**Name & ID**: Syed Asghar Abbas Zaidi **Date: 12th September 2023**

|  |
| --- |
| **EE-424L Data Communication & Networking**  **Fall 2021**  **Habib University**  **Dhanani School of Science & Engineering** |

LAB 4: **Switching Lab (VLAN & Trunks) on Packet Tracer**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lab #4 Marks distribution:**   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | |  |  | **LR2=30** | **LR5=40** | **LR9=10** | **AR4=20** | | **In-Lab Tasks** | **Task 1** | 10 | 15 | 10 | 20 | | **Task 2** | 10 | 15 | | **Post-Lab** | **Task 1** | 10 | 10 | | **Total Marks** | **100** | | | | |   **Lab #4 Marks Obtained:**   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | |  |  | **LR2=30** | **LR5=40** | **LR9=10** | **AR4=20** | | **In-Lab Tasks** | **Task 1** |  |  |  |  | | **Task 2** |  |  | | **Post-Lab** | **Task 1** |  |  | | **Marks Obt.** |  | | | | | |

|  |  |
| --- | --- |
| o**bjectives** | **The objective of this lab is to build a network to configure and verify VLANs on Packet Tracer.** |

**In-Lab Tasks:**

|  |
| --- |
| **Task 1: Implementation of VLAN on Packet Tracer (Topology 1)** |
| **Task 2: Implementation of VLAN on Packet Tracer (Topology 2)** |

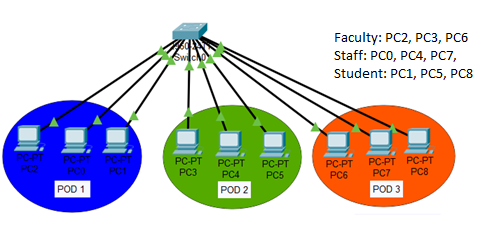
**Introduction**

**VLANs**

Virtual LANs (VLANs) allow network administrators to subdivide a physical network into separate logical broadcast domains. On a standard Layer 2 network, all hosts connected to a switch are members of the same broadcast domain; and broadcast domains can only be physically separated across different switches by routers.

A VLAN represents a broadcast domain. VLANs are identified by a VLAN ID (a number between 0 – 4095), with the default VLAN on any network being VLAN 1. Each port on a switch or router can be assigned to be a member of a VLAN (i.e., to allow receiving and sending traffic on that VLAN). For example: on a switch, traffic that is sent to a port that is a member of VLAN 100, may be forwarded to any other VLAN 100 port on the switch, and it can also travel across a trunk port (connections between switches) to another switch and forwarded to all VLAN 100 ports on that switch. Traffic won't, however, be forwarded to ports that are on a different VLAN ID. This effectively allows a network administrator to logically split up a switch, allowing multiple broadcast domains to coexist on the same hardware, but maintaining the isolation, security, and performance benefits of using completely separate switches**.**

To understand VLAN more clearly let's take an example.



Our campus has three pods. All pods are connected with back links via switch. In each pod, there are some Faculty, Staff and Students PCs available.

* Campus has mainly three departments Faculty, Staff and Students
* Faculty department has three computers.
* Staff department has three computers.
* Students department also has three computers.
* Each pod has one PC from faculty and one from both staff and students department.
* Faculty and Staff department have sensitive information and need to be separate from Students department.

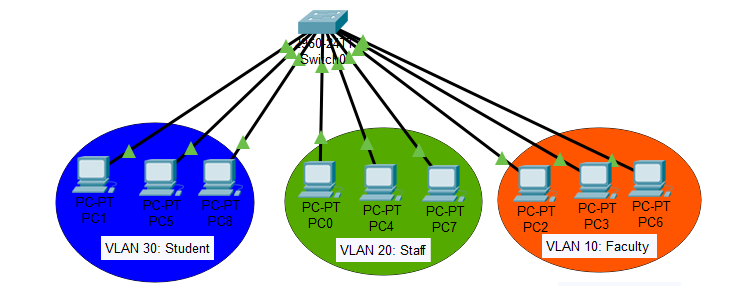
With default configuration, all computers share same broadcast domain. All departments can share the resources. With VLAN we could create logical boundaries over the physical network. Assume that we created three VLANs for our network and assigned them to the related computers.

VLAN **Faculty** for Faculty department

VLAN **Staff** for Staff department

VLAN **Stud** for Students department

Physically we changed nothing but logically we grouped devices according to their function. These groups [VLANs] need router to communicate with each other. Logically our network look likes following diagram.

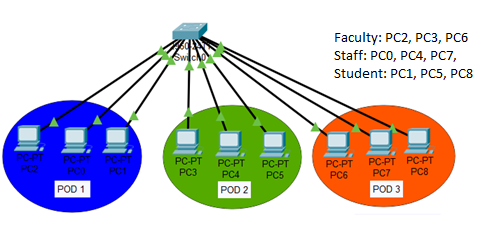


With the help of VLAN, we have separated our single network in three small networks. These networks do not share broadcast with each other improving network performance.

VLAN also enhances the security. Now faculty department cannot access the staff and students department directly.

**Task 1:**

TOPOLOGY: Consider the below Topology where one switch is connected with three different departments.



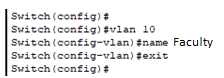
**Step 1:** Build this topology on Packet Tracer and write down your observation in terms of Ping, Broadcast and Collision domain. You can choose any one network address and assign IPs from that network to all PCs. Mention network address and IPs of all devices in Network topology.

|  |
| --- |
| **TOPOLOGY:  DESCRIPTION:**  In this star topology, we will be reserving the Network ID and in the diagram, every PCs’ IP Addresses and Mac Addresses have been written. I have also detailed which PCs belongs to whom. **OBSERVATION:**  Without Pinging, the switch was able to successfully able to know which PC the packet was intended for. There was no Collision observed in my simulation |

Step 2: Run show VLAN brief command in privilege mode and mention How many VLANs are there and mention number assigned to them? Write down number of ports/interfaces assigned to each VLAN?

|  |
| --- |
|  |

You can create VLAN 10 for faculty on switch 0 by using below commands. Similarly, Create VLAN 20 & 30 on Switch for Staff and Students respectively.

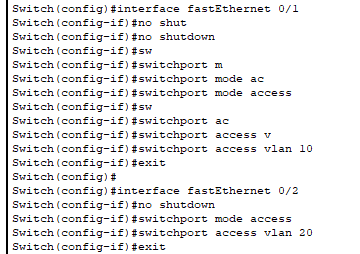
****

Run show VLAN brief command again and write down your observation.

|  |
| --- |
| Running the appropriate Commands:  Running the “Show VLAN” command in privilege mode again:  Now creating more VLANS 20 and 30:    As can be observed, VLAN 10,20,30 (Faculty, Staff, Students) were respectively successfully created. |

**Step 3:** Enable the Access Ports & assign ports/interfaces of switch to respective VLAN.

Note: Make sure to note which port of switch is connected with PCs. After enter in interface fast Ethernet 0/1, it is important to run “no shutdown” command to up the link.

****

Similarly, assign remaining ports of switch connected to VLAN 10, 20 and 30. Run show VLAN brief and write down your findings and attach screenshot.

|  |
| --- |
| **After doing the appropriate Coding:**  It’s important to note that PC0 is connected to Port 1 of our switch, PC2 is connected to Port 3 and so on.    **Attached this screenshot a bit later, so apologies for any discrepancies:**    **CLI Terminal Working:** |

Ping any two PCs of VLAN 10 and write down your observation.

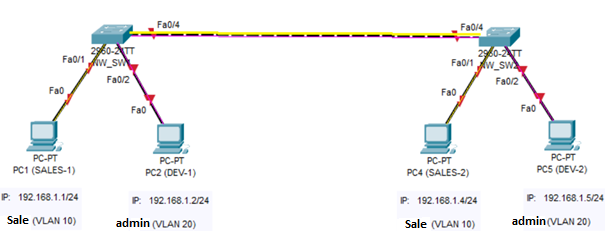
|  |
| --- |
| **Observations:** As can be observed, our PC0 (192.168.1.109) connected to Port 1 was successfully able to ping PC3(192.168.1.103) connected to Port 4. Both of these PCs belonged to VLAN 10 |

Ping any PC of VLAN 10 to any PC of VLAN 20 and write down your observation.

|  |
| --- |
| **Observations:** As can be observed, our PC0 (192.168.1.109) belonging to VLAN 10 connected to Port 1 of the Switch failed to ping PC1(192.168.1.101) belonging to VLAN 20 connected to Port 2. Both of these PCs belonged to different VLANs unlike the previous task we did! |

**Task 2:**

TOPOLOGY: Consider the following Lab Topology where two Switches are connected to each other and have different department PC’s connected to them:

****

**Step 1:** Build this topology on Packet Tracer and write down your observation in terms of Ping, Broadcast and Collision domain.

