LAB No 11 **Date:**

Design of VLANs Using GNS3

Objectives:

- To understand Virtual Lan(VLAN) Concepts

We can solve many of the problems associated with layer 2 switching with VLANs. VLANs work like this: Figure 12.1 shows all hosts in this very small company connected to one switch, meaning all hosts will receive all frames, which is the default behavior of all switches.

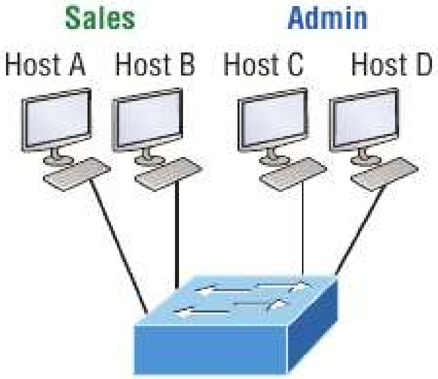


Fig 12.1 *One switch, one LAN: Before VLANs, there were no separations between hosts.*

If we want to separate the host's data, we could either buy another switch or create virtual LANs, as shown in Figure 12.2

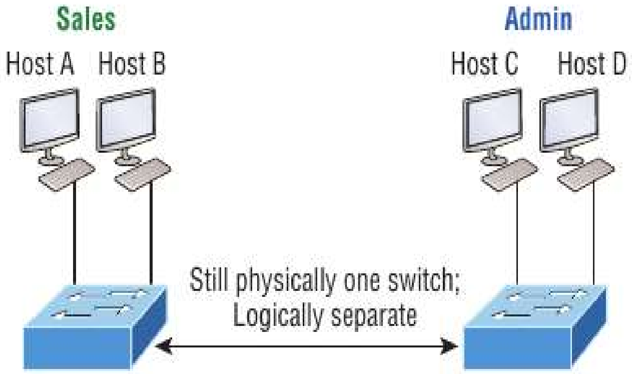


Fig 12.2 *One switch, two virtual LANs (logical separation between hosts): Still physically one switch, but this switch acts as many separate devices.*

In Figure 12.2 , we configured the switch to be two separate LANs, two subnets, two broadcast domains, two VLANs—they all mean the same thing—without buying another switch. We can do this 1,000 times on most Cisco switches, which saves thousands of Rupees and more!

There are two different types of ports in a switched environment. Let's take a look at the first type in Figure 12.3

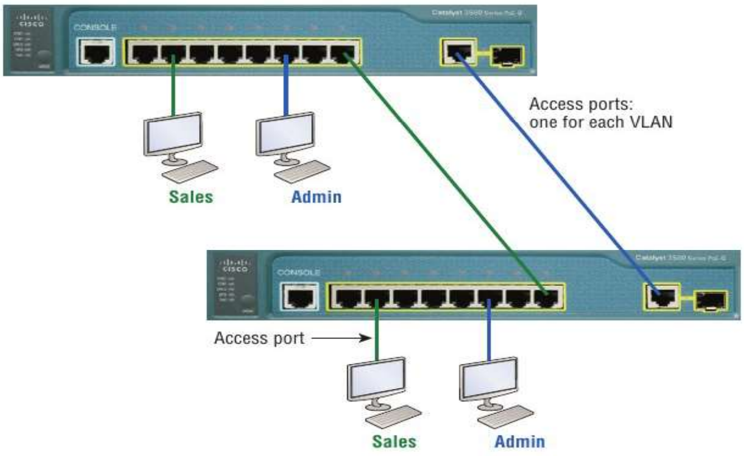


Fig 12.3 *Access Ports*

Notice there are access ports for each host and an access port between switches—one for each VLAN.

Access ports

An access port belongs to and carries the traffic of only one VLAN. Traffic is both received and sent in native formats with no VLAN information (tagging) whatsoever. Anything arriving on an access port is simply assumed to belong to the VLAN assigned to the port. Because an access port doesn't look at the source address, tagged traffic—a frame with added VLAN information—can be correctly forwarded and received only on trunk ports.

added VLAN information—can be correctly forwarded and received only on trunk ports.

