Chapter 7

VLAN & VTP

Hosts or LANs do not normally operate in isolation. They are connected to one another or to the Internet. To connect hosts or LANs, we use connecting devices. Connecting devices can operate in different layers of the Internet model. After discussing some connecting devices, we show how they are used to create virtual local area networks (VLANs).

7.1 Definition

A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs). A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area.

VLANs make it easy for network administrators to partition a single switched network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure. VLANs are often set up by larger businesses to re-partition devices for better traffic management.

7.2 Advantages of VLAN

Broadcast Control: Broadcasts are required for the normal function of a network. Many protocols and applications depend on broadcast communication to function properly. A layer 2 switched network is in a single broadcast domain and the broadcasts can reach the network segments which are so far where a particular broadcast has no scope and consume available network bandwidth. A layer 3 device (typically a Router) is used to segment a broadcast domain. If we segment a large LAN to smaller VLANs we can reduce broadcast traffic as each broadcast will be sent on to the relevant VLAN only.

Security: VLANs provide enhanced network security. In a VLAN network environment, with multiple broadcast domains, network administrators have control over each port and user. A malicious user can no longer just plug their workstation into any switch port and sniff the network traffic using a packet sniffer. The network administrator controls each port and whatever resources

it is allowed to use. VLANs help to restrict sensitive traffic originating from an enterprise department within itself.

Cost: Segmenting a large VLAN to smaller VLANs is cheaper than creating a routed network with routers because normally routers costlier than switches.

Easier fault management: Troubleshooting problems on the network can be simpler and faster when your different user groups are segmented and isolated from one another. If you know that complaints are only coming from a certain subset of users, you'll be able to quickly narrow down where to look to find the issue.

7.3 Trunk Port

Switch ports are layer 2 interfaces which are used to carry layer 2 traffic. A single switch port can carry single VLAN traffic whether it is an access port or trunk port. Frames are handled differently according to the type of link they are traversing.

Note: All switch ports are assigned VLAN 1 by default (VLAN 1 cannot be modified or deleted).

These switch ports belongs to and carry the traffic of more than one VLAN. This is a great advantage as to carry the traffic of group of VLAN, a single switch port can be used. These are of great use if user wants to exchange traffic between more than one switches having more than one vlan configured. To identify traffic belongs to which vlan, VLAN identification method (802.1q or ISL) are used. Also, to carry traffic between more than one vlan, then inter vlan routing is required, in which the link between router and switch is configured as trunk as the link has to carry the traffic of more than one VLAN (in case of router on a stick configuration not in inter vlan routing by layer 3 switches).

Note: Trunk links can carry the traffic of different VLANs across them but by default, if the links between switches are not trunk then only information from the configured access VLAN will be exchanged.

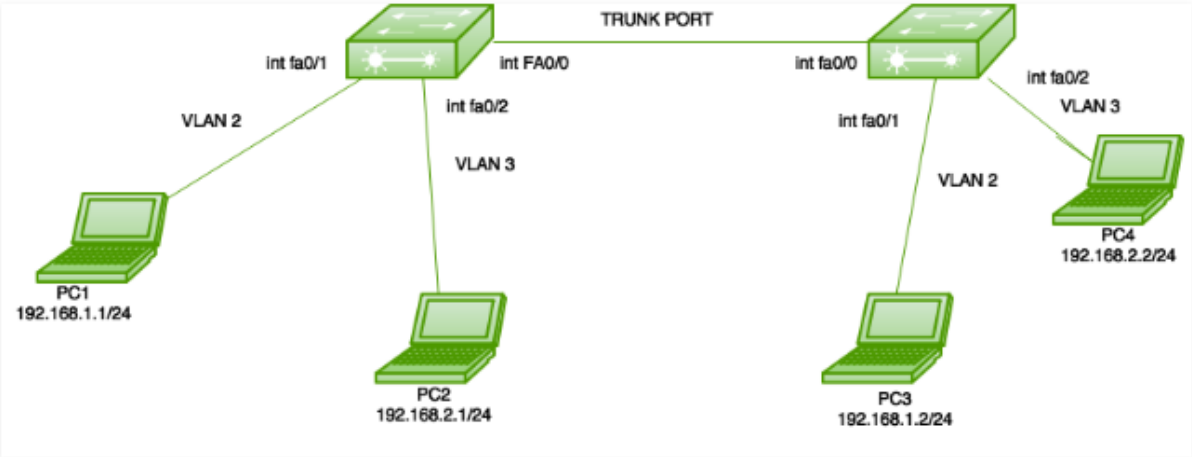

Figure 6.1 Trunk Port

Here is a simple topology in which 2 switches are connected and VLANs 2 and 3 are configured on both switches as shown.

