Virtual LAN (VLAN)

By,
Subrahmanya Bhat, Dept M.C.A
Srinivas University, Mangaluru.

VLAN

- 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.

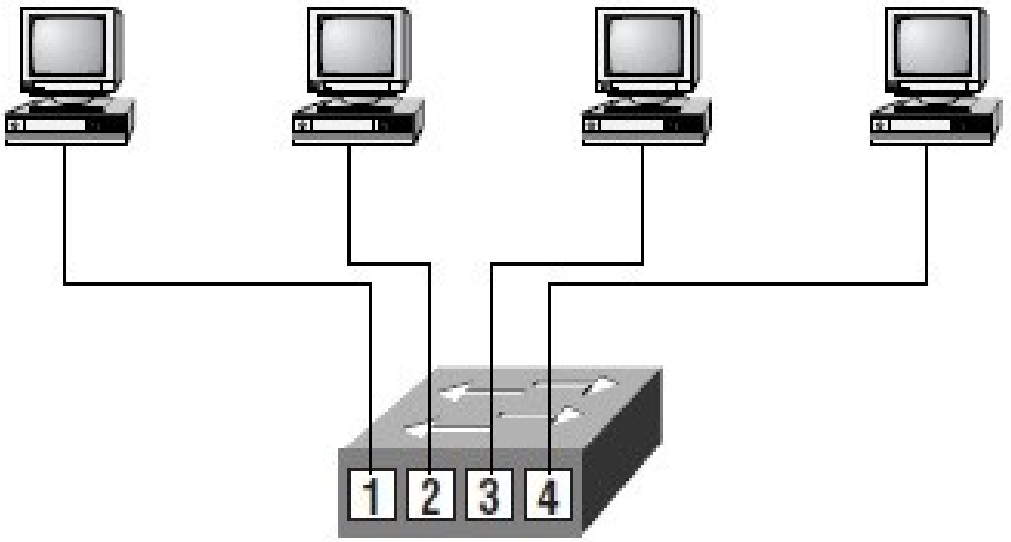
- VLANs can be organized by location, function, department, or even the application or protocol used, regardless of where the resources or users are located.

Flat Network

Is called a flat network because it is one broadcast domain.

Flat Network

FIGURE 6.1 Flat network structure



- Each segment has its own collision domain.
- All segments are in the same broadcast domain.

Problem with flat network

- Broadcast Control
- Security

Broadcast Controlling

As an administrator, you must make sure the network is properly segmented

The most effective way of doing this is through switching and routing

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 and receive all broadcasts.

Broadcasts sent out from a node in one VLAN will not be forwarded to ports configured in a different VLAN.

Security

Anyone connecting to the physical network could access the network resources

Any user could plug a network analyzer into the hub and see all the traffic in that network

Any user could join a workgroup by just plugging their workstations into the existing hub

With VLAN

By using VLANs and creating multiple broadcast groups, administrators now have control over each port and user.

With VLAN..

- 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 us

With VLAN..

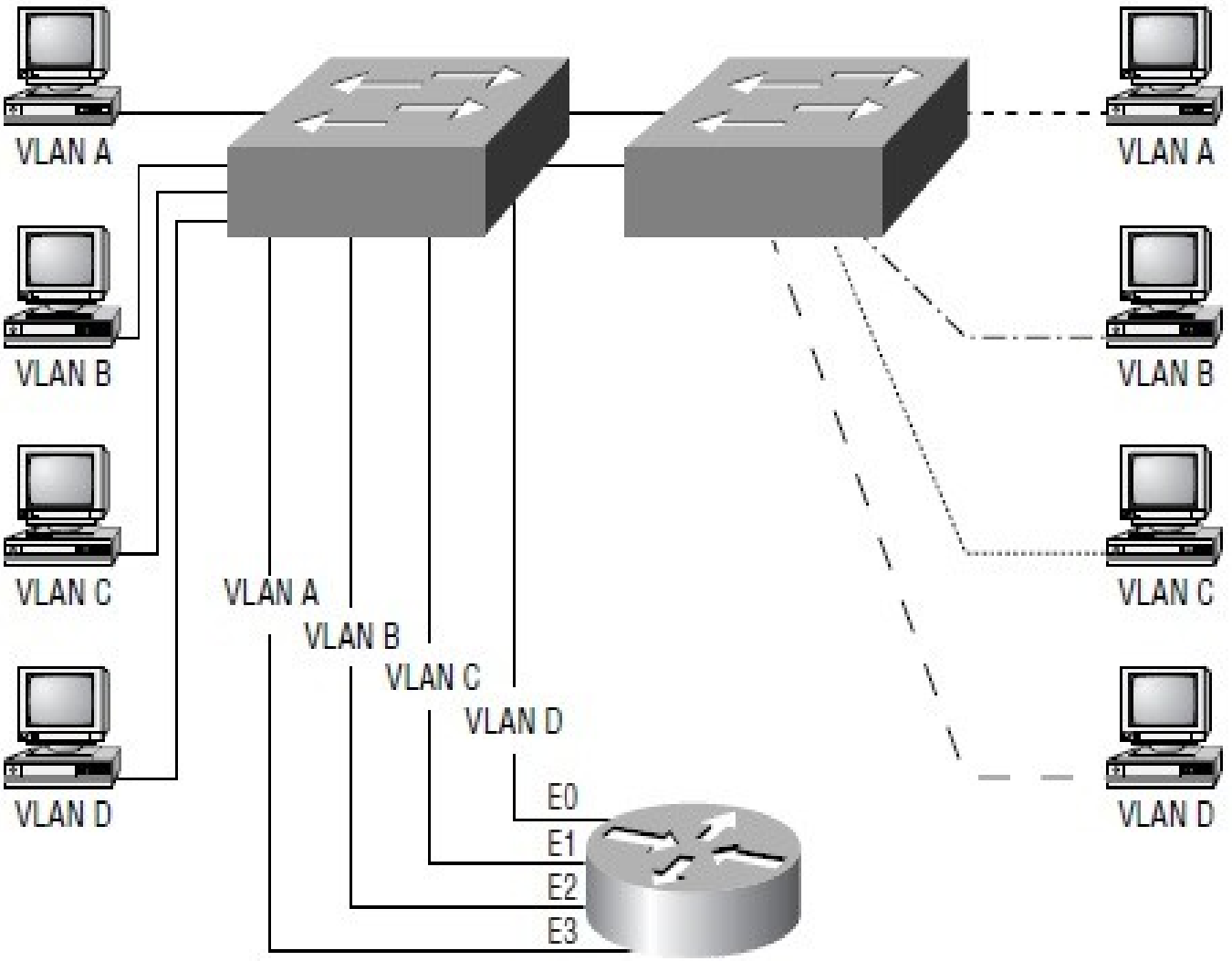
Switches can be configured to inform a network management station of any unauthorized access to network resources

With VLAN..

If inter-VLAN communication needs to take place, restrictions on a router can also be implemented

Communication between VLANs, must go through a layer-3 device, ie Router.

FIGURE 6.3 Switches removing the physical boundary



VLAN Memberships

VLANs are typically created by an administrator, who then assigns switch ports to the VLAN.

- Static VLANs
- Dynamic VLANs

Static VLANs

The switch port that you assign a VLAN association always maintains that association until an administrator changes the port assignment.

Static VLANs

This type of VLAN configuration is easy to set up and monitor

Works well in a network where the movement of users within the network is controlled

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 VLAN

Dynamic VLANs

MAC addresses cab be entered into a centralized VLAN management application

.

Then if a node is 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

Dynamic VLANs

If a user moves, the switch will automatically assign them to the correct VLAN

VMPS

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 contains a MAC address–to–VLAN mapping database.

Identifying VLANs

VLANs can span multiple connected switches.

Switches in this switchfabric must keep track of frames and which VLAN frames belong to.

Identifying VLANs

Frame tagging performs this function.

Switches can then direct frames to the appropriate port using this Frame Tag.

Link Types

Different types of links in a switched environment:

- Access links
- Trunk links

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

Access links

Switches remove any VLAN information from the frame before it is sent 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

Trunk links can carry multiple VLANs

Trunk links are used to connect switches to other switches, to routers, or even to servers.

Trunk links

Trunked links are supported on Fast Ethernet or Gigabit Ethernet only.

Trunk links are used to transport VLANs between devices and can be configured to transport all VLANs or just a few.

Trunk links

Trunk links still have a native, or default, VLAN that is used if the trunk link fails

Frame Tagging

Frame identification (frame tagging) uniquely assigns a user-defined ID to each frame

This is referred to as a VLAN ID or colour

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

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

There are multiple trunking methods:

- Inter-Switch Link (ISL)
- IEEE 802.1q
- LAN emulation (LANE)
- 802.10 (FDDI)

Inter-Switch Link (ISL)

Proprietary to Cisco switches

It is used for FastEthernet and Gigabit Ethernet links only

Used on a switch port, router interfaces, and server interface cards to trunk a 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.

Inter-Switch Link (ISL) Protocol

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

Inter-Switch Link (ISL) Protocol

This tagging information allows VLANs to be multiplexed over a trunk link through an external encapsulation method.

Inter-Switch Link (ISL) Protocol

By running ISL, you can interconnect multiple switches and still maintain VLAN information as traffic travels between switches on trunk links

Inter-Switch Link (ISL) Protocol

ISL provides a low-latency, full wire-speed performance over FastEthernet using either half- or full-duplex mode.

Inter-Switch Link (ISL) Protocol

ISL is an external tagging process, which means the original frame is not altered but instead encapsulated with a new 26-byte ISL header

Inter-Switch Link (ISL) Protocol

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

Inter-Switch Link (ISL) Protocol

So the frames can traverse multiple VLANs without going through a router, which reduces latency

Inter-Switch Link (ISL) Protocol

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

Inter-Switch Link (ISL) Protocol

Administrators can use the ISL technology to include file servers in multiple VLANs simul-taneously

Inter-Switch Link (ISL) Protocol

ISL VLAN information is added to a frame only if the frame is forwarded out a port configured as a trunk link

Inter-Switch Link (ISL) Protocol

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

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

Trunking

Trunked links carry the traffic of multiple VLANs, from 1 to 1005 at a time

You cannot run trunked links on 10Mbps links

Trunking

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

Trunking

This will stop users from having to cross a layer-3 device (router) to log in and use the server

By connecting switches together, trunk links can carry some or all VLAN information across the link.

Trunking

If you do not trunk these links between switches, then the switches will only send VLAN 1 information by default across the link.

Trunking

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 using either ISL or 802.1q

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

Routing between VLANs

To have hosts or any device communicate between VLANs, a layer-3 device is absolutely necessary

Routing between VLANs

To route between VLANs one can use a router that has an interface for each VLAN, or a router that supports ISL routing

Routing between VLANs

Ciscos 2600 series router supports ISL routing, but not the 1600, 1700, and 2500 series

Routing between VLANs

If you only had a few VLANs (two or three), then go for a router with two or three 10BaseT or FastEthernet interface

Routing between VLANs

However, if you have more VLANs than router interfaces, you can either run ISL routing on one FastEthernet interface or buy a route switch module (RSM)

Routing between VLANs

The RSM can support up to 1005 VLANs and run on the backplane of the switch

If you use one FastEthernet 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.

VLAN Trunk Protocol (VTP)

VTP allows an administrator to add, delete, and rename VLANs, which are then propagated to all switches

VTP benefits

Consistent VLAN configuration across all switches in the network

Allowing VLANs to be trunked over mixed networks, like Ethernet to ATM LANE or FDDI

VTP benefits..

Accurate tracking and monitoring of VLANs

Dynamic reporting of added VLANs to all switches

Plug-and-Play VLAN adding

Managing VLAN

To allow VTP to manage your VLANs across the network, you must first create a VTP server.

Managing VLAN

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

Managing VLAN

This means that a switch can only share VTP domain information with switches configured in the same VTP domain.

Managing VLAN

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.

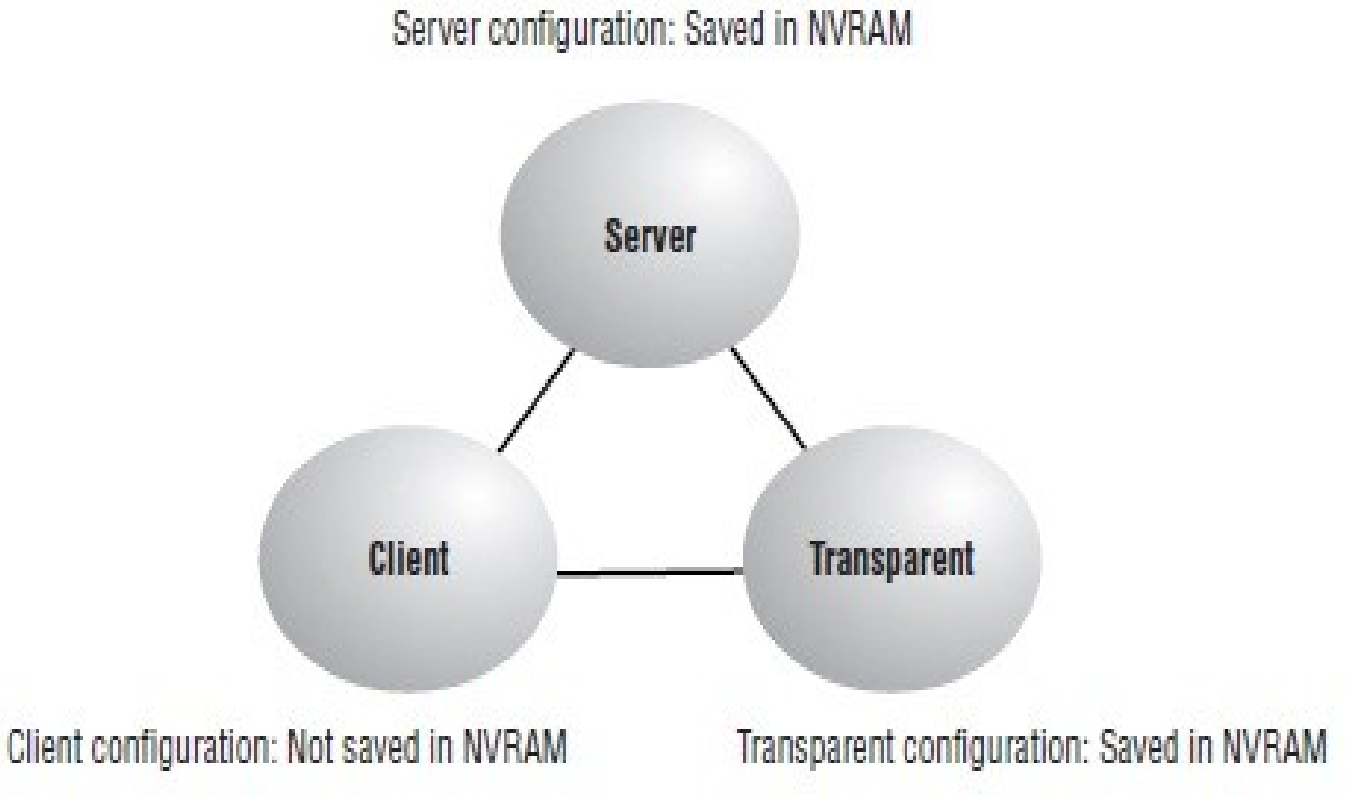
You can configure switches to forward VTP information through trunk ports but not accept information updates, nor update their VTP database.

This is called VTP transparent mode.

VTP Modes of Operation

There are three different modes of operation within a VTP domain

FIGURE 6.4 VTP modes



Server

You need at least one server in your VTP domain to propagate VLAN information throughout the domain.

Server

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

Client

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 forward VTP advertisements through the configured trunk links.

Transparent

VTP transparent switches can add and delete VLANs as the switch keeps its own database and does not share it with other switches

Configuration Revision Number

The revision number is the most important piece in the VTP advertisement.

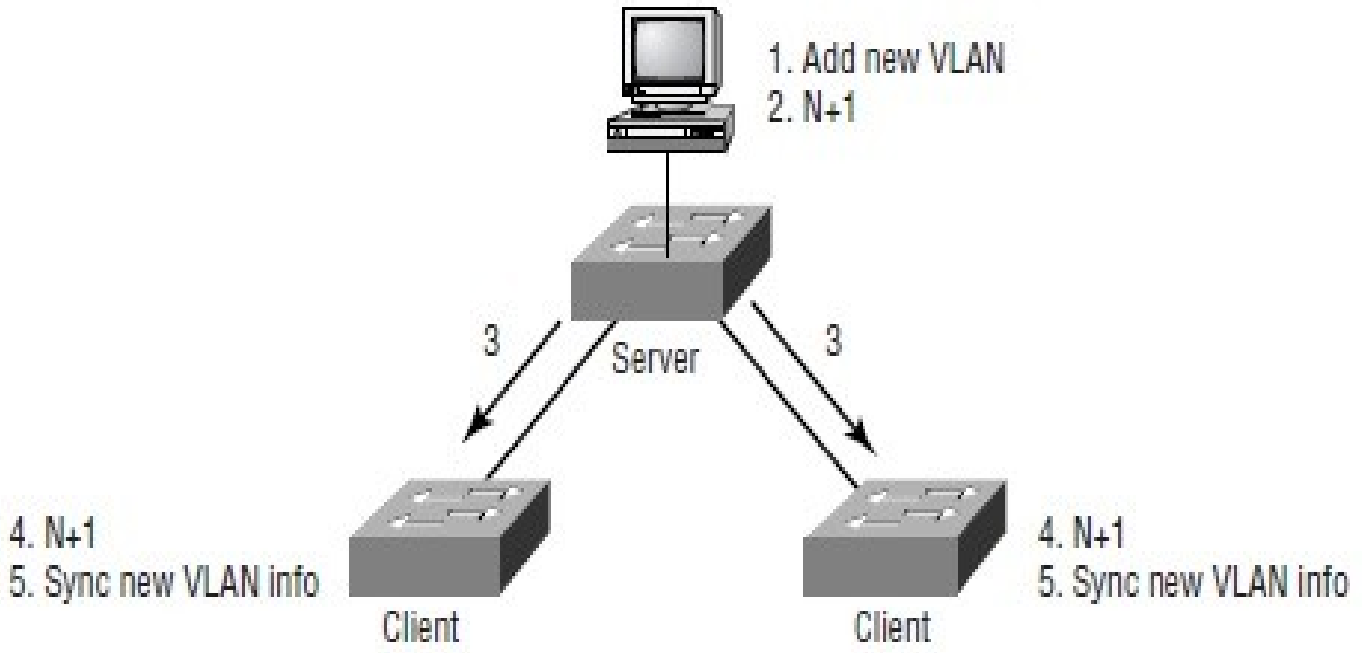
As a database is modified, the VTP server increments the revision number by 1

Configuration Revision Number

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

FIGURE 6.5 VTP revision number



VTP Pruning

You can preserve bandwidth by configuring the VTP to reduce the amount of broadcasts, multicasts, and other unicast packets

VTP 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

VTP Pruning

For example, if a switch does not have any ports configured for VLAN 5, and if a broadcast is sent throughout VLAN 5, the broadcast would not traverse the trunk link to this switch.

VTP Pruning

VTP pruning is disabled by default on all switches

Subrahmanya Bhat. Dept M.C.A
Srinivas University

Assignments

Subrahmanya Bhat. Dept M.C.A
Srinivas University