Course Name:	**Computer Communication and Networking**	**Semester:**	**VI**
Date of Performance:	**28 / 01 / 2025**	**Batch No.:**	**B - 2**
Faculty Name:	**Dr. Sudha Gupta**	**Roll No.:**	**16014022050**
Faculty Sign & Date:		**Grade/Marks:**	**___ / 25**

Experiment No.: 4

Title: To implement and study of Virtual LAN using cisco packet tracer.

Aim and Objective of the Experiment:

To implement and study of Virtual LAN using cisco packet tracer.

- Cofigure Virtual LAN.
- Learn & analyze various networking commands.

COs to be achieved:

CO1: Understand concept of computer communication & Network models.

CO2: Describe different data link and transmission protocol for transmission and control.

Theory:

A virtual local area network (VLAN) is a LAN which is not configured by physical wiring but it is configured by software. A VLAN is logical group of network devices that appear to be on same LAN despite their geographical distribution. A VLAN is implemented so that network administrators can connect a group of host in the same domain inspite of their physical location to achieve scalability and improve security features.

To subdivide a network into virtual LANs, one configures a network switch or router. Simpler network devices can partition only per physical port (if at all) , in which case each VLAN is connected with a dedicated network cable (and VLAN connectivity is limited by the number of hardware ports available) More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs. VLAN can greatly simplify network design and deployment, because VLAN membership can be configured through software.

Circuit Diagram/ Block Diagram:

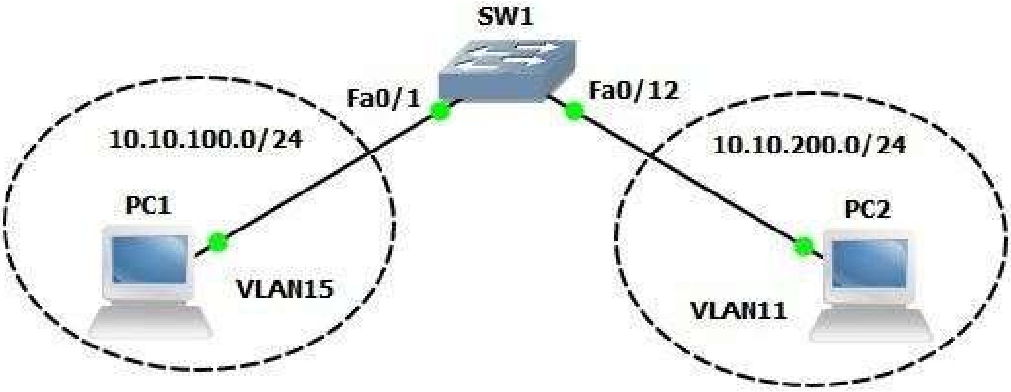


Fig. VLAN Network

Stepwise-Procedure:

1. Open packet tracer software.
2. Design star network topology.
3. Go To switch CLI.
4. Configure two VLAN in a switch.
5. As per design, assign membership of VLAN to port using following command # switch port access vlan2 or vlan3
6. Check status of VLAN.

Cisco IOS Modes of Operation:

- The Cisco IOS software provides access to several different command modes. Each command mode provides a different group of related commands.
- For security purposes, the Cisco IOS software provides two levels of access to commands:
    - User mode
    - Privileged mode
- The unprivileged user mode is called user EXEC mode. The privileged mode is called privileged EXEC mode and requires a password. The commands available in user EXEC mode are a subset of the commands available in privileged EXEC mode.
- The following table describes some of the most commonly used modes, how to enter the modes, and the resulting prompts. The prompt helps you identify which mode you are in and, therefore, which commands are available to you.

Modes of Operation	Usage	How to enter the mode	Prompt

User EXEC	Change terminal settings on a temporary basis, perform basic tests, and list system information.	First level accessed.	Router>
Privileged EXEC	System administration, set operating parameters.	From user EXEC mode, enter enable password command	Router#
Global Config	Modify configuration that affect the system as a whole.	From privileged EXEC, enter configure terminal.	Router(config)#
Interface Config	Modify the operation of an interface.	From global mode, enter interface type number.	Router(config-if)#
Setup	Create the initial configuration.	From privileged EXEC mode, enter command setup.	Prompted dialog

User EXEC Mode:
When you are connected to the router, you are started in user EXEC mode. The user EXEC commands are a subset of the privileged EXEC commands.

Privileged EXEC Mode:
Privileged commands include the following:

- Configure – Changes the software configuration.
- Debug – Display process and hardware event messages.
- Setup – Enter configuration information at the prompts.

Enter the command disable to exit from the privileged EXEC mode and return to user EXEC mode.

