kenet
Kenya Education Network

VLANS

Jackline Cherotich

Description of VLANs

- When you break a large LAN into smaller LANs, you create VLANs.
- VLANs are smaller LANs. VLANs create a boundary for broadcast messages.
-
- A VLAN is a logical grouping of network resources connected to administratively defined ports on a switch.
- VLANs break a large broadcast domain into smaller broadcast domains.
- Each VLAN creates a separate broadcast domain.

VLAN Ranges

- VLAN 1 - This is a default VLAN of switches. You cannot delete or edit this VLAN, but it can be used
- VLAN 2-1001- It is a normal VLAN range. You can create, edit, and delete it
- VLAN 1002-1005- These ranges are CISCO defaults for token rings and FDDI. You cannot delete this VLAN
- VLAN 1006-4094- It is an extended range of VLANs.
- VLAN 0 and 4095- Reserved VLAN. It can not been seen and cant be used

How to create VLANs

- We create two VLANs: **VLAN-10** and **VLAN-20** on the switch. We assign port-1 to 4 to **VLAN-10** and port-5 to 8 to **VLAN-20**. After this, ports 1, 2, 3, and 4 will share broadcast in **VLAN-10**, and ports 5, 6, 7, and 8 will share broadcast in **VLAN-20**.
-

- VLANs are similar to network segment. Devices in different VLANs cannot directly communicate. You need to connect them through a router.

Advantages of VLANs

•The main advantages of VLANs are the following.

- Solve broadcast problem
- Reduce the size of broadcast domains
- Allow us to add an additional layer of security
- Make device management easier
- Allow us to implement the logical grouping of devices by function instead of location

Disadvantages of VLANs

kenet
Kenya Education Network

•The main disadvantages of VLANs are the following.

- Increase network cost
- Add complexity to the network

Access Link and Trunk Link

Access Link and Trunk Link

- A switch supports two types of VLAN connections:
- Access link
- Trunk link.
- An access link connection carries the traffic of a single VLAN, whereas a trunk link connection carries the traffic of multiple VLANs.

Access link

- An **access link** belongs to and carries the traffic of only one VLAN.
- It transports the traffic in native formats with no VLAN information. It connects an end device to an access port.
- An access port works only with a single VLAN. Any device attached to an access port through an access link is unaware of a VLAN membership. It does not understand the VLAN concept and physical network topology. It assumes the connected link and network as a single broadcast domain.
- Switches remove all VLAN information from frames before forwarding them through access ports.

Trunk link

Trunk link

•A **trunk link** belongs to and carries the traffic of multiple VLANs. It transports the traffic with VLAN information. It connects another switch or the device that understands VLANs to a trunk port.

•A trunk port works with multiple VLANs. It adds VLAN information to frames before forwarding them. Since it attaches VLAN information to frames, the device connected to it must understand VLAN concepts. You can attach a switch or a router to a trunk port.

•

•Encapsulation modes

Encapsulation modes

•A trunk port adds VLAN information to frames before forwarding them. It can use one of two trunking protocols to add VLAN information. These protocols are **ISL** and **802.1Q**. **802.1Q** is the default encapsulation protocol. The following command changes the default encapsulation method to **ISL**.

•ISL

ISL

•ISL stands for Inter-Switch Link. It is a Cisco proprietary trunking protocol. By default, a switch port works only with a single VLAN. A trunking protocol allows it to work with multiple VLANs.

