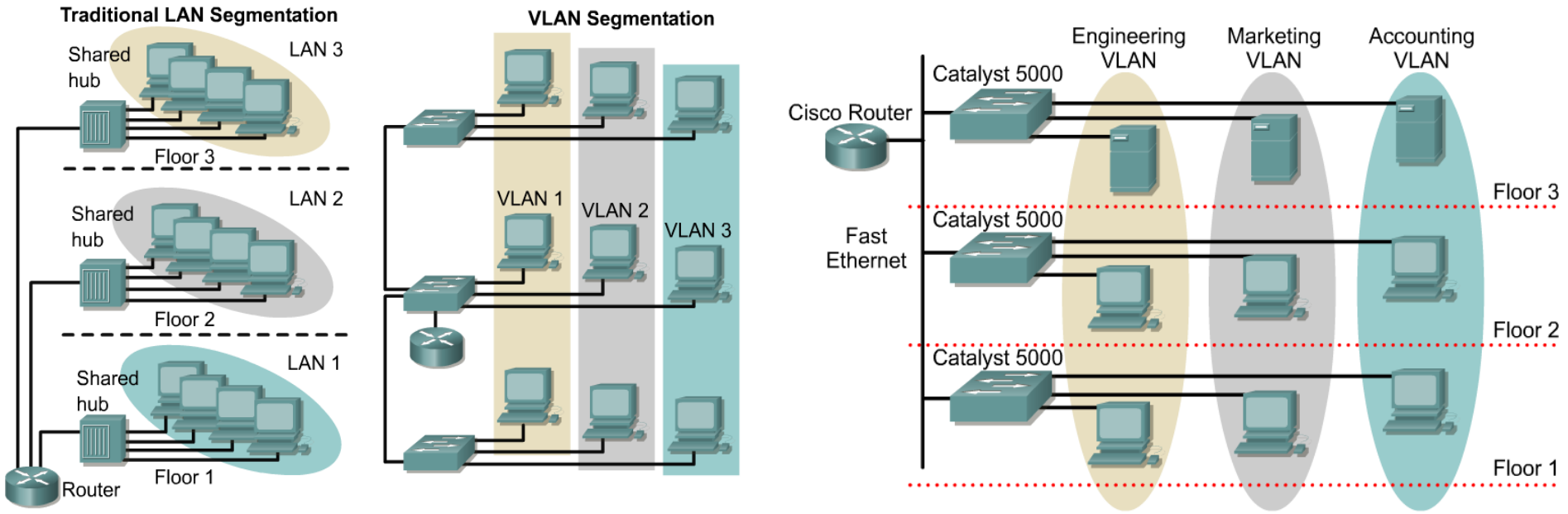
# Virtual LAN

Slide Set 7

# Overview

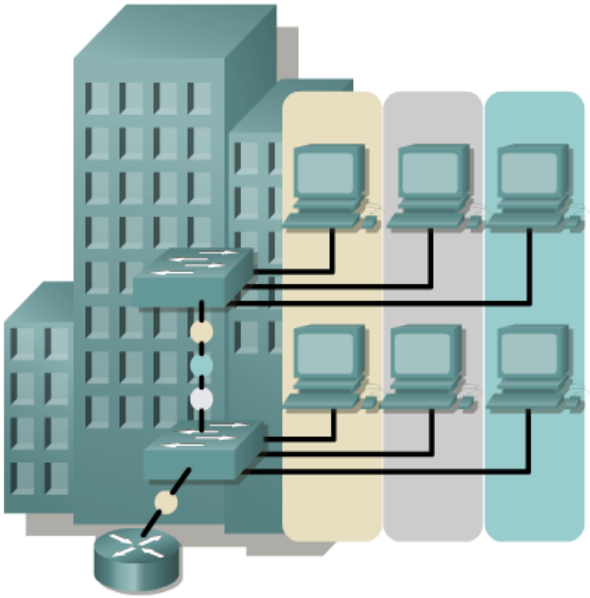
- Define VLANs
- List the benefits of VLANs
- Explain how VLANs are used to create broadcast domains
- Explain how routers are used for communication between VLANs
- List the common VLAN types
- Define ISL and 802.1Q
- Explain the concept of geographic VLANs
- Configure static VLANs on 29xx series Catalyst switches
- Verify and save VLAN configurations
- Delete VLANs from a switch configuration

# 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.

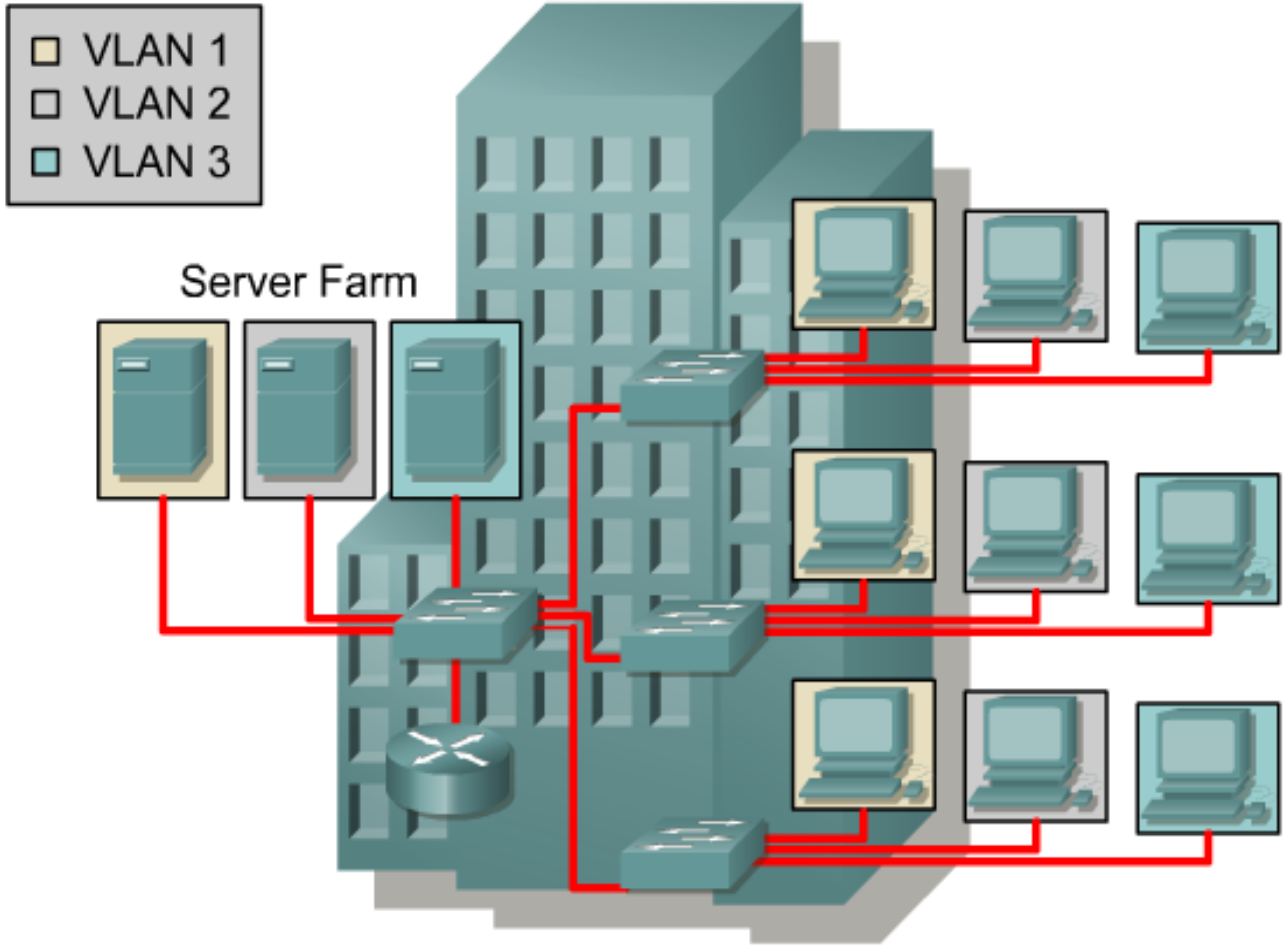
# VLAN introduction



- 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.

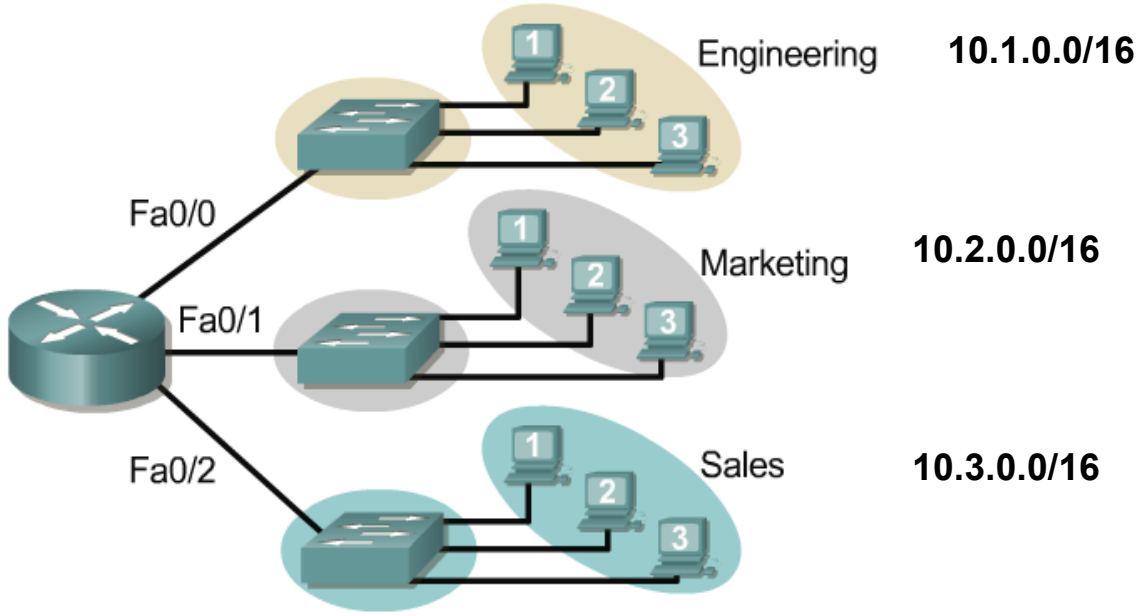
# Broadcast domains with VLANs and routers




- 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

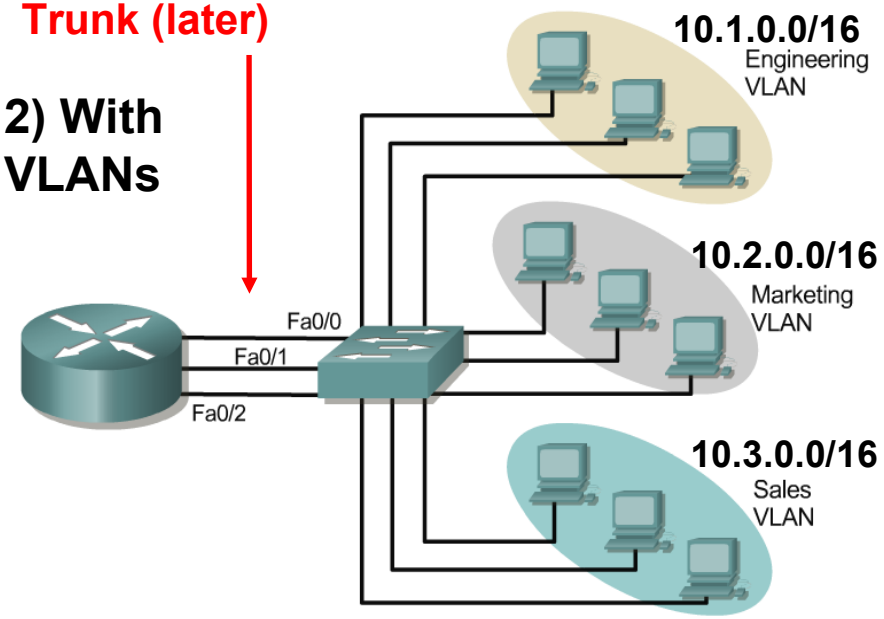
**1) Without VLANs**




- 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**

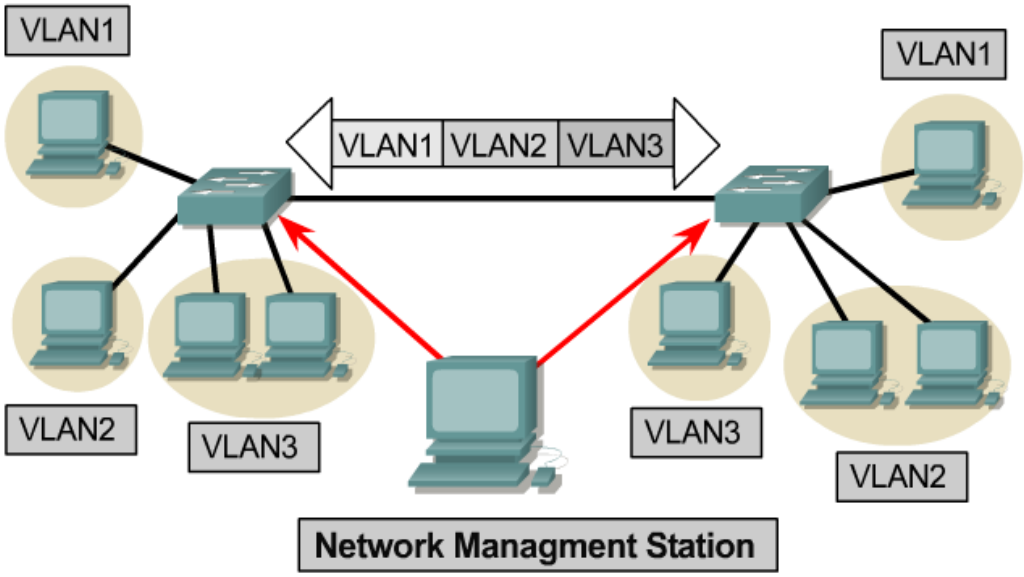


# VLAN operation

| Configuring VLANs | Description |
|---|---|
| Statically | Network administrators configure port-by-port.<br><br>Each Port is associated with a specific VLAN.<br><br>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.<br><br>Uses a software database of MAC address to VLAN mappings (which the network administrator must set up first). |

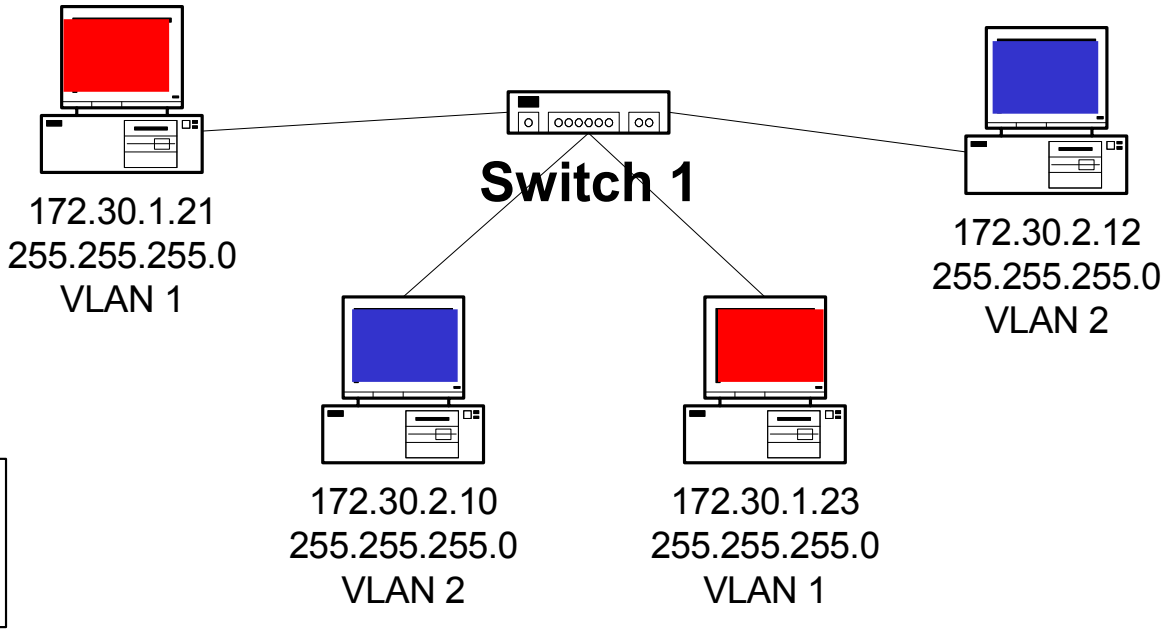
- Each switch port can be assigned to a different VLAN.
- Ports assigned to the same VLAN share broadcasts.
- Ports that do not belong to that VLAN do not share these broadcasts.

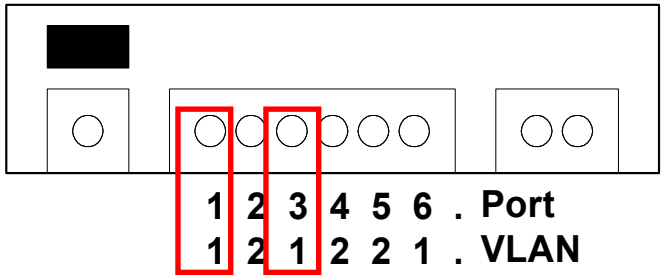
# VLAN operation




- **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




**Two VLANs**

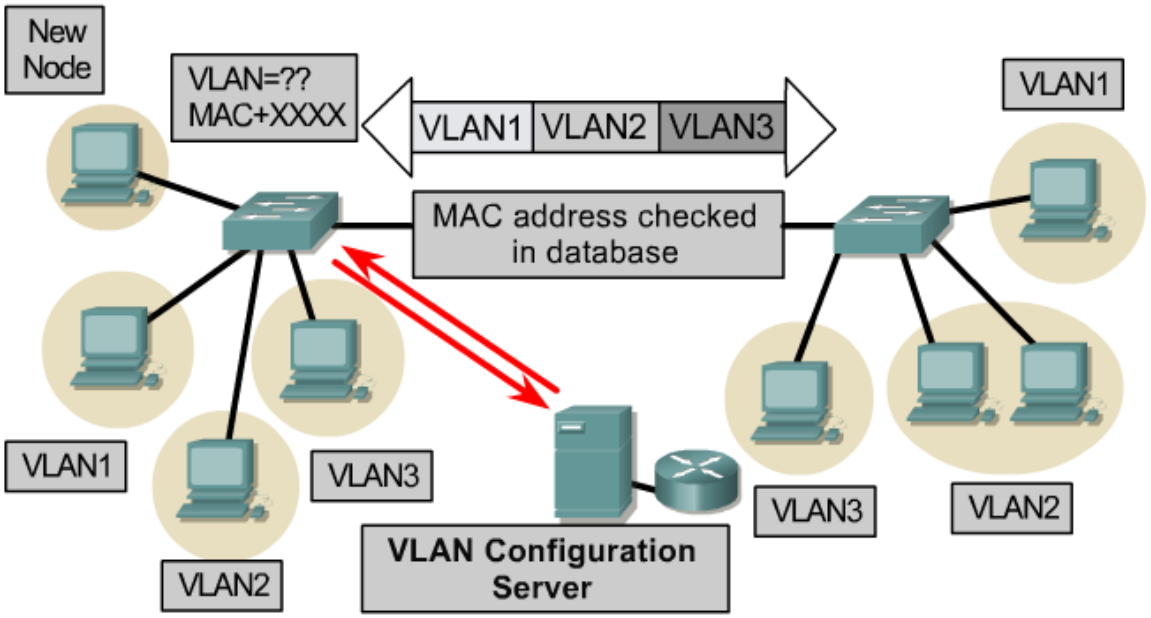
- Two Subnets

Important notes on VLANs:

1. VLANs are assigned on the switch port. There is no "VLAN" assignment done on the host (usually).
2. 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
3. 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 memebership

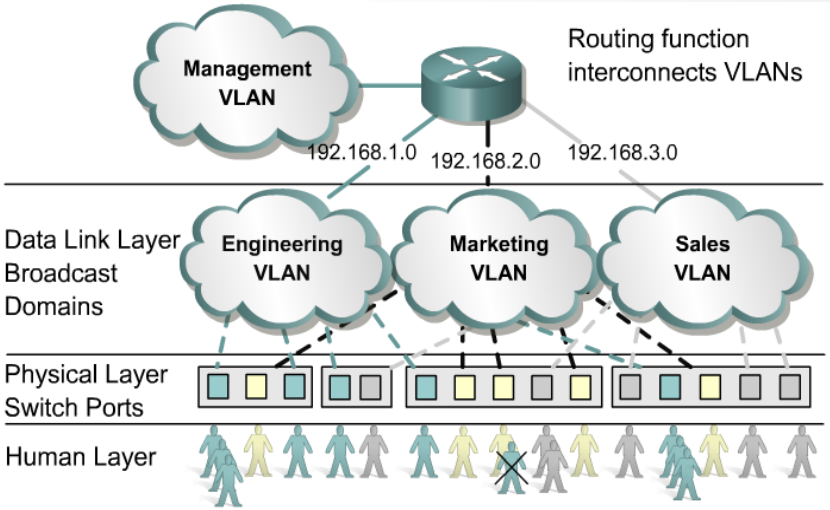
# VLAN operation




- **Dynamic membership VLANs are created through network management software. (Not as common as static VLANs)**
- **CiscoWorks 2000 or CiscoWorks for Switched Internetworks** 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

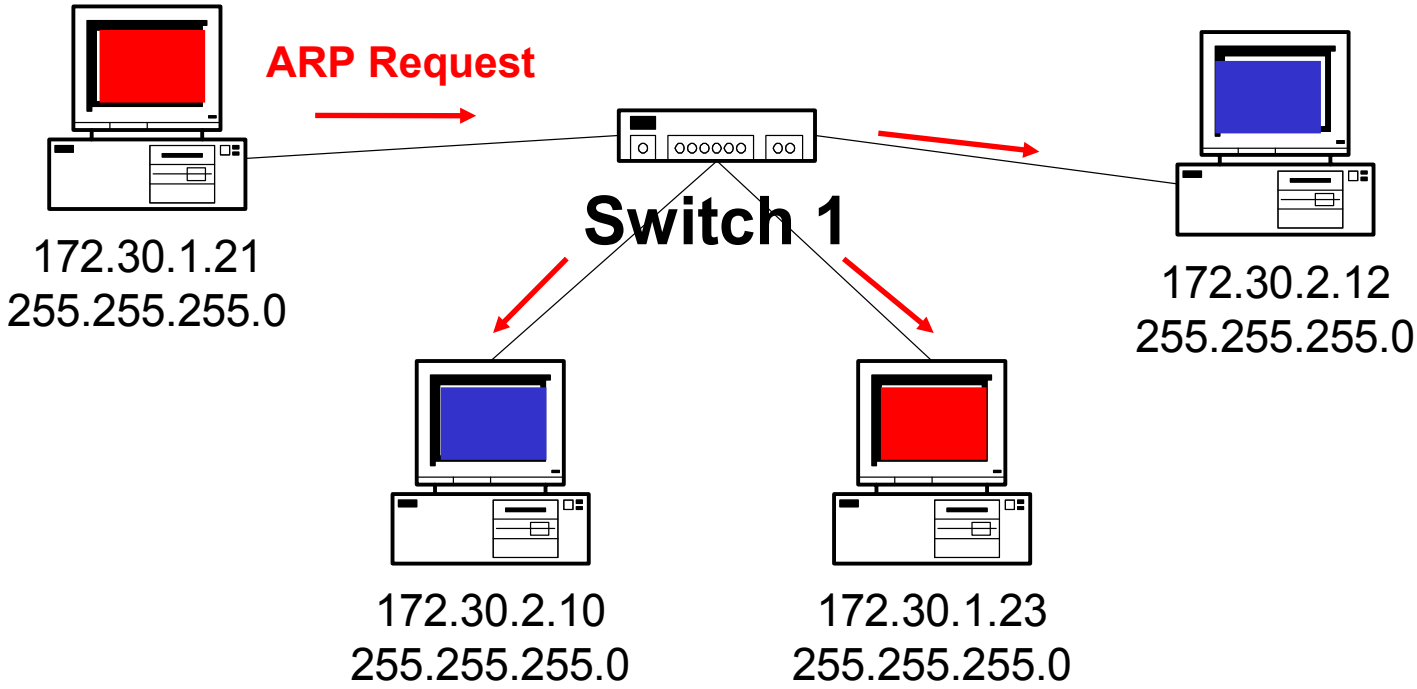
All users attached to the same switch port must be in the same VLAN.




**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

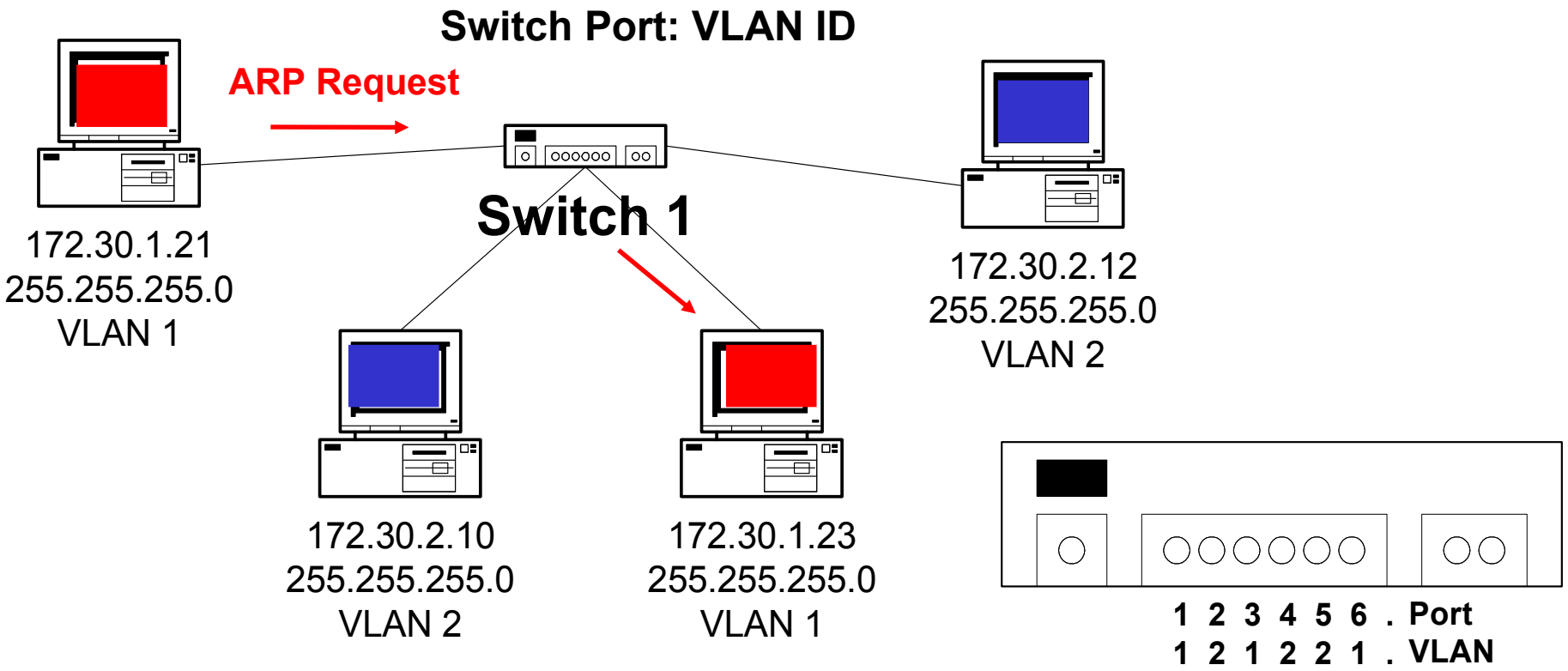



**No VLANs**

- 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.

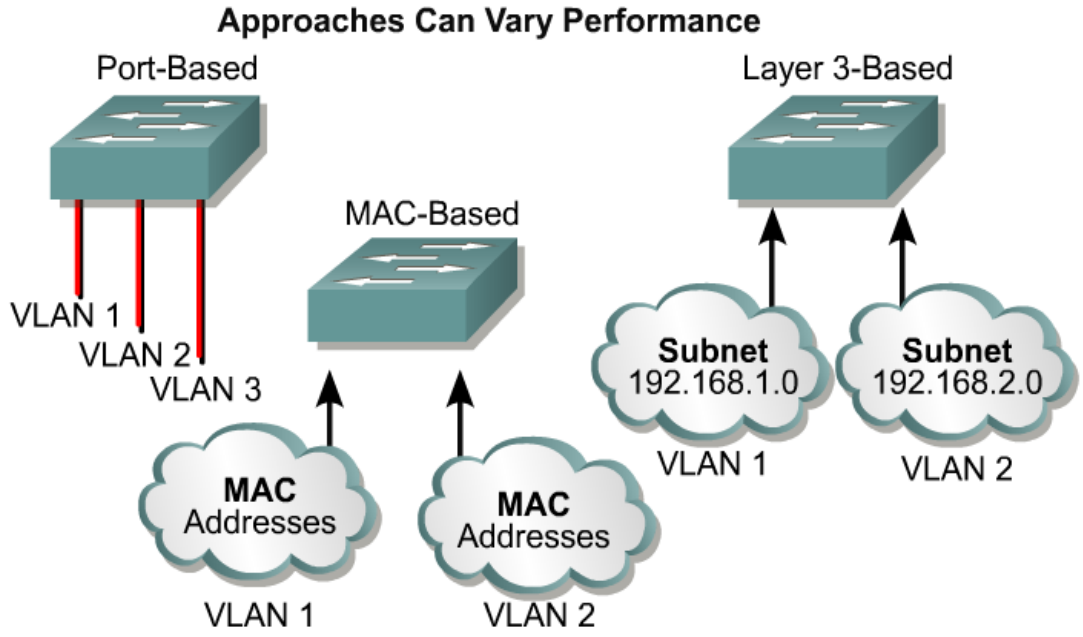
# With VLANs – Broadcast Control




**Two VLANs**

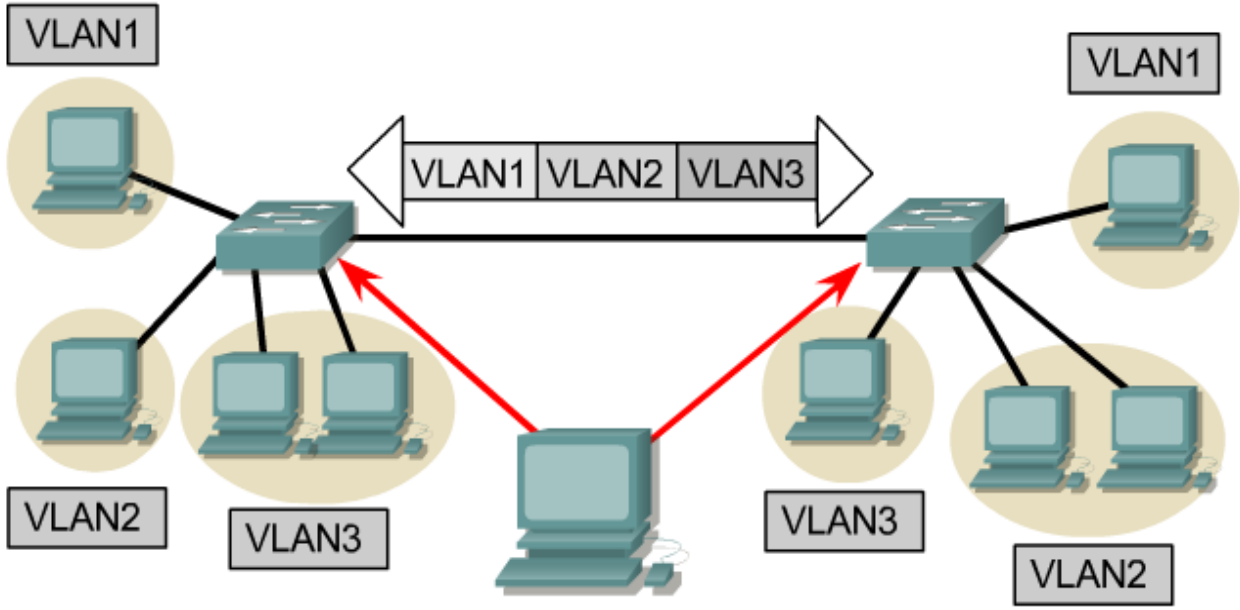
- Two Subnets

# VLAN Types



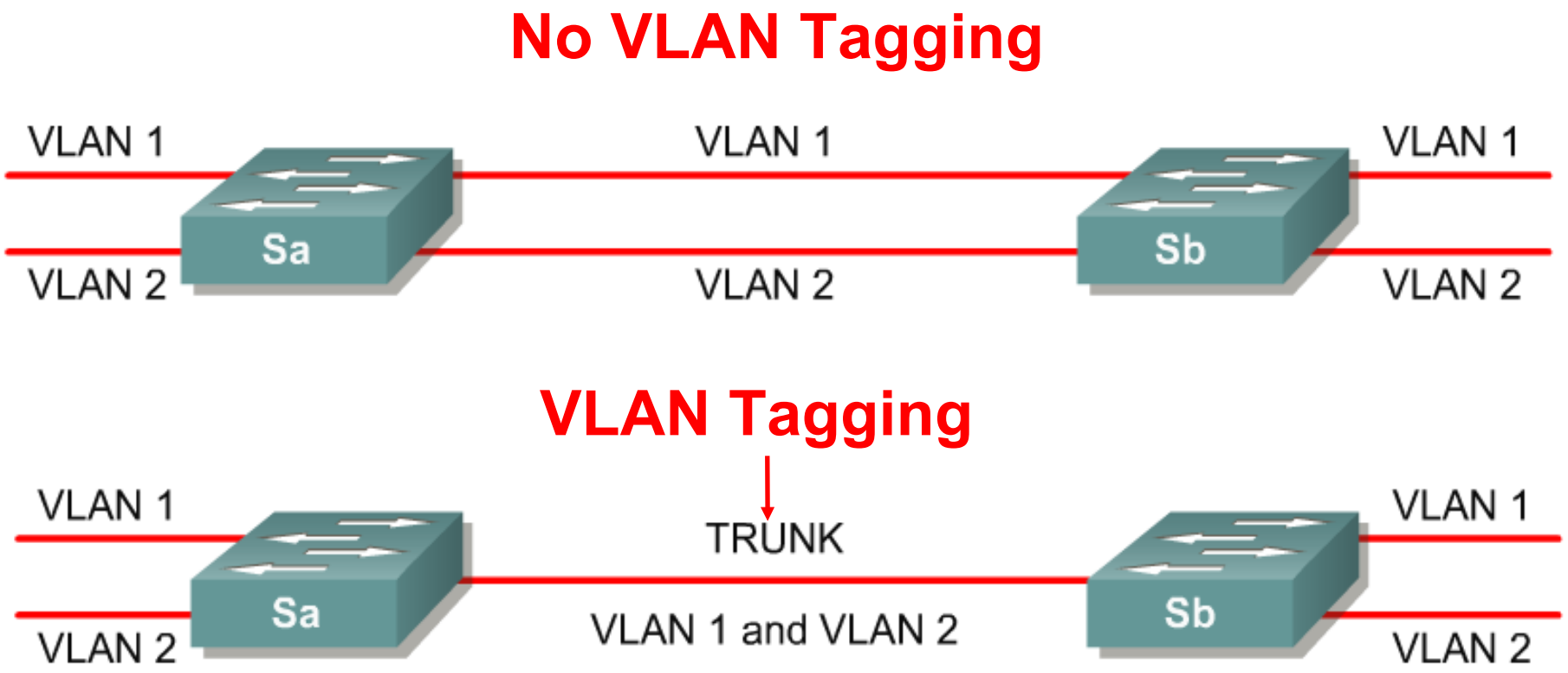

| VLAN Types | Description |
|---|---|
| Port-based | • Most common configuration method.<br>• Ports assigned individually, in groups, in rows, or across 2 or more switches.<br>• Simple to use.<br>• Often implemented where Dynamic Host Control Protocol (DHCP) is used to assign IP addresses to network hosts. |
| MAC address | • Rarely implemented today.<br>• Each address must be entered into the switch and configured individually.<br>• Users find it useful.<br>• Difficult to administer, troubleshoot and manage. |
| Protocol Based | • Configured like MAC addresses, but instead uses a logical or IP address.<br>• 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




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

# VLAN Tagging

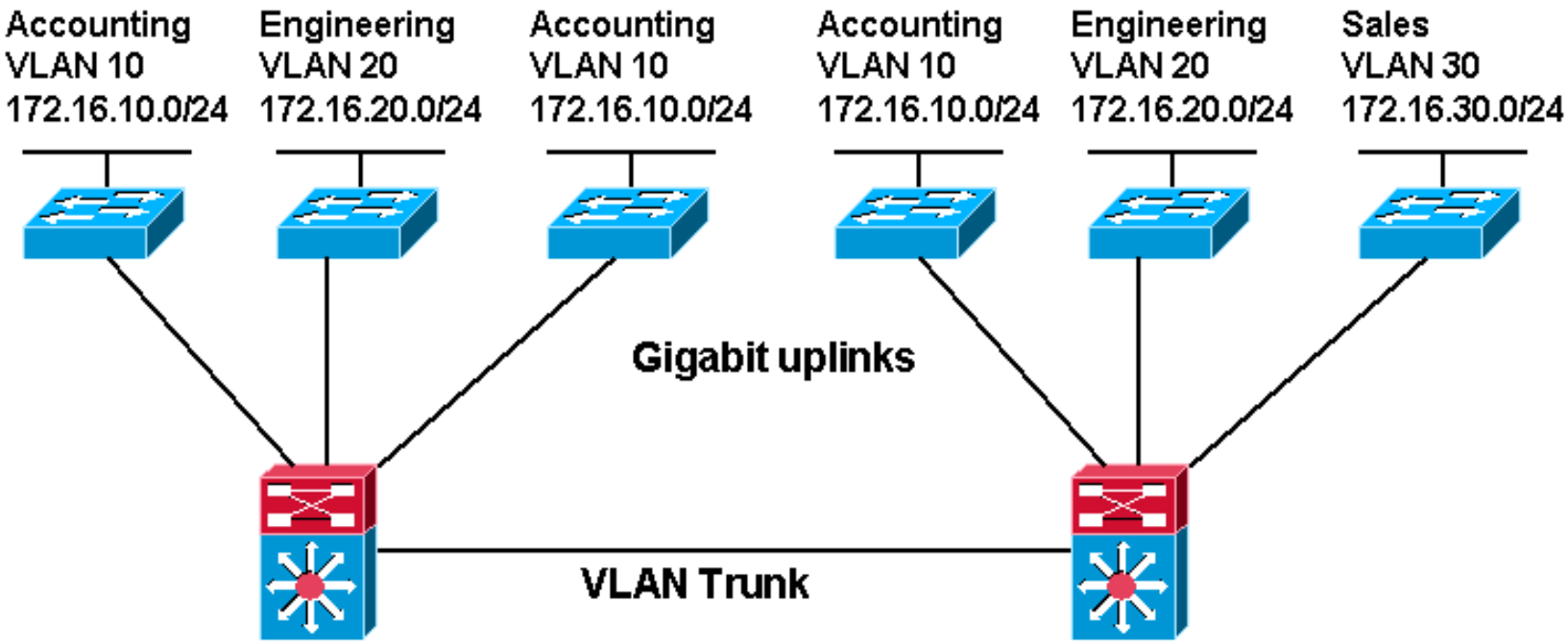
| Tagging | Method | Media | Description |
|---|---|---|---|
| Inter-Switch Link (ISL) | Fast Ethernet | ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header | Frame is lengthened. |
| 802.IQ | Fast Ethernet | IEEE defined Ethernet VLAN protocol | Header is modified. |
| 802.IQ | 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 slide set 8.

# Two Types of VLANs

- End-to-End or Campus-wide VLANs
- Geographic or Local VLANs

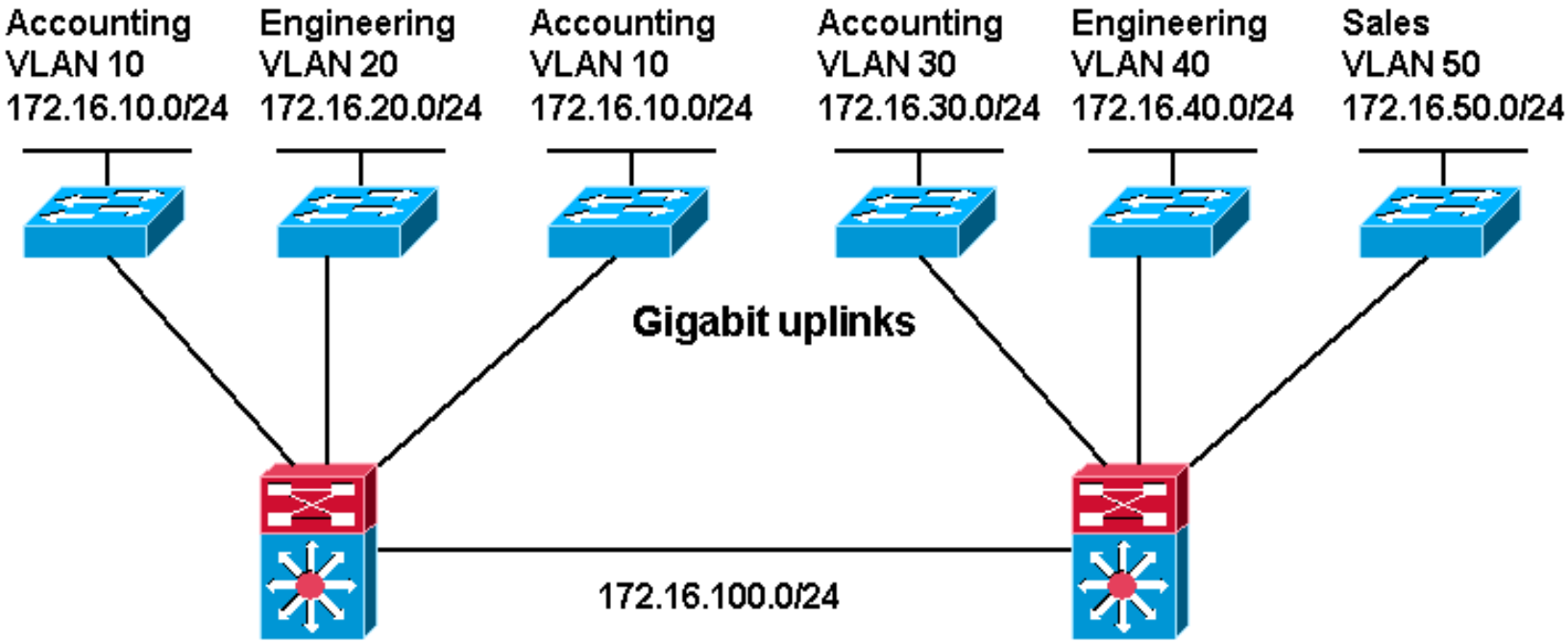
# End-to-End or Campus-wide VLANs




Campus-wide or End-to-End VLAN Model

- VLANs based on functionality
- "VLAN everywhere" model
- VLANs with the same VLAN ID, I.e. Accounting VLAN 10, can be anywhere in the network

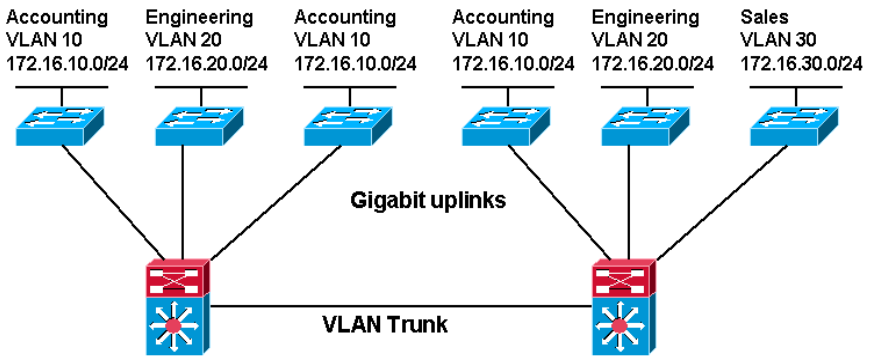
# Geographic or Local VLANs




**Local or Geographic VLAN Model**

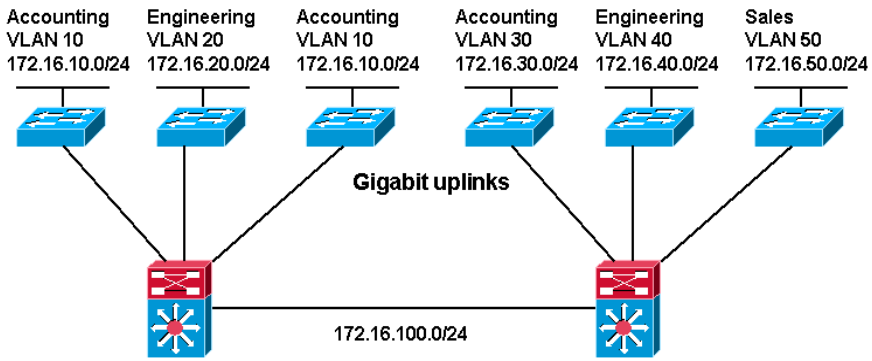
- VLANs based on physical location
- VLANs dedicated to each access layer switch cluster
- Accounting users connected to different layer 3 switches are on different VLANs, I.e. Accounting VLAN 10 and VLAN 30

# End-to-End or Campus-wide VLANs




Campus-wide or End-to-End VLAN Model

- VLANs based on functionality
- "VLAN everywhere" model
- VLANs with the same VLAN ID, I.e. Accounting VLAN 10, can be anywhere in the network

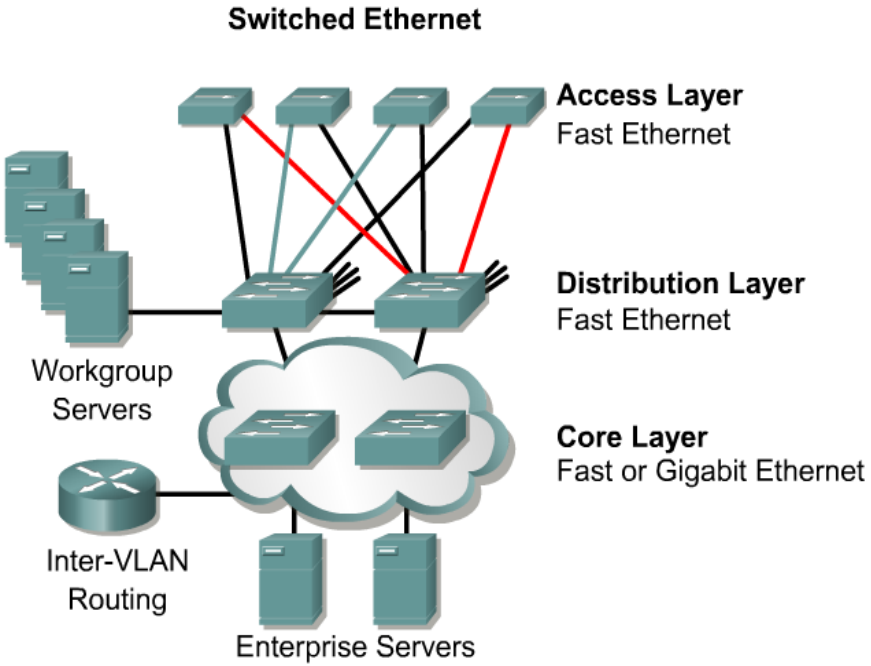


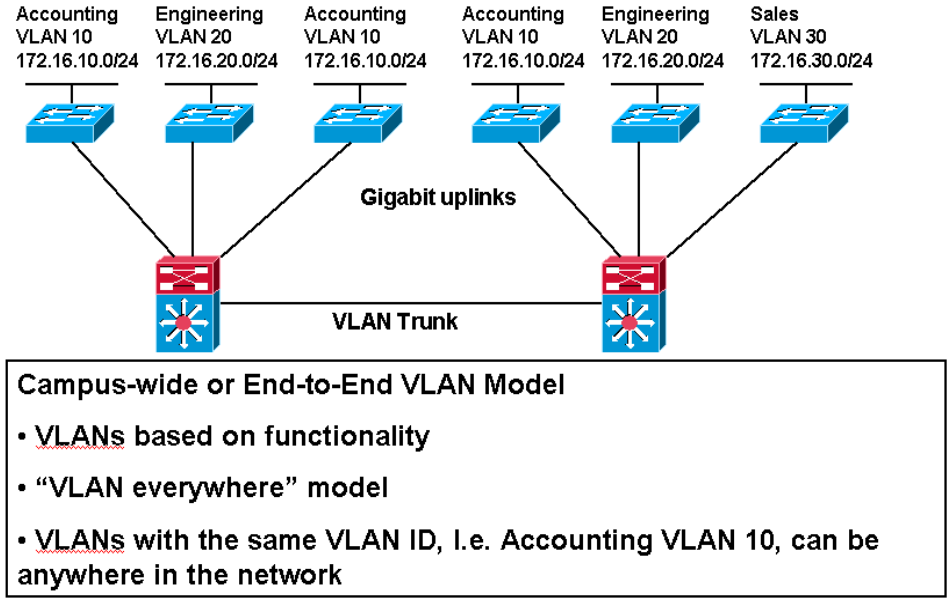

Local or Geographic VLAN Model

- VLANs based on physical location
- VLANs dedicated to each access layer switch cluster
- Accounting users connected to different layer 3 switches are on different VLANs, I.e. Accounting VLAN 10 and VLAN 30

- End-to-End or Campus-wide VLANs
  - Same VLAN/Subnet no matter what the location is on the network
  - Trunking at the Core
  - Usually not recommended by Cisco or other Vendors
  - Adds complexity to network administration
  - Does not resolve Layer 2 Spanning Tree issues

# End-to-End or Campus-wide VLANs

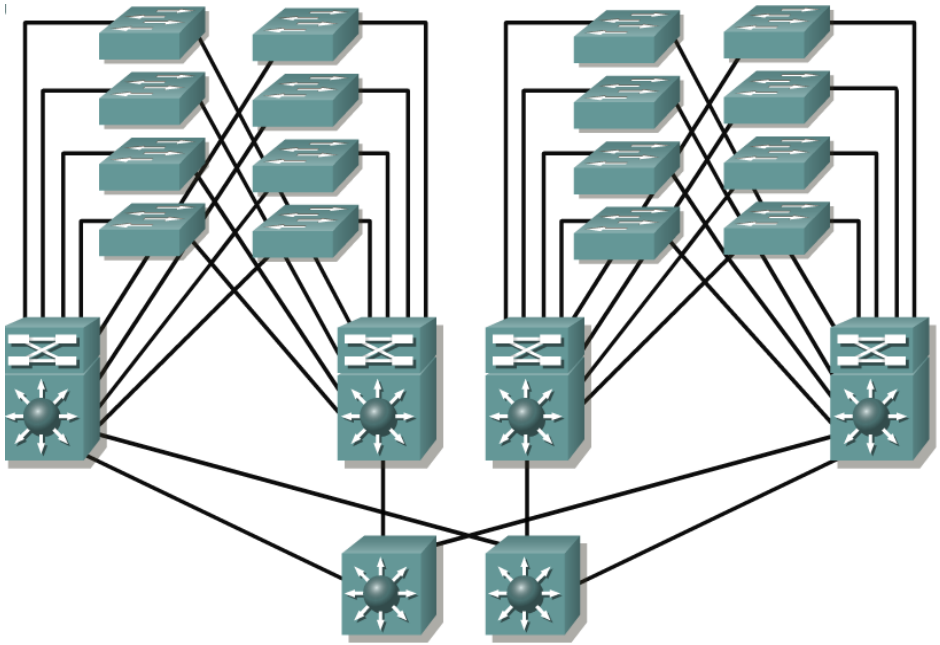


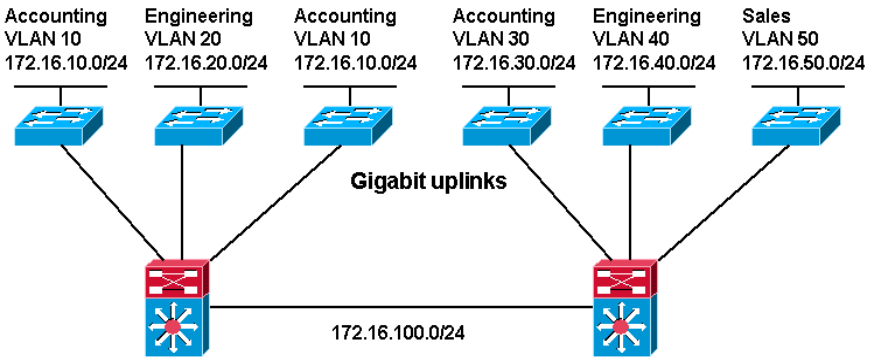




When to use End-to-End?

- Since the core layer router is being used to route between subnets (VLANs), the rule is:
  - **The network is engineered to have 80 percent of the traffic contained within a VLAN.**
  - The remaining 20 percent crosses the router to the enterprise servers and to the Internet and WAN.
  - **Note: This is known as the 80/20 rule. With today's traffic patterns, this rule is becoming obsolete.**

# Geographic or Local VLANs



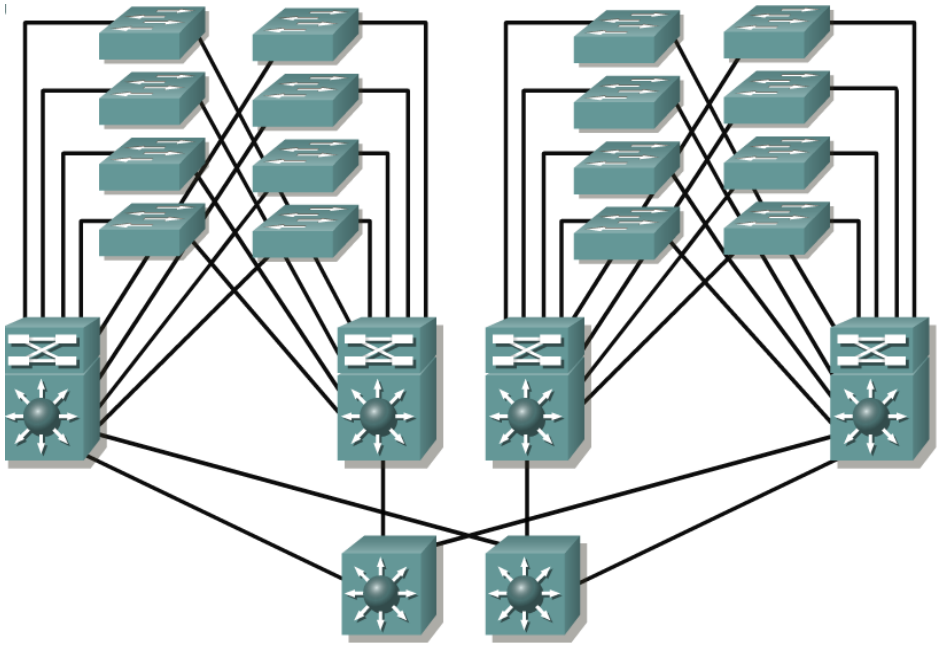


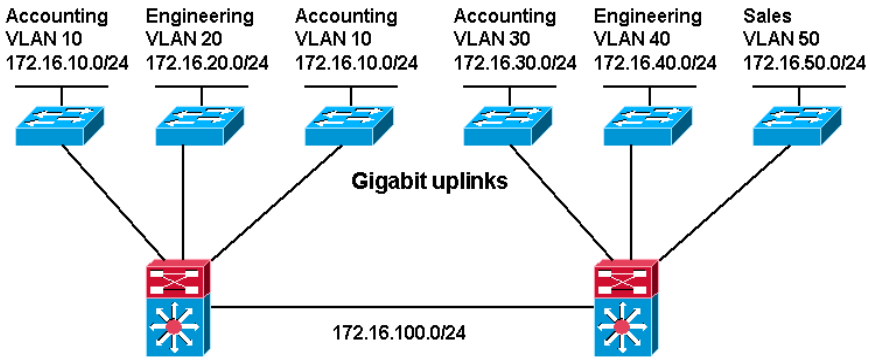

**Local or Geographic VLAN Model**

- VLANs based on physical location
- VLANs dedicated to each access layer switch cluster
- Accounting users connected to different layer 3 switches are on different VLANs, I.e. Accounting VLAN 10 and VLAN 30

- As many corporate networks have moved to centralize their resources, end-to-end VLANs have become more difficult to maintain.
- Users are required to use many different resources, many of which are no longer in their VLAN.
- Because of this shift in placement and usage of resources, VLANs are now more frequently being created around geographic boundaries rather than commonality boundaries.

# Geographic or Local VLANs



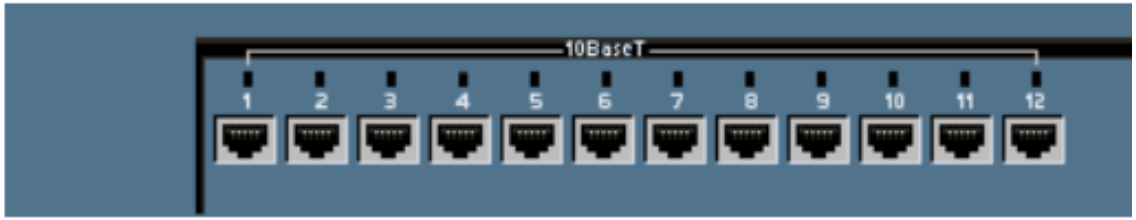



Local or Geographic VLAN Model

- VLANs based on physical location
- VLANs dedicated to each access layer switch cluster
- Accounting users connected to different layer 3 switches are on different VLANs, I.e. Accounting VLAN 10 and VLAN 30

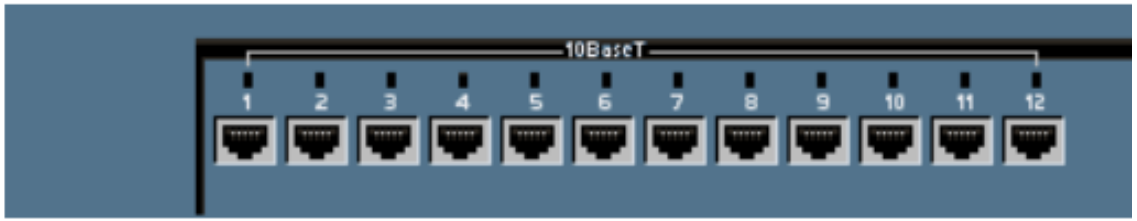
- This geographic location can be as large as an entire building or as small as a single switch inside a wiring closet.
- **In a VLAN structure, it is typical to find the new 20/80 rule in effect. 80 percent of the traffic is remote to the user and 20 percent of the traffic is local to the user.**
- Although this topology means that the user must cross a Layer 3 device in order to reach 80 percent of the resources, this design allows the network to provide for a deterministic, consistent method of accessing resources.

# 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.
  - "The switch must be in VTP server mode to create, add, or delete VLANs." **(This is not true. Switch could be in VTP Transparent mode. VTP will be discussed in a moment.)**

# Creating VLANs




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

  `Switch(config)#`**`interface fastethernet 0/9`**

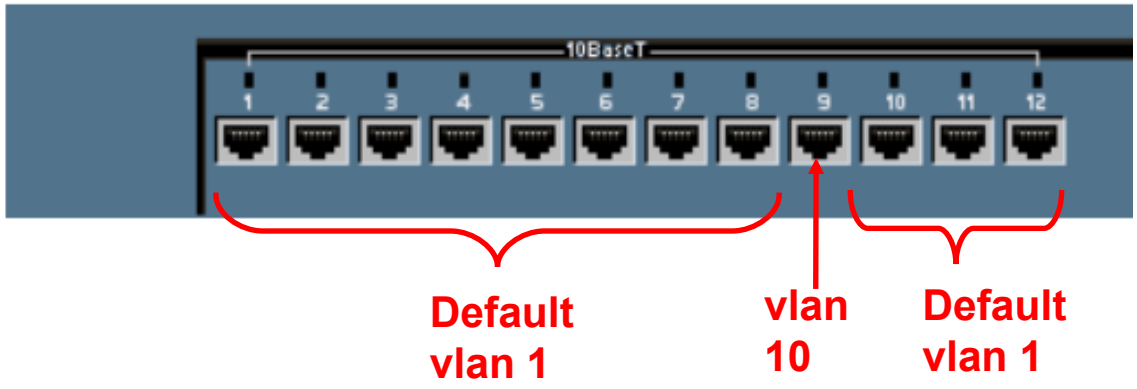
  `Switch(config-if)#`**`switchport access vlan`** ***`vlan_number`***

- **Create the VLAN:** `Switch#`**`vlan database`**

  `Switch(vlan)#`**`vlan`** *`vlan_number`*

  `Switch(vlan)#`**`exit`**

# Creating VLANs

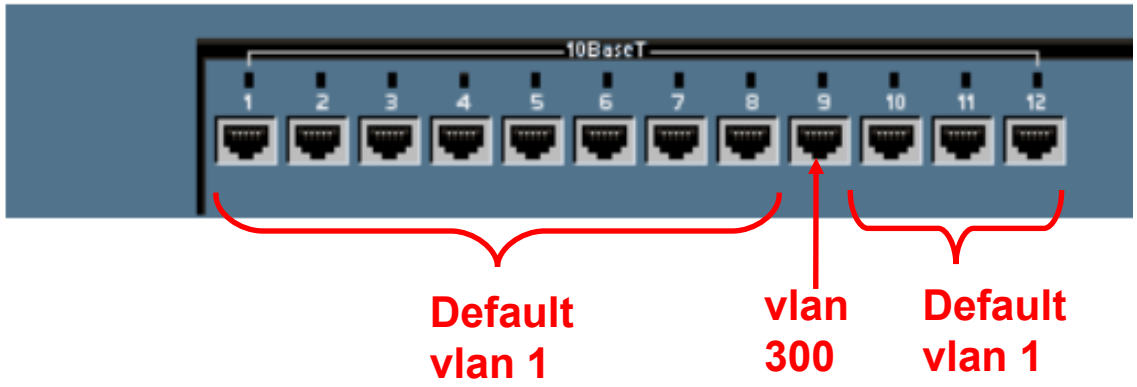



- Assign ports to the VLAN

```
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)

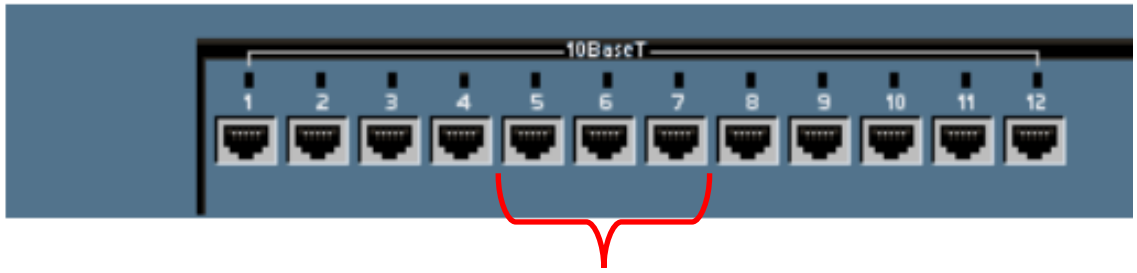
# Creating VLANs




Cisco

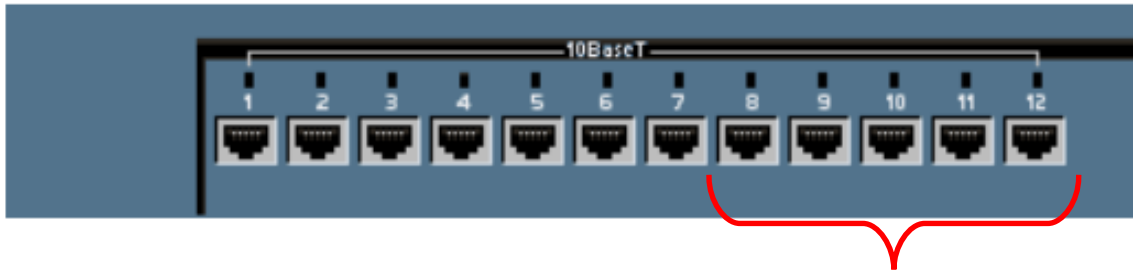
```
Enter configuration commands, one per line. End with CNTL/Z.

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
```

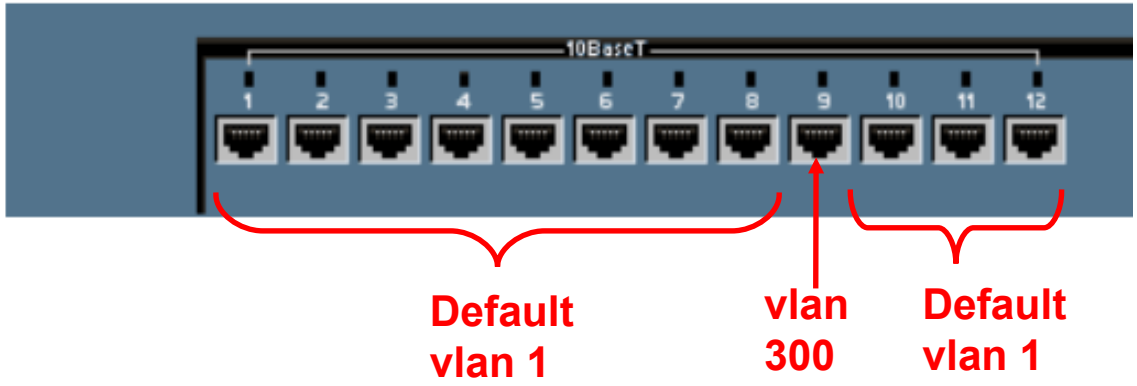
# Configuring Ranges of VLANs




```
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.**

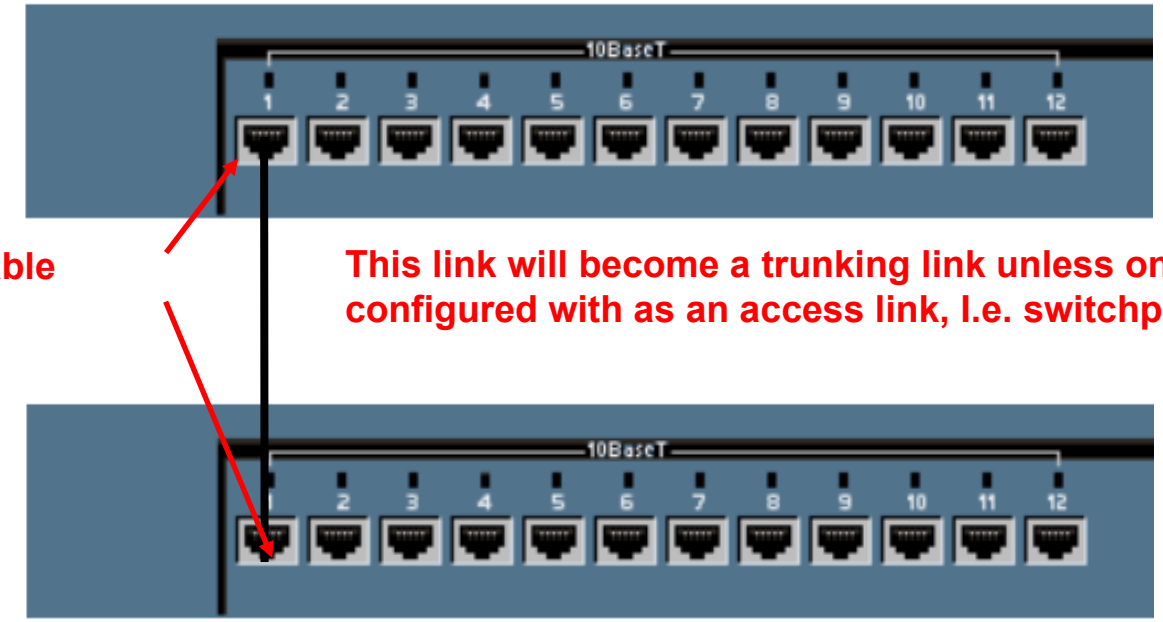
# Creating VLANs




```
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.

# Creating VLANs

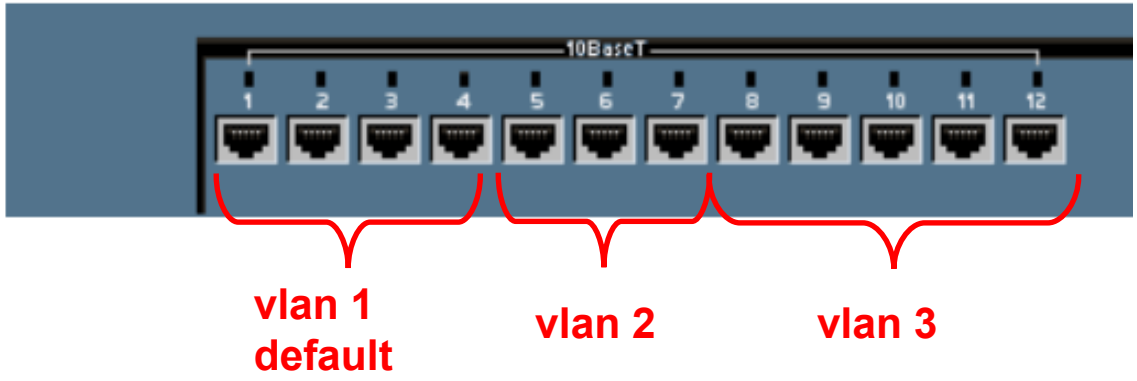



**Default: dynamic desirable**

**This link will become a trunking link unless one of the ports is configured with as an access link, I.e. switchport mode access**

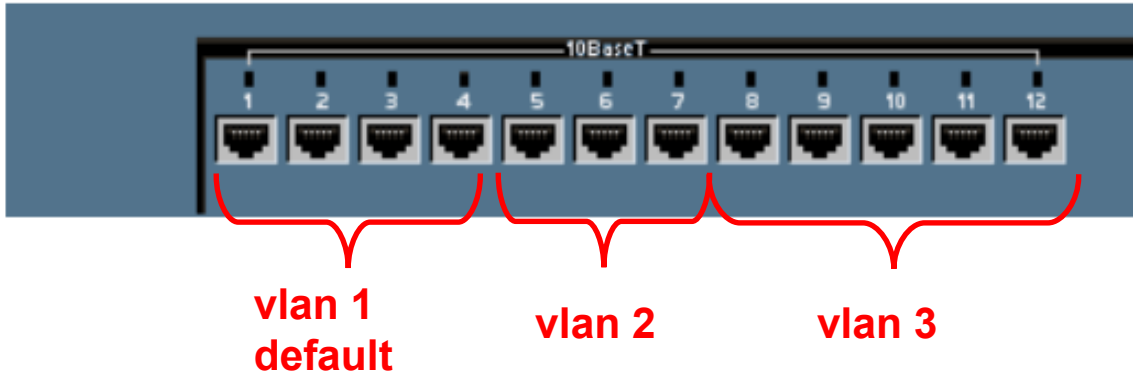
- By default, all ports are configured as **`switchport mode dynamic desirable`**, which means that if the port is connected to another switch with an port configured with the same default mode (or desirable or auto), this link will become a trunking link. (See my article on DTP on my web site for more information.)
- When the `switchport access vlan` command is used, the `switchport mode access` command is not necessary since the `switchport access vlan` command configures the interface as an "access" port (non-trunk port).

# 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 in Slide Set 8).
- 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**