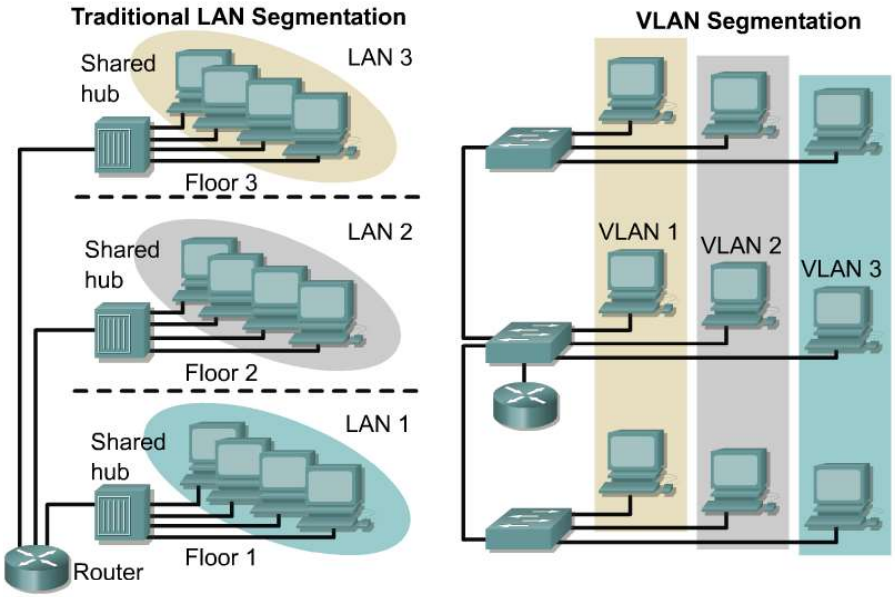
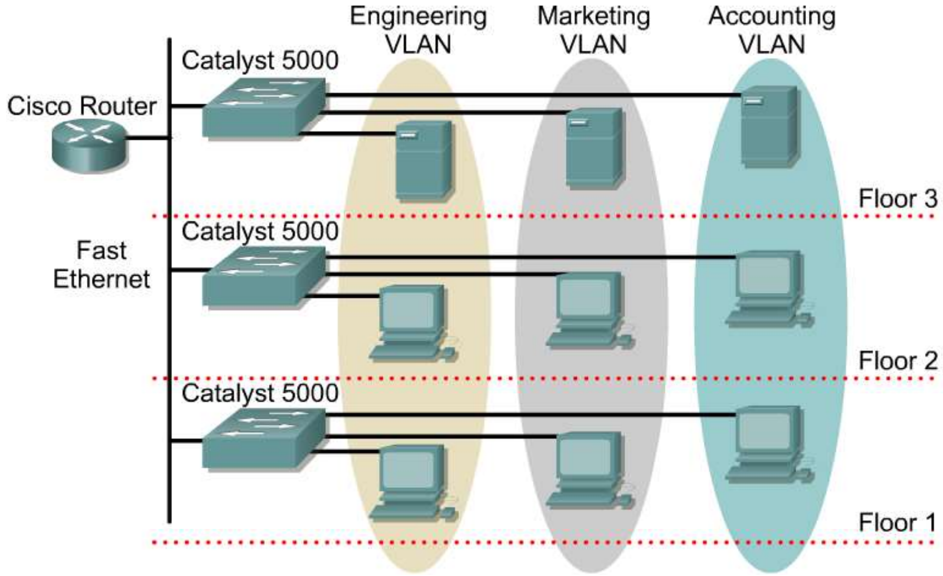
Overview

- VLAN
- Trunking
- Configure
- Troubleshoot

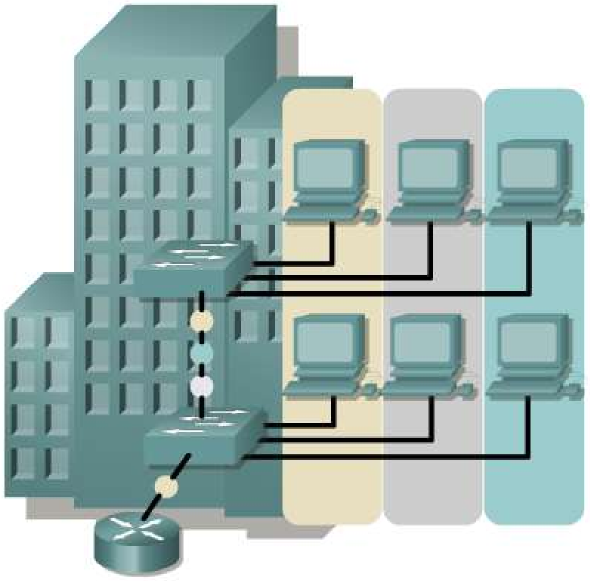
VLAN introduction





- **VLANs provide segmentation based on broadcast domains.**
- VLANs logically segment switched networks based on the functions, 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.

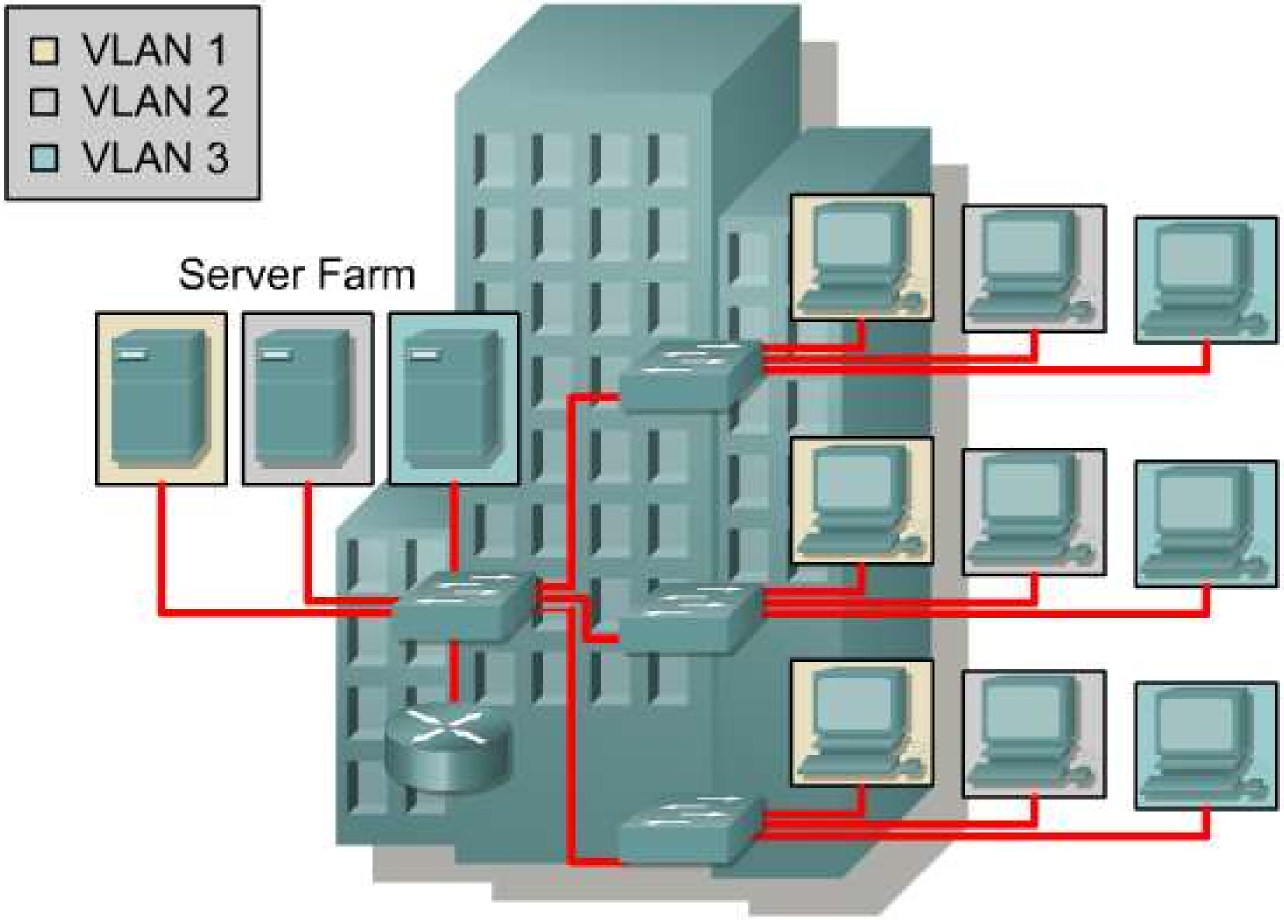
VLAN introduction



- 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.

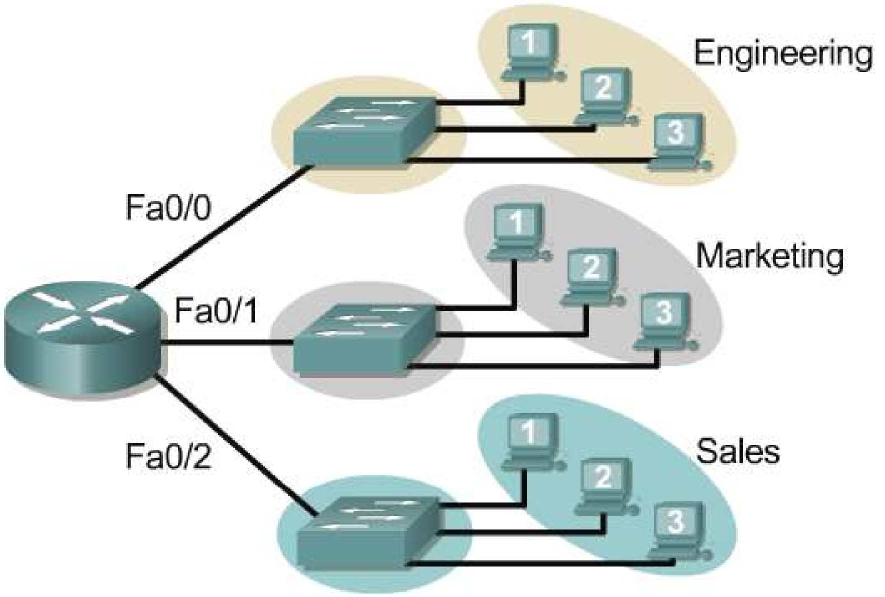
Broadcast domains with VLANs and routers



- 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



10.1.0.0/16

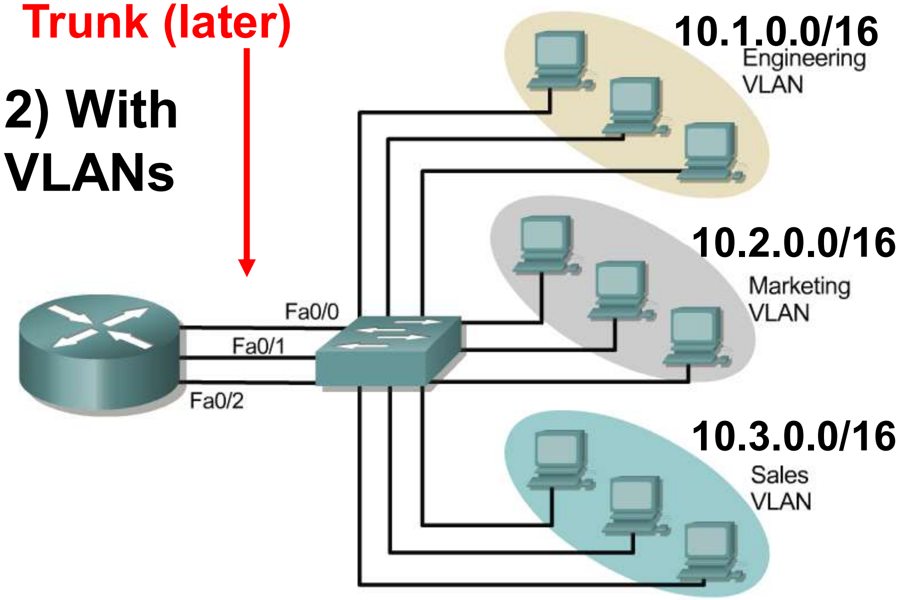
10.2.0.0/16

10.3.0.0/16

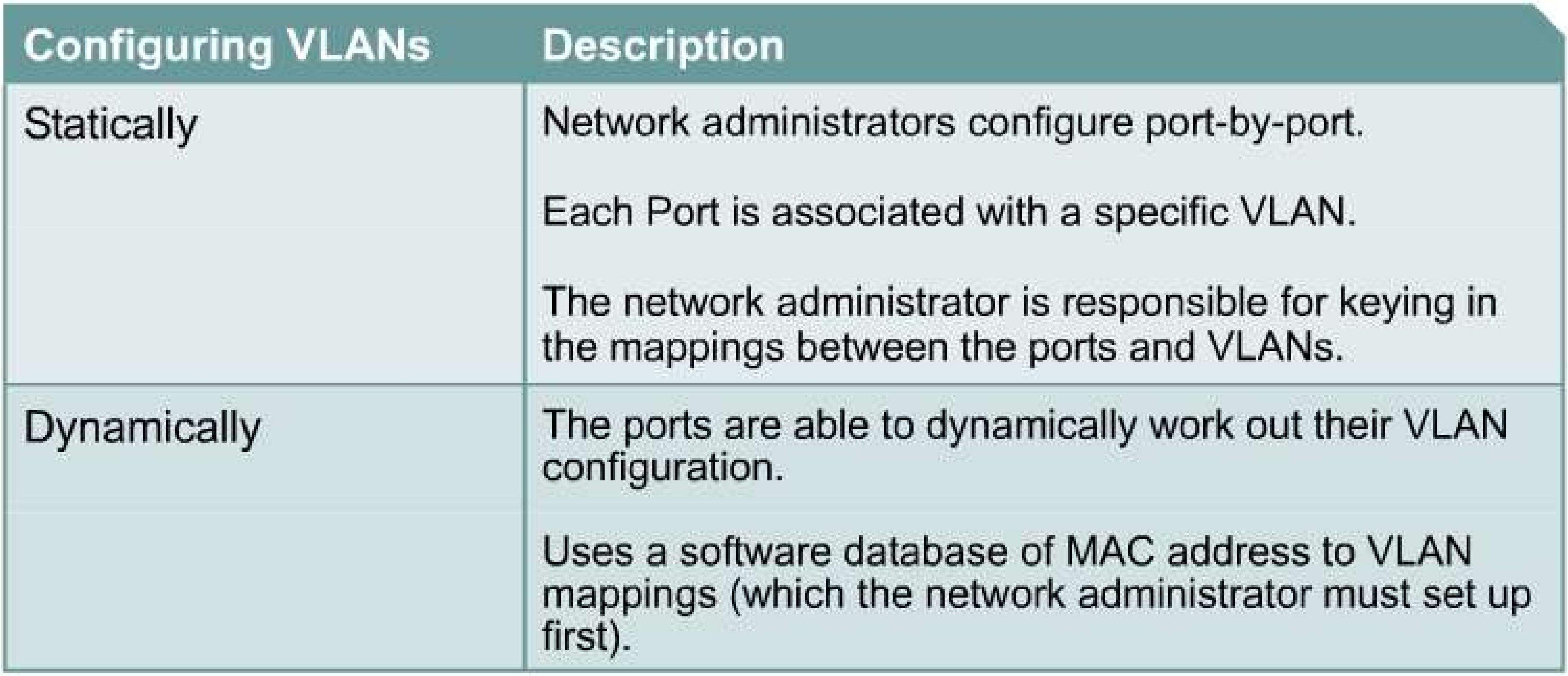
- 1) Without VLANs, each group is on a different IP network and on a different switch.
- 2) Using VLANs. Switch is configured with the ports on the appropriate VLAN. Still, each group on a different IP network; however, They are all on the same switch.
- What are the broadcast domains in each?

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

2) With VLANs



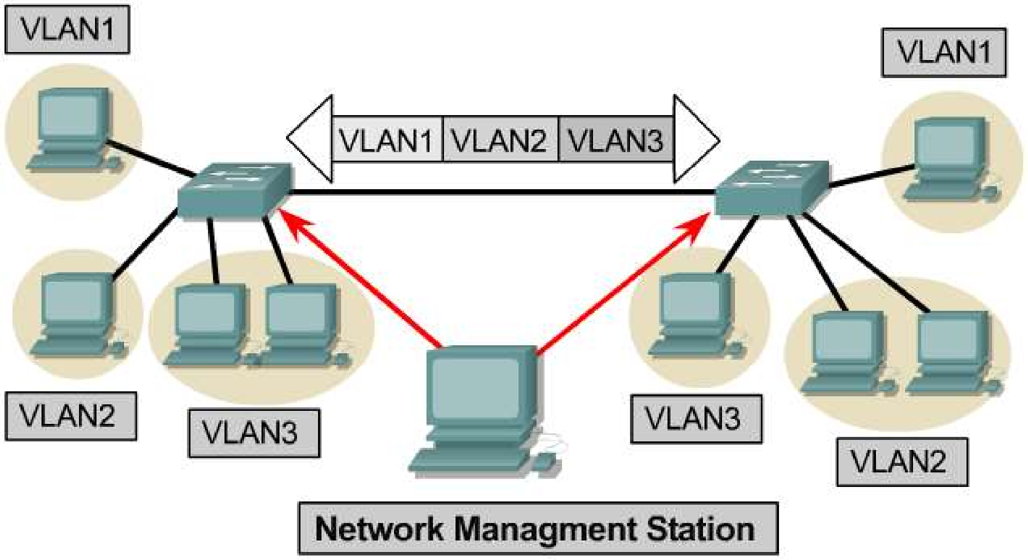
VLAN operation



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).

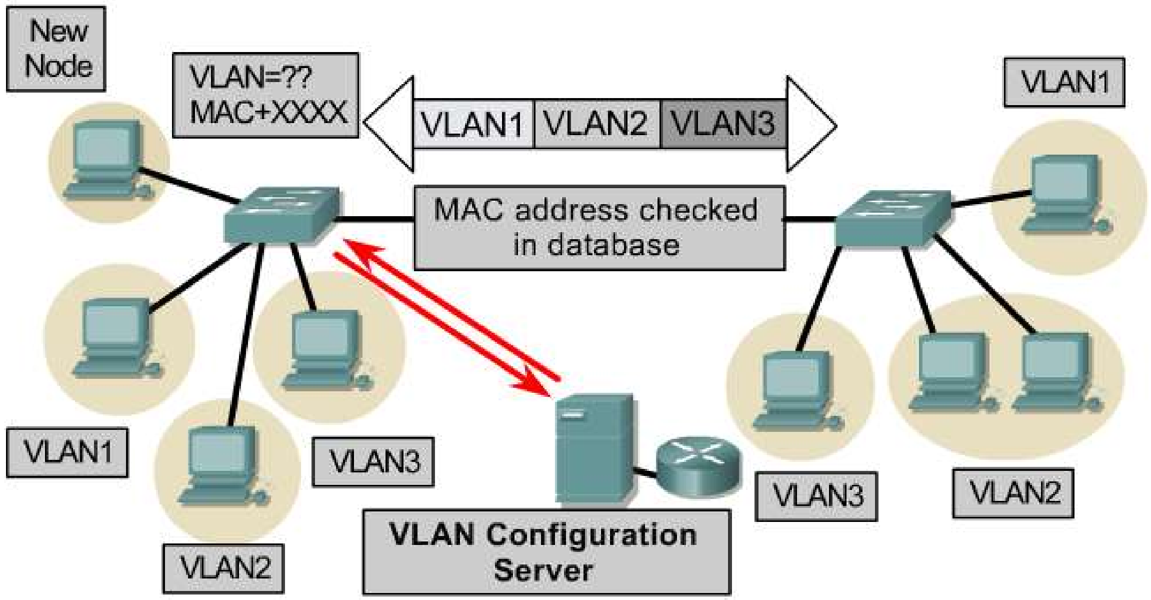
- Each switch port can be assigned to a different VLAN.
- Ports assigned to the same VLAN share broadcasts.
- Ports that do not belong to that VLAN do not share these broadcasts.

VLAN operation



- **Static membership VLANs are called port-based and port-centric membership 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. The management VLAN is always VLAN 1 **and may not be deleted."**
  - ***This statement does not give the whole story. We will examine Management, Default and other VLANs at the end.***
- All other ports on the switch may be reassigned to alternate VLANs.
- More on VLAN 1 later.

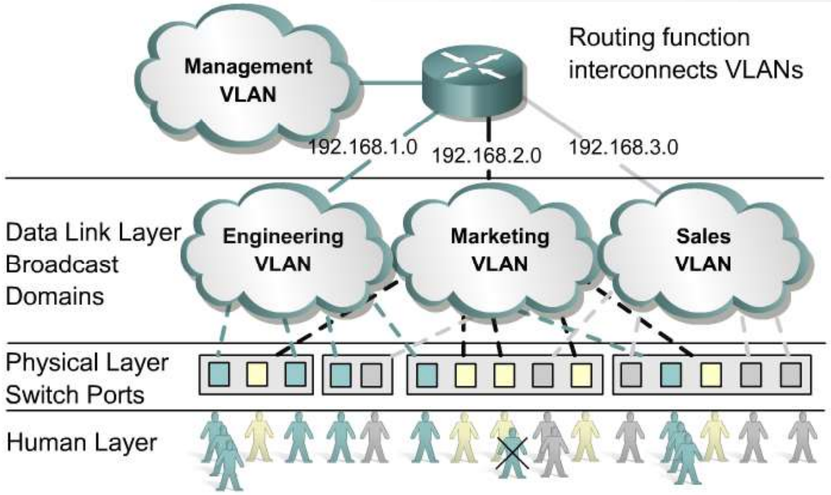
VLAN operation



- **Dynamic membership VLANs are created through network management software. (<u>Not</u> as common as static VLANs)**
- **<u>CiscoWorks 2000 or CiscoWorks for Switched Internetworks</u>** is used to create Dynamic 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

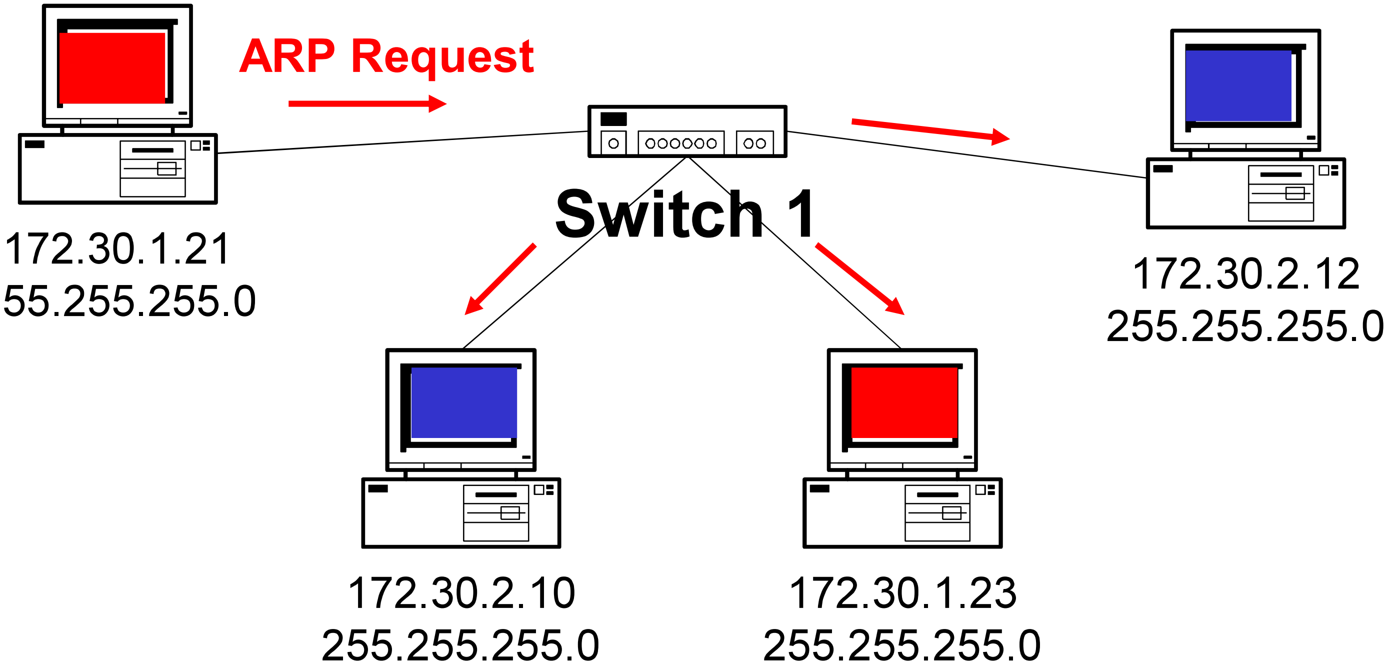
All users attached to the same switch port must be in the same VLAN.



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.

Without VLANs – No Broadcast Control

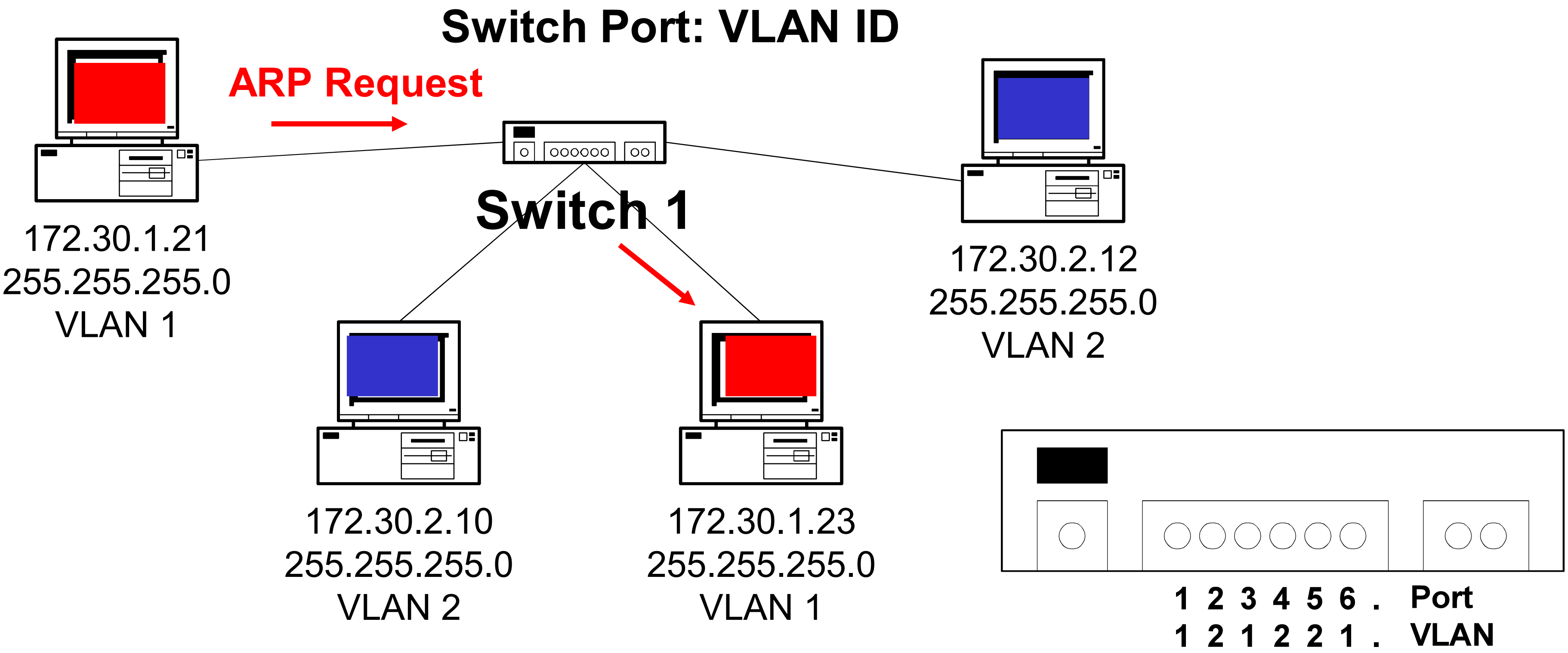


No VLANs

- Same as a single VLAN
- Two Subnets

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

With VLANs – Broadcast Control



Switch Port: VLAN ID

ARP Request

Switch 1

172.30.1.21
255.255.255.0
VLAN 1

172.30.2.12
255.255.255.0
VLAN 2

172.30.2.10
255.255.255.0
VLAN 2

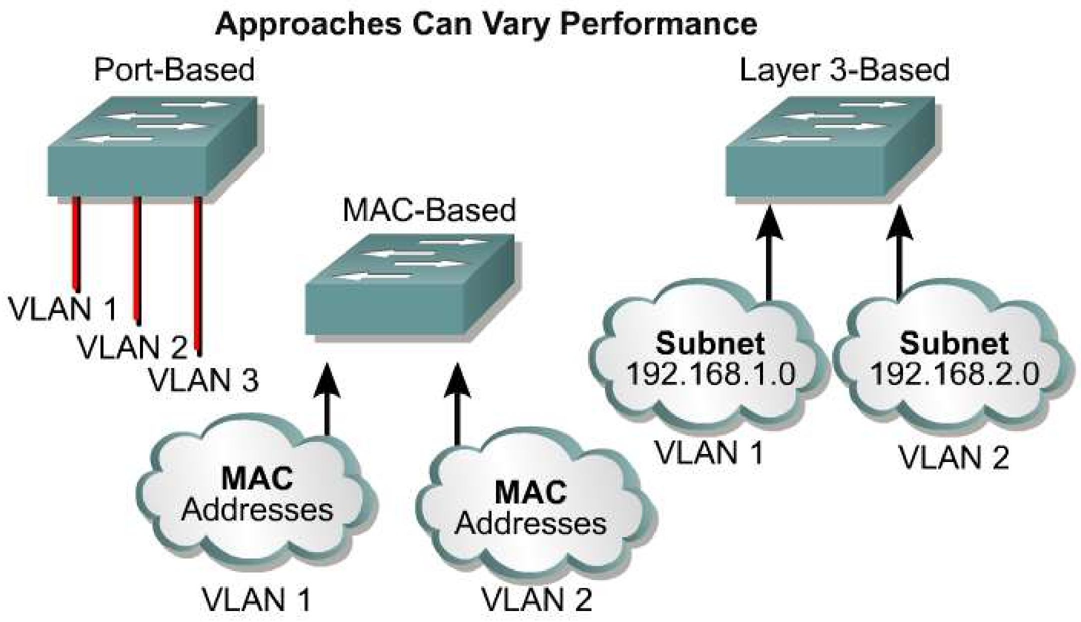
172.30.1.23
255.255.255.0
VLAN 1

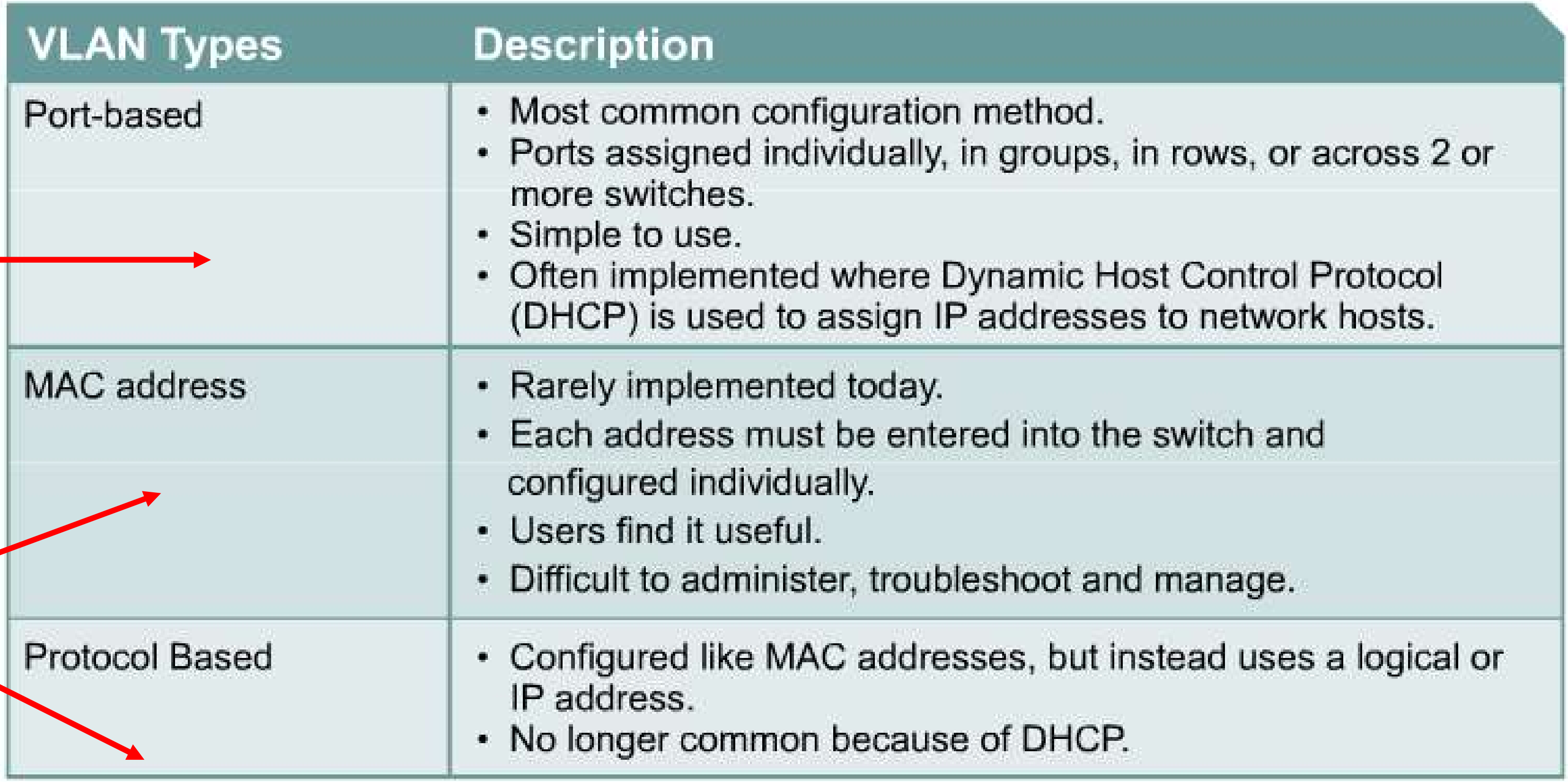
1	**2**	**3**	**4**	**5**	**6**	**.**	**Port**
1	**2**	**1**	**2**	**2**	**1**	**.**	**VLAN**

Two VLANs

- Two Subnets

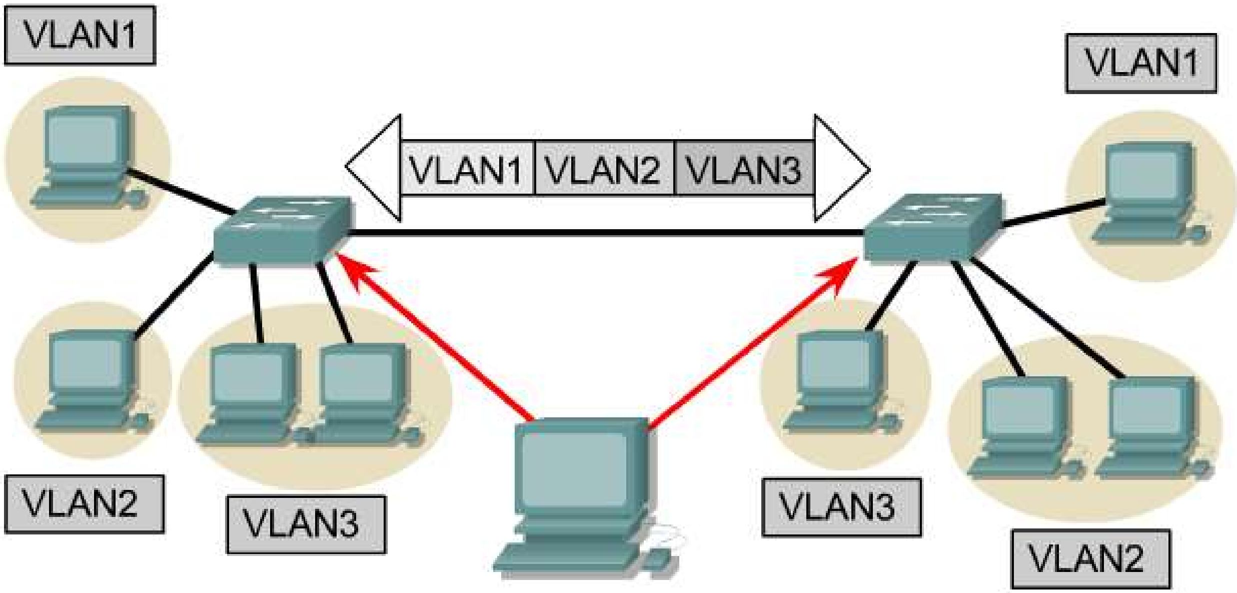
VLAN Types





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.

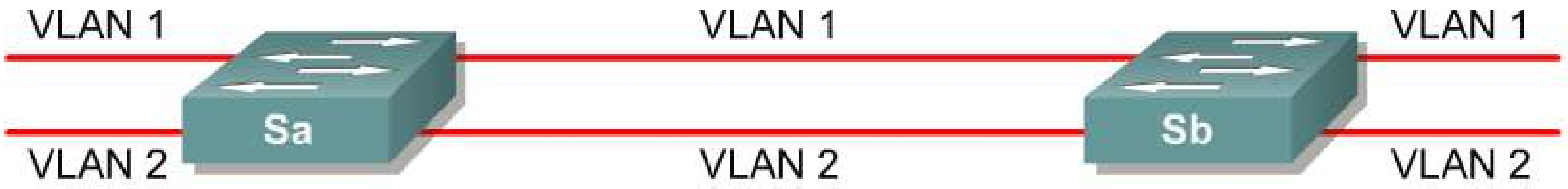
VLAN Tagging



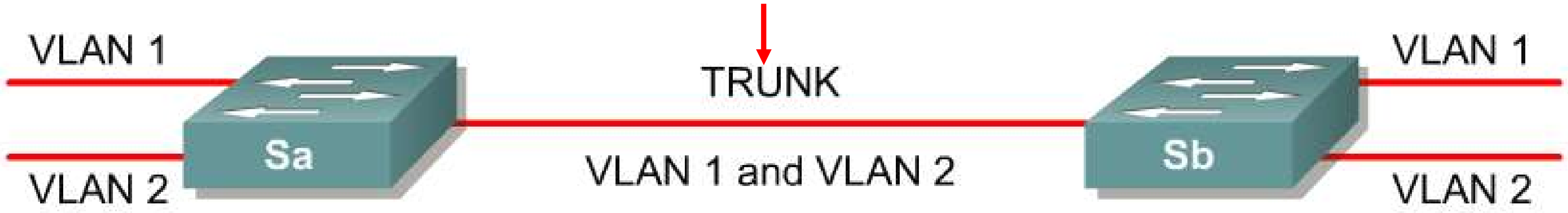
- **VLAN Tagging is used when a link needs to carry traffic for more than one VLAN.**
  - **Trunk link:** As packets are received by the switch from any attached end-station device, a unique packet identifier is added within each header.
- **This header information designates the VLAN membership of each 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

No VLAN Tagging

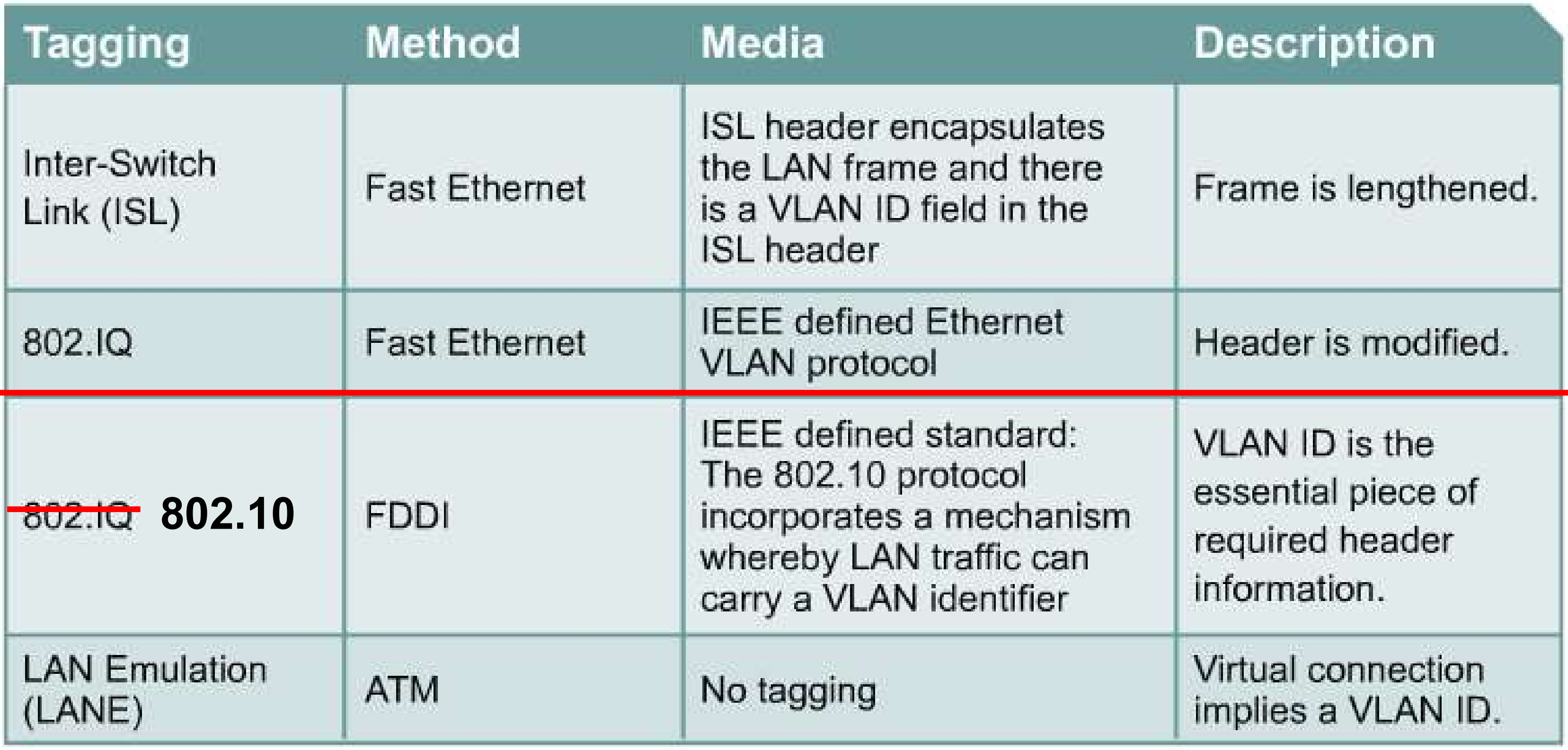


VLAN Tagging



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

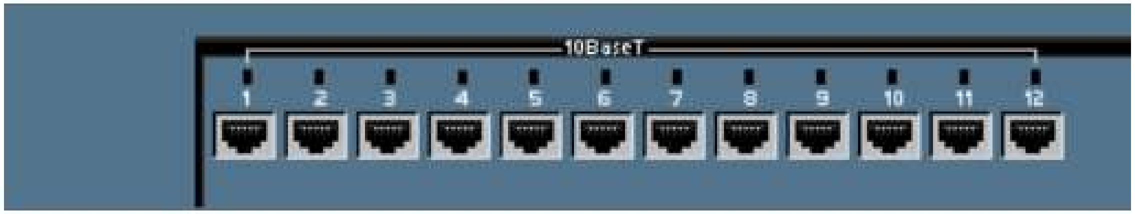
VLAN Tagging



Tagging	Method	Media	Description
Inter-Switch Link (ISL)	Fast Ethernet	ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header	Frame is lengthened.
802.IQ	Fast Ethernet	IEEE defined Ethernet VLAN protocol	Header is modified.
~~802.IQ~~ **802.10**	FDDI	IEEE defined standard: The 802.10 protocol incorporates a mechanism whereby LAN traffic can carry a VLAN identifier	VLAN ID is the essential piece of required header information.
LAN Emulation (LANE)	ATM	No tagging	Virtual connection implies a VLAN ID.

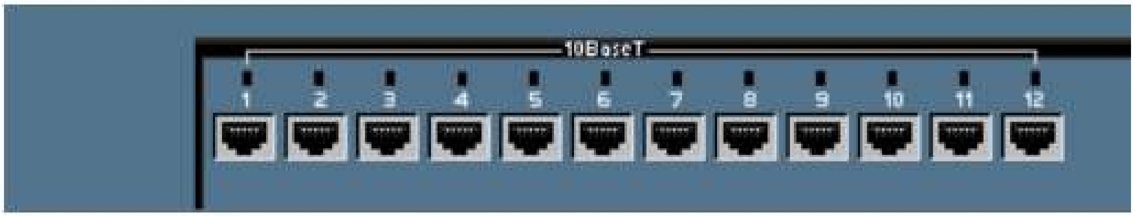
- There are two major methods of frame tagging, Cisco proprietary **Inter-Switch Link (ISL)** and **IEEE 802.1Q**.
- ISL used to be the most common, but is now being replaced by 802.1Q frame tagging.
- Cisco recommends using 802.1Q.
- VLAN Tagging and Trunking will be discussed in the next chapter.

Configuring static VLANs



- The following guidelines must be followed when configuring VLANs on Cisco 29xx switches:
  - The maximum number of VLANs is switch dependent.
    - 29xx switches commonly allow 4,095 VLANs
  - VLAN 1 is one of the factory-default VLANs.
  - VLAN 1 is the default Ethernet VLAN.
  - Cisco Discovery Protocol (CDP) and VLAN Trunking Protocol (VTP) advertisements are sent on VLAN 1.
  - The Catalyst 29xx IP address is in the VLAN 1 broadcast domain by default.

Creating VLANs



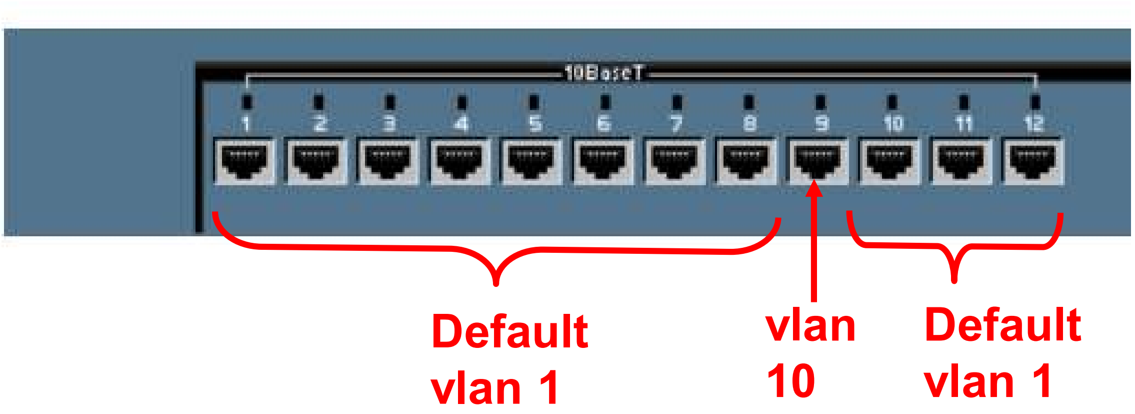
- **Assigning access ports (non-trunk ports) to a specific VLAN**

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan vlan_number
```

- **Create the VLAN:**

```
Switch#vlan database
Switch(vlan)#vlan vlan_number
Switch(vlan)#exit
```

Creating VLANs



Default vlan 1

vlan 10

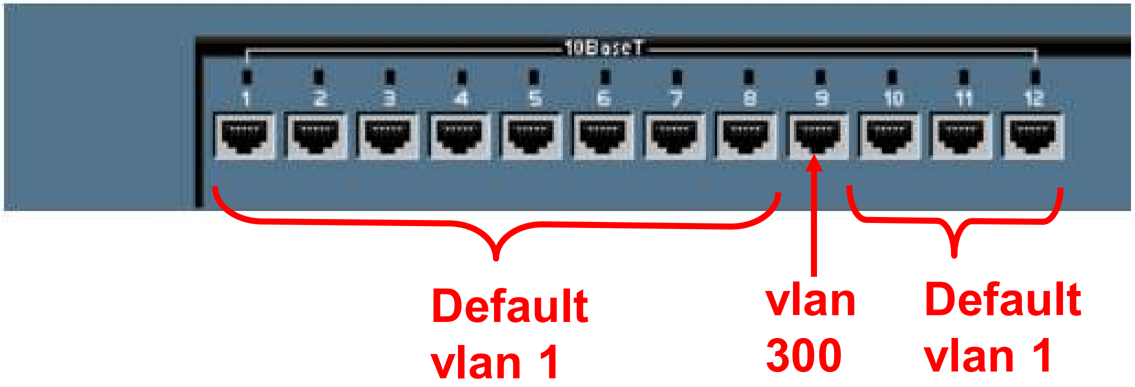
Default vlan 1

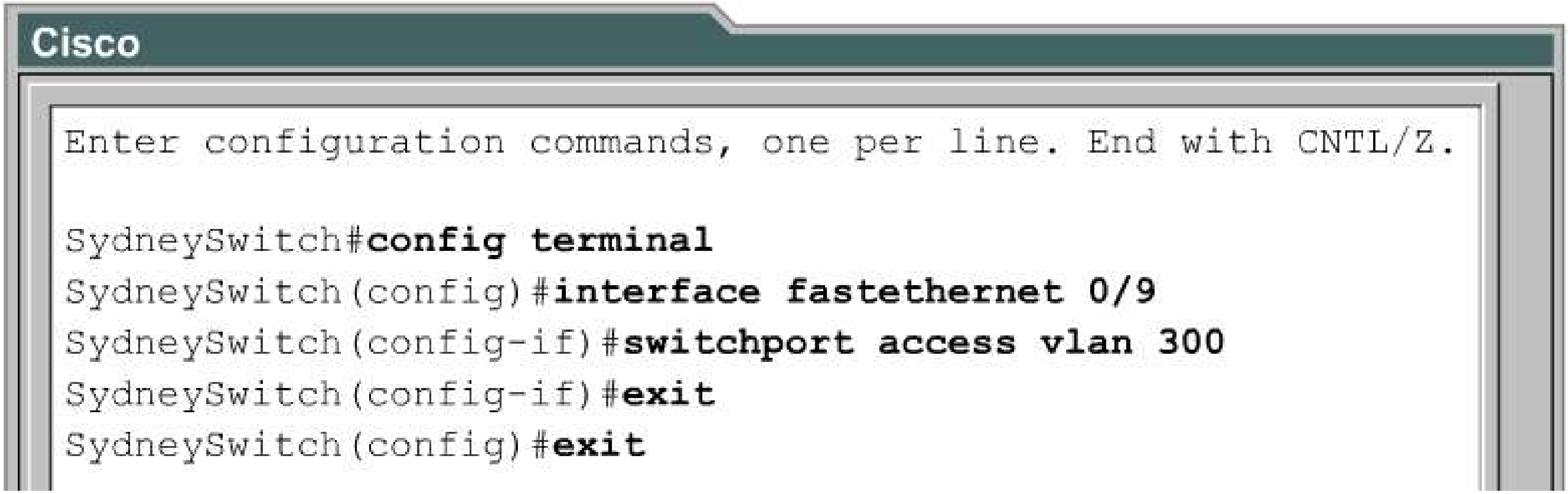
- Assign ports to the VLAN

```
 Switch(config)#interface fastethernet 0/9
 Switch(config-if)#switchport access vlan 10
```

- **access** – Denotes this port as an access port and not a trunk link (later)

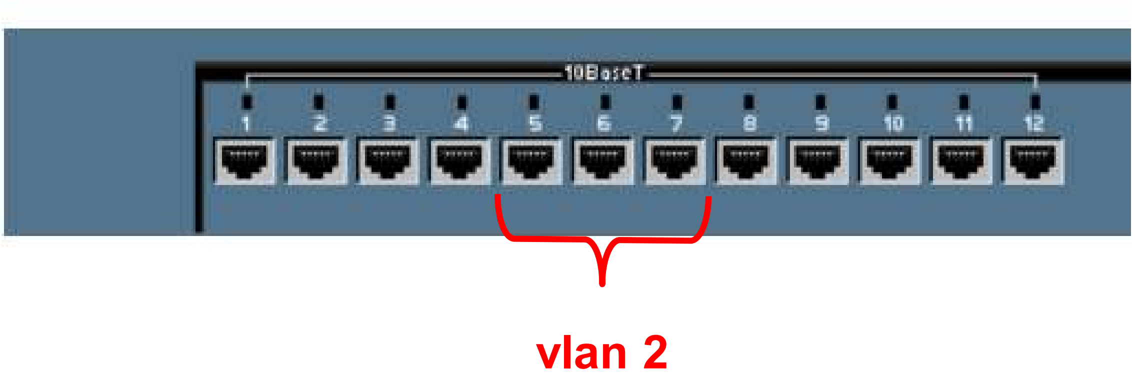
Creating VLANs





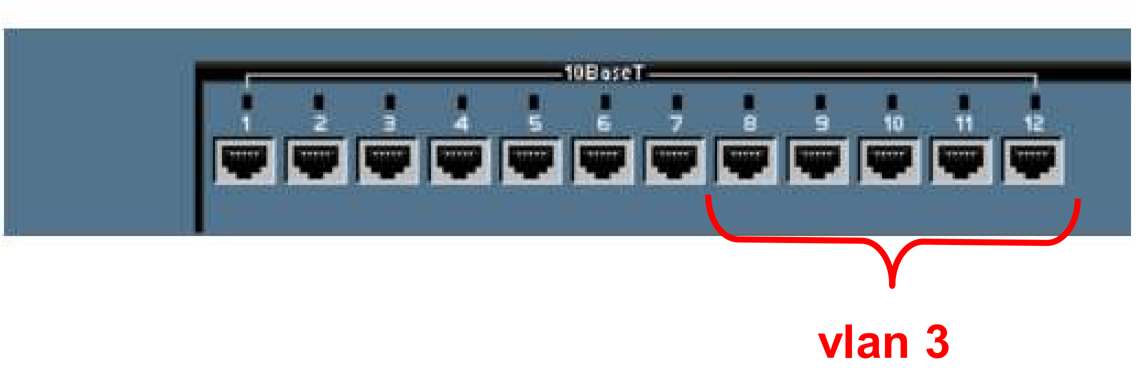
```
Enter configuration commands, one per line. End with CNTL/Z.

SydneySwitch#config terminal
SydneySwitch(config)#interface fastethernet 0/9
SydneySwitch(config-if)#switchport access vlan 300
SydneySwitch(config-if)#exit
SydneySwitch(config)#exit
```

Configuring Ranges of VLANs



```
SydneySwitch(config)#interface fastethernet 0/5
SydneySwitch(config-if)#switchport access vlan 2
SydneySwitch(config-if)#exit
SydneySwitch(config)#interface fastethernet 0/6
SydneySwitch(config-if)#switchport access vlan 2
SydneySwitch(config-if)#exit
SydneySwitch(config)#interface fastethernet 0/7
SydneySwitch(config-if)#switchport access vlan 2
```

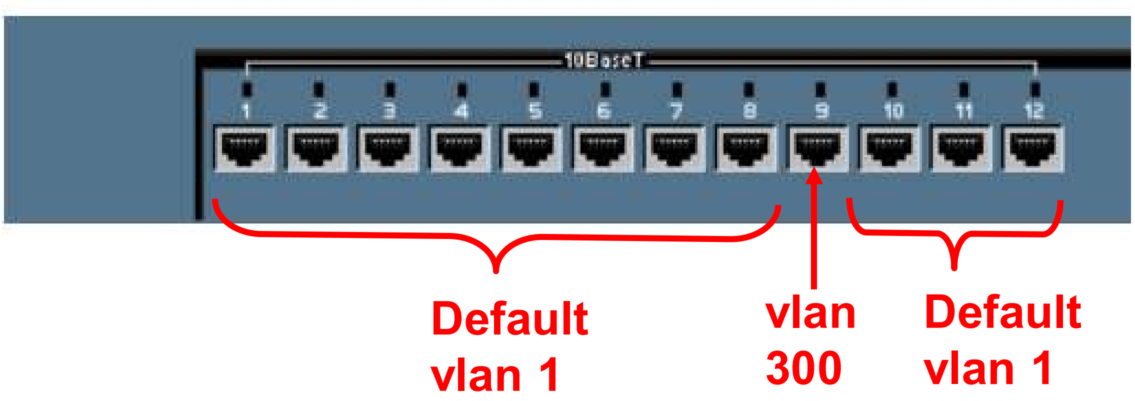
Configuring Ranges of VLANs



```
SydneySwitch(config)#interface range fastethernet 0/8,
   fastethernet 0/12
SydneySwitch(config-if)#switchport access vlan 3
SydneySwitch(config-if)#exit
```

This command does not work on all 2900 switches, such as the 2900 Series XL. It does work on the 2950.

Creating VLANs



Default
vlan 1

vlan
300

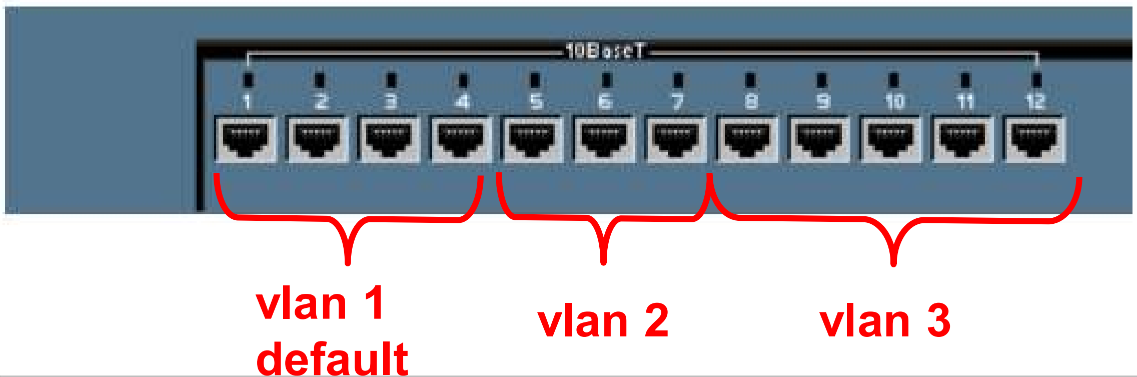
Default
vlan 1

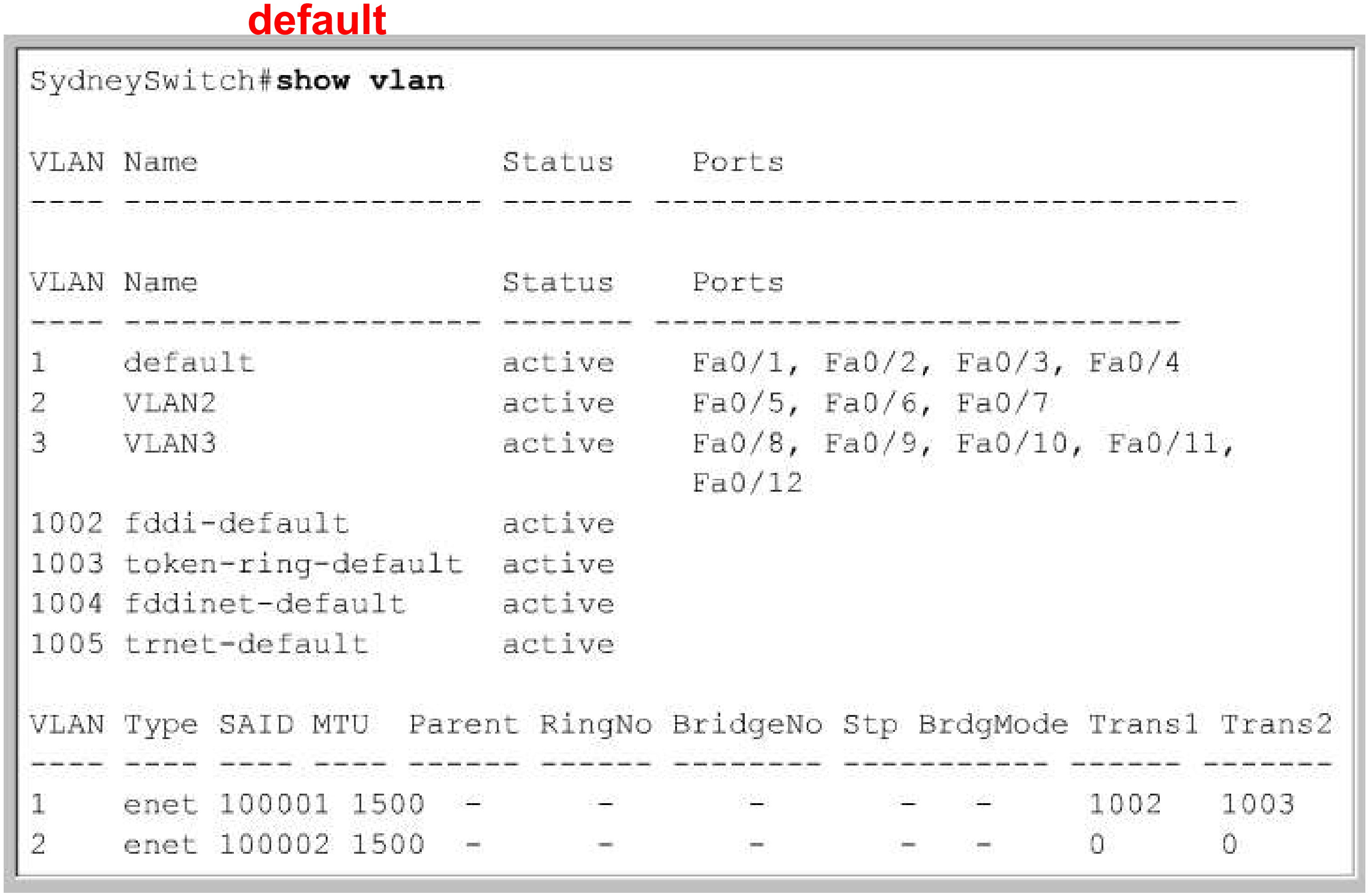
```
SydneySwitch(config)#interface fastethernet 0/1
SydneySwitch(config-if)#switchport mode access
SydneySwitch(config-if)#exit
```

Note: The `switchport mode access` command should be configured on all ports that the network administrator does not want to become a trunk port.

- This will be discussed in more in the next chapter, section on DTP.

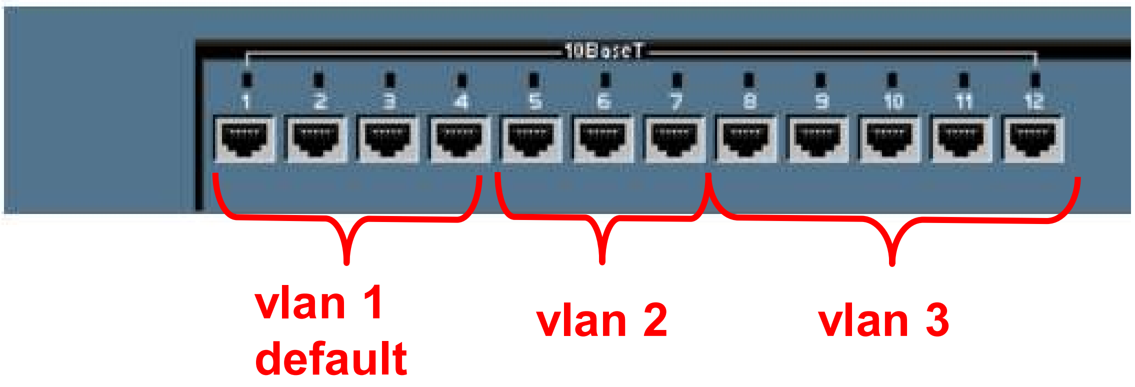
Verifying VLANs – show vlan

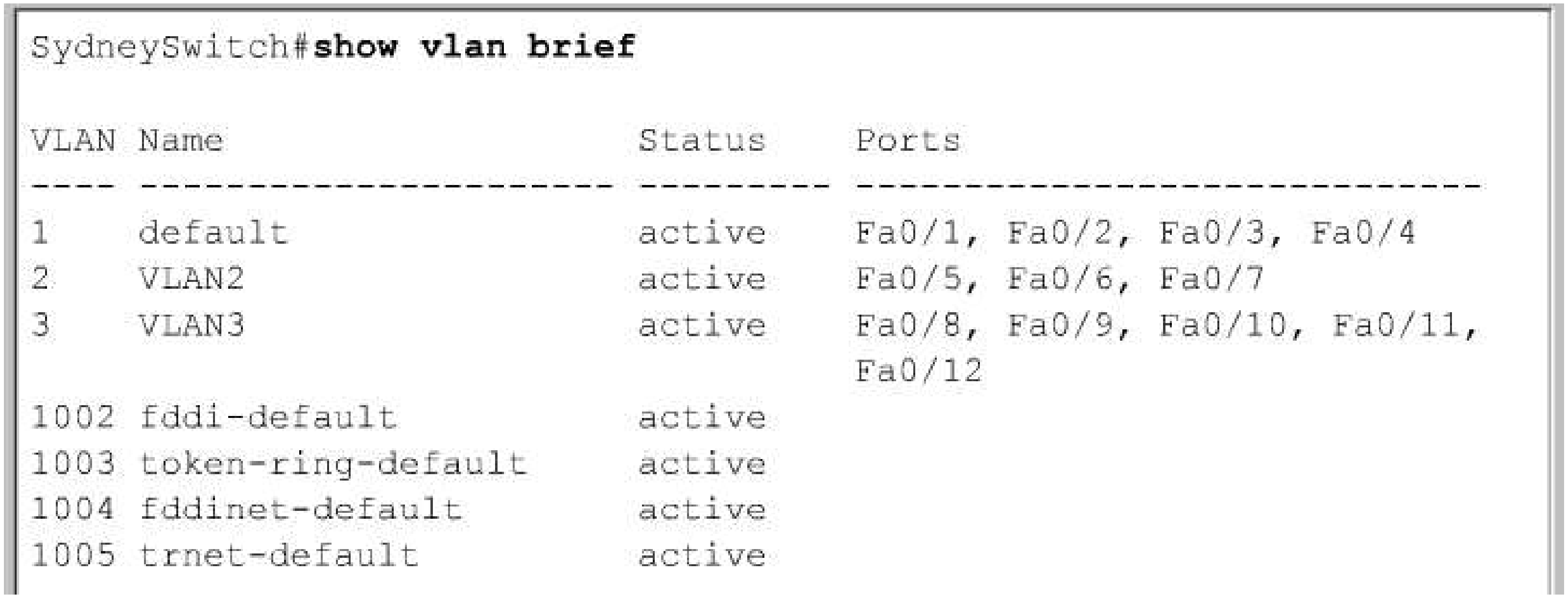




```
SydneySwitch#show vlan

VLAN Name                 Status    Ports
---- -------------------- ------- -------------------------------


VLAN Name                 Status    Ports
---- -------------------- ------- -----------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                    Fa0/12
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active

VLAN Type SAID MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ---- ---- ---- ------ ------ -------- ----------- ------ -------
1    enet 100001 1500 -      -       -       -    -      1002   1003
2    enet 100002 1500 -      -       -       -    -      0      0
```

Verifying VLANs – show vlan brief





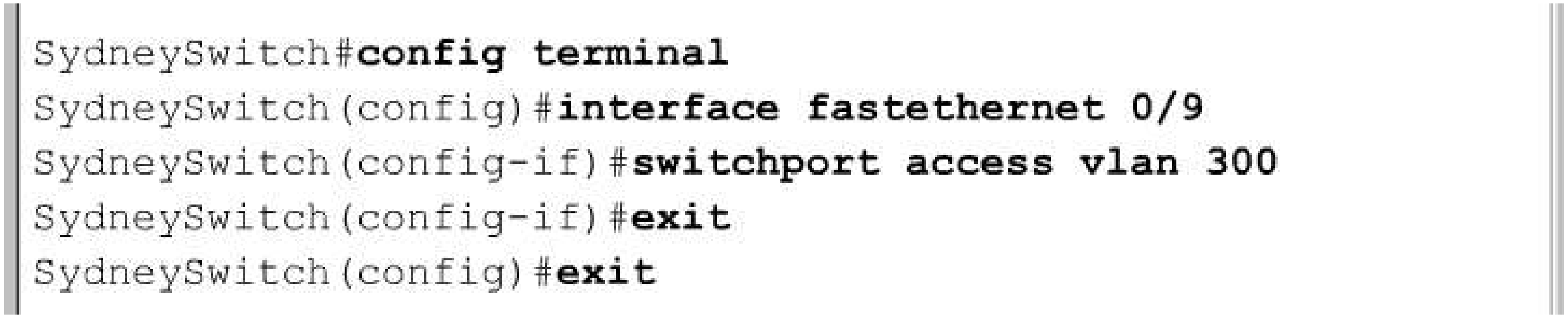
```
SydneySwitch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                            active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                            active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                                Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

vlan database commands

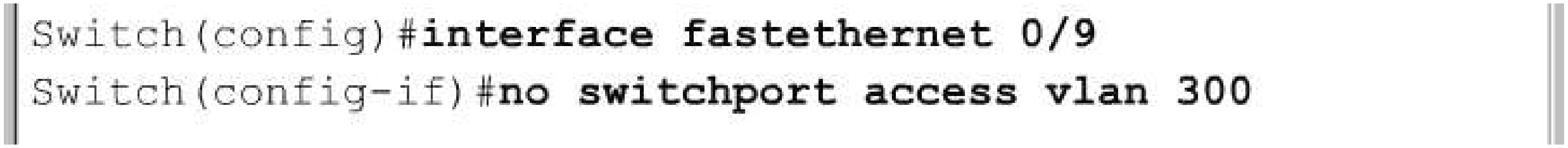
- Optional Command to add, delete, or modify VLANs.
- VLAN names, numbers, and **VTP** (VLAN Trunking Protocol) information can be entered which “may” affect other switches besides this one. (Discussed later).
- This does not assign any VLANs to an interface.

```
Switch#vlan database
Switch(vlan)#?
VLAN database editing buffer manipulation commands:
  abort   Exit mode without applying the changes
  apply   Apply current changes and bump revision number
  exit    Apply changes, bump revision number, and exit mode
  no      Negate a command or set its defaults
  reset   Abandon current changes and reread current database
  show    Show database information
  vlan    Add, delete, or modify values associated with a single VLAN
  vtp     Perform VTP administrative functions.
```

Deleting a Port VLAN Membership



```
SydneySwitch#config terminal
SydneySwitch(config)#interface fastethernet 0/9
SydneySwitch(config-if)#switchport access vlan 300
SydneySwitch(config-if)#exit
SydneySwitch(config)#exit
```



```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#no switchport access vlan 300
```

```
Switch(config-if)#no switchport access vlan vlan_number
```

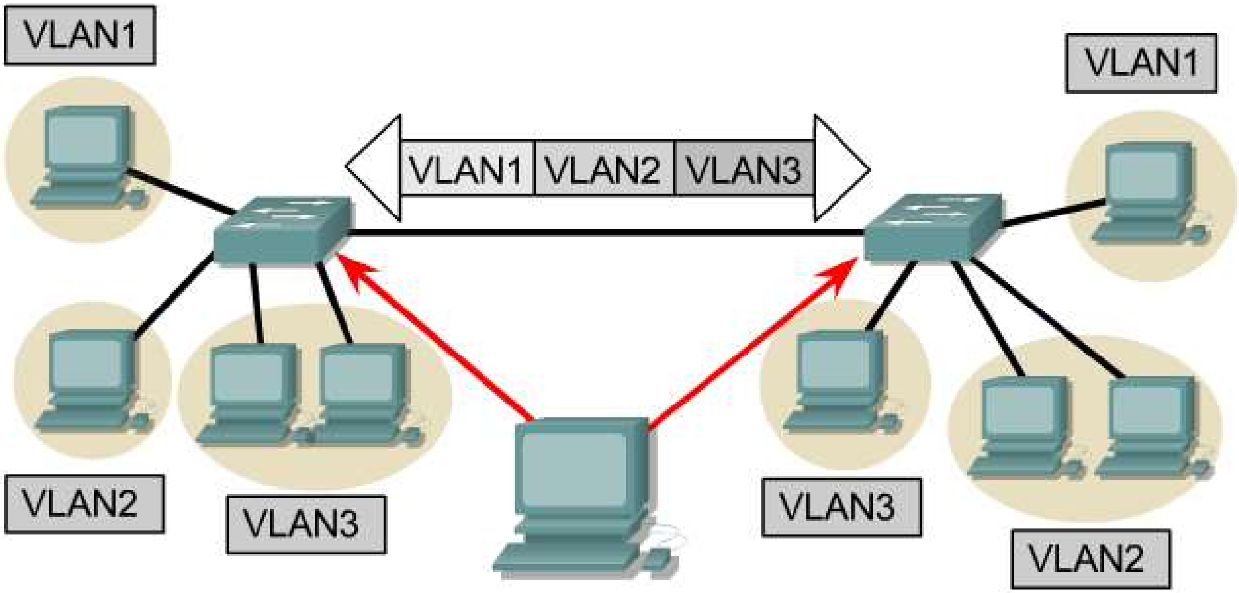
Deleting a VLAN

-
  ```
  Switch#vlan database
   Switch(vlan)#No vlan vlan_number
   Switch(vlan)#exit
  ```

VLAN Tagging

We will begin with a review of VLAN tagging and a closer look at ISL and IEEE 802.1Q.

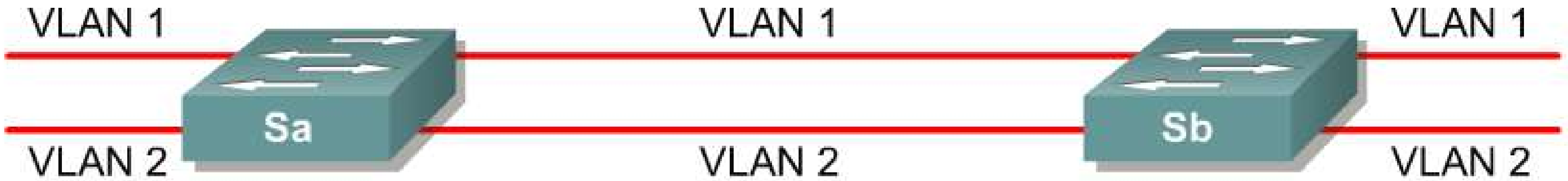
VLAN Tagging



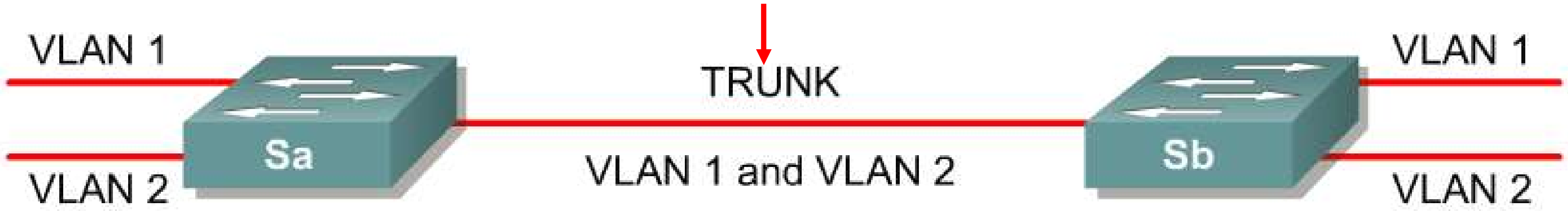
- **VLAN Tagging is used when a link needs to carry traffic for more than one VLAN.**
  - **Trunk link:** As packets are received by the switch from any attached end-station device, a unique packet identifier is added within each header.
- **This header information designates the VLAN membership of each 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

No VLAN Tagging

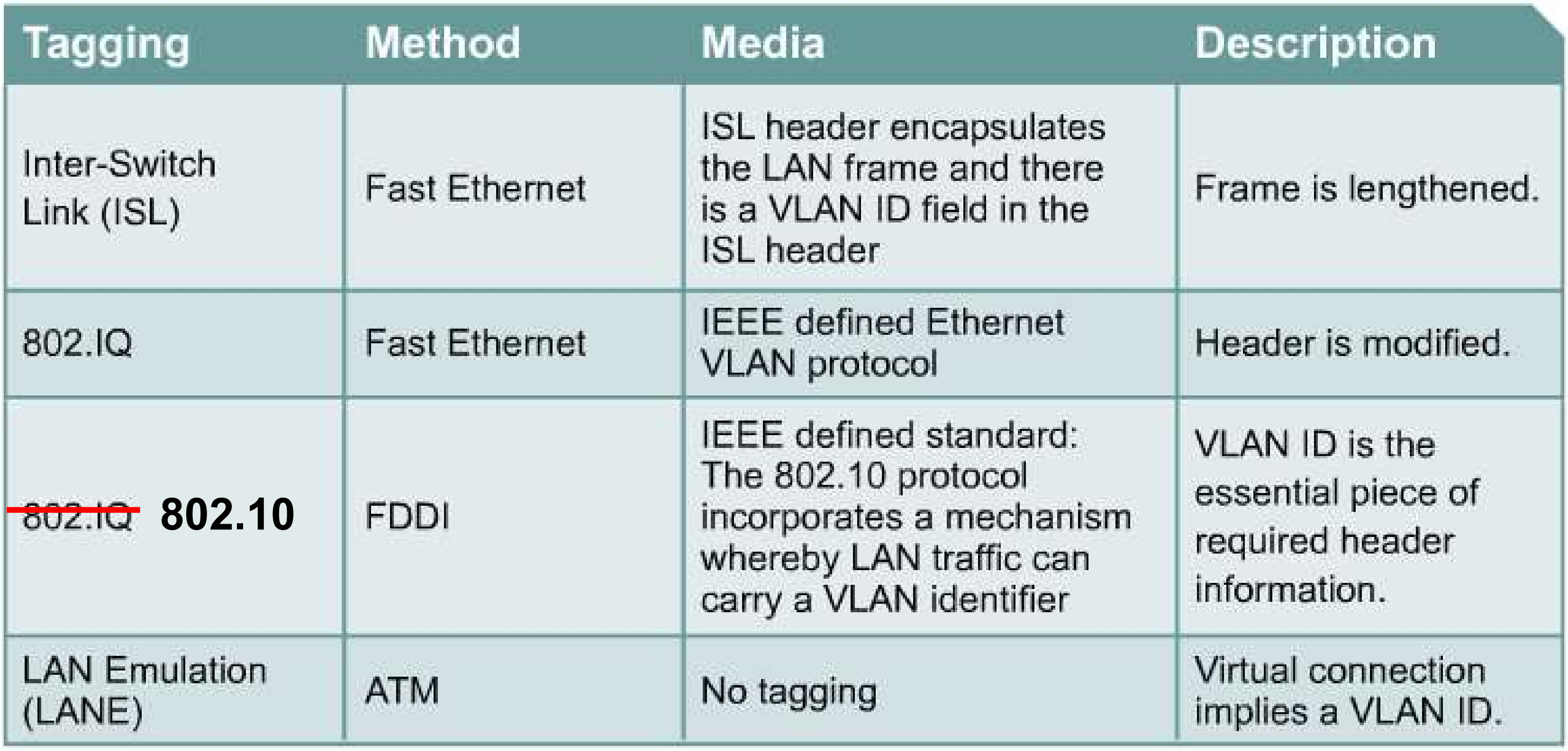


VLAN Tagging



- VLAN Tagging is used when a link needs to carry traffic for more than one VLAN.
- Tagging is used so the receiving switch knows which ports in should flood broadcast and unknown unicast traffic (only those ports belonging to the same VLAN).

VLAN Tagging

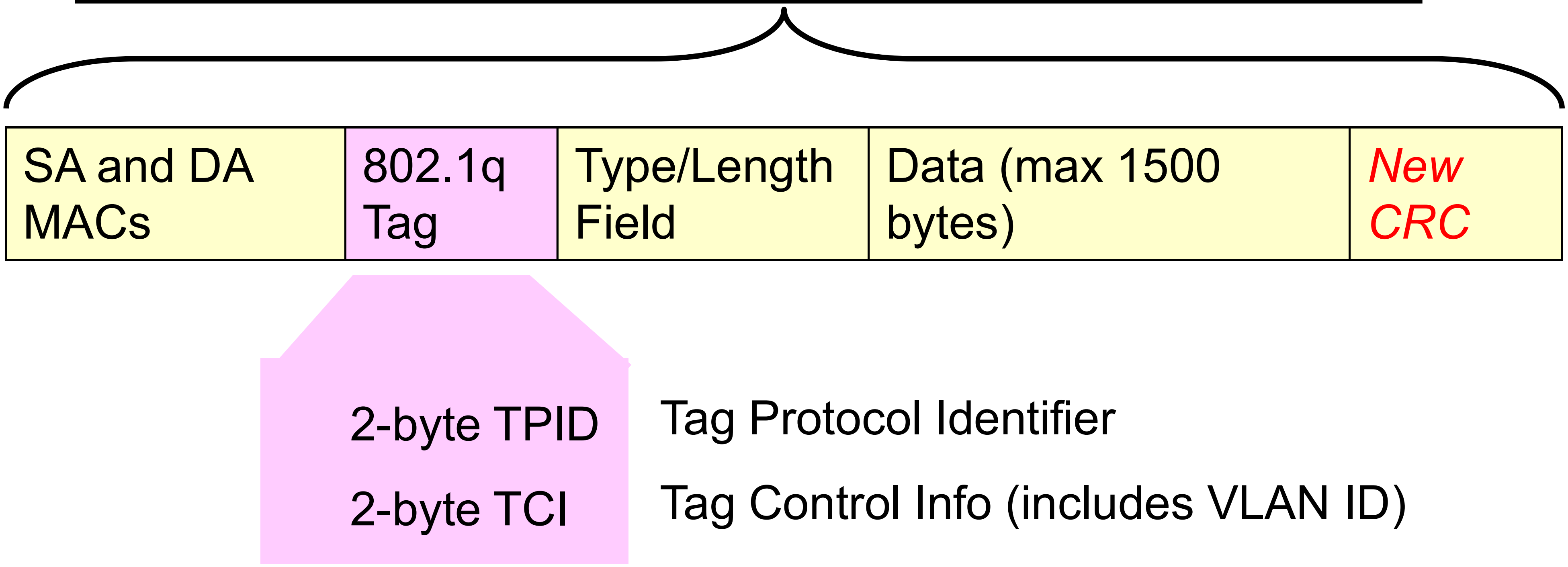


Tagging	Method	Media	Description
Inter-Switch Link (ISL)	Fast Ethernet	ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header	Frame is lengthened.
802.IQ	Fast Ethernet	IEEE defined Ethernet VLAN protocol	Header is modified.
~~802.IQ~~ **802.10**	FDDI	IEEE defined standard: The 802.10 protocol incorporates a mechanism whereby LAN traffic can carry a VLAN identifier	VLAN ID is the essential piece of required header information.
LAN Emulation (LANE)	ATM	No tagging	Virtual connection implies a VLAN ID.

- There are two major methods of frame tagging, Cisco proprietary **Inter-Switch Link (ISL)** and **IEEE 802.1Q**.
- ISL used to be the most common, but is now being replaced by 802.1Q frame tagging. ISL Increases the frame header overhead by **<u>30 bytes</u>**.
- Cisco recommends using 802.1Q. This type of encapsulation adds only 4 bytes to the Ethernet header
- VLAN Tagging and Trunking will be discussed in the next chapter.

IEEE 802.1Q

NIC cards and networking devices can understand this “baby giant” frame (1522 bytes). However, a Cisco switch must remove this encapsulation before sending the frame out on an access link.



SA and DA MACs	802.1q Tag	Type/Length Field	Data (max 1500 bytes)	*New CRC*

2-byte TPID	Tag Protocol Identifier
2-byte TCI	Tag Control Info (includes VLAN ID)

- Significantly less overhead than the ISL
- As opposed to the 30 bytes added by ISL, 802.1Q inserts only an additional 4 bytes into the Ethernet frame

802.1q

- A 4-byte tag header containing a tag protocol identifier (TPID) and tag control information (TCI) with the following elements:

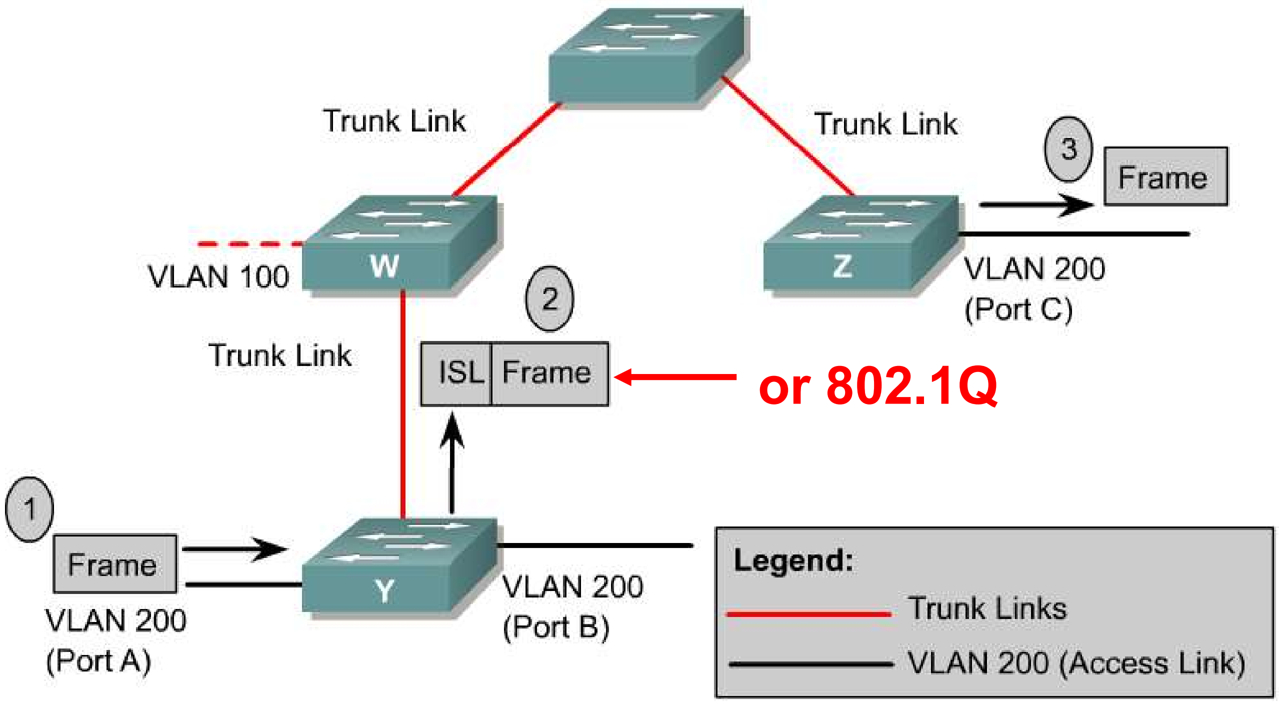
TPID (Tab Protocol Identifier)

- A 2-byte TPID with a fixed value of 0x8100.
- This value indicates that the frame carries the 802.1Q/802.1p tag information.

TCI (Tag Control Information)

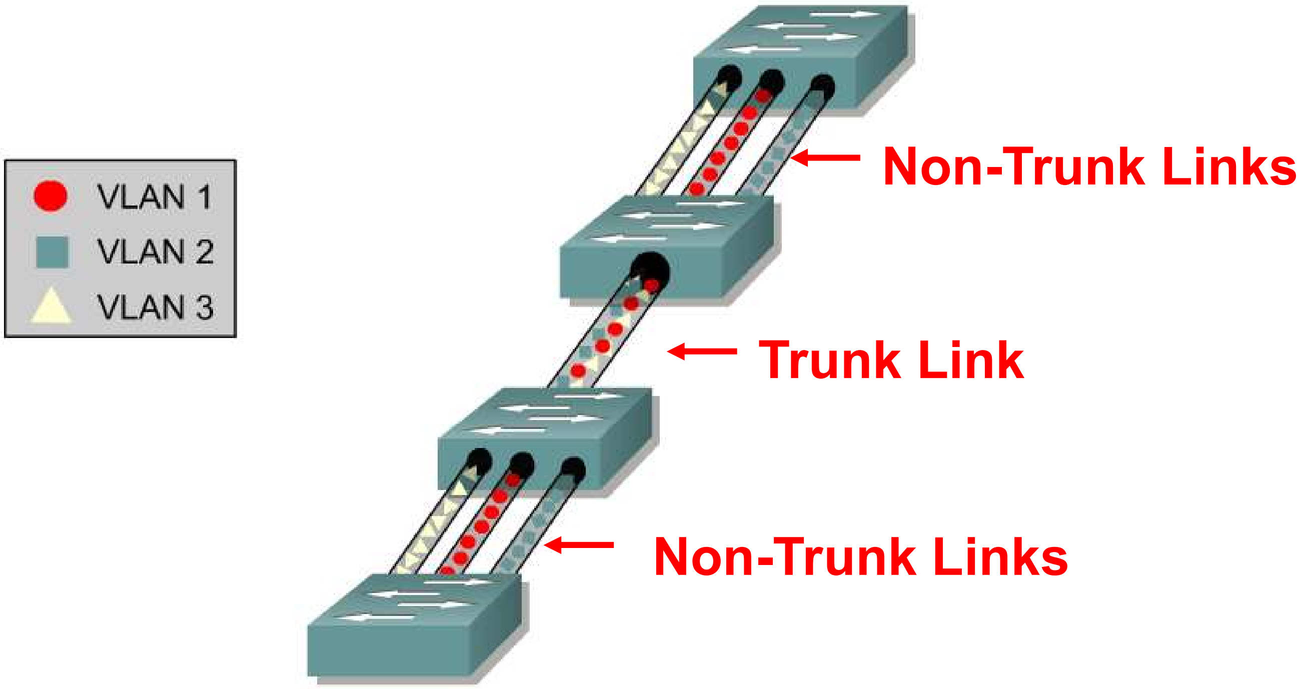
- A TCI containing the following elements:
  - Three-bit user priority (8 priority levels, 0 thru 7)
  - One-bit canonical format (CFI indicator), 0 = canonical, 1 = noncanonical, to signal bit order in the encapsulated frame (www.faqs.org/rfcs/rfc2469.html - “A Caution On the Canonical Ordering of Link-Layer Addresses”)
  - Twelve-bit VLAN identifier (VID)-Uniquely identifies the VLAN to which the frame belongs, defining 4,096 VLANs, with 0 and 4095 reserved.

Trunking operation



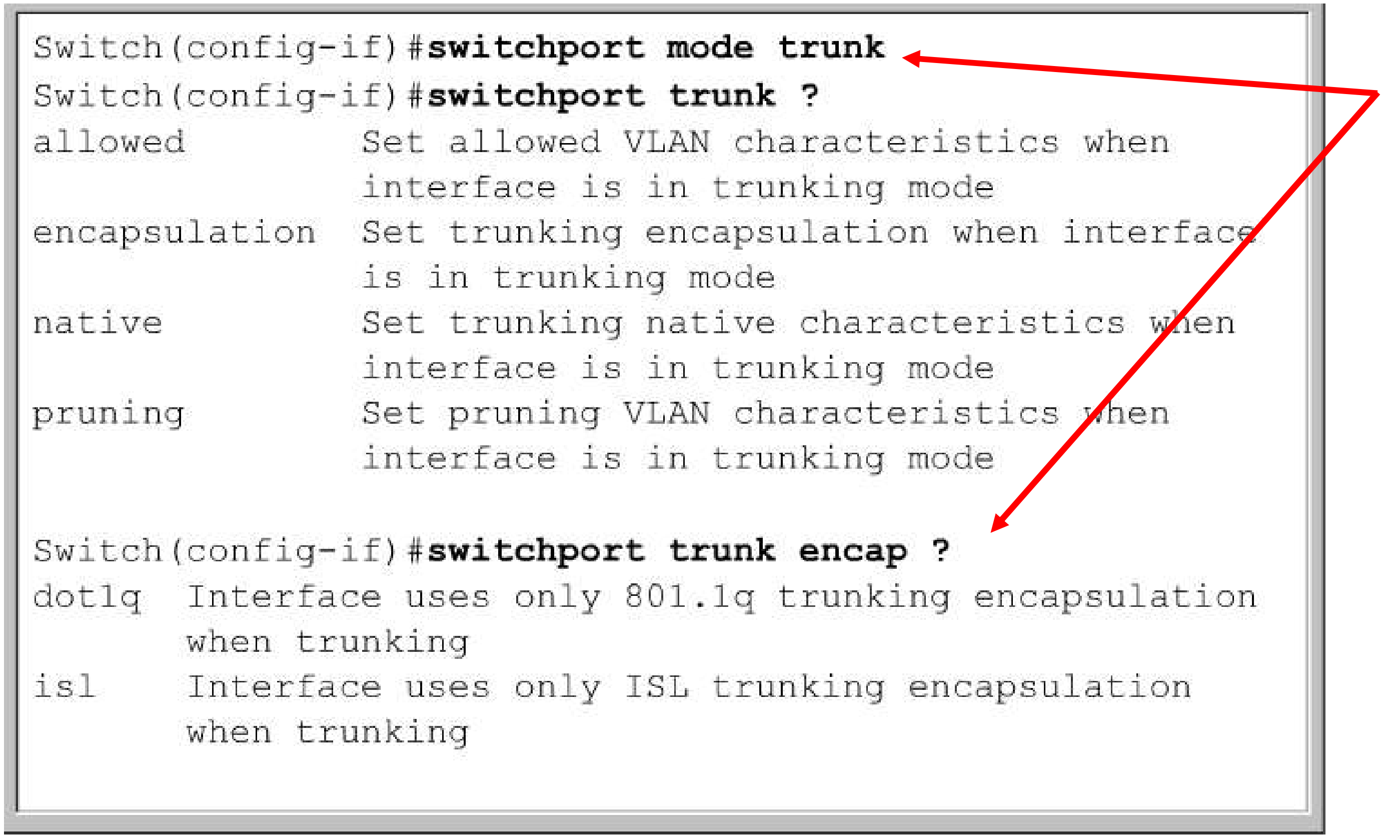
- **Trunking protocols were developed to effectively manage the transfer of frames from different VLANs on a single physical line.**
- The trunking protocols establish agreement for the distribution of frames to the associated ports at both ends of the trunk.
- Trunk links may carry traffic for all VLANs or only specific VLANs.

VLANs and trunking



- It is important to understand that a trunk link does not belong to a specific VLAN.
- The responsibility of a trunk link is to act as a conduit for VLANs between switches and routers (or switches and switches).

Configuring Trunking

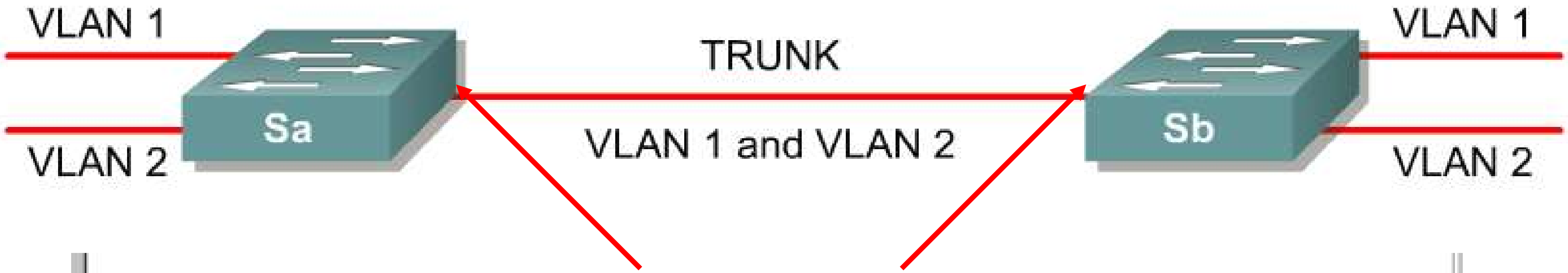


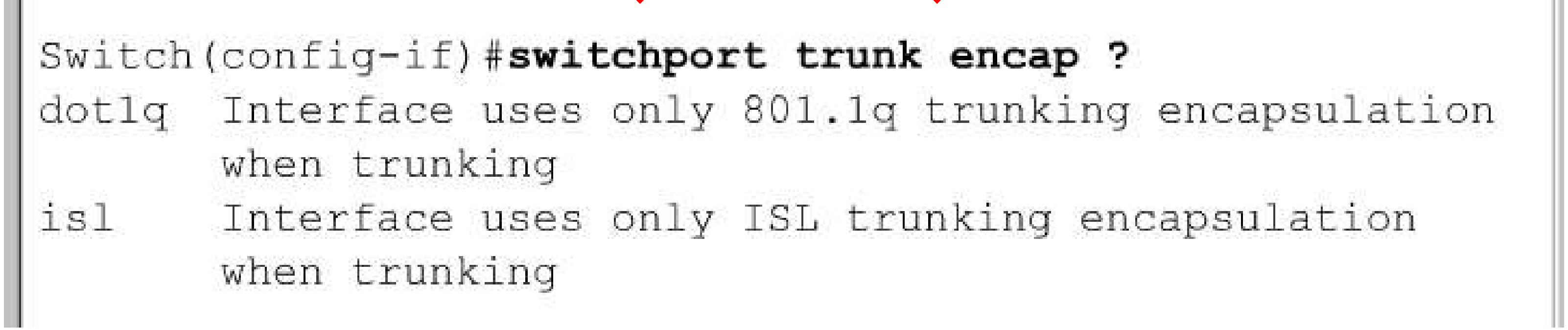
```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk ?
allowed        Set allowed VLAN characteristics when
               interface is in trunking mode
encapsulation  Set trunking encapsulation when interface
               is in trunking mode
native         Set trunking native characteristics when
               interface is in trunking mode
pruning        Set pruning VLAN characteristics when
               interface is in trunking mode

Switch(config-if)#switchport trunk encap ?
dot1q   Interface uses only 801.1q trunking encapsulation
        when trunking
isl     Interface uses only ISL trunking encapsulation
        when trunking
```

Note: On many switches, the **`switchport trunk encapsulation`** command must be done **BEFORE** the **`switchport mode trunk`** command.

- These commands will be explained in the following slides.

Configuring Trunking



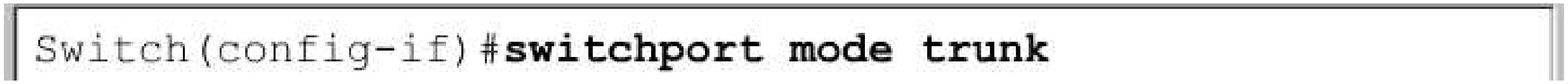


```
Switch(config-if)#switchport trunk encap ?
dot1q  Interface uses only 801.1q trunking encapsulation
       when trunking
isl    Interface uses only ISL trunking encapsulation
       when trunking
```

`Switch(config-if)switchport trunk encapsulation [dot1q|isl]`

- This command configures VLAN tagging on an interface if the switch supports multiple trunking protocols.
- The two options are:
  - **`dot1q`** – IEEE 802.1Q
  - **`isl`** – ISL
- **<u>The tagging must be the same on both ends.</u>**

Configuring Trunking



```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)switchport mode [access|trunk]
```

- An access port means that the port (interface) can only belong to a single VLAN.
- Access ports are used when:
  - Only a single device is connected to the port
  - Multiple devices (hub) are connected to the port, all belonging to the same VLAN
  - Another switch is connected to this interface, but this link is only carrying a single VLAN (non-trunk link).
- Trunk ports are used when:
  - Another switch is connected to this interface, and this link is carrying multiple VLANa (trunk link).