

CCNA (200-301) Cisco Certified Network Associate

Prepared by Eng. Taghreed Elsayed

Lecture 4

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

مزيد من التفاصيل

VLAN Concepts



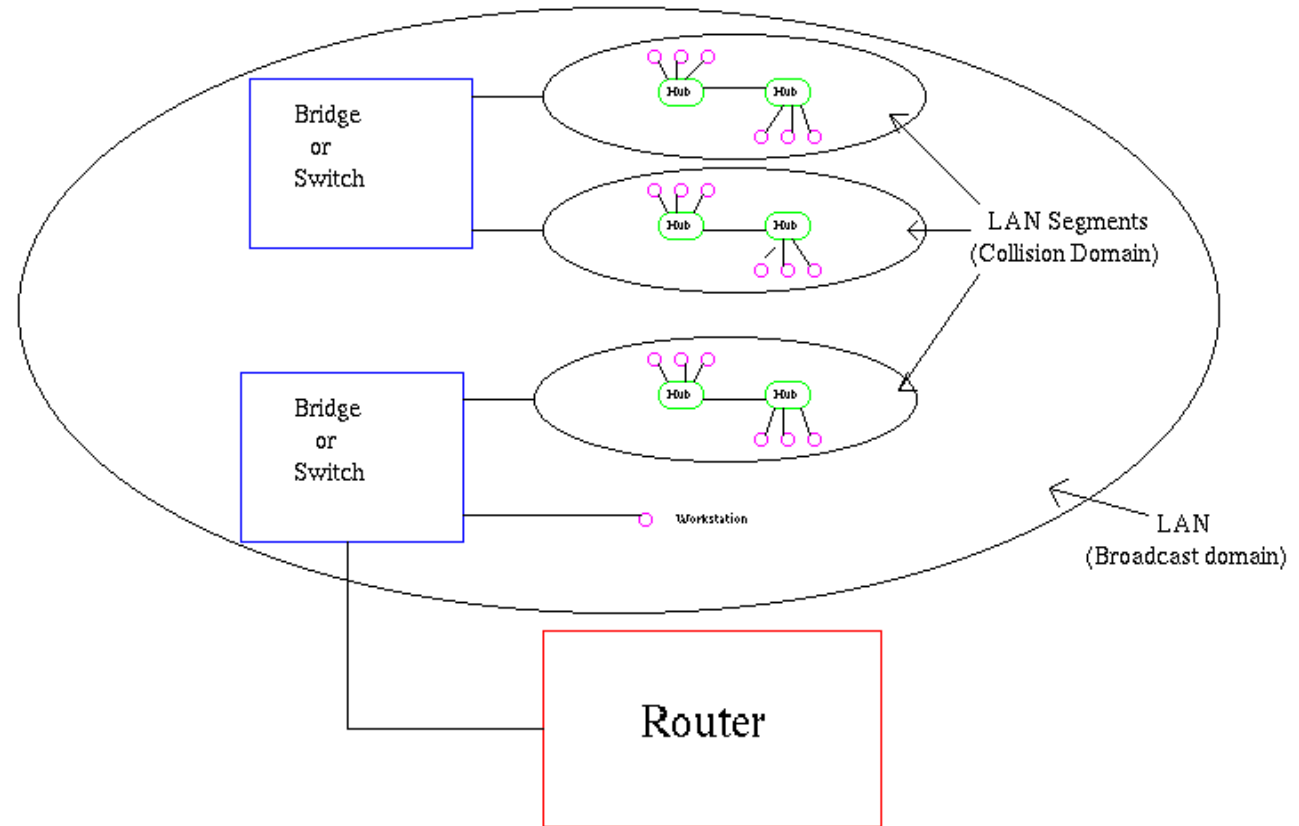
جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

What are VLAN's?

