Practical-5

* Aim → Introduction to VLAN (Virtual local Area Network) and Implementation of VLAN in Cisco Packet Tracer.

* Theory → * VLAN → A VLAN (Virtual Local Area Network) is a technology used in computer networking to create logically separate networks within a single physical network infrastructure. VLAN's help improve the performance, security and management of network resources by segmenting the network into smaller, isolated broadcast domains.

* What is VLAN?

⇒ A VLAN is a way to divide a single physical network into multiple logical networks. These virtual network allow devices to communicate as if they were on the same local network, even if they are physically located on different network segments.

i) VLAN's are created using network switches.
ii) They work by assigning a specific identifier (VLAN ID) to each VLAN.
iii) Devices within the same VLAN can

communicate with each other without passing traffic to other VLAN's unless configured to do so.

* How VLAN's Work → When VLAN's are implemented on a switch, each port of the switch can be assigned to a specific VLAN. Traffic from devices on the same VLAN is isolated from traffic on other VLAN's. The switch forwards traffic only to ports within the same VLAN unless it is configured to route traffic between VLAN's.

* Eg → i) VLAN 10 might be used for the Sales department.
ii) VLAN 20 might be used for the IT department.

→ Even though these departments share the same physical switch, their network traffic is isolated unless routing is explicitly allowed.

* Types of VLAN's → i) Data VLAN → Also called user VLAN's these are used to carry user-generated traffic.

ii) Voice VLAN → Used for Voice Over IP (VoIP) traffic, prioritizing voice data for better quality.

iii) Management VLAN → Reserved for network management traffic, allowing administrators to remotely configure and manage devices without interference from user data.

iv) Native VLAN → The default VLAN that carries untagged traffic. Any device that connects without a VLAN tag is placed into the native VLAN.

* Advantages of VLAN's → i) Improved Security → VLANs isolate sensitive data. Eg → employee data and guest traffic can be on separate VLAN's to prevent unauthorized access.

ii) Better Network Performance → VLAN's reduce the size of broadcast domains. This minimizes the amount of broadcast traffic and improves overall network efficiency.

iii) Flexibility and Scalability → VLAN's allow you to group devices by function rather than physical location. Eg → all HR computers can be in the same VLAN regardless of their physical location.

iv) Simplified Network Management → VLAN's make it easier to manage large networks by segmenting them into smaller, more manageable parts.

Implementation of VLAN's in Cisco Packet Tracer →

→ Creating VLAN's in Cisco Packet Tracer:

1) Setting up the Network:
   i) Devices → Use switches, routers and PC's for the VLAN configuration.
   ii) Network Topology → Build a simple topology with one switch and four PC's.
   iii) PC1 and PC2 will belong to VLAN 10 (e.g. HR Department).
   iv) PC3 and PC4 will belong to VLAN 20 (e.g. IT Department).

2) Step-by-Step VLAN Creation:
   i) Step 1 → Access the switch in Cisco Packet Tracer.
      · Click on the switch, go to the CLI (Command Line Interface).
   ii) Step 2 → Enter Privileged EXEC mode:

```
Switch> enable
Switch # configure terminal
```

iii) Step 3: Create VLAN 10(HR) and VLAN 20(IT):

```
Switch(config)# vlan 10
Switch(config-vlan)# name HR
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name IT
Switch(config-vlan)# exit
```

iv) Assigning Port to VLAN's →

```
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

Switch(config)# interface fastEthernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit
```

VLAN Configuration And Testing →

1) Verifying VLAN Configuration:
- Use the following command to verify the VLAN's on the switch:
Switch # show vlan brief
- This command will display the VLAN ID, name and the ports appigned to each VLAN.

2) Inter-VLAN Communication:
- By default, devices on different VLAN's cannot communicate directly.
- To enable communication between VLAN's, a router or a layer 3 switch is required for Inter VLAN Routing.

3) Testing VLAN Configuration:
Step 1 → Ping between PC's on the same VLAN (PC1 ↔ PC2 on VLAN 10, & PC3 ↔ PC4 on VLAN 20). They should successfully communicate.
Step 2 → Ping between PC's on different VLAN's (PC1 ↔ PC3 or PC4). The ping should fail as they belong to different VLAN's and no router is configured for inter VLAN routing.

Conclusion → i) VLANs effectively isolate network segments. ii) In the next step, inter VLAN routing can be configured for communication over VLAN's.