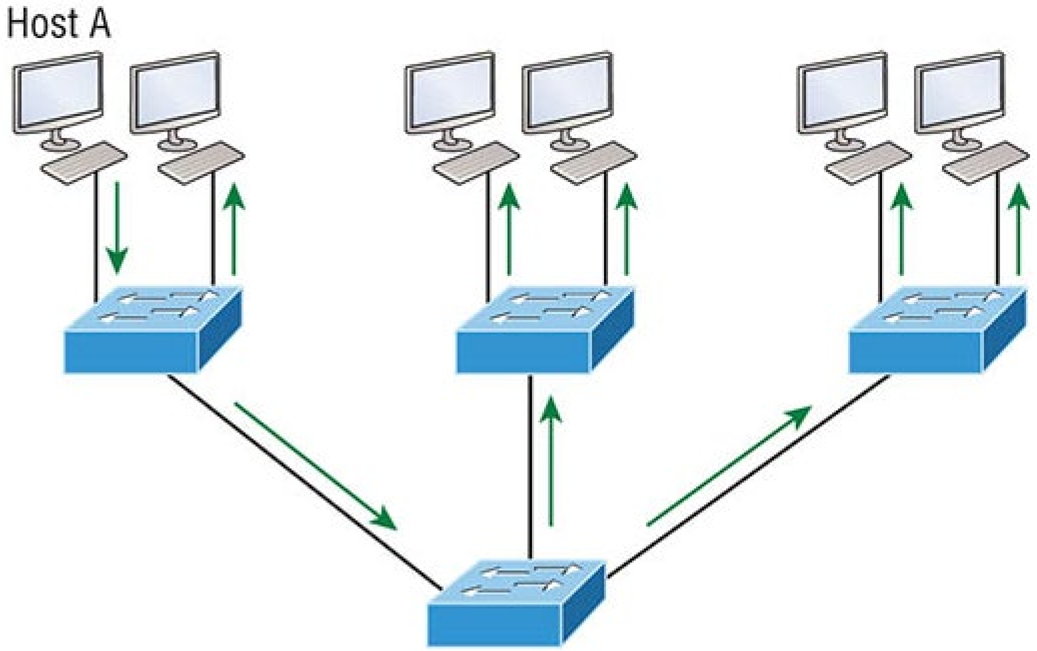
ECCS-3631
Networks and Data Communications

Module 3-3
Virtual Local Area Network (VLAN)

Dr. Ajmal Khan

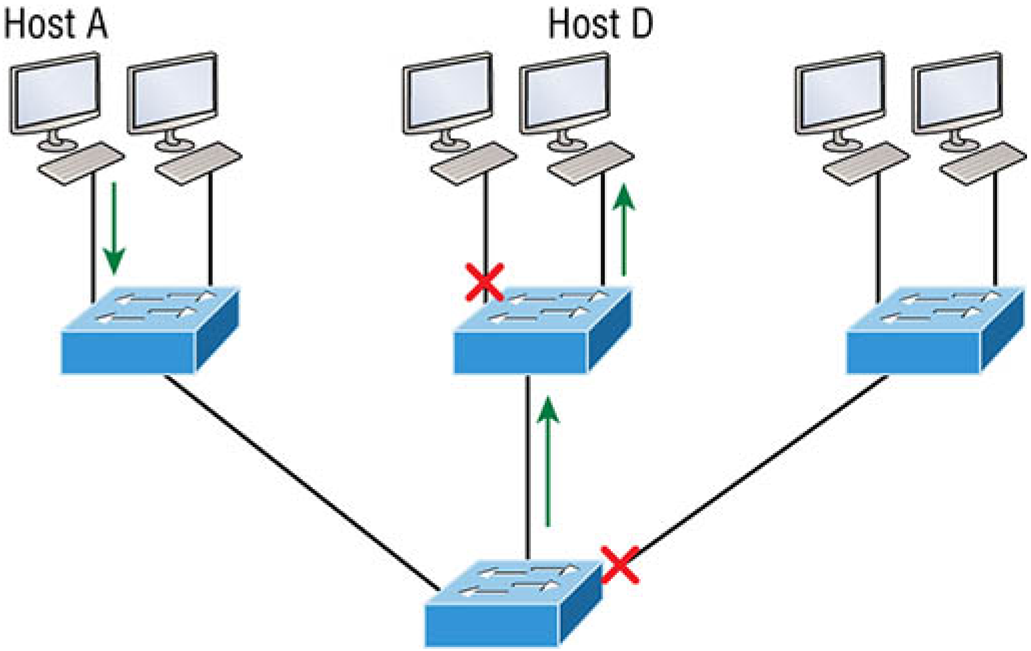
Broadcast

- Every broadcast packet transmitted is seen by every device on the network
- In the Figure, Host A sending out a broadcast and all ports on all switches forwarding it—all except the port that originally received it.



Switched Network

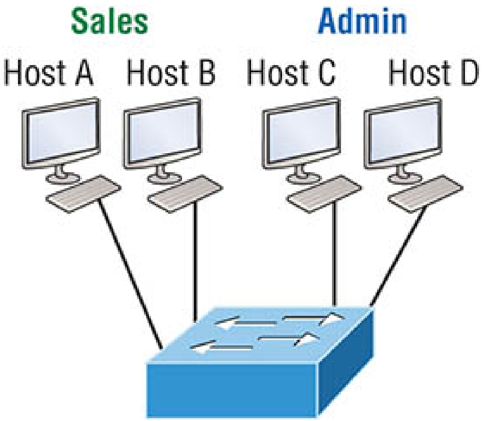
- In switched network, Host A sending a frame with Host D as its destination.
- Clearly, the important factor here is that the frame is only forwarded out the port where Host D is located.



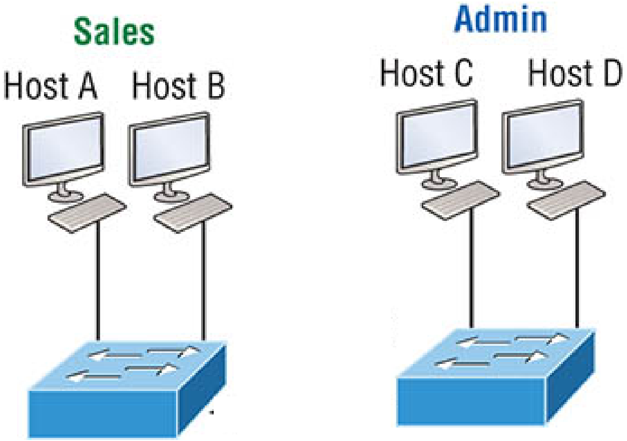
Benefits of a Switch

- A layer 2 switched network creates individual collision domain segments for each device plugged into each port on the switch.
- Allows us to build larger networks.
- However, the more users and devices that populate and use a network, the more broadcasts and packets each switch has to deal with.
- **Security!** all users can see all devices by default. Can’t stop devices from broadcasting, plus can’t stop users from trying to respond to broadcasts. This means your security options are dismally limited to placing passwords on your servers and other devices.
- **Simple Solution!** Put them in different networks
- **Disadvantage!** Requires more switches, and of course cabling

Switches in our Lab: Why A & B ???



One switch, one LAN.

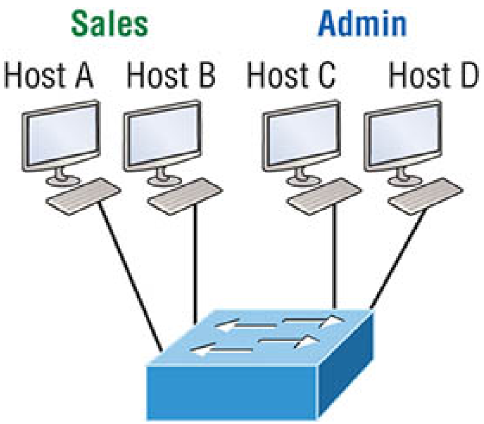


TWO switches, TWO LANs.

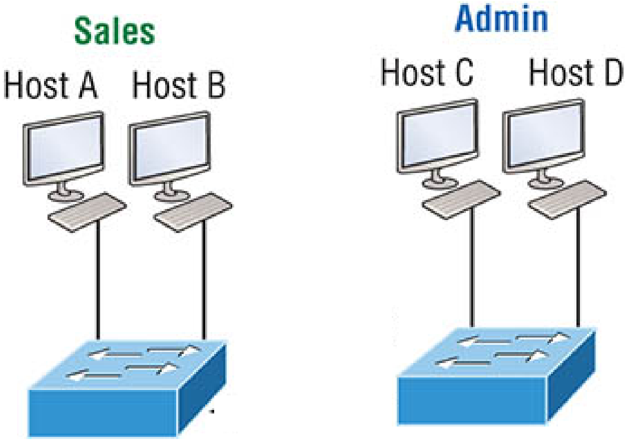
- How many networks do you connect with one switch in the lab?

VLAN Motivation

- **Expert Solution!** Create VLANs

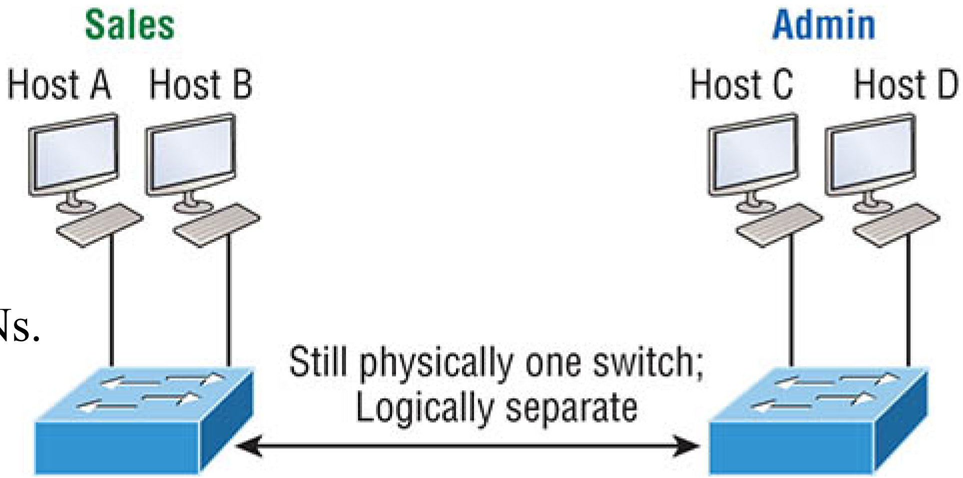


One switch, one LAN.



TWO switches, TWO LANs.

ONE switch, TWO Virtual LANs.

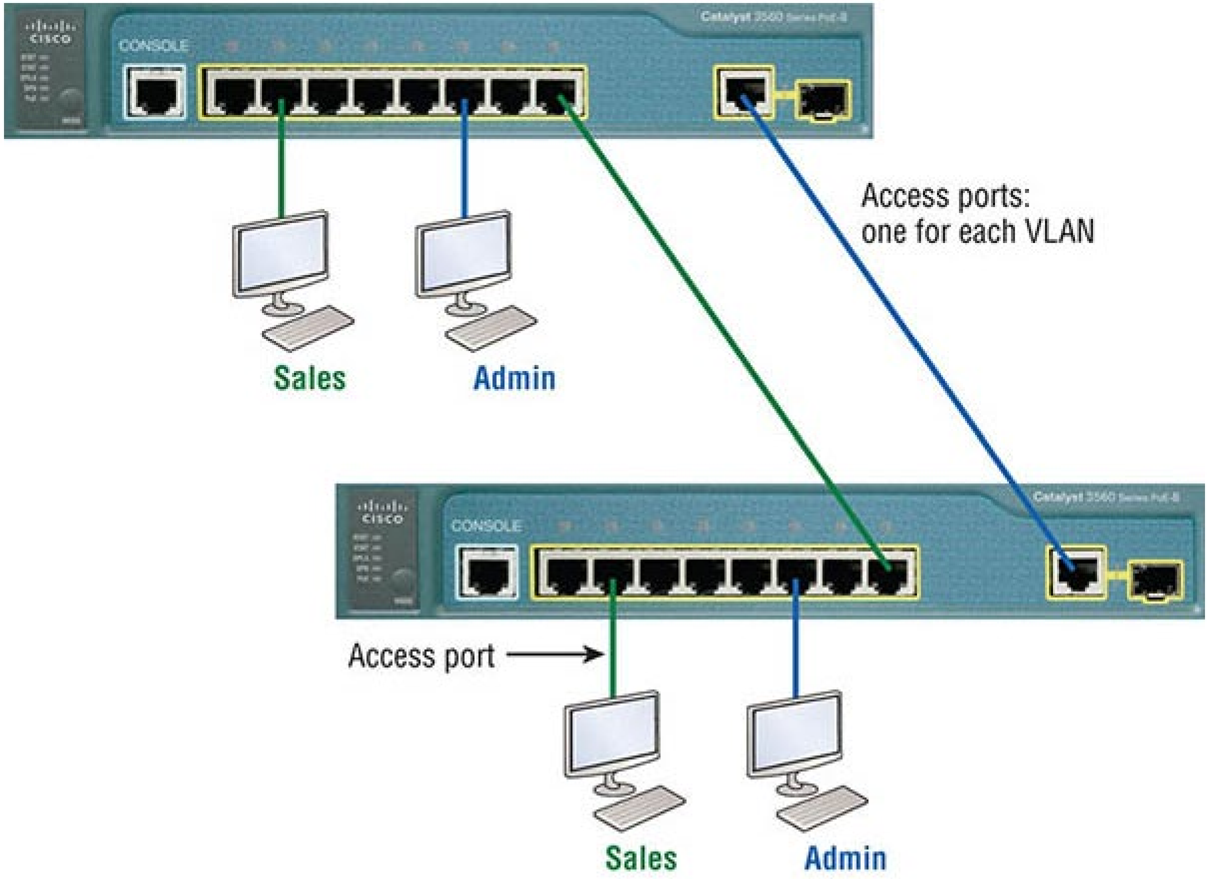


VLAN Advantages

- Network adds, moves, and changes are achieved with ease by just configuring a port into the appropriate VLAN.
- VLANs increase the number of broadcast domains while decreasing their size.
- A group of users that need an unusually high level of security can be put into its own VLAN so that users outside of that VLAN can't communicate with that group's users.
- As a logical grouping of users by function, VLANs can be considered independent from their physical or geographic locations.
- VLANs greatly enhance network security if implemented correctly.

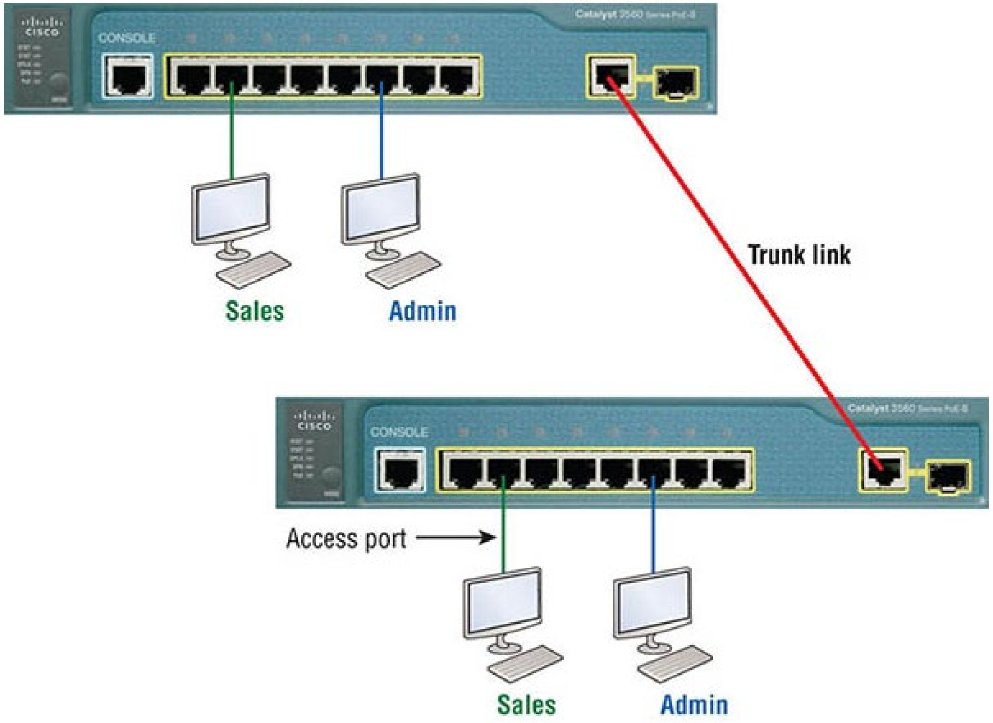
Identifying VLANs – Access Ports

- An *access port* belongs to and carries the traffic of only one VLAN.VLANs increase the number of broadcast domains while decreasing their size.
- Any device attached to an *access link* is unaware of a VLAN membership – the device just assumes it is part of some broadcast domain.



Identifying VLANs – Trunk Ports

- The term *trunk port* was inspired by the telephone system trunks, which carry multiple telephone conversations at a time. So it follows that trunk ports can similarly carry multiple VLANs at a time as well.
- Trunk port carries the traffic of multiple VLANs - from 1 to 4,094 VLANs at a time.
- Instead of an access link for each VLAN between switches, Create a trunk link



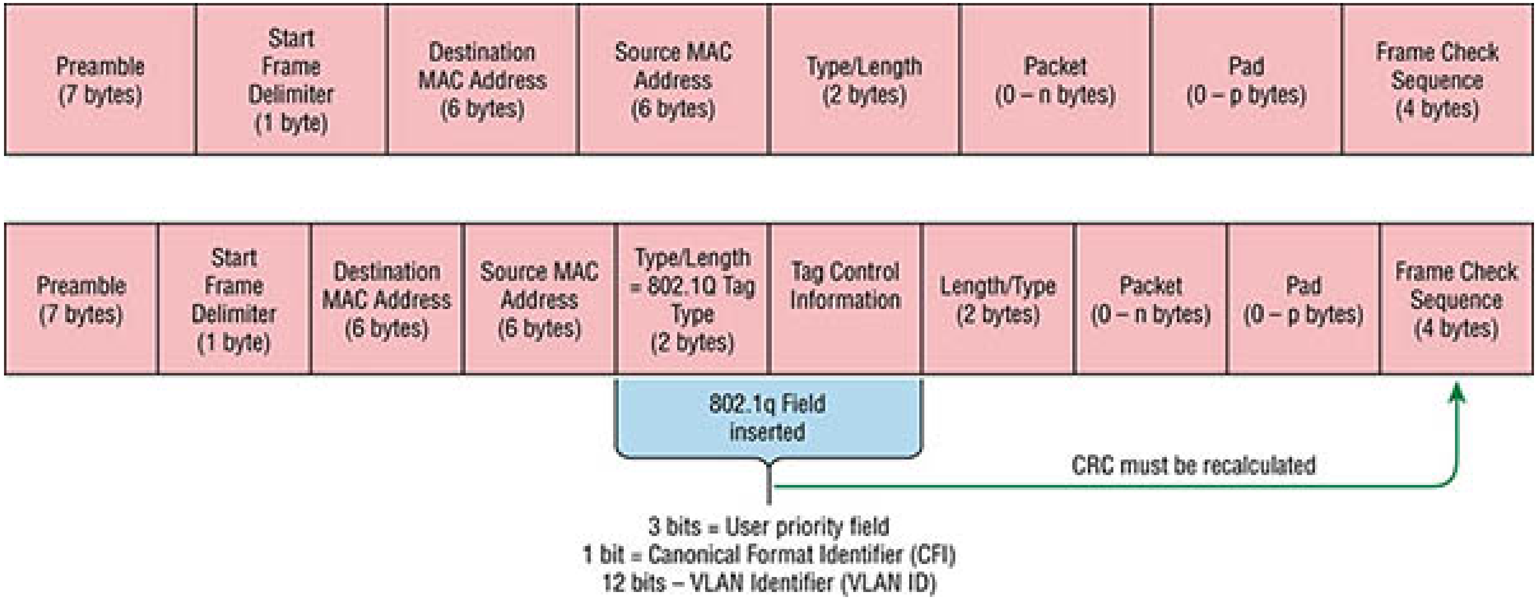
Frame Tagging

- Once within the switch, each switch that the frame reaches must first identify the VLAN ID from the frame tag. It then finds out what to do with the frame by looking at the information in what's known as the filter table. If the frame reaches a switch that has another trunked link, the frame will be forwarded out of the trunk-link port.

- Once the frame reaches an exit that's determined by the forward/filter table to be an access link matching the frame's VLAN ID, the switch will remove the VLAN identifier. This is so the destination device can receive the frames without being required to understand their VLAN identification information.

VLAN Identification

- Created by the IEEE as a standard method of frame tagging,
- IEEE 802.1q actually inserts a field into the frame to identify the VLAN.
- VLAN identifier (VLAN ID) is 12 bit, support up to 4,094 VLANs
- VLAN 1 is the default native VLAN
- The native VLAN accepts information without any frame tag



Preamble (7 bytes)	Start Frame Delimiter (1 byte)	Destination MAC Address (6 bytes)	Source MAC Address (6 bytes)	Type/Length (2 bytes)	Packet (0 – n bytes)	Pad (0 – p bytes)	Frame Check Sequence (4 bytes)

Preamble (7 bytes)	Start Frame Delimiter (1 byte)	Destination MAC Address (6 bytes)	Source MAC Address (6 bytes)	Type/Length = 802.1Q Tag Type (2 bytes)	Tag Control Information	Length/Type (2 bytes)	Packet (0 – n bytes)	Pad (0 – p bytes)	Frame Check Sequence (4 bytes)

802.1q Field inserted

CRC must be recalculated

3 bits = User priority field
1 bit = Canonical Format Identifier (CFI)
12 bits – VLAN Identifier (VLAN ID)

IEEE 802.1q encapsulation with and without the 802.1q tag

VLAN Identification

- Created by the IEEE as a standard method of frame tagging,
- IEEE 802.1q actually inserts a field into the frame to identify the VLAN.
- VLAN identifier (VLAN ID) is 12 bit, support up to 4,094 VLANs
- VLAN 1 is the default native VLAN
- The native VLAN accepts information without any frame tag
- The basic purpose of 802.1q frame-tagging methods is to provide inter-switch VLAN communication.
- 802.1q frame tagging is removed if a frame is forwarded out an access link—tagging is used internally and across trunk links only!

VLAN Communication

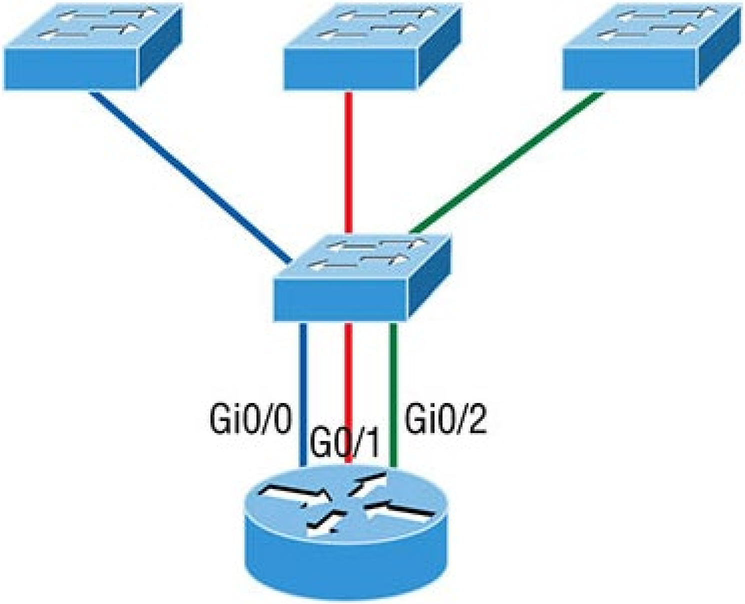
- Hosts in a VLAN live in their own broadcast domain and can communicate freely.
- VLANs create network partitioning and traffic separation at layer 2 of the OSI.
- We know that, if we want hosts or any other IP-addressable device to communicate between VLANs, we must have a layer 3 device to provide routing.
- For this, we can use a router that has an interface for each VLAN

  OR a router that supports ISL or 802.1q routing.

Inter-VLAN Routing

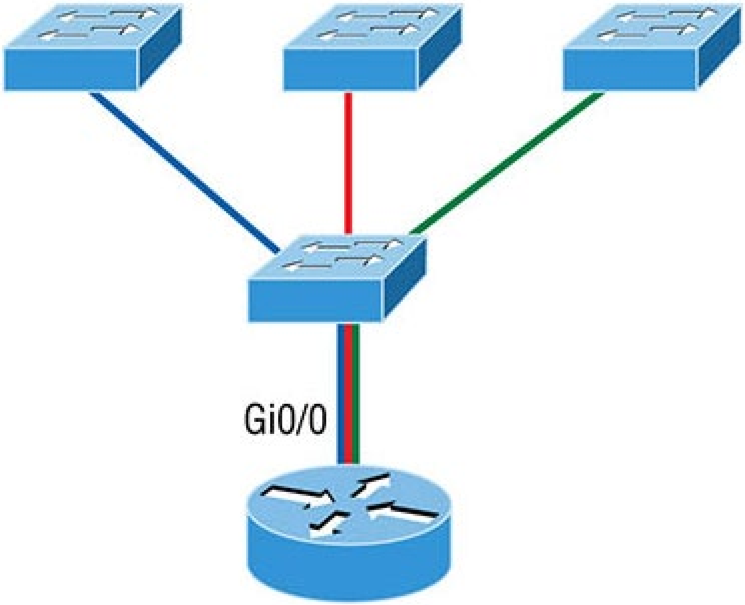
- If you had two or three VLANs, you could get by with a router equipped with two or three FastEthernet connections.
- each router interface is plugged into an access link.
- This means that each of the routers' interface IP addresses would then become the default gateway address for each host in each respective VLAN.

- **Disadvantage**: Needs as many ports on the router as number of VLANs. Thus, more cabling and more cost of a router.



Router on a Stick

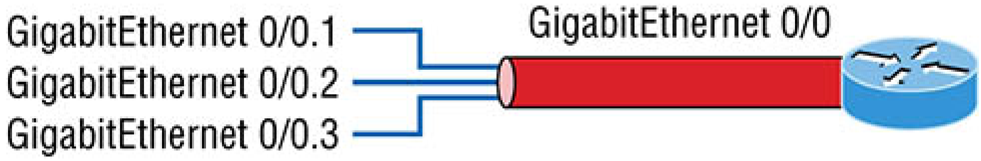
- If you have more VLANs available than router interfaces, you can configure trunking on one FastEthernet interface
- Instead of using a router interface for each VLAN, you can use one FastEthernet interface and run ISL or 802.1q trunking.
- This allows all VLANs to communicate through one interface. Also, known as a router on a stick (ROAS)



Router on a Stick (ROAS)

Logical Interfaces on a Router

- Router has one physical interface, **what about gateway for each VLAN**?
- Router creates Logical Interfaces
- Physical interface divided into multiple subinterfaces, with one subnet assigned per VLAN.
- Each subinterface being the default gateway address for each VLAN/subnet.



A router creates Logical Interfaces

Review Question

- What is the maximum number of VLANs that can be configured on a switch supporting the 802.1Q protocol? Why?

In 802.1Q there is a 12- bit VLAN identifier.

Thus 2^{12} = 4,098 – 2 = 4,096 VLANs can be supported.