Corso di Laurea in Ingegneria Informatica

Corso di Reti di Calcolatori I

Roberto Canonico (roberto.canonico@unina.it)
Giorgio Ventre (giorgio.ventre@unina.it)

Virtual LAN: VLAN

I lucidi presentati al corso sono uno strumento didattico
che NON sostituisce i testi indicati nel programma del corso
I lucidi sono adattati dagli originali di J. Kurose e K. Ross e fanno riferimento al testo
***Reti di calcolatori e Internet - Un approccio top-down* (4a ed.)**

Nota di copyright per le slide COMICS

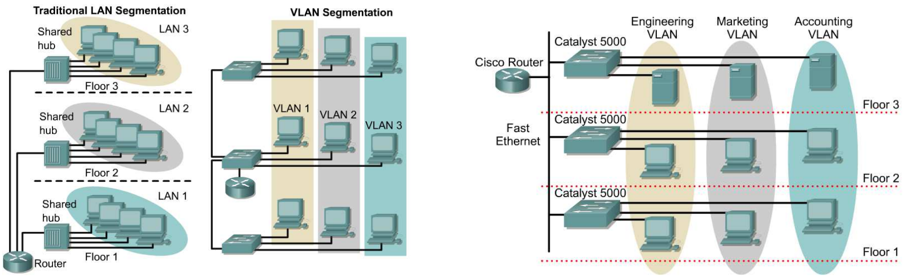
Nota di Copyright

Autori:
Simon Pietro Romano, Antonio Pescapè, Stefano Avallone,
Marcello Esposito, Roberto Canonico, Giorgio Ventre

VLAN

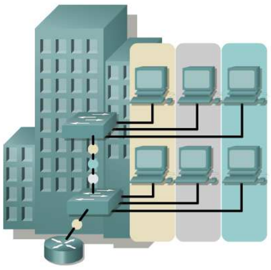
- **<u>Problema</u>**: far coesistere sulla stessa infrastruttura di rete fisica due o più reti IP distinte
- Gli switch possono gestire gruppi di porte in modo che gli host connessi a ciascun gruppo costituiscano una ***rete Ethernet virtuale*** separata dalle altre (VLAN)

VLAN introduction



- **VLANs provide segmentation based on broadcast domains**
- VLANs logically segment switched networks based on the project teams, or applications of the organization regardless of the physical location or connections to the network
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location

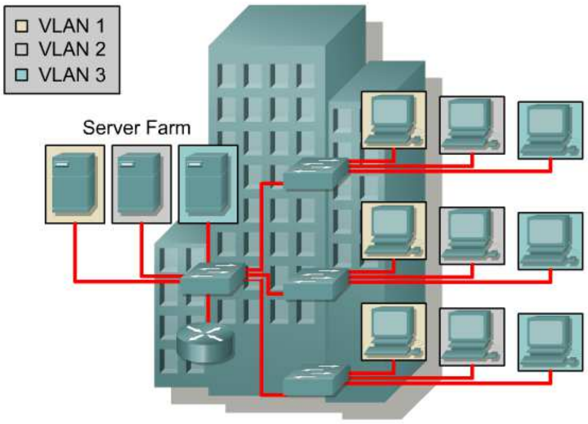
VLAN introduction (2)



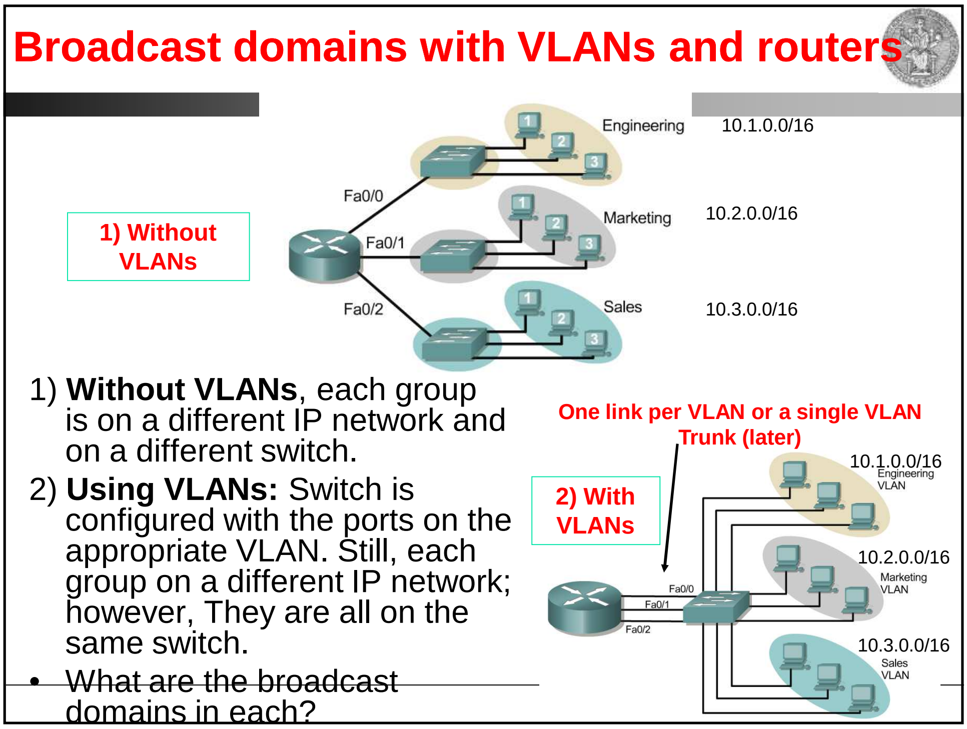
- A group of ports or users in same broadcast domain
- Can be based on port ID, MAC address, protocol, or application
- LAN switches and network management software provide a mechanism to create VLANs
- Frame tagged with VLAN ID

- VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations
- VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain
- **Traffic should only be routed between VLANs**

Broadcast domains with VLANs and routers



- A VLAN is a broadcast domain created by one or more switches
- The network design above creates three separate broadcast domains



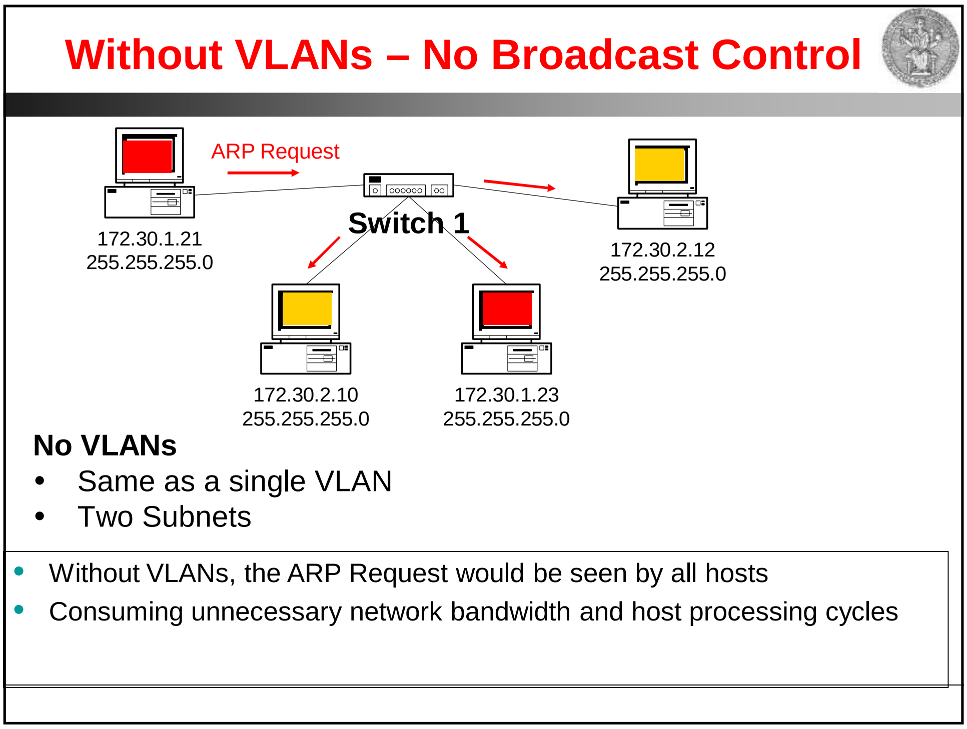
Broadcast domains with VLANs and routers

1) **Without VLANs**, each group is on a different IP network and on a different switch.

2) **Using VLANs:** Switch is configured with the ports on the appropriate VLAN. Still, each group on a different IP network; however, They are all on the same switch.

- What are the broadcast domains in each?

One link per VLAN or a single VLAN Trunk (later)



Without VLANs – No Broadcast Control

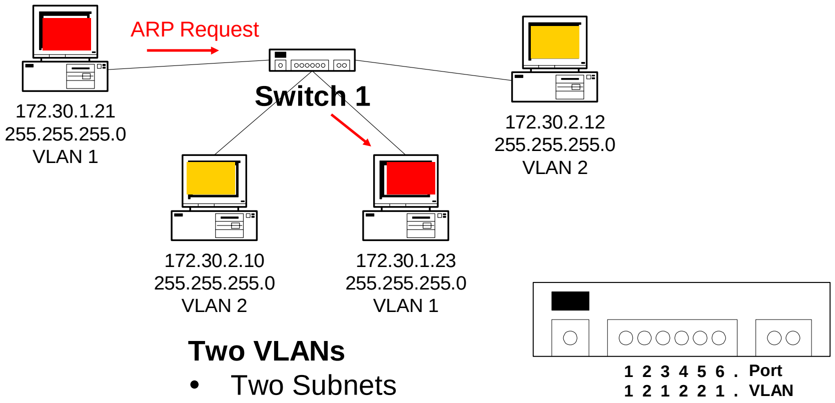
No VLANs

- Same as a single VLAN
- Two Subnets

- Without VLANs, the ARP Request would be seen by all hosts
- Consuming unnecessary network bandwidth and host processing cycles

With VLANs – Broadcast Control

Switch Port: VLAN ID

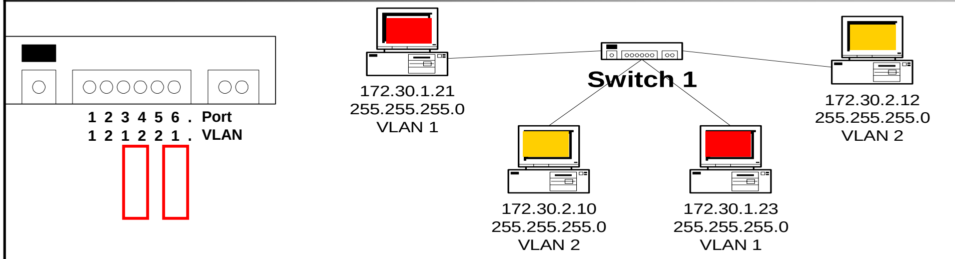


1	2	3	4	5	6	.	Port
1	2	1	2	2	1	.	VLAN

Two VLANs

- Two Subnets

VLAN operation



1	2	3	4	5	6	.	Port
1	2	1	2	2	1	.	VLAN

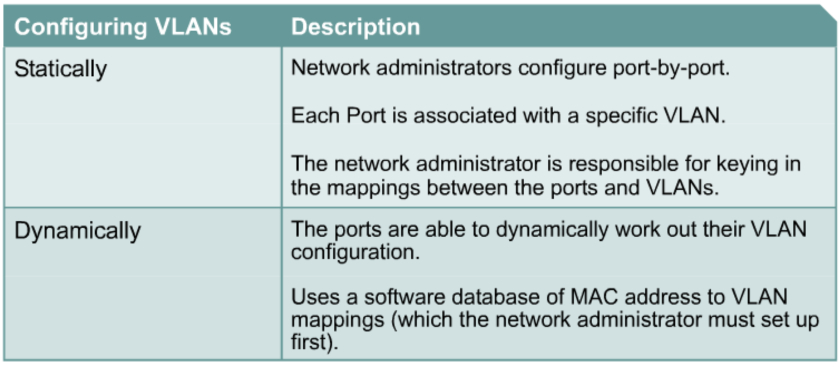
Two VLANs

- Two Subnets

Important notes on VLANs:

- VLANs are assigned on the switch port
  There is no “VLAN” assignment done on the host (usually)
- In order for a host to be a part of that VLAN, it must be assigned an IP address that belongs to the proper subnet. Remember: VLAN = Subnet
- Assigning a host to the correct VLAN is a 2-step process:
  1. Connect the host to the correct port on the switch
  2. Assign to the host the correct IP address depending on the VLAN membership

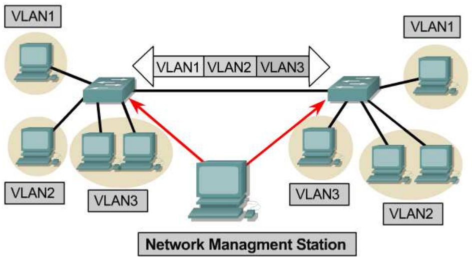
VLAN operation



Configuring VLANs	Description
Statically	Network administrators configure port-by-port. Each Port is associated with a specific VLAN. The network administrator is responsible for keying in the mappings between the ports and VLANs.
Dynamically	The ports are able to dynamically work out their VLAN configuration. Uses a software database of MAC address to VLAN mappings (which the network administrator must set up first).

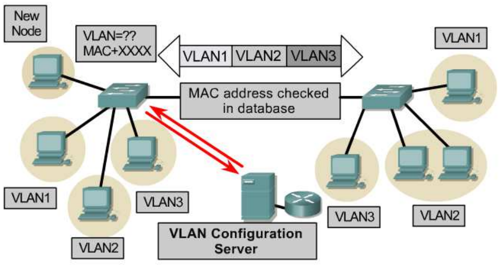
- Each switch port can be assigned to a different VLAN
- Ports assigned to the same VLAN share broadcasts
- Ports that do not belong to that VLAN do not share these broadcasts

VLAN operation



- **Static membership VLANs are called port-based VLANs**
- As a device enters the network, it automatically assumes the VLAN membership of the port to which it is attached
- The **default VLAN** for every port in the switch is the management VLAN (VLAN1) and **<u>may not be deleted</u>**
- All other ports on the switch may be reassigned to alternate VLANs

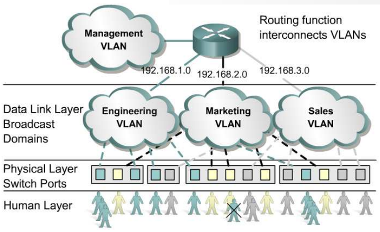
VLAN operation



- Dynamic membership VLANs are created through network management software
  - Not as common as static VLANs
- Dynamic VLANs allow for membership based on the MAC address of the device connected to the switch port
- As a device enters the network, it queries a database within the switch for a VLAN membership

Benefits of VLANs

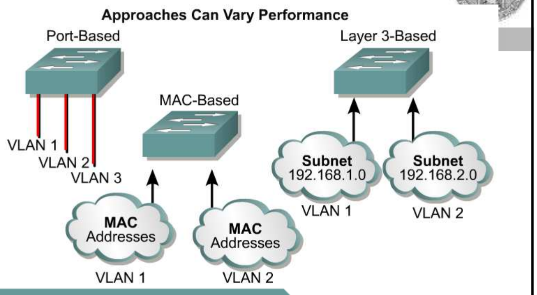
All users attached to the same switch port must be in the same VLAN.



If a hub is connected to VLAN port on a switch, all devices on that hub must belong to the same VLAN

- The key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically
- This means that an administrator is able to do all of the following:
  - Easily move workstations on the LAN
  - Easily add workstations to the LAN
  - Easily change the LAN configuration
  - Easily control network traffic
  - Improve security

VLAN Types

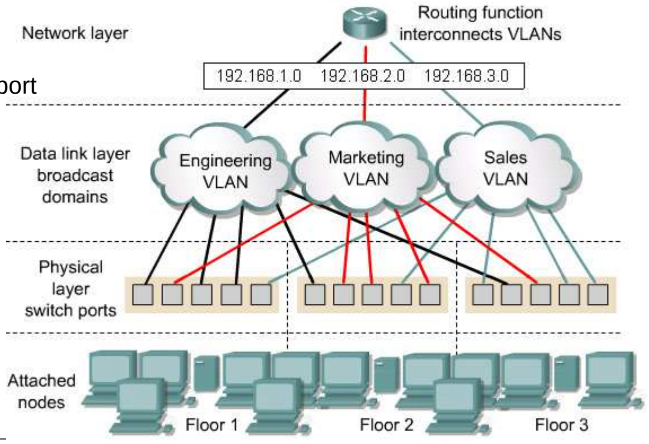


VLAN Types	Description
Port-based	• Most common configuration method. • Ports assigned individually, in groups, in rows, or across 2 or more switches. • Simple to use. • Often implemented where Dynamic Host Control Protocol (DHCP) is used to assign IP addresses to network hosts.
MAC address	• Rarely implemented today. • Each address must be entered into the switch and configured individually. • Users find it useful. • Difficult to administer, troubleshoot and manage.
Protocol Based	• Configured like MAC addresses, but instead uses a logical or IP address. • No longer common because of DHCP.

VLAN operation

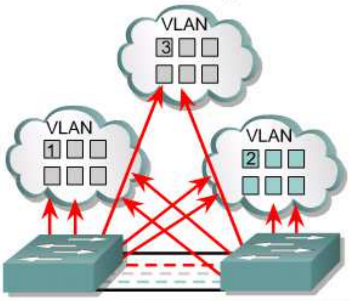
- In port-based or port-centric VLAN membership, the port is assigned to a specific VLAN membership independent of the user or system attached to the port.

- All users of the same port must be in the same VLAN



Membership by Port

Maximizes Forwarding Performance



- User assigned by port association
- Requires no lookup if done in ASICs
- Easily administered via GUIs
- Maximizes security between VLANs
- Packets do not "leak" into other domains
- Easily controlled across network

Membership by MAC-Addresses

Requires Filtering, Impacts Performance

MAC Address Tables
VLAN 1 020701AEF1A OA032192FA2A 026765175GA3A
VLAN 2 050503G4GF2A 040404THTB3A 070706GGGF3A

Table Exchange

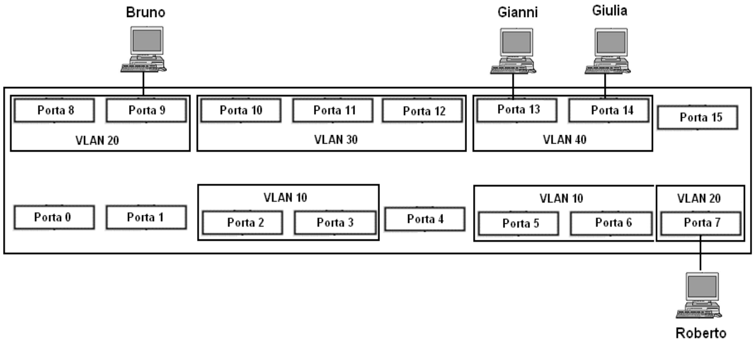
MAC Address Tables
VLAN 1 020701AEF1A OA032192FA2A 026765175GA3A
VLAN 2 050503G4GF2A 040404THTB3A 070706GGGF3A

Table Adds
Administrative Overhead

- User assigned based on MAC addresses
- Offers flexibility, yet adds overhead
- Impacts performance, scalability, and administration
- Offers similar process for higher layers

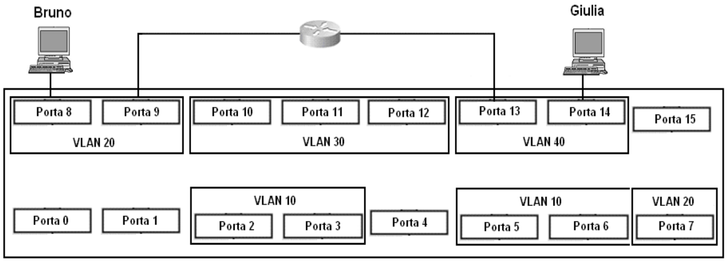
Comunicazione con VLAN

- Nella configurazione di VLAN rappresentata in figura, Gianni può inviare frame soltanto a Giulia



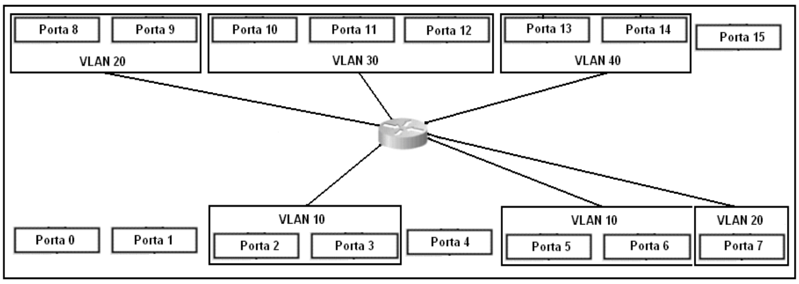
Comunicazione tra VLAN diverse

- Per fare comunicare VLAN diverse occorre creare un ponte attraverso un dispositivo apposito
  - bridge se opera a livello Ethernet (L2)
  - router se opera a livello rete (L3)



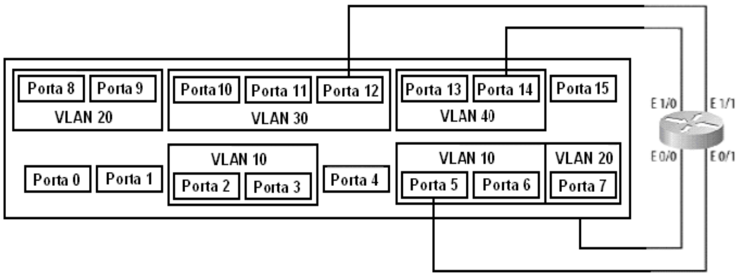
Switch/router

- Molti produttori offrono dispositivi in grado di svolgere contemporaneamente le funzioni di switch a livello Ethernet e di router a livello 3
- Questi dispositivi creano la connessione tra VLAN a livello 3



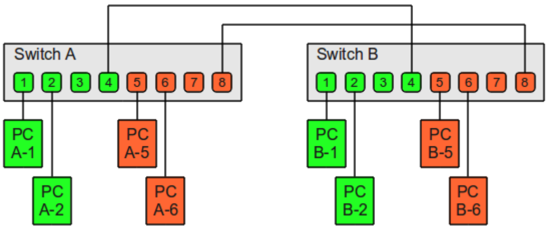
Connessione a livelli superiori (1)

- In linea di principio, si potrebbe ottenere lo stesso risultato collegando le interfacce di un router a tutte le coppie di VLAN



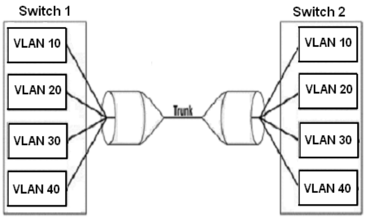
VLAN Trunking (1)

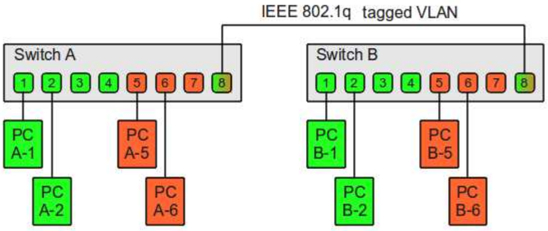
- La presenza delle VLAN crea un problema nella connessione tra due o più switch
  - Se collego la porta di uno switch a una porta di un altro switch, la connessione riguarderà solo le VLAN che comprendono le due porte utilizzate
  - Occorrerebbero quindi tanti collegamenti quante sono le VLAN da collegare



VLAN trunking (2)

- Il trunking abilita la connessione tra le VLAN di switch diversi
  - Perché lo switch di destinazione sappia a quale VLAN inoltrare i frame in arrivo su una porta di trunking, occorre *taggare* (contrassegnare) i frame con l'identificativo della VLAN di destinazione
  - Questo non è previsto dal protocollo Ethernet originale

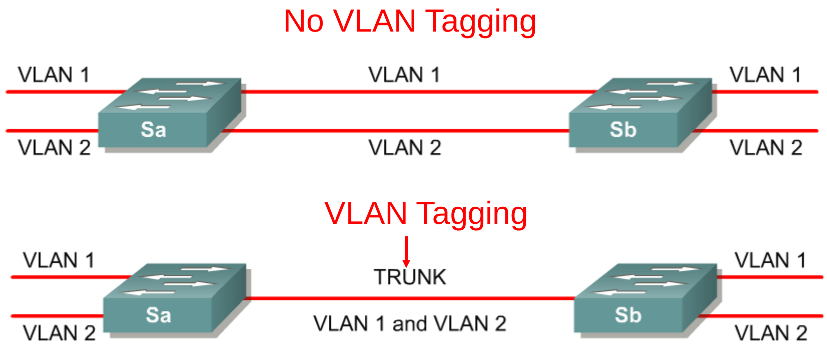




VLAN Tagging

- **VLAN Tagging is used when a link needs to carry traffic for more than one VLAN**
  - **Trunk link:** As packets are received by the switch from any attached end-station device, a unique packet identifier is added within each header.
- **This header information designates the VLAN membership of each packet**
- The packet is then forwarded to the appropriate switches or routers based on the VLAN identifier and MAC address
- Upon reaching the destination node (Switch) the VLAN ID is removed from the packet by the adjacent switch and forwarded to the attached device
- Packet tagging provides a mechanism for controlling the flow of broadcasts and applications while not interfering with the network and applications
- This is known as a trunk link or VLAN trunking

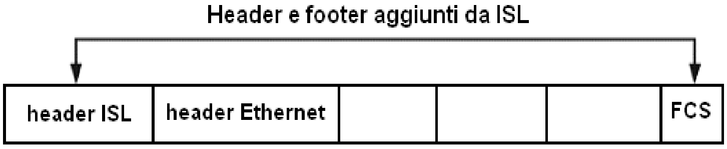
VLAN Tagging



- VLAN Tagging is used when a single link needs to carry traffic for more than one VLAN

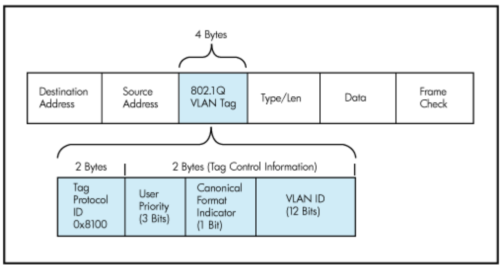
Protocolli di trunking (1)

- **Protocolli a incapsulamento**
  - Viene aggiunto uno header al frame Ethernet per indicare la VLAN di destinazione
  - Es. Cisco Inter-Switch Link (ISL)



Protocolli di trunking (2)

- Protocolli a piggyback (IEEE.802Q)
  - L’identificativo della VLAN (12 bit) è parte di un campo da 4 byte inserito nel frame Ethernet tra i campi indirizzo sorgente e tipo
  - Occorre ricalcolare il CRC all’ingresso e all’uscita dal trunk


4 Bytes
Destination Address
Source Address
802.1Q VLAN Tag
Type/Len
Data
Frame Check
2 Bytes
2 Bytes (Tag Control Information)
Tag Protocol ID 0x8100
User Priority (3 Bits)
Canonical Format Indicator (1 Bit)
VLAN ID (12 Bits)