CHAPTER 1

VLAN

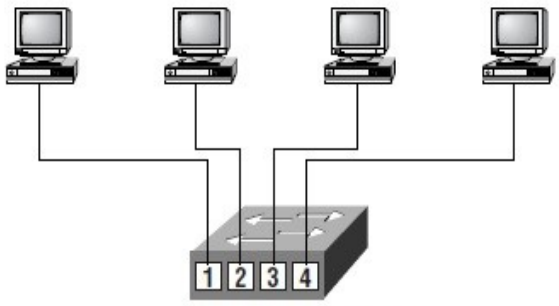
A Virtual Local Area Network (VLAN) is a logical grouping of network users and resources connected to administratively defined ports on a switch. By creating VLANs, you are able to create smaller broadcast domains within a switch by assigning different ports in the switch to different sub-networks. A VLAN is treated like its own subnet or broadcast domain. This means that frames broadcasted onto a network are only switched between ports in the same VLAN. Using virtual LANs, you're no longer confined to creating workgroups by physical locations. VLANs can be organized by location, function, department, or even the application or protocol used, regardless of where the resources or users are located.

In this chapter, you will learn what a VLAN is and how VLAN member- ships are used in a switched internetwork. Also, I'll discuss how Virtual Trunk Protocol (VTP) is used to update switch databases with VLAN information. Trunking Fast Ethernet links will also be discussed. Trunking allows you to send information about all VLANs across one link.

Virtual LANs:

In a layer-2 switched network, the network is flat, as shown in Figure 6.1. Every broadcast packet transmitted is seen by every device on the network, regardless of whether the device needs to receive the data.

FIGURE 6.1 Flat network structure



Broadcast Control

Broadcasts occur in every protocol, but how often they occur depends upon the protocol, the application(s) running on the internetwork, and how these services are used.

Some older applications have been rewritten to reduce their bandwidth needs. However, there is a new generation of applications that are bandwidth- greedy, consuming all they can find. These are multimedia applications that use broadcasts and multicast extensively. Faulty equipment, inadequate segmentation, and poorly designed firewalls can also add to the problems of broadcast-intensive applications. This has added a new chapter to network design, since broadcasts can propagate through the switched network. Routers, by default, send broadcasts only within the originating network but switches forward broadcasts to all

segments. This is called a *flat* network because it is one broadcast domain.

As an administrator, you must make sure the network is properly segmented to keep one segment's problems from propagating through the inter- network. The most effective way of doing this is through switching and routing. Since switches have become more cost-effective, many companies are replacing the flat network with a pure switched network and VLANs. All devices in a VLAN are members of the same broadcast domain receive all broadcasts. The broadcasts, by default, are filtered from all ports on a switch that are not members of the same VLAN.

Routers, layer-3 switches, or route switch modules (RSMs) must be used in conjunction with switches to provide connections between networks (VLANs), which can stop broadcasts from propagating through the entire internetwork.

Security

One problem with the flat internetwork is that security was implemented by connecting hubs and switches together with routers. Security was maintained at the router, but anyone connecting to the physical network could access the network resources on that physical LAN. Also, a user could plug a network analyzer into the hub and see all the traffic in that network. Another problem was that users could join a workgroup by just plugging their workstations into the existing hub.

By using VLANs and creating multiple broadcast groups, administrators now have control over each port and user. Users can no longer just plug their workstations into any switch port and have access to network resources. The administrator controls each port and whatever resources it is allowed to use.

Because groups can be created according to the network resources a user requires, switches can be configured to inform a network management station of any unauthorized access to network resources. If inter VLAN communication needs to take place, restrictions on a router can also be implemented. Restrictions can also be placed on hardware addresses, protocols and applications.

Flexibility and Scalability

Layer-2 switches only read frames for filtering; they do not look at the Net- work layer protocol. This can cause a switch to forward all broadcasts. However, by creating VLANs, you are essentially creating broadcast domains. Broadcasts sent out from a node in one VLAN will not be for- warded to ports configured in a different VLAN. By assigning switch ports or users to VLAN groups on a switch or group of connected switches (called a *switch fabric*), you have the flexibility to add only the users you want in the broadcast domain regardless of their physical location. This can stop broad- cast storms caused by a faulty network interface card (NIC) or an application from propagating throughout the entire internetwork.

When a VLAN gets too big, you can create more VLANs to keep the broadcasts from consuming too much bandwidth. The fewer users in a VLAN, the fewer users affected by broadcasts.

