

EXPERIMENT 2

Aim

Simulation of Virtual Local Area Network

Prerequisite

Nil

Outcome

To impart knowledge of Computer Networking Technology

Theory

A Virtual Local Area Network (VLAN) is a logical segmentation of a physical network into isolated groups. VLANs enable devices to communicate as if they are on separate networks, even if physically connected. This enhances efficiency, security, and management in various ways:

- **Efficiency:** VLANs segment network traffic, reducing congestion and enhancing performance. Broadcasts are limited to devices within the same VLAN, preventing unnecessary network overload.
- **Security:** Devices in different VLANs are isolated, limiting unauthorized communication. Inter-VLAN communication requires routing, enhancing control over data flow and security.
- **Flexibility:** VLANs can be organized by department, function, or need, regardless of physical location. This simplifies network management and optimizes resource allocation.
- **Management:** VLANs enable logical network segmentation, easing administration and troubleshooting. VLAN identification tags manage traffic flow.
- **Inter-VLAN Communication:** Routers or Layer 3 switches facilitate communication between VLANs by routing data.
- **Configuration:** VLAN setup involves configuring devices to recognize VLAN tags. Port-Based, Tagged, and Dynamic VLANs cater to various needs.

In summary, VLANs enhance network efficiency, security, and management by logically segmenting a physical network into isolated groups, enabling better resource utilization, security, and adaptability.

Procedure

1. Open Cisco Packet Tracer and simulate the sample topologies with required size of VLAN.
2. Perform Necessary Operation on Switch to create and configure VLAN.
3. Check the connectivity between the devices.

Steps

1. Launch Cisco Packet Tracer.
2. Create a basic network topology.
3. Connect devices using Ethernet cables.
4. Configure VLAN support on switches.
5. Assign ports to specific VLANs on switches.
6. Configure computers in the same VLAN.
7. Configure different computers in separate VLANs.
8. Test ping commands between devices in same/different VLANs.
9. Enable routing between sub-interfaces.
10. Test ping commands between devices in different VLANs.
11. Observe and analyse device behaviour within VLANs.