With an access link, this can be referred to as the configured VLAN of the port. Any device attached to an access link is unaware of a VLAN membership—the device just assumes it's part of some broadcast domain. But it doesn't have the big picture, so it doesn't understand the physical network topology at all.

Another good bit of information to know is that switches remove any VLAN information from the frame before it's forwarded out to an access-link device. Remember that access-link devices can't communicate with devices outside their VLAN unless the packet is routed. Also, you can only create a switch port to be either an access port or a trunk port—not both. So you've got to choose one or the other and know that if you make it an access port, that port can be assigned to one VLAN only. In Figure 12.3, only the hosts in the Sales VLAN can talk to other hosts in the same VLAN. This is the same with Admin VLAN, and they can both communicate to hosts on the other switch because of an access link for each VLAN configured between switches.

Trunk ports

The term trunk port was inspired by the telephone system trunks, which carry multiple telephone conversations at a time. So it follows that trunk ports can similarly carry multiple VLANs at a time as well.

A trunk link is a 100, 1,000, or 10,000 Mbps point-to-point link between two switches, between a switch and router, or even between a switch and server, and it carries the traffic of multiple VLANs—from 1 to 4,094 VLANs at a time. But the amount is really only up to 1,001 unless you're going with something called extended VLANs.

Instead of an access link for each VLAN between switches, we'll create a trunk link demonstrated in Figure 12.4. Trunking can be a real advantage because with it, you get to make a single port part of a whole bunch of different VLANs at the same time. This is a great feature because you can actually set ports up to have a server in two separate broadcast domains simultaneously so your users won't have to cross a layer 3 device (router) to log in and access it.

Another benefit to trunking comes into play when you're connecting switches. Trunk links can carry the frames of various VLANs across them, but by default, if the links between your switches aren't trunked, only information from the configured access VLAN will be switched across that link.

It's also good to know that all VLANs send information on a trunked link unless you clear each VLAN by hand.

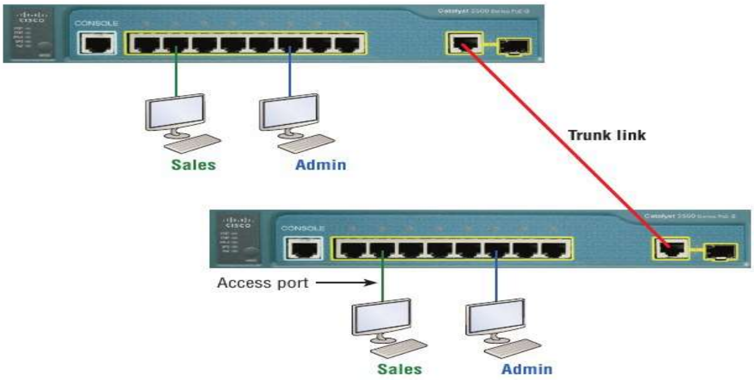


Fig 12.4 *VLANs can span across multiple switches by using trunk links, whichcarry traffic for multiple VLANs.*

Frame Tagging

As you now know, you can set up your VLANs to span more than one connected switch. You can see that going on in Figure 12.4, which depicts hosts from two VLANs spread across two switches. This flexible, power-packed capability is probably the main advantage to implementing VLANs, and we can do this with up to a thousand VLANs and thousands upon thousands of hosts!

All this can get kind of complicated—even for a switch—so there needs to be a way for each one to keep track of all the users and frames as they travel the switch fabric. And this just happens to be where frame tagging enters the scene.

This frame identification method uniquely assigns a user-defined VLAN ID to each frame.

Here's how it works: Once within the switch fabric, each switch that the frame reaches must first identify the VLAN ID from the frame tag. It then finds out what to do with the frame by looking at the information in what's known as the filter table. If the frame reaches a switch that has another trunked link, the frame will be forwarded out of the trunk-link port.

Once the frame reaches an exit that's determined by the forward/filter table to be an access link matching the frame's VLAN ID, the switch will remove the VLAN identifier. This is so the destination device can receive the frames without being required to understand their VLAN identification information.