To understand how a VLAN looks to a switch, it's helpful to begin by first looking at a traditional collapsed backbone. Figure 6.2 shows a collapsed backbone created by connecting physical LANs to a router.

FIGURE 6.3 Switches removing the physical boundary

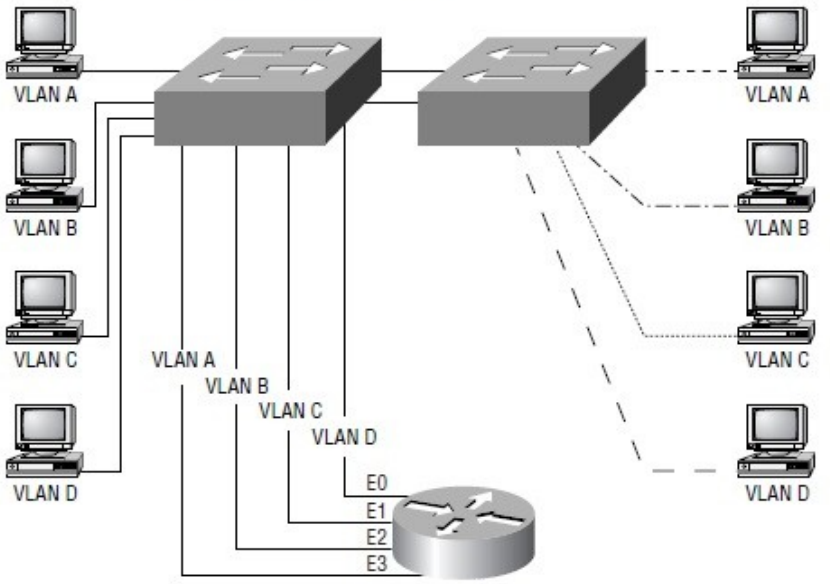


Figure 6.3 switches removing the physical boundary

Each network is attached to the router and has its own logical network number. Each node attached to a particular physical network must match that network number to be able to communicate on the internetwork. Now let's look at what a switch accomplishes. Figure 6.3 shows how switches remove the physical boundary.

Switches create greater flexibility and scalability than routers can by themselves. You can group users into communities of interest, which are known as VLAN organizations. Because of switches, we don't need routers anymore, right? Wrong. In Figure 6.3, notice that there are four VLANs or broadcast domains. The nodes within each VLAN can communicate with each other, but not with any other VLAN or node in another VLAN. When configured in a VLAN, the nodes think they are actually in a collapsed backbone as in Figure 6.2. What do the hosts in Figure 6.2 need to do to communicate to a node or host on a different network? They need to go through the router, or other layer-3 device, just like when they are configured for VLAN communication, as shown in Figure 6.3. Communication between VLANs, just as in physical networks, must go through a layer-3 device.

VLAN Memberships

VLANs are typically created by an administrator, who then assigns switch ports to the VLAN. These are called static VLANs. If the administrator wants to do a little more work up front and assign all the host devices' hardware addresses into a database, the switches can be configured to assign VLANs dynamically.

Static VLANs

Static VLANs are the typical way of creating VLANs and the most secure. The switch port that you assign a VLAN association always maintains that association until an administrator changes the port assignment. This type of VLAN configuration is easy to set up and monitor, working well in a net- work where the movement of users within the network is controlled. Using network management software to configure the ports can be helpful but is not mandatory.

Dynamic VLANs

Dynamic VLANs determine a node's VLAN assignment automatically. Using intelligent management software, you can enable hardware (MAC) addresses, protocols, or even applications to create dynamic VLANs. For example, suppose MAC addresses have been entered into a centralized VLAN management application. If a node is then attached to an unassigned switch port, the VLAN management database can look up the hardware address and assign and configure the switch port to the correct VLAN. This can make management and configuration easier for the administrator. If a user moves, the switch will automatically assign them to the correct VLAN. However, more administration is needed initially to set up the database.

Cisco administrators can use the VLAN Management Policy Server (VMPS) service to set up a database of MAC addresses that can be used for dynamic addressing of VLANs. VMPS is a MAC address–to–VLAN map- ping database.

Identifying VLANs

VLANs can span multiple connected switches. Switches in this switch fabric must keep track of frames and which VLAN frames belong to. Frame tagging performs this function. Switches can then direct frames to the appropriate port.