7.4 Trunking

Trunking is a technique used in data communications transmission systems to provide many users with access to a network by sharing multiple lines or frequencies. As the name implies, the system is like a tree with one trunk and many branches. Trunking is commonly used in very-high-frequency (VHF) radio and telecommunication systems.
Trunking can also be defined as a network that handles multiple signals simultaneously. The data transmitted through trunking can be audio, video, controlling signals or images.
Telecommunication networks all across the globe are based on trunking. Trunking reduces the size of a telecom network and increases bandwidth. VHF radio used by police and control centers is also based on trunking. There has been a rapid development in data communications over the past few years, including the creation of the concept of trunking. Users share connections with each other where trunking is applied so the connections are less dense and more understandable.
Trunking uses communication media in parallel with increased bandwidth and communication speed.

Trunking is the mechanism used to form an internetwork, or Internet, comprised of local area networks (LANs), virtual LANS (VLANs) or wide area networks (WANs). The switches are interconnected to establish these networks using trunking. Trunking is not limited to any medium since its main purpose is to maximize the bandwidth available in any type of network.
Cisco networks have trunk ports and access ports. The trunk port allows traffic to be carried for either all of the VLANs or any of the VLANs. The access ports, however, allow traffic to be carried to a specified VLAN only. The trunk ports use the tagging process while carrying data. Each tag is checked by a switch to analyze which switch will receive the traffic. Access ports do not have a tag because they carry or transmit data to a specific VLAN.

7.5 Router on Stick

Switches divide broadcast domain through VLAN (Virtual LAN). VLAN is a partitioned broadcast domain from a single broadcast domain. Switch doesn't forward packets across different VLANs by itself. If we want to make these virtual LANs communicate with each other, a concept of **Inter VLAN Routing** is used.

Inter VLAN Routing :
Inter VLAN routing is a process in which we make different virtual LANs to communicate with each other irrespective of where the VLANs are present (on same switch or different switch). Inter VLAN Routing can be achieved through a layer-3 device i.e. Router or layer-3 Switch. When the Inter VLAN Routing is done through the Router it is known as **Router on a stick**.

Router On a Stick: The Router's interface is divided into sub-interfaces, which acts as a default gateway to their respective VLANs.

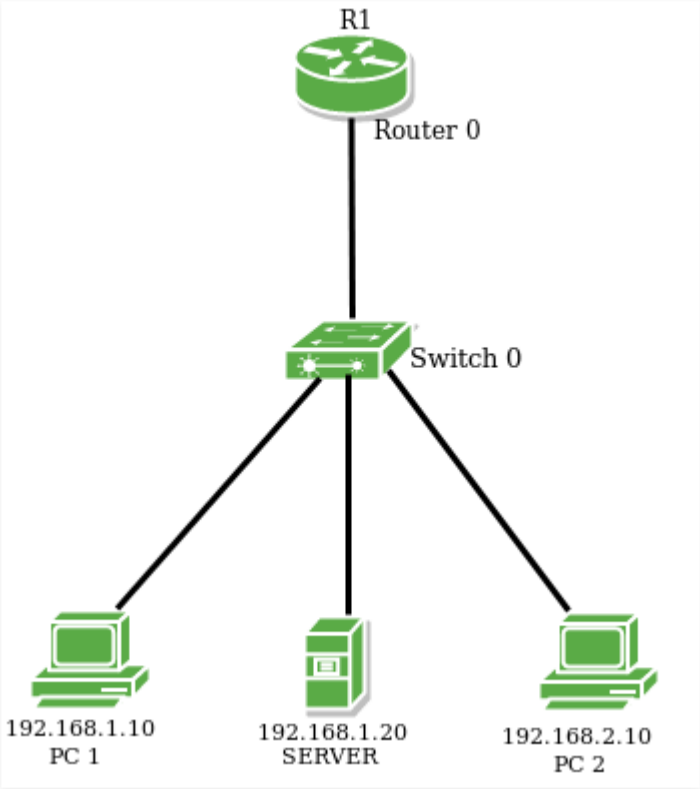

Figure 6.2 Router on Stick

Here is a topology in which there is a router and a switch and some end hosts. 2 different VLANs have been created on the switch. The router's interface is divided into 2 sub-interfaces (as there are 2 different VLANs) which will acts as a default gateway to their respective VLANs. Then router will perform Inter VLAN Routing and the VLANs will be communicate with each other.

7.6 VTP

VTP (Virtual Trunking Protocol) is a Cisco proprietary protocol used by Cisco switches to exchange VLAN information. With VTP, you can synchronize VLAN information (such as VLAN ID or VLAN name) with switches inside the same VTP domain. A VTP domain is a set of trunked switches with the matching VTP settings (the domain name, password and VTP version). All switches inside the same VTP domain share their VLAN information each other.