Another great thing about trunk ports is that they'll support tagged and untagged traffic

simultaneously if you're using 802.1q trunking. The trunk port is assigned a default port VLAN ID (PVID) for a VLAN upon which all untagged traffic will travel. This VLAN is also called the native VLAN and is always VLAN 1 by default, but it can be changed to any VLAN number. Similarly, any untagged or tagged traffic with a NULL (unassigned) VLAN ID is assumed to belong to the VLAN with the port default PVID. Again, this would be VLAN 1 by default. A packet with a VLAN ID equal to the outgoing port native VLAN is sent untagged and can communicate to only hosts or devices in that same VLAN. All other VLAN traffic has to be sent with a VLAN tag to communicate within a particular VLAN that corresponds with that tag.

VLAN Identification Methods:

1. Inter-Switch Link (ISL)

Inter-Switch Link (ISL) is a way of explicitly tagging VLAN information onto an Ethernet

frame. This tagging information allows VLANs to be multiplexed over a trunk link through an external encapsulation method. This allows the switch to identify the VLAN membership of a frame received over the trunked link.

2. IEEE 802.1q

Created by the IEEE as a standard method of frame tagging, IEEE 802.1q actually inserts a field into the frame to identify the VLAN. If you're trunking between a Cisco switched link and a different brand of switch, you've got to use 802.1q for the trunk to work.

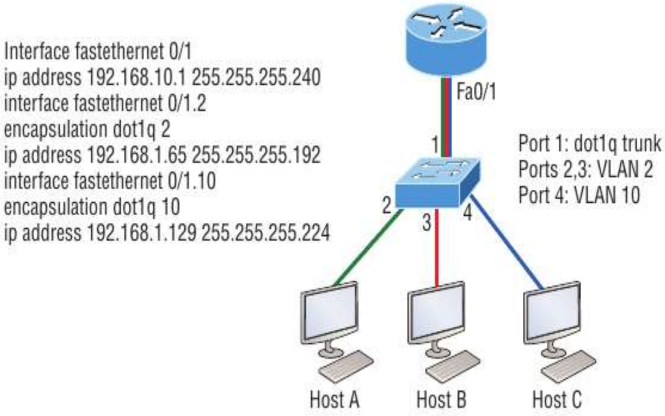
Unlike ISL, which encapsulates the frame with control information, 802.1q inserts an

802.1q field along with tag control information

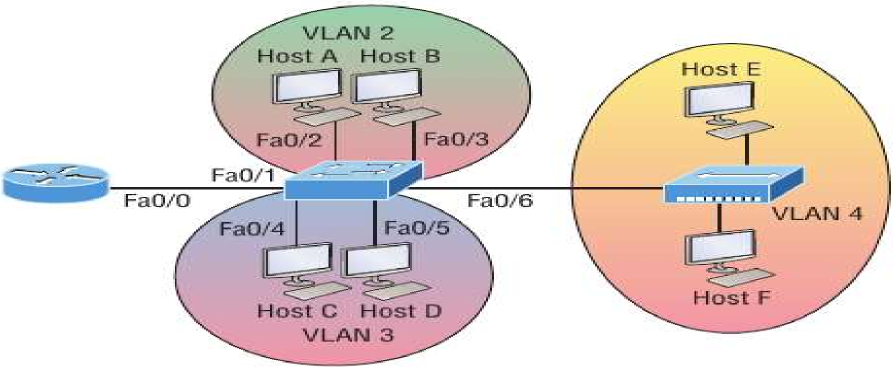
LAB EXERCISE

Configure following inter-VLAN example in GNS3 and verify the working using wireshark tool.

1.


Interface fastethernet 0/1
ip address 192.168.10.1 255.255.255.240
interface fastethernet 0/1.2
encapsulation dot1q 2
ip address 192.168.1.65 255.255.255.192
interface fastethernet 0/1.10
encapsulation dot1q 10
ip address 192.168.1.129 255.255.255.224
Fa0/1
1
Port 1: dot1q trunk
Ports 2,3: VLAN 2
Port 4: VLAN 10
2
3
4
Host A
Host B
Host C

2.


VLAN 2
Host A
Host B
Fa0/2
Fa0/3
Host E
Fa0/1
Fa0/0
Fa0/6
Fa0/4
Fa0/5
VLAN 4
Host C
Host D
VLAN 3
Host F