There are two different types of links in a switched environment:

Access links Links that are only part of one VLAN and are referred to as the native VLAN of the port. Any device attached to an access link is unaware of a VLAN membership. This device just assumes it is part of a broadcast domain, with no understanding of the physical network. Switches remove any VLAN information from the frame before it is set to an access link device. Access link devices cannot communicate with devices outside their VLAN unless the packet is routed through a router.

Trunk links Trunks can carry multiple VLANs. Originally named after trunks of the telephone system, which carries multiple telephone conversations, trunk links are used to connect switches to other switches, to routers, or even to servers. Trunked links are supported on Fast or Gigabit Ethernet only. To identify the VLAN that a frame belongs to with Ether- net technology, Cisco switches support two different identification techniques: ISL and 802.1q. Trunk links are used to transport VLANs between devices and can be configured to transport all VLANs or just a few. Trunk links still have a native, or default, VLAN that is used if the trunk link fails.

Frame Tagging

The switch in an internetwork needs a way of keeping track of users and frames as they travel the switch fabric and VLANs. A switch fabric is a group of switches sharing the same VLAN information. Frame identification (*frame tagging*) uniquely assigns a user-defined ID to each frame. This is sometimes referred to as a VLAN ID or color.

Cisco created frame tagging to be used when an Ethernet frame traverses a trunked link. The VLAN tag is removed before exiting trunked links. Each switch that the frame reaches must identify the VLAN ID, then determine what to do with the frame based on the filter table. If the frame reaches a switch that has another trunked link, the frame will be forwarded out the trunk link port. Once the frame reaches an exit to an access link, the switch removes the VLAN identifier. The end device will receive the frames without having to understand the VLAN identification.

VLAN Identification Methods

To keep track of frames traversing a switch fabric, VLAN identification is used to identify which frames belong to which VLANs. There are multiple trunking methods:

Inter-Switch Link (ISL) Proprietary to Cisco switches, it is used for FastEthernet and Gigabit Ethernet links only. Can be used on a switch port, router interfaces, and server interface cards to trunk a server. This server trunking is good if you are creating functional VLANs and don't want to break the 80/20 rule. The server that is trunked is part of all VLANs (broadcast domains) simultaneously. The users do not have to cross a layer-3 device to access a company-shared server.

IEEE 802.1q Created by the IEEE as a standard method of frame tagging. It actually inserts a field into the frame to identify the VLAN. If you are trunking between a Cisco switched link and a different brand of switch, you have to use 802.1q for the trunk to work.LAN emulation (LANE) Used to communicate multiple VLANs over ATM.802.10 (FDDI) Used to send VLAN information over FDDI. Uses a SAID field in the frame header to identify the VLAN. This is proprietary to Cisco devices.

The CCNA exam covers only the ISL method of VLAN Identification.

Inter-Switch Link (ISL) Protocol

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. By running ISL, you can interconnect multiple switches and still maintain VLAN information as traffic travels between switches on trunk links. ISL provides a low-latency, full wire-speed performance over FastEthernet using either half- or full-duplex mode.

Cisco created the ISL protocol, and therefore ISL is proprietary in nature to Cisco devices only. If you need a non-proprietary VLAN protocol, use the 802.1q, which is covered in the *CCNP:* Switching Study Guide. ISL is an external tagging process, which means the original frame is not altered but instead encapsulated with a new 26-byte ISL header. It also adds a second 4-byte frame check sequence (FCS) field at the end of the frame. Because the frame is encapsulated with information, only ISL-aware devices can read it. Also, the frame can be up to 1522 bytes long. Devices that receive an ISL frame may record this as a giant frame because it is over the maximum of 1518 bytes allowed on an Ethernet segment.

On multi-VLAN (trunk) ports, each frame is tagged as it enters the switch. ISL network interface cards (NICs) allow servers to send and receive frames tagged with multiple VLANs so the frames can traverse multiple VLANs without going through a router, which reduces latency. This technology can also be used with probes and certain network analyzers. It makes it easy for users to attach to servers quickly and efficiently, without going through a router every time they need to communicate with a resource. Administrators can use the ISL

technology to include file servers in multiple VLANs simultaneously, for example.
It is important to understand that ISL VLAN information is added to a frame only if the frame is forwarded out a port configured as a trunk link. The ISL encapsulation is removed from the frame if the frame is forwardedout an access link.

Trunking

Trunk links are 100- or 1000Mbps point-to-point links between two switches, between a switch and router, or between a switch and server. Trunked links carry the traffic of multiple VLANs, from 1 to 1005 at a time. You cannot run trunked links on 10Mbps links. Trunking allows you to make a single port part of multiple VLANs at the same time. The benefit of trunking is that a server, for example, can be in two broadcast domains at the same time. This will stop users from having to cross a layer-3 device (router) to log in and use the server. Also, where connecting switches together, trunk links can carry some or all VLAN information across the link. If you do not trunk these links between switches, then the switches will only send VLAN 1 information by default across the link. All VLANs are configured on a trunked link unless cleared by an administrator by hand.
Cisco switches use the Dynamic Trunking Protocol (DTP) to manage trunk negation in the Catalyst-switch engine software release 4.2 or later, using either ISL or 802.1q. DTP is a point-to-point protocol that was created to send trunk information across 802.1q trunks.

Routing between VLANs

Hosts in a VLAN are within their own broadcast domain and communicate freely. VLANs create network partitioning and traffic separation at layer 2 of the OSI specifications. To have hosts or any device communicate between VLANs, a layer-3 device is absolutely necessary.
You can use a router that has an interface for each VLAN, or a router that supports ISL routing. The least expensive router that supports ISL routing is the 2600 series router. The 1600, 1700, and 2500 series do not support ISL routing. If you only had a few VLANs (two or three), you could get a router with two or three 10BaseT or Fast Ethernet connections. 10BaseT is OK, but Fast Ethernet will work really well. However, if you have more VLANs available than router interfaces, you can either run ISL routing on one Fast Ethernet interface or buy a route switch module (RSM) for a 5000 series switch. The RSM can support up to
1005 VLANs and run on the backplane of the switch. If you use one Fast- Ethernet interface and run ISL routing, Cisco calls this a router-on-a-stick.

VLAN Trunk Protocol (VTP)

Cisco created VLAN Trunk Protocol (VTP) to manage all the configured VLANs across a switched internetwork and to maintain consistency throughout the network. VTP allows an administrator to add, delete, and rename VLANs, which are then propagated to all switches. VTP provides the following benefits to a switched network:

- Consistent VLAN configuration across all switches in the network.
- Allowing VLANs to be trunked over mixed networks, like Ethernet to ATM LANE or FDDI.
- Accurate tracking and monitoring of VLANs.
- Dynamic reporting of added VLANs to all switches .
- Plug-and-Play VLAN adding

To allow VTP to manage your VLANs across the network, you must first create a VTP server. All servers that need to share VLAN information must use the same domain name, and a switch can only be in one domain at a time. This means that a switch can only share VTP domain information with switches configured in the same VTP domain.

A VTP domain can be used if you have more than one switch connected in a network. If all switches in your network are in only one VLAN, then you don't need to use VTP. VTP information is sent between switches via a trunk port.

Switches advertise VTP-management domain information, as well as a configuration revision number and all known VLANs with any specific parameters. You can configure switches to forward VTP information through trunk ports but not accept information updates, nor update their VTP database. This is called VTP transparent mode.

If you are having problems with users adding switches to your VTP domain, you can add passwords, but remember that every switch must be set up with the same password, which may be difficult.

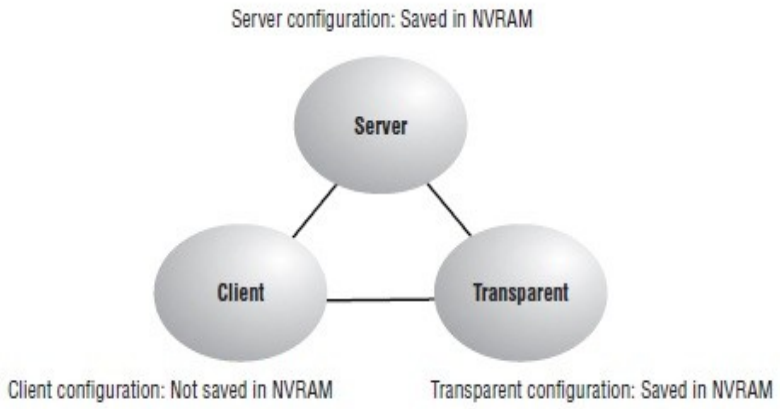
Switches detect the additional VLANs within a VTP advertisement and then prepare to receive information on their trunk ports with the newly defined VLAN in tow. The information would be VLAN ID, 802.10 SAID fields, or LANE information. Updates are sent out as revision numbers that are the notification plus 1. Anytime a switch sees a higher revision number, it knows the information it is receiving is more current and will overwrite the current database with the new one.

VTP Modes of Operation

There are three different modes of operation within a VTP domain. Figure 6.4 shows all three.