In a traditional LAN, workstations are connected to each other by means of a hub or a repeater. These devices propagate any incoming data throughout the network. However, if two people attempt to send information at the same time, a collision will occur and all the transmitted data will be lost. Once the collision has occurred, it will continue to be propagated throughout the network by hubs and repeaters. The original information will therefore need to be resent after waiting for the collision to be resolved, thereby incurring a significant wastage of time and resources. To prevent collisions from traveling through all the workstations in the network, a bridge or a switch can be used. These devices will not forward collisions, but will allow broadcasts (to every user in the network) and multicasts (to a pre-specified group of users) to pass through. A router may be used to prevent broadcasts and multicasts from traveling through the network.

VLAN concepts

- ❖ The workstations, hubs, and repeaters together form a LAN segment. A LAN segment is also known as a collision domain since collisions remain within the segment. The area within which broadcasts and multicasts are confined is called a broadcast domain or LAN .
- ❖ Thus a LAN can consist of one or more LAN segments. Defining broadcast and collision domains in a LAN depends on how the workstations, hubs, switches, and routers are physically connected together. This means that everyone on a LAN must be located in the same area.

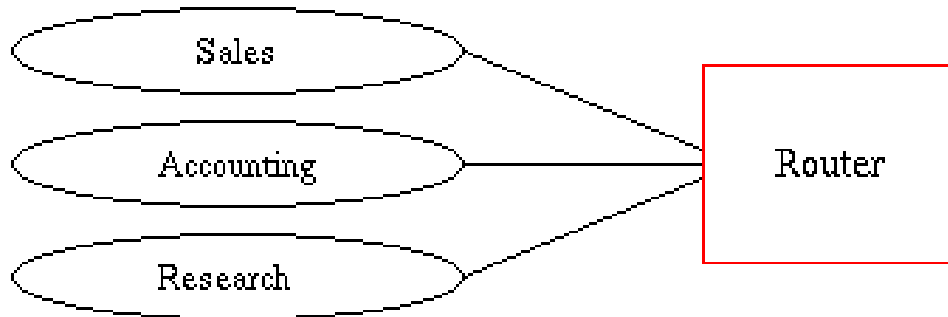


VLAN concepts

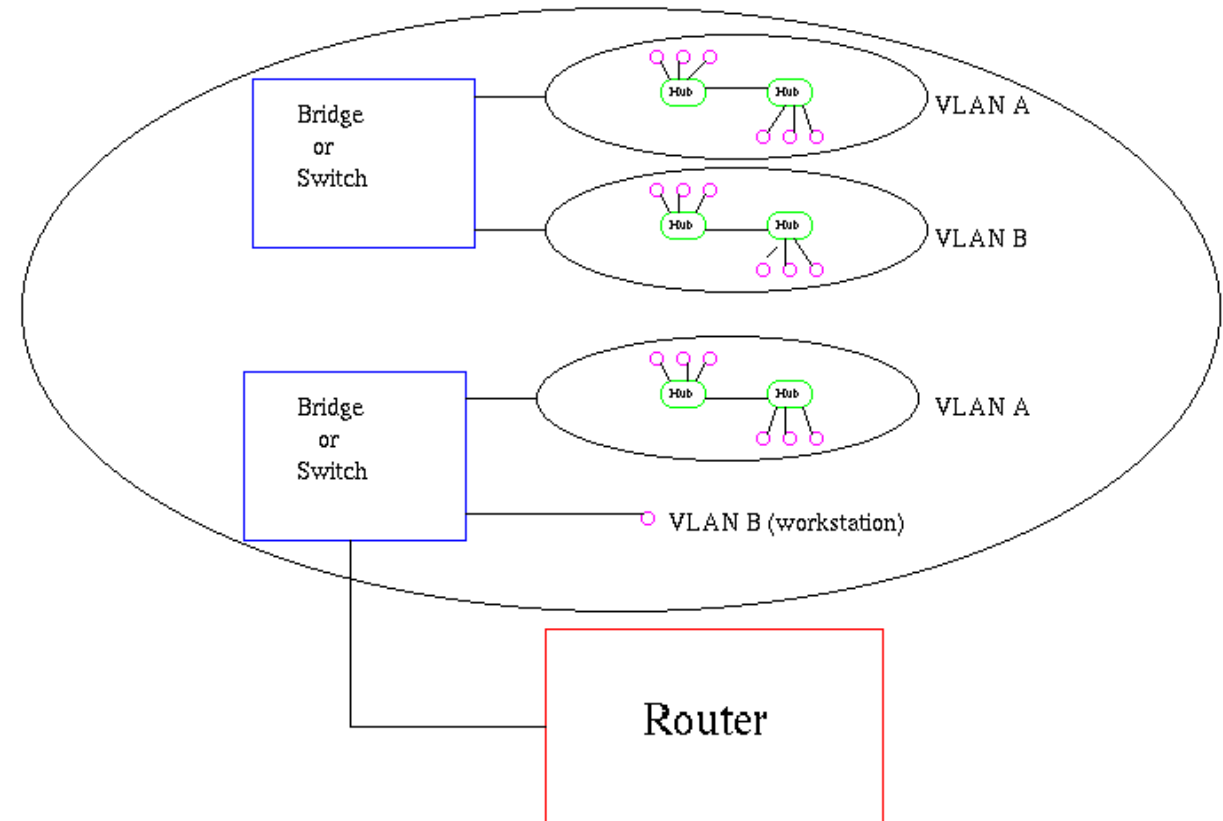
- ❖ VLAN's allow a network manager to logically segment a LAN into different broadcast domains. Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together. Users on different floors of the same building, or even in different buildings can now belong to the same LAN.
- ❖ VLAN's also allow broadcast domains to be defined without using routers. Bridging software is used instead to define which workstations are to be included in the broadcast domain. Routers would only have to be used to communicate between two VLAN's

VLAN Concepts

Logical View



Physical View



Why use VLAN's?

VLAN's offer a number of advantages over traditional LAN's. They are:

1) Performance

In networks where traffic consists of a high percentage of broadcasts and multicasts, VLAN's can reduce the need to send such traffic to unnecessary destinations. For example, in a broadcast domain consisting of 10 users, if the broadcast traffic is intended only for 5 of the users, then placing those 5 users on a separate VLAN can reduce traffic .

Compared to switches, routers require more processing of incoming traffic. As the volume of traffic passing through the routers increases, so does the latency in the routers, which results in reduced performance. The use of VLAN's reduces the number of routers needed, since VLAN's create broadcast domains using switches instead of routers.

2) Formation of Virtual Workgroups

Nowadays, it is common to find cross-functional product development teams with members from different departments such as marketing, sales, accounting, and research. These workgroups are usually formed for a short period of time. During this period, communication between members of the workgroup will be high. To contain broadcasts and multicasts within the workgroup, a VLAN can be set up for them. With VLAN's it is easier to place members of a workgroup together. Without VLAN's, the only way this would be possible is to physically move all the members of the workgroup closer together.

3) Security

Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a VLAN can reduce the chances of an outsider gaining access to the data. VLAN's can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion.

4) Simplified Administration

Seventy percent of network costs are a result of adds, moves, and changes of users in the network. Every time a user is moved in a LAN, recabling, new station addressing, and reconfiguration of hubs and routers becomes necessary. Some of these tasks can be simplified with the use of VLAN's. If a user is moved within a VLAN, reconfiguration of routers is unnecessary. In addition, depending on the type of VLAN, other administrative work can be reduced or eliminated. However the full power of VLAN's will only really be felt when good management tools are created which can allow network managers to drag and drop users into different VLAN's or to set up aliases.

Despite this saving, VLAN's add a layer of administrative complexity, since it now becomes necessary to manage virtual workgroups.

5) Reduced Cost

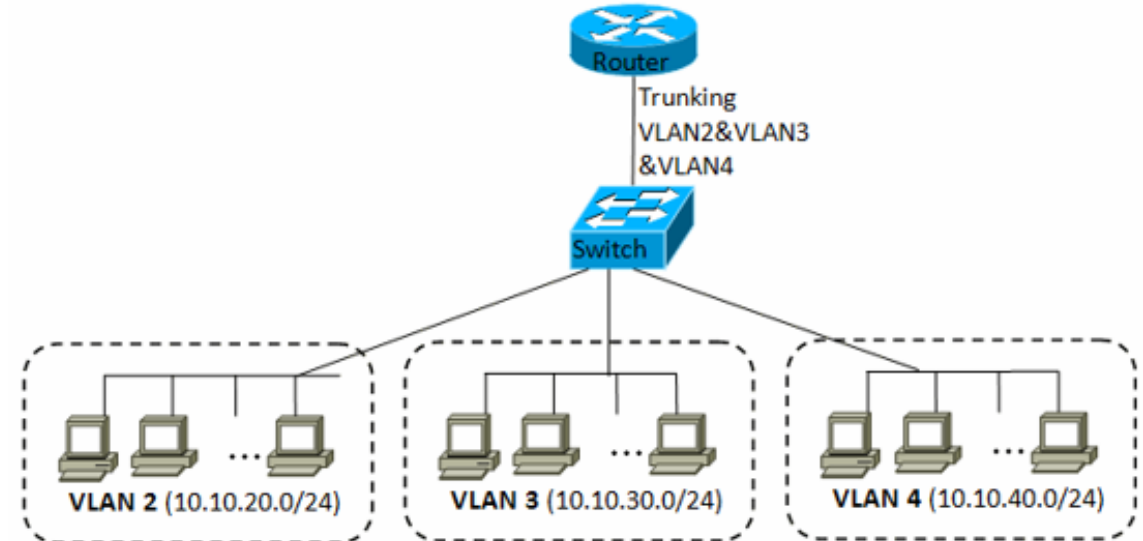
VLAN's can be used to create broadcast domains which eliminate the need for expensive routers.

❑ Saving VLAN Configuration

- ❖ VLAN Configuration is stored inside **Flash** in a file called **VLAN.dat**.

❑ Default VLANS is found on CISCO device

- ❖ For Ethernet ports all ports by default on **VLAN1**.
- ❖ For legacy system VLANS [1002-1005] is found but, no active.



VLAN

Switches port modes

Administrative mode

1. Dynamic Desirable (default)
2. Dynamic Auto
3. Trunk
4. Access

Operational mode

1. Trunk
2. Static Access

Chapter 02

VLAN

SW1 F1/0 Administrative mode	SW2 F1/0 Admin mode	Operational mode
Dynamic Desirable (active : negotiate trunking)	D.D	Trunk
	D.A	Trunk
	T	Trunk
	A	Access
Dynamic Auto	D.D	Trunk
	T	Trunk
	DA	Access
	A	Access
trunk	D.D	Trunk
	D.A	Trunk
	T	Trunk
	A	Down
Access	D.D	Access
	D.A	Access
	A	Access
	T	Down



❖ Access port

- ☐ Belong to single VLAN.
- ☐ NO VLAN ID attached on the packet.
- ☐ (NO tagging) so we can not use it between different switches to connect between the same VLAN in different switches.
- ☐ Used with hosts.

❖ Trunk Port

- ☐ Belong all VLANS on switch
- ☐ Used to tag the packets exchanged between switches with source VLAN ID Using one of two protocols:

A. ISL

B. IEEE 802.1Q(dot 1q)

❖ VLAN Tagging :

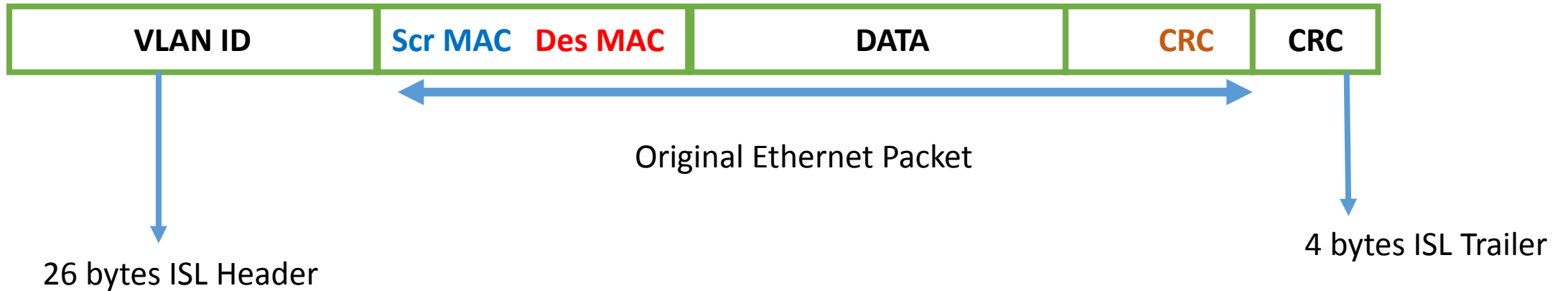
The original Ethernet packet did not contain VLAN ID



VLAN Tagging : means that we are using **trunking protocols** to insert the Source VLAN ID on the packet

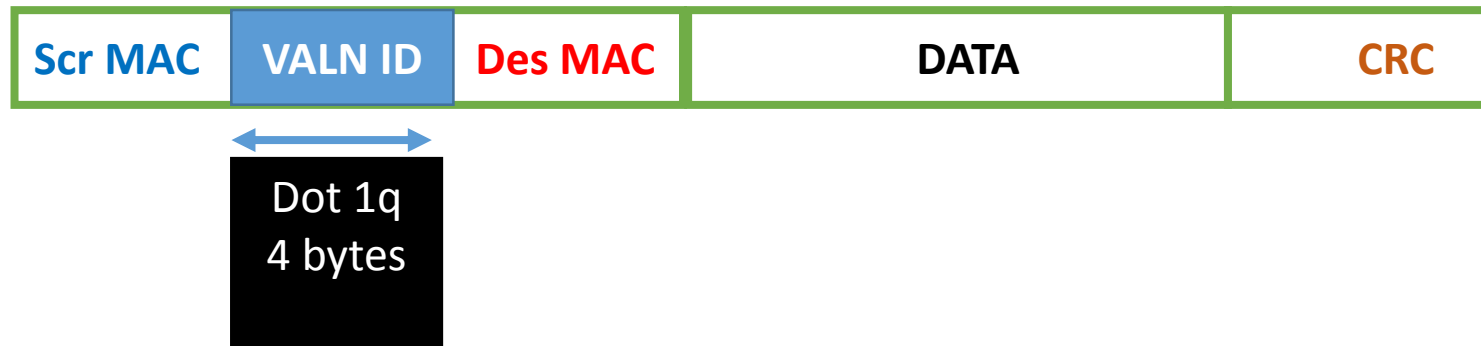
❖ ISL (Inter Switch Layer)

- ❑ CISCO Trunking Protocol
- ❑ Used only between CISCO switches
- ❑ ISL adds 26 bytes header & 4 bytes trailer to the original Ethernet packet (frame)
[totally ,added 30 bytes].



❖ IEEE 802.1q (dot 1q)

- ❑ Industry standard trunking protocol
- ❑ Modify the original Ethernet header by adding 4 bytes field contains VLAN ID , then recalculate CRC



❖ dot 1q

- ☐ Use Native VLAN
- ☐ Packets from Native VLAN untagged
- ☐ BY default VLAN1 is the Native VLAN
- ☐ Only one Native VLAN is defined in the switch
- ☐ If we change Native VLAN in one switch , we must change it in the others.



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