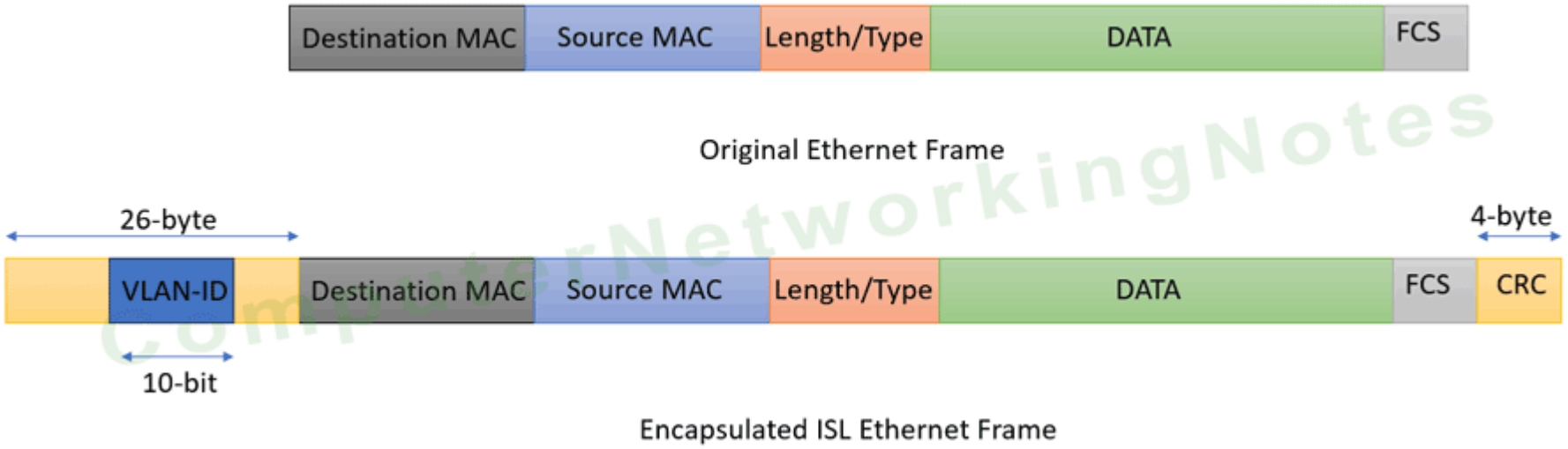
•The **switchport mode trunk** command converts an access port into a trunk port. This command runs in interface configuration mode. The following commands convert the **FastEthernet 0/1** port into a trunk port.

How ISL trunking protocol works

How ISL trunking protocol works

- ISL trunking protocol uses a 26-byte header and a 4-byte trailer to carry VLAN information with frames. It uses the header to store VLAN information. Each header contains a 10-bit VLAN ID. In addition to the header, it appends a 4-byte CRC to the end of each frame. This CRC is in addition to FCS that the Ethernet frame requires.

ISL Encapsulation



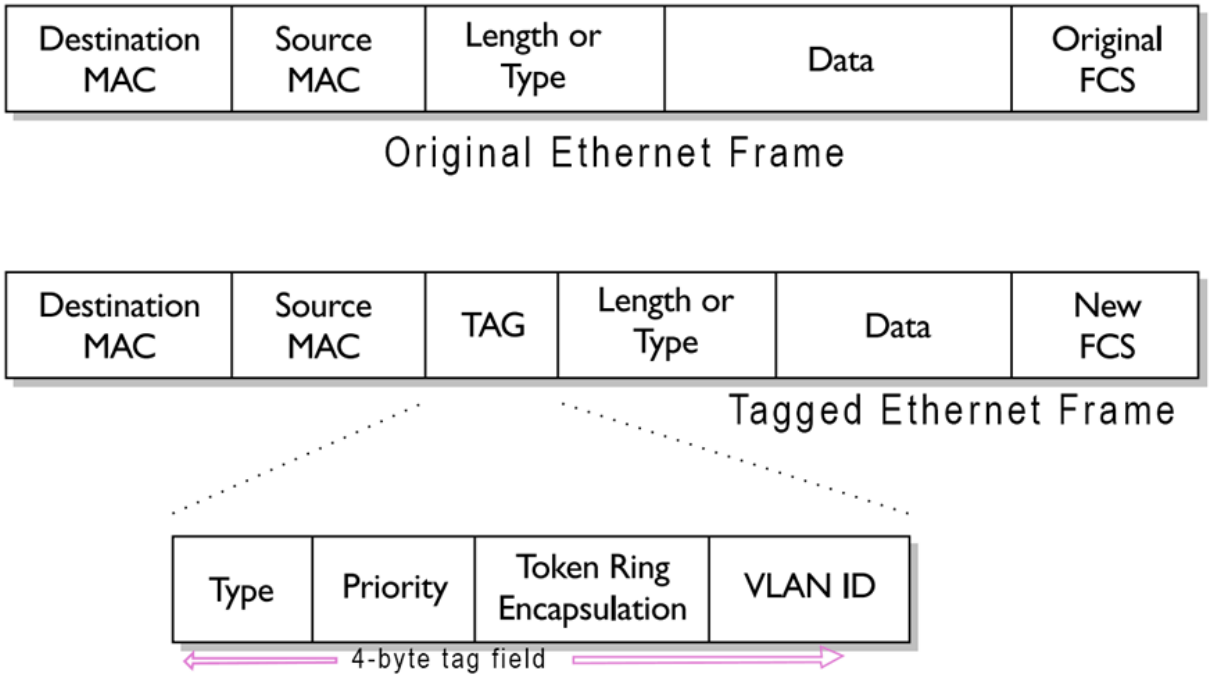
- On the sending device, it adds a header and trailer to frames. On the receiving device, it uses the VLAN ID stored in the header to identify the VLAN the frame belongs to. It uses CRC to verify the state of the frame. It removes the header and trailer from frames before forwarding them to their native VLAN ports.