Configuration Mode:
Configuration mode has a set of sub-modes that you use for modifying interface settings, routing protocol settings, line settings, and so forth. Use caution with configuration mode because all changes you enter take effect immediately.
To enter configuration mode, enter the command configure terminal and exit by pressing Ctrl-Z.

Note: Almost every configuration command also has a no form. In general, use the no form to disable a feature or function. Use the command without the keyword no to re-enable a disabled feature or to enable a feature that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, enter the no IP routing command and enter IP routing to re-enable it.

Stepwise-Procedure:
Creating a simple LAN network using packet tracer –

Step 1: Select 12 PCs from the end devices and one fast ethernet switch (2950/24 ports)

Step 2: Connect PCs and switch via copper cable from the panel. Connection can be verified by appearance of all green dots on the links.

Step 3: For PCs to communicate click on PC0.

- Dialog box for PC0 appears.
- Click on desktop applications by packet tracer.
- Go to IP configuration.
- Enter IP address to identify host i.e., PC0 (for example: 192.168.1.1)
- Subnet mask-by default already set one can change it as per his/her specification.

Step 4: Repeat step 3 for PC1.

Step 5: Ping the PCs and check their working status.

Step 6: Simple PDU (Protocol Data Unit) to simulate network traffic by sending ICMP PDU to assess the network traffic. View simulation in simulation mode

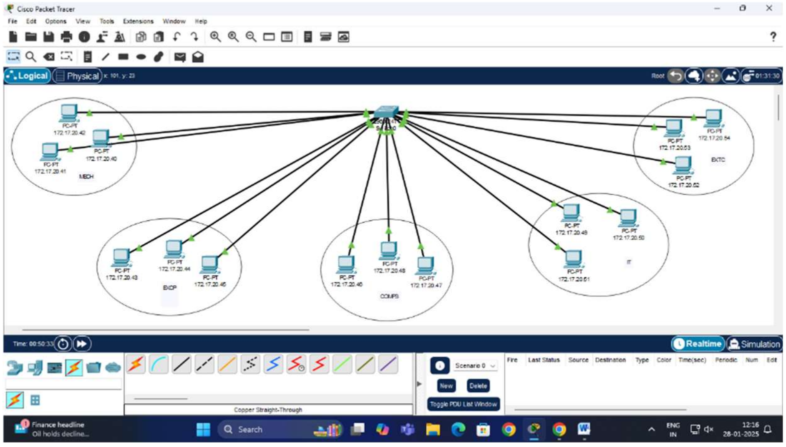
Step 7: Configure two VLAN in a switch in 6 verticals.

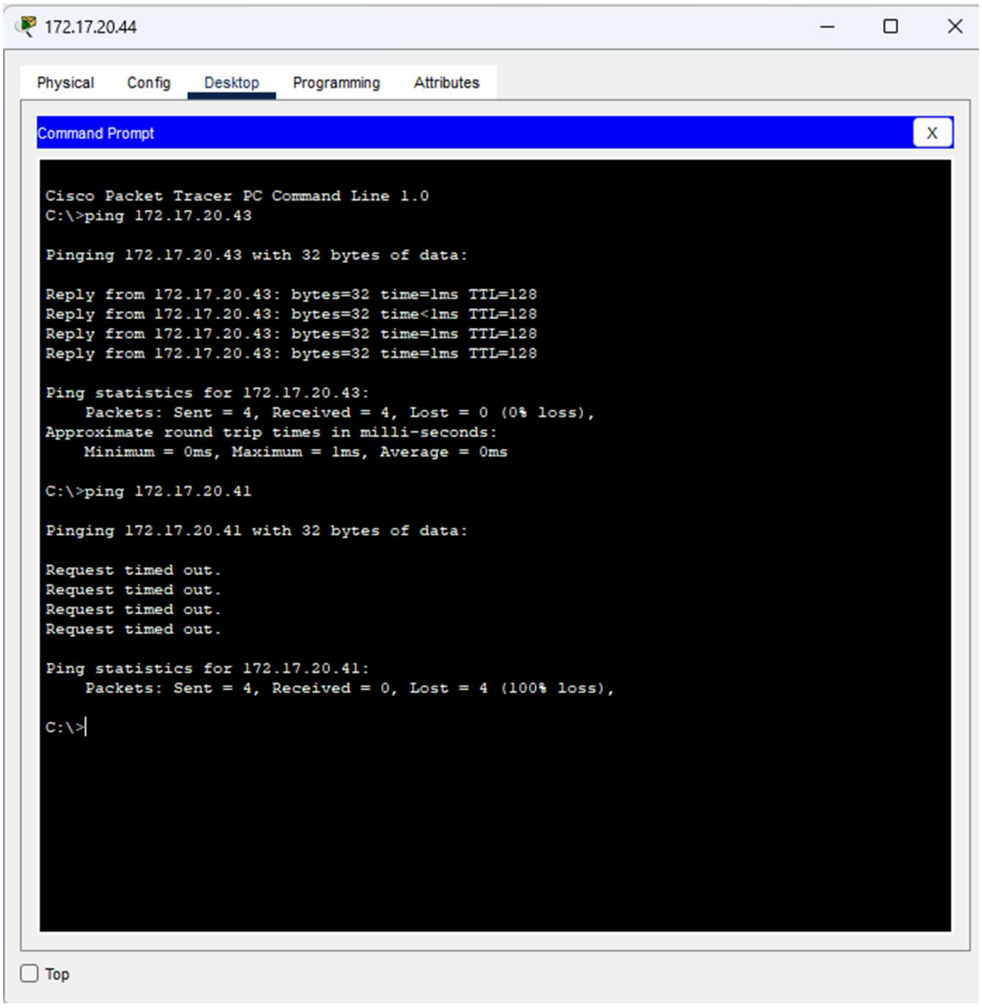
Step 8: As per design, assign membership of VLAN to port using following command.

```
# switch port access vlan2 or vlan3
```

