports to each VLAN.
   - Configure the router with a "router on a stick" setup to enable communication between the VLANs.

Conclusion: This practical demonstrated the fundamental principles of network segmentation. We observed how switches break up a network into multiple collision domains and how routers create separate broadcast domains. This knowledge is crucial for designing efficient and secure network architectures.

Viva / Oral Questions:

1. What is a collision domain, and how does a switch help reduce collisions?
2. What is a broadcast domain, and how does a router affect it?
3. How do VLANs provide an additional layer of network segmentation?
4. What is the "router on a stick" configuration, and why is it used?
5. Why is network segmentation important for security?

CLI COMMANDS

On Switch 0:

Switch> enable

Switch# configure terminal

Switch(config)# vlan 10

Switch(config-vlan)# name Dept_A

Switch(config-vlan)# exit

Switch(config)# interface fastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config-if)# exit

On Switch 1:

Switch> enable

Switch# configure terminal

Switch(config)# vlan 20

Switch(config-vlan)# name Dept_B

Switch(config-vlan)# exit

Switch(config)# interface fastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 20

Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 20

Switch(config-if)# exit

On Router:

Router> enable

Router# configure terminal

! For VLAN 10

Router(config)# interface gig0/0.10

Router(config-subif)# encapsulation dot1Q 10

Router(config-subif)# ip address 192.168.10.1 255.255.255.0

Router(config-subif)# no shutdown

! For VLAN 20

Router(config)# interface gig0/0.20

Router(config-subif)# encapsulation dot1Q 20

Router(config-subif)# ip address 192.168.20.1 255.255.255.0

Router(config-subif)# no shutdown

VERIFY CONNECTIVITY:

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms