HACETTEPE UNIVERSITY
COMPUTER ENGINEERING DEPARTMENT
COMPUTER NETWORKS LABORATORY

EXPERIMENT 2

Virtual LAN - VLAN

INTRODUCTION

Reading part from course text book, Chapter 5

5.4.4 Virtual Local Area Networks (VLANs)

In our earlier discussion of Figure 5.15, we noted that modern institutional LANs are often configured hierarchically, with each workgroup (department) having its own switched LAN connected to the switched LANs of other groups via a switch hierarchy. While such a configuration works well in an ideal world, the real world is often far from ideal. Three drawbacks can be identified in the configuration in Figure 5.15:

- *Lack of traffic isolation.* Although the hierarchy localizes group traffic to within a single switch, broadcast traffic (e.g., frames carrying ARP and DHCP messages or frames whose destination has not yet been learned by a selflearning switch) must still traverse the entire institutional network. Limiting the scope of such broadcast traffic would improve LAN performance. Perhaps more importantly, it also may be desirable to limit LAN broadcast traffic for security/privacy reasons. For example, if one group contains the company's executive management team and another group contains disgruntled employees running Wireshark packet sniffers, the network manager may well prefer that the executives' traffic never even reaches employee hosts. This type of isolation could be provided by replacing the center switch in Figure 5.15 with a router. We'll see shortly that this isolation also can be achieved via a switched (layer 2) solution
- *Inefficient use of switches.* If instead of three groups, the institution had 10 groups, then 10 first-level switches would be required. If each group were small, say less than 10 people, then a single 96-port switch would likely be large enough to accommodate everyone, but this single switch would not provide traffic isolation.
- *Managing users.* If an employee moves between groups, the physical cabling must be changed to connect the employee to a different switch in Figure 5.15. Employees belonging to two groups make the problem even harder.

Fortunately, each of these difficulties can be handled by a switch that supports **virtual local area networks** (**VLANs**). As the name suggests, a switch that supports VLANs allows multiple *virtual* local area networks to be defined over a single *physical* local area network infrastructure. Hosts within a VLAN communicate with each other as if they (and no other hosts) were connected to the switch. In a port-based VLAN, the switch's ports (interfaces) are divided into groups by the network manager. Each group constitutes a VLAN, with the ports in each VLAN forming a broadcast domain (i.e., broadcast traffic from

one port can only reach other ports in the group). Figure 5.25 shows a single switch with 16 ports. Ports 2 to 8 belong to the EE VLAN, while ports 9 to 15 belong to the CS VLAN (ports 1 and 16 are unassigned).

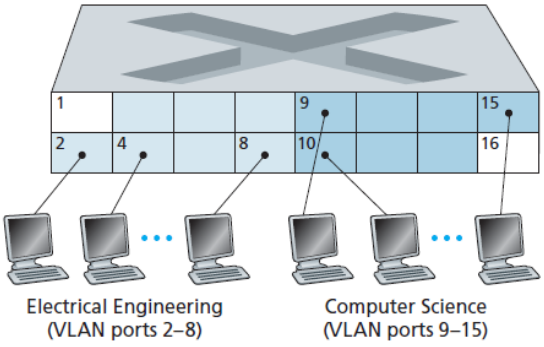

Figure 5.25 ♦ A single switch with two configured VLANs

This VLAN solves all of the difficulties noted above— EE and CS VLAN frames are isolated from each other, the two switches in Figure 5.15 have been replaced by a single switch, and if the user at switch port 8 joins the CS Department, the network operator simply reconfigures the VLAN software so that port 8 is now associated with the CS VLAN. One can easily imagine how the VLAN switch is configured and operates—the network manager declares a port to belong to a given VLAN (with undeclared ports belonging to a default VLAN) using switch management software, a table of port-to-VLAN mappings is maintained within the switch; and switch hardware only delivers frames between ports belonging to the same VLAN.

But by completely isolating the two VLANs, we have introduced a new difficulty! How can traffic from the EE Department be sent to the CS Department? One way to handle this would be to connect a VLAN switch port (e.g., port 1 in Figure 5.25) to an external router and configure that port to belong both the EE and CS VLANs. In this case, even though the EE and CS departments share the same physical switch, the logical configuration would look as if the EE and CS departments had separate switches connected via a router. An IP datagram going from the EE to the CS department would first cross the EE VLAN to reach the router and then be forwarded by the router back over the CS VLAN to the CS host. Fortunately, switch vendors make such configurations easy for the network manager by building a single device that contains both a VLAN switch *and* a router, so a separate external router is not needed. A homework problem at the end of the chapter explores this scenario in more detail.

Returning again to Figure 5.15, let's now suppose that rather than having a separate Computer Engineering department, some EE and CS faculty are housed in a separate building, where (of course!) they need network access, and (of course!) they'd like to be part of their department's VLAN. Figure 5.26 shows a second 8-port switch, where the switch ports have been defined as belonging to the EE or the CS VLAN, as needed. But how should these two switches be interconnected? One easy solution would be to define a port belonging to the CS VLAN on each switch (similarly for the EE VLAN) and to connect these ports to each other, as shown in Figure 5.26(a). This solution doesn't scale, however, since *N* VLANS would require *N* ports on each switch simply to interconnect the two switches.

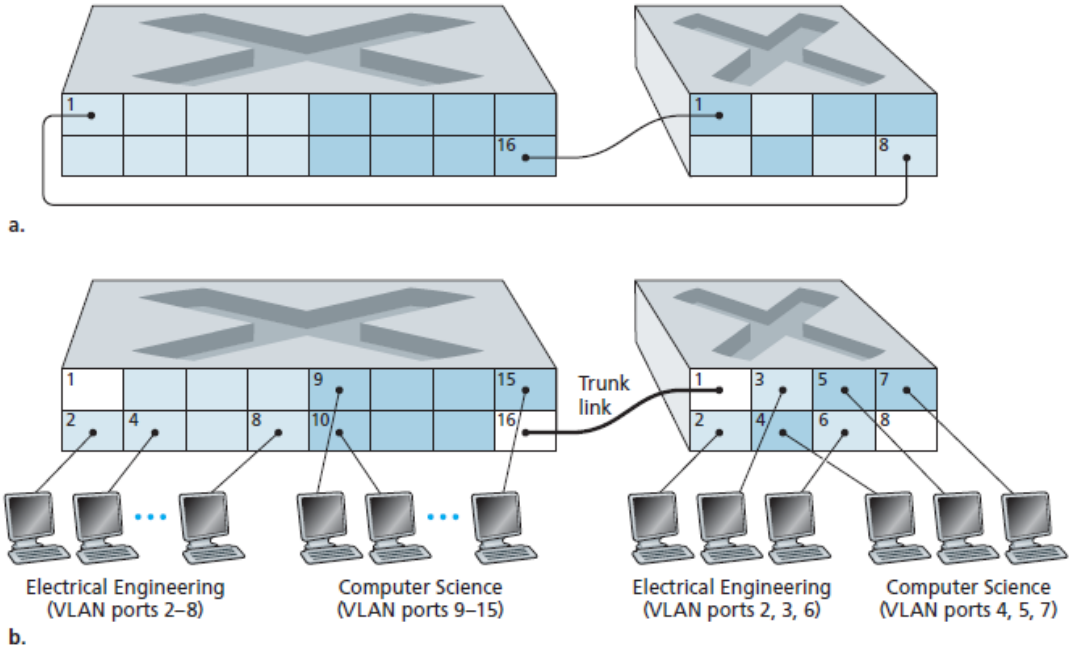

Figure 5.26 ♦ Connecting two VLAN switches with two VLANs: (a) two cables (b) trunked

A more scalable approach to interconnecting VLAN switches is known as **VLAN trunking**. In the VLAN trunking approach shown in Figure 5.26(b), a special port on each switch (port 16 on the left switch and port 1 on the right switch) is configured as a trunk port to interconnect the two VLAN switches. The trunk port belongs to all VLANs, and frames sent to any VLAN are forwarded over the trunk link to the other switch. But this raises yet another question: How does a switch know that a frame arriving on a trunk port belongs to a particular VLAN? The IEEE has defined an extended Ethernet frame format, 802.1Q, for frames crossing a VLAN trunk. As shown in Figure 5.27, the 802.1Q frame consists of the standard Ethernet frame with a four-byte **VLAN tag** added into the header that carries the identity of the VLAN to which the frame belongs. The VLAN tag is added into a frame by the switch at the sending side of a VLAN trunk, parsed, and removed by the switch at the receiving side of the trunk. The VLAN tag itself consists of a 2-byte Tag Protocol Identifier (TPID) field (with a fixed hexadecimal value of 81-00), a 2-byte Tag Control Information field that contains a 12-bit VLAN identifier field, and a 3-bit priority field that is similar in intent to the IP datagram TOS field.

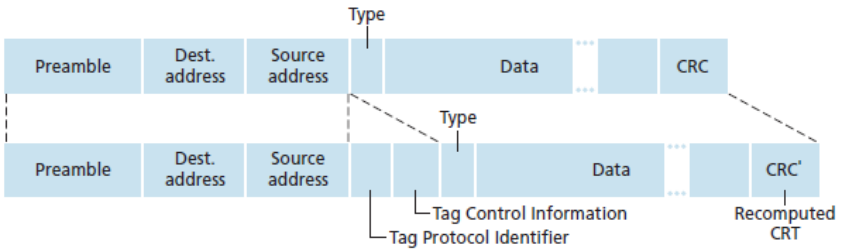

Figure 5.27 ♦ Original Ethernet frame (top), 802.1Q-tagged Ethernet VLAN frame (below)

In this discussion, we've only briefly touched on VLANs and have focused on port-based VLANs. We should also mention that VLANs can be defined in several other ways. In MAC-based VLANs, the network manager specifies the set of MAC addresses that belong to each VLAN; whenever a device attaches to a port, the port is connected into the appropriate VLAN based on the MAC address of the device. VLANs can also be defined based on network-layer protocols (e.g., IPv4, IPv6, or Appletalk) and other criteria. See the 802.1Q standard [IEEE 802.1q 2005] for more details.

EXPERIMENT STEPS

1. In this experiment you're going to create a network similar to one in previous lab. You should virtually group computers as shown in Figure-1 using VLAN configuration on Cisco Switches.

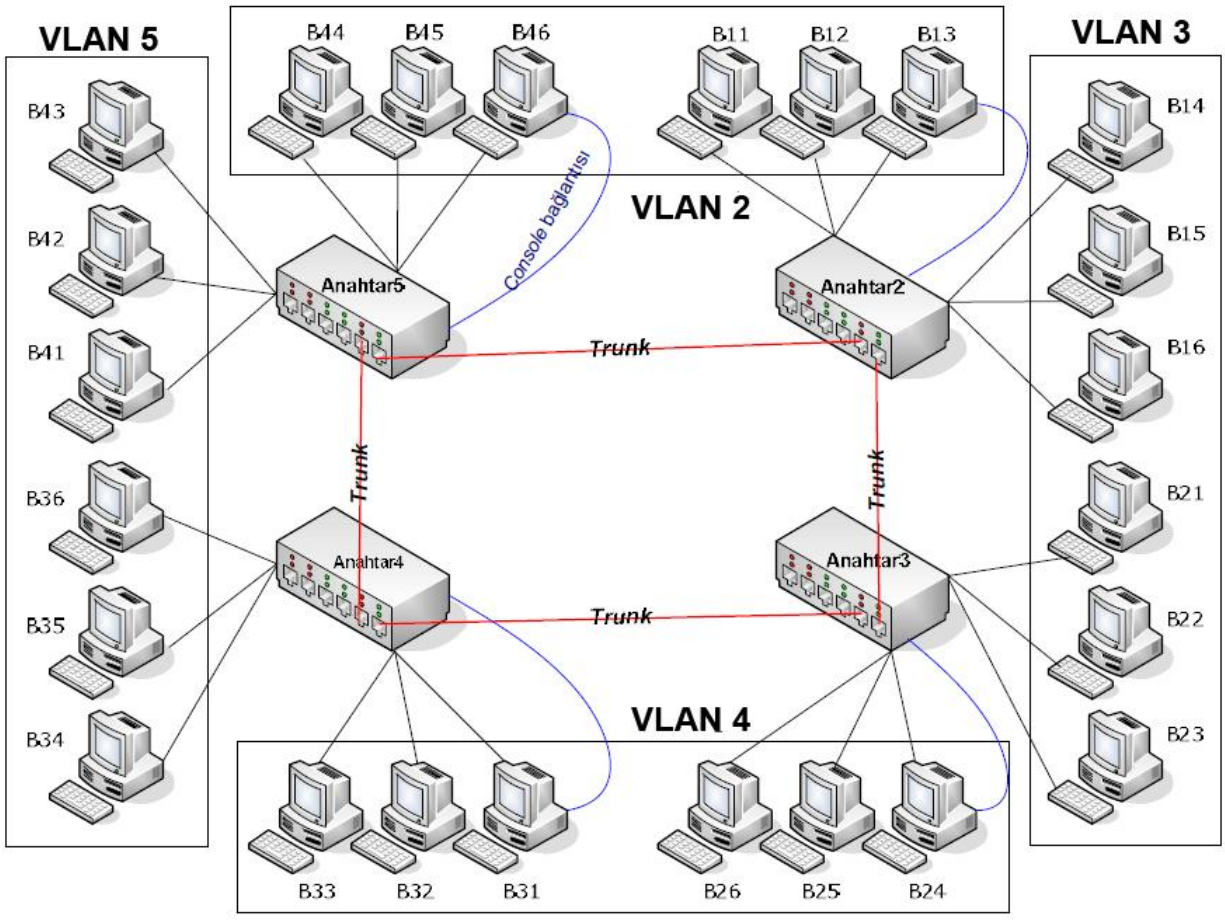

Figure 1 - VLAN grouping

2. Assign IP addresses to your computers' *eth0* adapter as described in the Table-1 similar to previous Lab. Make sure that all computers are connected to the network and all can be pinged.

Group name	IP address	Subnet mask
Grup1	10.100.10.1 - 10.100.10.6	255.255.0.0
Grup2	10.100.20.1 - 10.100.20.6	255.255.0.0
Grup3	10.100.30.1 - 10.100.30.6	255.255.0.0
Grup4	10.100.40.1 - 10.100.40.6	255.255.0.0

3. Switches can be configured via telnet or console connection. We are going to use console connection using console (blue) cable. You should select one computer from

your group which has a console cable attached to its onboard serial port. Then just plug the RJ-45 end of the cable to Switch's console port on the back side.

4. In Unix systems, there is a tool called **minicom** which can use serial port of the system and send keystrokes to the terminal attached. So enter *minicom* from console of the computer (which is connected to the switch) and enter into the Cisco device command line interface.
5. You should see something like: **Switch>** after pressing Enter for a couple of times.
6. Now you are in the Cisco IOS operating system, and you can only use Cisco commands for configuration or troubleshooting. You can enter **?** command and see which commands you can use in that level.
7. Now you are ready to configure VLAN settings according to Figure-1. You have to associate related ports with described VLANs and define Trunk links between Switch connections.
8. Here is the commands that you are going to use:

Creating a new VLAN
Switch> enable
Switch# vlan database
Switch(vlan)# vlan <VLAN ID> [name <vlan name>]
Switch(vlan)# exit
Switch#

Assignment of a switch port to a VLAN
Switch> enable
Switch# configure terminal
Switch(config)# interface fastEthernet0/<port no>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan <vlan numarası>
Switch(config-if)# exit
Switch(config)# Ctrl-Z
Switch#

Assignment of a switch port to trunk mode
Switch> enable
Switch# configure terminal
Switch(config)# interface fastEthernet0/<port no>
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
Switch(config)# Ctrl-Z
Switch#

Displaying vlan-interface table
Switch> enable
Switch# show vlan

9. If all four switch configurations were completed, now ping from a computer to one that is in your group but in a different VLAN. And try ping to another group but in the same VLAN.

REFERENCES

- Computer Networks: A top-down approach, Kurose and Ross, 6th Edition, Addison-Wesley
- http://www.ciscopress.com/articles/article.asp?p=2181836&seqNum=4
- http://www.cisco.com/c/en/us/td/docs/ios/lanswitch/command/reference/lsw_book.pdf