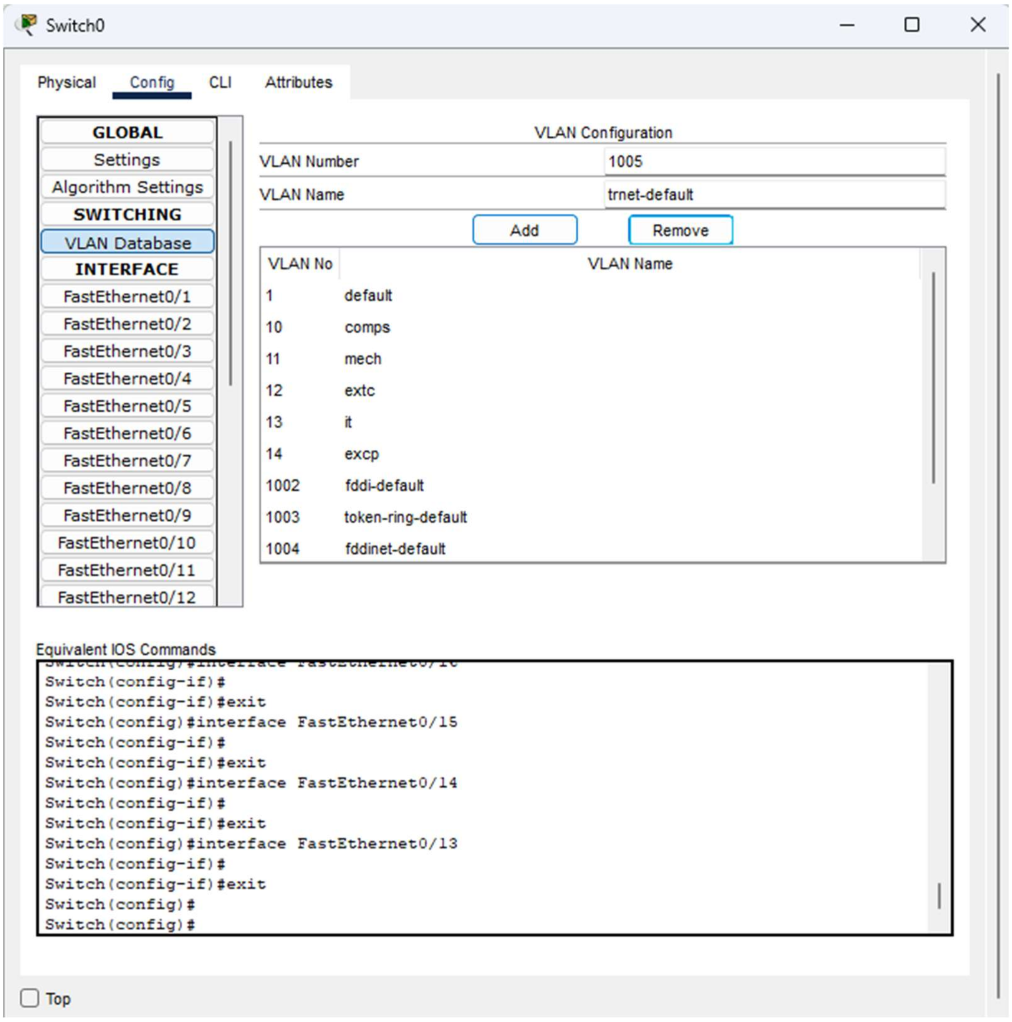
Step 9: Check the status of VLAN.