Output

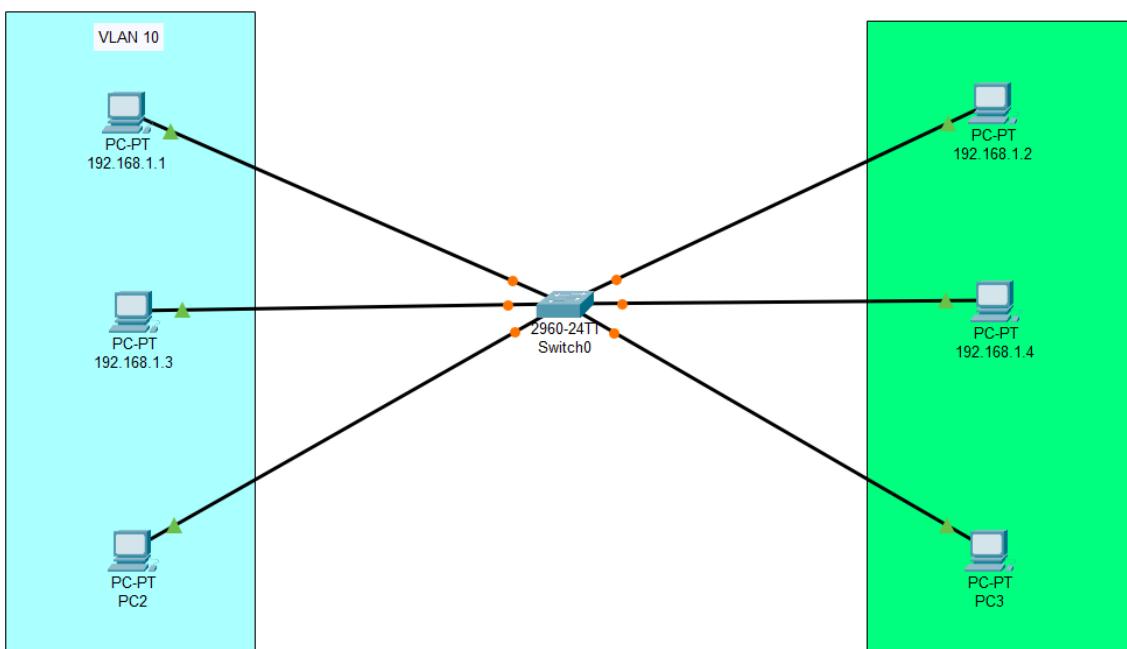


Figure 1. Topology

Configuration

```

Switch(config)#vlan 10
Switch(config-vlan)#name IT
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Sales

Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range f0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#int range fa0/4-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20

```

VLAN	Name	Status	Ports
1	default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	IT	active	Fa0/1, Fa0/2, Fa0/3
20	Sales	active	Fa0/4, Fa0/5, Fa0/6
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fdtnet-default	active	
1005	trnet-default	active	

FastEthernet0 Connection: (default port)

```
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2D0:BCFF:FE06:BC89
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                           0.0.0.0
```

Bluetooth Connection:

```
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
                           0.0.0.0
```

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Ping statistics for 192.168.1.2:

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

```
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
```

Ping statistics for 192.168.1.3:

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Approximate round trip times in milli-seconds:

```
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Observation & Learning

- Devices within the same VLAN can communicate freely, while communication between devices in different VLANs requires routing.
- VLANs segregate broadcast domains, reducing unnecessary traffic.
- Trunk ports allow traffic exchange between switches for different VLANs.
- VLAN tagging aids in directing traffic accurately to specific VLANs.
- Inter-VLAN communication necessitates routing devices.
- VLANs enhance network efficiency by controlling traffic and broadcasts.
- Security is improved as devices in different VLANs are isolated.
- Inter-VLAN communication is enabled through routers or Layer 3 switches.
- Proper VLAN tagging and trunk configuration are vital for correct data routing.
- Simulations assist in understanding VLAN behaviour and configurations.

Conclusion

Simulating Virtual Local Area Networks (VLANs) using Cisco Packet Tracer offers valuable insights into network segmentation and behaviour. The experiment revealed that VLANs effectively isolate and manage network traffic, enhance security, and streamline network management. Inter-VLAN communication can be achieved through routing devices. VLAN tagging and trunk ports are pivotal for ensuring accurate data transmission. By understanding the concepts and simulating scenarios, network professionals can confidently implement VLANs to optimize network efficiency, security, and management in real-world scenarios.

Questions

1. What is the maximum number of VLAN can be created in a network?

The maximum number of VLANs that can be created in a network depends on the networking equipment being used. In most cases, modern networking switches support up to 4096 VLANs, as defined by the IEEE 802.1Q standard. However, practical limits may vary based on the switch's hardware capabilities and the network's overall design.

2. What is mean by MTU? What is the value of MTU in Ethernet?

MTU (Maximum Transmission Unit) refers to the maximum size of a data packet that can be transmitted over a network without being fragmented. In Ethernet, the standard MTU size is 1500 bytes for most networks. This value accounts for the Ethernet frame header and payload, leaving 1500 bytes for the actual data. Jumbo frames, which have larger MTU sizes, are sometimes used to improve data transfer efficiency, but their use requires compatible hardware and configurations across the network.

3. What happen when the broadcast operation is performed from a system in certain VLAN?

When a broadcast operation, such as an ARP (Address Resolution Protocol) request, is performed from a system in a certain VLAN, the broadcast will only propagate within that specific VLAN. Broadcast traffic does not cross VLAN boundaries. This isolation ensures that broadcast storms and unnecessary traffic are contained within the intended VLAN, preventing them from affecting devices in other VLANs. This segmentation enhances network performance and security by preventing unnecessary broadcast traffic from affecting the entire network.