To better understand the true value of VTP, consider an example network with 100 switches. Without VTP, if you want to create a VLAN on each switch, you would have to manually enter VLAN configuration commands on every switch! VTP enables you to create the VLAN only on a single switch. That switch can then propagate information about the VLAN to every other switch

on the network and cause other switches to create it. Likewise, if you want to delete a VLAN, you only need to delete it on one switch, and the change is automatically propagated to every other switch inside the same VTP domain. The following network topology explains the concept more thoroughly:

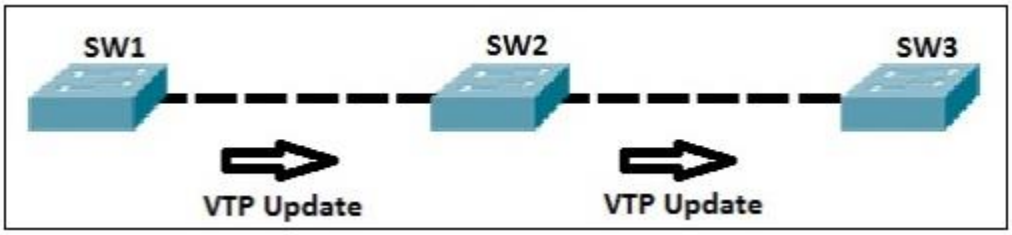

Figure 6.3 VTP Scenario

On SW1, we have created a new VLAN. SW1 sends a VTP update about the new VLAN to SW2, which in turn sends its VTP update to SW3. These updates will cause SW2 and SW3 to create the same VLAN. You can see how this simplifies network administration – the engineer only had to log in and create the VLAN on the first switch. Other switches have created the same VLAN automatically.

Note: VTP does not advertise information about which switch ports are assigned to which VLAN.

Three VTP versions are available – V1, V2, and V3. The first two versions are similar except that V2 adds support for token ring VLANs. V3 adds the following features:

- enhanced authentication
- support for extended VLANs (1006 to 4094). VTP versions 1 and 2 can propagate only VLANs 1 to 1005.
- support for private VLAN
- VTP primary server and VTP secondary servers
- VTP mode off that disables VTP
- backward compatibility with VTP V1 and V2
- the ability to be configured on a per-port basis

7.7 VTP Modes

Each switch can use one of four different VTP modes:

- **VTP client mode** – a switch using this mode can't change its VLAN configuration. That means that a VTP client switch cannot create or delete VLANs. However, received VTP updates are processed and forwarded.
- **VTP server mode** – a switch using this mode can create and delete VLANs. A VTP server switch will propagate VLAN changes. This is the default mode for Cisco switches.

- **VTP transparent mode** – a switch using this mode doesn't share its VLAN database, but it forwards received VTP advertisements. You can create and delete VLANs on a VTP transparent switch, but these changes will not be sent to other switches.
- **VTP mode off** – similar to VTP transparent mode, with a difference that a switch using this mode will not forward received VTP updates. This command is supported only in VTP V3.

As mentioned above, all switches are configured as VTP servers by default. This is fine in smaller networks without too many VLANs and VLAN changes, since all VLAN information can easily be stored in each switch's NVRAM. However, in larger networks, it is recommended to specify a couple of higher-quality switches to serve as VTP servers. All other switches in the network should be set up as VTP clients.

Consider the following example:

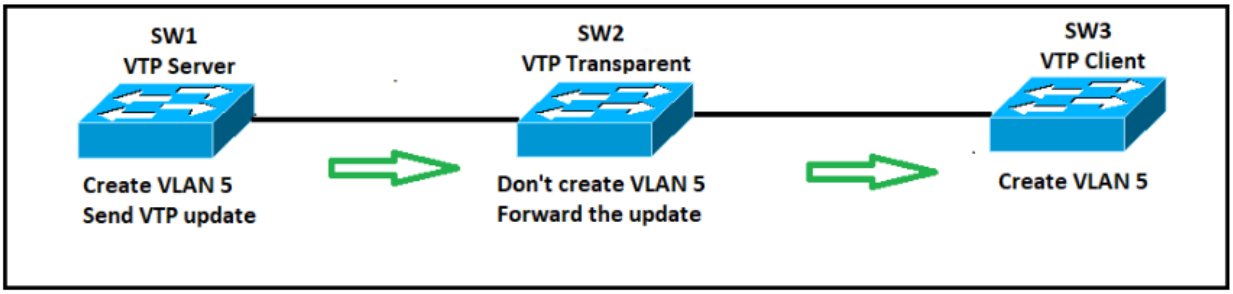

Figure 6.4 VTP Modes

We have a simple network of three switches. SW1 is configured as VTP server. After the VLAN 5 is created on SW1, this switch will notify the connected switch (SW2) about the created VLAN. SW2 will receive the update but, since it uses the VTP transparent mode, it will not create this VLAN in its configuration. However, it will forward the VTP update to SW3. Since SW3 is configured as VTP client, it will process the update and create VLAN 5.