|  |
| --- |
| **Observations:** I am pinging from PC1 to PC3, I observe the packet going to Switch 0, which broadcasts to Switch 1 and PC2, PC2 rejects the packet here.  In Switch 1, the packet is then broadcasted to PC3 and PC4, PC4 rejects the packet while PC3 accepts the packet and sends it back to the switch 1, which then redirects the packet to switch 0, which redirects the packet to PC1. |

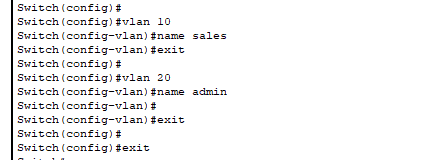
**Step 2: Configure VLANs on SW1 and SW2**

**Attach screenshot of your Network Topology and fill the below table as per you network requirements.**

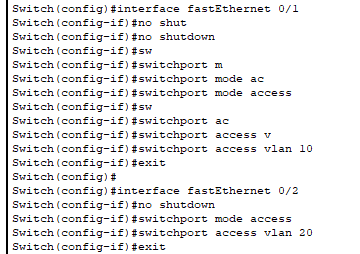
|  |
| --- |
| **Topology: All labelled interfaces, IPs, VLANs should be shown in network topology diagram.** |

|  |  |  |
| --- | --- | --- |
| **Device** | **Switch port and which PC connected to Switch** | **VLAN (to be assigned)** |
| **SW1** | PC1 (SALES-1) | 10 |
| **SW1** | PC2 (DEV-1) | 20 |
| **SW1** | -- | -- |
| **SW2** | PC-3 (SALES-2) | 10 |
| **SW2** | PC-4 (DEV-2) | 20 |
| **SW2** | -- | -- |

You can create VLAN 10 by using below commands. Similarly, Create VLANs on Switch 1 and Switch 2.

****

Enable the Access Ports & assign VLANs accordingly on SW1 and SW2:

****

Similarly, assign remaining ports to other VLANs.

|  |
| --- |
| **Showcasing setup of VLAN 10 and 20 on Switch (Our First Switch):**    **Showcasing setup of VLAN 10 and 20 on Switch-1 (Our Second Switch):** |

Run **show Vlan Brief** command on both switches. Write down your observation and attach the screenshot below:

|  |
| --- |
| **Running “show Vlan Brief” on privileged mode on Switch-0:**    **Running “show Vlan Brief” on privileged mode on Switch-1:** |

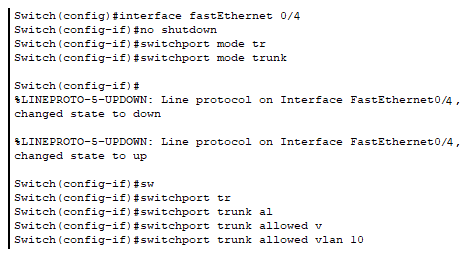
**Verification of VLANs:**

1. Ping PC1(SALES-1) to PC4(SALES-2)
2. Ping PC2(admin-1) to PC5(admin-2)
3. Ping PC1(SALES-1) to PC2(admin-1)

Comment on above verification.

|  |
| --- |
| **Ping PC1(SALES-1) to PC3(SALES-2): LOSS**    **Ping PC2(DEV-1) to PC4(DEV-2): LOSS**    **Ping PC1(SALES-1) to PC2(DEV-1): LOSS**  **OBSERVATIONS:** All packets were lost in all scenarios! |

Configure the Trunk Ports & Allow the VLANs through them:

****

**Verification of VLANs:**

1. Ping PC1(SALES-1) to PC4(SALES-2)
2. Ping PC2(admin-1) to PC5(admin-2)
3. Ping PC1(SALES-1) to PC2(admin-1)

Comment on above verification.

|  |
| --- |
| **Ping PC1(SALES-1) to PC3(SALES-2): SUCCESSFUL**    **Ping PC2(DEV-1) to PC4(DEV-2):**    **Ping PC1(SALES-1) to PC2(DEV-1):**  **OBSERVATIONS:**  Here, we can observe the result of us truncating VLAN 10 in both switches. It is now allowing me to successfully ping the other PC that is connected to “other” switch, but cause they both share the same VLAN, or are part of the same Virtual LAN, it is allowing me to ping it. However, as we still haven’t truncated VLAN 20, it is not allowing to ping from DEV to DEV (Admin to Admin). As Sales and Dev (Admin) belong to different VLAN, their failure to connect is to be expected. |

Now allow VLAN 20 in trunk mode and note down your observation.

|  |
| --- |
| **Doing this at both switches:**    **Ping PC1(SALES-1) to PC3(SALES-2): Failed**    **Ping PC2(DEV-1) to PC4(DEV-2): SUCCESSFUL**    **Ping PC1(SALES-1) to PC2(DEV-1): FAILED**    **Observations:** We can observe that as we have truncated VLAN 20 in both switches, it has resulted in VLAN 10 Truncation being removed. As such, both Sales’ PCs that existed beyond different switches weren’t able to ping each other this time. However, as we DID truncate VLAN 20, the Devs’ PCs that existed beyond different switches successfully pinged each other. Even in this scenario, cause Sales and Dev are on different VLANs, our last case failed even though the Dev PC in-question didn’t exist beyond “different switch” |

What do you understand by Access and Trunk port?

|  |
| --- |
| **ACCESS PORT:**  This is the “port” that can be assigned to a single VLAN (Virtual Local Area Network), or to a device that belongs to any “specific” VLAN. **TRUNK PORT:**  Trunk Port is the “port” on the switch that is connected to another “switch” device (similar devices) |

Run show interface trunk command in privilege mode and discuss the results.

|  |
| --- |
| **Running this command on Switch 0:** |

After checking the above tasks to RA. Remove the configured VLANs, Assign the interfaces back to VLAN 1. Write down the commands below and attach screenshot too. Check this to RA.

|  |
| --- |
| **CODE:**  **Observe how our Ports weren’t assigned to VLAN 1 despite us removing VLAN 10 and 20. We need to re-assign those ports back!!**  **SHOWING VLANS!** |

**Post Lab: Have it so that you are able to truncate both VLAN 10 and 20 “together”, allow both switches to handle VLAN 10 and 20 traffic together.**

|  |
| --- |
| **LOGIC:** Truncating VLAN 10 and 20 both together so that it allows both of their traffic together.  **Coding:**  **Verification:**  **Ping PC1(SALES-1) to PC3(SALES-2): SUCCESSFUL**    **Ping PC2(DEV-1) to PC4(DEV-2): SUCCESSFUL**    **Ping PC1(SALES-1) to PC2(DEV-1): FAILED**    **VERIFIED!!**  **OBSERVATIONS:**  As we are allowing the traffic of both VLAN 10 and 20 between our switches, Sales-1 was successfully able to ping Sales-2, Dev-1 (Admin-1) was successfully able to ping Dev-2 (Admin-2) however, as Sales-1 and Dev-1 are on a different VLAN (Virtual Local Area Network), it is to be expected that the ping will not succeed. We can observe all of these results above in the screenshots as well as “pkt” file I have attached.  **Thank you!** |

**Lab Evaluation Assessment Rubric**

**EE-424 Lab 4**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Assessment Elements** | **Level 1: Unsatisfactory**  **Points 0-1** | **Level 2: Developing**  **Points 2** | **Level 3: Good**  **Points 3** | **Level 4: Exemplary**  **Points 4** |
| **LR2** | **Program/Code/ Simulation Model/ Network Model** | Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software. | Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software. | Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine. | Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software. |
| **LR5** | **Results & Plots** | Figures/ graphs / tables are not developed or are poorly constructed with erroneous results. Titles, captions, units are not mentioned. Data is presented in an obscure manner. | Figures, graphs and tables are drawn but contain errors. Titles, captions, units are not accurate. Data presentation is not too clear. | All figures, graphs, tables are correctly drawn but contain minor errors or some of the details are missing. | Figures / graphs / tables are correctly drawn and appropriate titles/captions and proper units are mentioned. Data presentation is systematic. |
| **LR9** | **Report** | All the in-lab tasks are not included in report. | Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. | Good summary of most of the in-lab tasks is included in report. The work is supported by figures and plots with explanations. | Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables. |
| **AR2** | **Attendance** | Marked attendance and did not attend the lab or left very early. | Present but very late (31-60 minutes) or left early (31-60 minutes) without completing the tasks. | \*Present but late (15-30 minutes), or left early (30 minutes) without completing the tasks. | Present and entered the lab on time and left on time. |
| **AR4** | **\*Report Submission** | Late submission after 1 week and in between 2 weeks. | Late submission after 2 days and within a week. | Late submission after the lab timing and within 2 days of the due date. | Timely submission of the report and in the lab time. |

**\*Report:** Report will not be accepted after 1 week of due date