Figure 6.4 VTP modes

FIGURE 6.4 VTP modes



VTP advertisements are sent every five minutes or whenever there is a change.

Server Is the default for all Catalyst switches. You need at least one server in your VTP domain to propagate VLAN information throughout the domain. The switch must be in server mode to be able to create, add, or delete VLANs in a VTP domain. Changing VTP information must also be done in server mode. Any change made to a switch in server mode is advertised to the entire VTP domain.

Client Receives information from VTP servers and send and receives updates, but cannot make any changes. No ports on a client switch can be added to a new VLAN before the VTP server notifies the client switch of the new VLAN. If you want a switch to become a server, first make it a client so it receives all the correct VLAN information, then change it to a server.

Transparent Does not participate in the VTP domain but will still for- ward VTP advertisements through the configured trunk links. VTP transparent switches can add and delete VLANs as the switch keeps its own database and does not share it with other switches. Transparent is considered only locally significant.

Configuration Revision Number

The revision number is the most important piece in the VTP advertisement. Figure 6.5 shows an example of how a revision number is used in an advertisement.

This figure shows a configuration revision number as "N." As a database is modified, the VTP server increments the revision number by 1. The VTP server then advertises the database with the new configuration revision number. When a switch receives an advertisement that has a higher revision number, it overwrites the database in NVRAM with the new database being advertised.

VTP Pruning

You can preserve bandwidth by configuring the VTP to reduce the amount of broadcasts, multicasts, and other unicast packets, which helps preserve bandwidth. This is called pruning. VTP pruning only sends broadcasts to trunk links that must have the information; any trunk link that does not need the broadcasts will not receive them. For example, if a switch does not have any ports configured for VLAN 5, and a broadcast is sent throughout VLAN 5, the broadcast would not traverse the trunk link to this switch. VTP pruning is disabled by default on all switches. When you enable pruning on a VTP server, you enable it for the entire domain. By default, VLANs 2–1005 are pruning-eligible. VLAN 1 can never prune because it is an administrative VLAN.

Summary

This chapter introduced Virtual LANs and described how Cisco switches can use them. VLANs break up broadcast domains in a switched internetwork. This is important because layer-2 switches only break up collision domains and, by default, all switches make up one large broadcast domain. This chapter also described trunked VLANs across a Fast Ethernet link. Trunking is important in a network with multiple switches running several VLANs We also discussed Virtual Trunk Protocol (VTP), which really has nothing to do with trunking. What it does is send VLAN information down a trunked link, but the trunk configuration is not part of VTP.

Key Terms

Be sure you're familiar with the following terms before taking the exam.

- Access link
- Broadcast domain
- collision domain
- dynamic VLAN
- flat network
- ISL routing
- Static VLAN
- Virtual LAN
- VLAN Trunk Protocol (VTP)
- Switch
- Trunk Link

Assignments

One Mark Questions:

1. VLAN stands for _____
2. Which is Flat Network?
3. Define VMPS?
4. VMPS stands for_____
5. What is Frame Color?
6. ISL stands for_____
7. Name the VLAN tagging protocol of CISCO_____
8. _____link carries traffic along in to multiple VLAN
9. What is the size of ISL tag for the frame?
10. If network has multiple vendor switches then which frame tagging protocol needs to be used?
11. FDDI stands for_____
12. All VLAN traffics are configured on a trunk link by default(true/false)
13. _____is used Trunk negation
14. RSN stands for_____
15. Define static and dynamic membership?
16. VTP stands for____
17. Define router on a stick?
18. What is configuration revision number?
19. DTP is _____

20. What is a Switch Fabric?

7 Marks Questions:

1. What is Flat network? What are the drawbacks of flat network?
2. Give the significance of VLAN implementation with diagram.
3. What are the different approaches of VLAN membership?explain.
4. What are the different VLAN identification?
5. What are the VLAN tagging method?
6. What are the link types & its significance with vlan?
7. Give the structure of Ethernet frame with ISL tag
8. Write a note on ISL protocol?
9. What are the alternatives available to achieve Routing between two vlans?
10. Write a note on VTP?
11. What are the benefits with VTP?
12. What is VTP Pruning? How it reduces the network bandwidth?

10 Marks Questions:

1. Design network with 3 VLANs for a organization. Use a router to implement inter VLAN routing, using IOS commands.
2. What are the different VLAN Tagging methods? Explain each of then in brief.
3. Whatare the methods to achieve inter VLAN routing? Explain