**Title:   
Design of campus area network using Virtual Local Area Network(VLAN) with Physical Network Security Implementation and connectivity of Internet with wired and wireless access.**

***ABSTRACT***

A LAN includes all the user devices, servers, switches, routers, cables, and wireless access points in one location. A LAN includes all devices in the same broadcast domain. A broadcast domain includes the set of all LAN-connected devices, so that when any of the devices sends a broadcast frame, all the other devices get a copy of the frame. So, from one perspective, a LAN and a broadcast domain as being basically the same thing. Without VLANs, a switch considers all its interfaces to be in the same broadcast domain. That is, for one switch, when a broadcast frame entered one switch port, the switch forwarded that broadcast frame out all other ports. With that logic, to create two different LAN broadcast domains, needs two different Ethernet LAN switches.

With support for VLANs, a single switch can accomplish the same goals of the design to create two broadcast domains—with a single switch. With VLANs, a switch can configure some interfaces into one broadcast domain and some into another, creating multiple broadcast domains. These individual broadcast domains created by the switch are called virtual LANs (VLAN).

Designing campus LANs to use more VLANs, each with a smaller number of devices, often helps improve the LAN in many ways. For example, a broadcast sent by one host in a VLAN will be received and processed by all the other hosts in the VLAN—but not by hosts in a different VLAN. Limiting the number of hosts that receive a single broadcast frame reduces the number of hosts that waste effort processing unneeded broadcasts. It also reduces security risks, because fewer hosts see frames sent by any one host.   
These are just a few reasons for separating hosts into different VLANs.

The following list summarizes the most common reasons for choosing to create smaller broadcast domains (VLANs):

* To reduce CPU overhead on each device by reducing the number of devices that receive each broadcast frame.
* To reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood (broadcasts, multicasts, and unknown unicasts)
* To improve security for hosts that send sensitive data by keeping those hosts on a separate VLAN
* To create more flexible designs that group users by department, or by groups that work together, instead of by physical location
* To solve problems more quickly, because the failure domain for many problems is the same set of devices as those in the same broadcast domain.

**Project Description**

In this Project trainee should design a college campus area Network with VLANs with different Hosts and Departments as per the following requirement.

1. College campus is a (Ground + 4 ) 5 Floor building.
2. Ground Floor have 100Mbps connectivity to ISP for Internet with a CISCO 2811 Router with a single LAN port .
3. First, second, Third and Fourth floors have Hosts belongs to CSC/IT//ECE/EEE departments related to I year, II year, III Year and Final year students class rooms. Each Floor has a switch connecting these hosts.
4. Switch from the top floor is connected directly to its next floor switch and finally from the First floor switch, a cable is extended to ground floor to the LAN port of CISCO Router 2811.
5. Administrator has been asked to configure the departments in different VLAN domains and also instructed that the communication between the departments is also required.
6. Administrator has been asked to place an Access point for wireless connectivity with security password from the Fourth Floor on need basis
7. Administrator has been asked to create security credentials for login to the Router and Switches such that authorized person only logs in.
8. Administrator has been asked to make sure that if anyone connect a PC in the vacant ports of switch in any floor they should not be connected to Network.
9. Administrator has been asked to allocate 40 Mbps bandwidth to CSC department, 30 Mbps bandwidth to IT department, 20 Mbps bandwidth for ECE department & 10 Mbps bandwidth to EEE department for Internet access.
10. ISP has given 10.10.10.0/30 subnet to college and asked the administrator to configure the WAN link IP 10.10.10.1 at College side WAN interface on Router. The Internet IP pool given to college by ISP is 117.117.117.0/29.
11. Administrator has been instructed to make sure that all computers available in the campus should be connected with Internet (except 192.168.2.3)
12. Administrator has been asked put college website IP as 117.117.117.3 and this website has to be accessed from Internet.  
     (Please Take any Class C, IP Pool s for the LAN networks connectivity)
13. DHCP Protocol and Configuration of DHCP on CISCO Router for automatic assignment of IP addresses.
14. Configuration of DNS entries for browsing using URL.

Note :

1. Sessions will be taken on the required topics of the project in the third week.
2. Trainee is the college Network Administrator and he/she has to design the campus area network in CISCO Packet Tracer software and complete the jobs mentioned above.
3. A Project review will be there on Monday ( 4Th Week First day).
4. After completion of the project trainee has to prepare the final project report in soft copy format and submit on the last day of the course.
5. After evaluation / discussion certificate will be issued.

[deviprasadmadiraju@gmail.com](mailto:deviprasadmadiraju@gmail.com)

9490118909