802.1Q Encapsulation

•802.1Q Encapsulation

•802.1Q is a trunking protocol. IEEE developed it for trunk connections. A trunk connection carries traffic of multiple VLANs. 802.1Q adds VLAN information in each frame to identify its VLAN. To add VLAN information, it uses a 4-byte field called a **tag**. It inserts the tag into the header of the Ethernet frame.

Tagged Frames



Native VLAN concept of 802.1Q

•802.1Q allows us to configure a native VLAN. A native VLAN is a VLAN that you configure on the trunk port. For example, if you configure VLAN-20 on the trunk port, VLAN-20 becomes the native VLAN.

•802.1Q does not insert VLAN identification tags into frames that belong to the native VLAN. It forwards them in their original condition. It inserts a VLAN identification tag into a frame only if the frame does not belong to the native VLAN.

•For example, if you configure VLAN-20 on a trunk port, it does not tag frames that the switch receives on ports having VLAN-20. It will tag frames that the switch receives on ports not having VLAN-20.

Key points:-

- 802.1Q trunks support two types of frames: tagged and untagged.
- An untagged frame does not carry any VLAN identification information in it.
- A tagged frame carries VLAN identification information in it.

Inter-VLAN routing

•Inter-VLAN routing

•A VLAN is a logical subnet. Devices in different VLANs can not communicate directly. They can communicate through a router. To provide connectivity between different VLANs, you need to configure one router interface in each VLAN.

•

•

•To provide connectivity between these VLANs, they need many Ethernet interfaces. For example, they need 25 routers having two Ethernet ports to connect 50 VLANs.

•Virtualization solves this problem. It allows us to turn a physical interface into many virtual interfaces. Each virtual interface works as a separate interface. On router, this feature is also known as **router-on-stick**.

Inter-VLAN routing

kenet
Kenya Education Network

- To create a virtual interface and enter interface configuration mode, we use the same command we use on the physical interface. The only difference is we add a number to the physical interface's number.
- In interface configuration mode, we need to configure two options: the protocol type of the incoming traffic and an IP address.
- This port will receive traffic from a trunk port. A trunk port uses the **dot1Q** protocol. The *encapsulation dot1Q* command sets the encapsulation type to **dot1Q**. This command also needs a VLAN number as an argument. We need to specify the VLAN whose traffic this virtual interface will process.
- After configuring the encapsulation type, we need to assign an IP address to this interface.
- The IP address, we configure here works as the default gateway of the VLAN.
-

Configuration steps

- The following command creates a virtual interface for VLAN-10.

```
Router(config)#interface FastEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.0.0.1 255.0.0.0
Router(config-subif)#exit
```

- The following command creates a virtual interface for VLAN-20.

```
Router(config)#interface FastEthernet 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 20.0.0.1 255.0.0.0
Router(config-subif)#exit
Router(config)#
```

kenet
Kenya Education Network

Q & A

kenet
Kenya Education Network

THANK YOU

www.kenet.or.ke
Jomo Kenyatta Memorial
Library, University of Nairobi
P. O Box 30244-00100, Nairobi.
0732 150 500 / 0703 044 500
support@kenet.or.ke / jcherotich@kenet.or.ke