IMPLEMENTATION: (printout of code)





```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.17.20.43

Pinging 172.17.20.43 with 32 bytes of data:

Reply from 172.17.20.43: bytes=32 time=1ms TTL=128
Reply from 172.17.20.43: bytes=32 time<1ms TTL=128
Reply from 172.17.20.43: bytes=32 time=1ms TTL=128
Reply from 172.17.20.43: bytes=32 time=1ms TTL=128

Ping statistics for 172.17.20.43:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 172.17.20.41

Pinging 172.17.20.41 with 32 bytes of data:

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

Ping statistics for 172.17.20.41:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



VLAN Configuration

VLAN Number	1005
VLAN Name	trnet-default

VLAN No	VLAN Name
1	default
10	comps
11	mech
12	extc
13	it
14	excp
1002	fddi-default
1003	token-ring-default
1004	fddinet-default

Equivalent IOS Commands

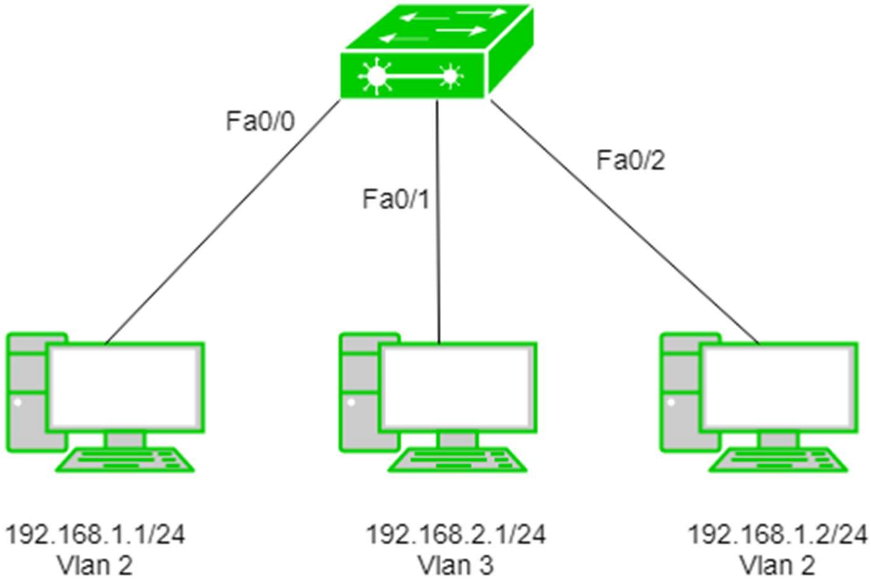
```
Switch(config)#interface FastEthernet0/16
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/15
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/14
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/13
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#
Switch(config)#
```

Post Lab Subjective/Objective type Questions:

1. **Describe the concept of Virtual LAN with the help of suitable diagram.**
   A Virtual Local Area Network (VLAN) is a logically segmented network within a single physical LAN. Instead of grouping devices based on physical connections, VLANs group them logically, improving network performance, security, and manageability.

   Key Characteristics of VLAN
   - Logical Segmentation: Devices in the same VLAN can communicate as if they were on the same physical network, even if they are in different locations.
   - Reduced Broadcast Traffic: VLANs create smaller broadcast domains, reducing unnecessary network congestion.
   - Enhanced Security: Devices in one VLAN cannot communicate with those in another VLAN unless explicitly allowed via a router or Layer 3 switch.
   - Flexibility: Devices can be reassigned to different VLANs without changing physical

cabling.



2. **Compare LAN with VLAN.**

A Local Area Network (LAN) is a network where all connected devices share the same broadcast domain. This means that any broadcast traffic is sent to all devices, which can lead to congestion as the network grows. LANs are simple to set up but lack flexibility in terms of segmentation and security.

On the other hand, a Virtual LAN (VLAN) is a logical subdivision of a LAN those groups devices based on function rather than physical location. VLANs create multiple smaller broadcast domains, reducing unnecessary traffic and improving network efficiency. Unlike a regular LAN, VLANs allow better security by isolating network segments, ensuring that only authorized devices can communicate. VLANs also provide greater flexibility, as devices can be reassigned to different VLANs without needing physical reconfiguration.

In summary, while a traditional LAN connects all devices in a shared environment, a VLAN enhances security, performance, and management by logically segmenting the network.

3. **State the benefits of implementing VLAN.**

- Improved Security: Isolates sensitive data and restricts access.
- Better Network Performance: Reduces broadcast traffic, preventing congestion.
- Scalability: Easier to manage large networks by logically grouping devices.
- Flexibility: Devices can be moved without changing physical connections.
- Cost Savings: Reduces the need for additional physical hardware.
- Simplified Management: VLANs can be managed centrally using software.

Conclusion:
We have successfully implemented virtual local area Network (LAN) connection and analyzed various networking commands.

Signature of faculty in-charge with Date: