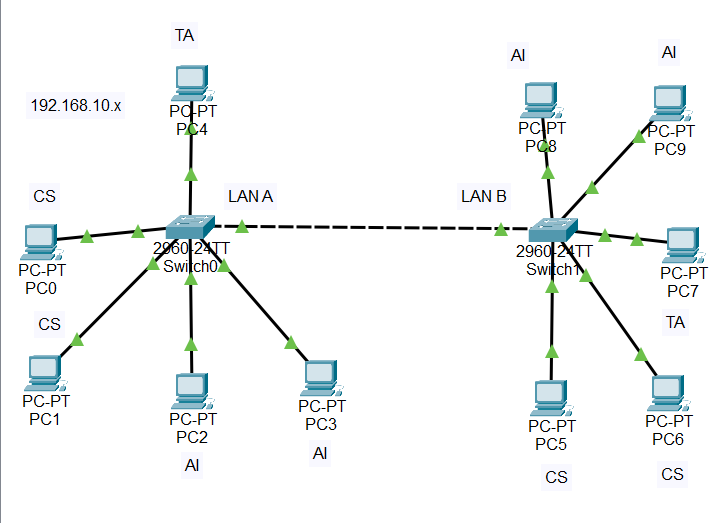
***CS21B2028***

***NITIN REDDY K***

**VLAN Implementation:**

****

Here we have taken two switches each having 2 CS students,2 AI Students, and 1 TA respectively.

We have connected TA first, that is TA gets Ethernet port 1.

Next two CS students get connected, and they get Ethernet ports 2 and 3.

Next two AI students get connected, and they get Ethernet ports 4 and 5.

The switch configuration is done so that in VLan Database, we enter the following:

VLan No of TA is 300, CS Student is 100, and AI student is 200. We configure fast ethernet accordingly.

**(a)Advantages of VLAN:**

**Network Segmentation**: VLANs allow you to logically segment a physical network into smaller, isolated virtual networks. This segmentation helps in isolating different groups of devices, departments, or traffic types, preventing unnecessary communication and enhancing network efficiency.

**Security**: VLANs enhance network security by isolating sensitive or critical data from other parts of the network. This isolation prevents unauthorized access and reduces the risk of data breaches. Even if an attacker gains access to one VLAN, they won't automatically have access to other VLANs.

**Broadcast Control**: In traditional Ethernet networks, broadcasts and multicasts are sent to all devices on the same physical network segment. With VLANs, broadcast domains are divided, reducing unnecessary broadcast traffic and preventing broadcast storms that can degrade network performance.

**Efficient Resource Utilization**: VLANs allow for better utilization of network resources. By segregating traffic, you can allocate bandwidth more effectively and prioritize critical applications over less important ones.

**Flexibility and Scalability**: VLANs enable network administrators to easily add, remove, or relocate devices without changing the physical network infrastructure. This makes network expansion and changes more efficient and cost-effective.

**(b)Disadvantages of VLAN:**

**Complexity**: Implementing and managing VLANs can be complex, especially for larger networks. Proper planning, configuration, and monitoring are required to ensure that VLANs are set up correctly and functioning as intended.

**Configuration** **Errors**: Misconfiguration of VLANs can lead to network issues, security vulnerabilities, and communication problems. If VLANs are not set up properly, devices from different VLANs might not be able to communicate when they should or could communicate when they shouldn't.

**Administrative Overhead**: While VLANs can simplify network management in some ways, they can also increase administrative workload. Network administrators need to be proficient in configuring and troubleshooting VLANs, which may require specialized knowledge and training.

**Resource Overallocation**: Poorly planned VLAN configurations can lead to inefficient use of network resources. If VLANs are created in excess without proper segmentation, it can result in unnecessary complexity and reduced overall network performance.

**Limited Broadcast Domain**: While VLANs help control broadcast traffic, they can also limit certain types of communication that require broadcast or multicast capabilities across multiple VLANs. This might necessitate additional network infrastructure to enable cross-VLAN communication.

**(c) Inter-VLAN communication:**

While VLANs by default keep traffic separate, they can still communicate with each other through a router. This controlled communication enables secure data exchange between isolated VLANs.