Module : Internetworking

Switching, VLANs & Inter-VLAN Routing

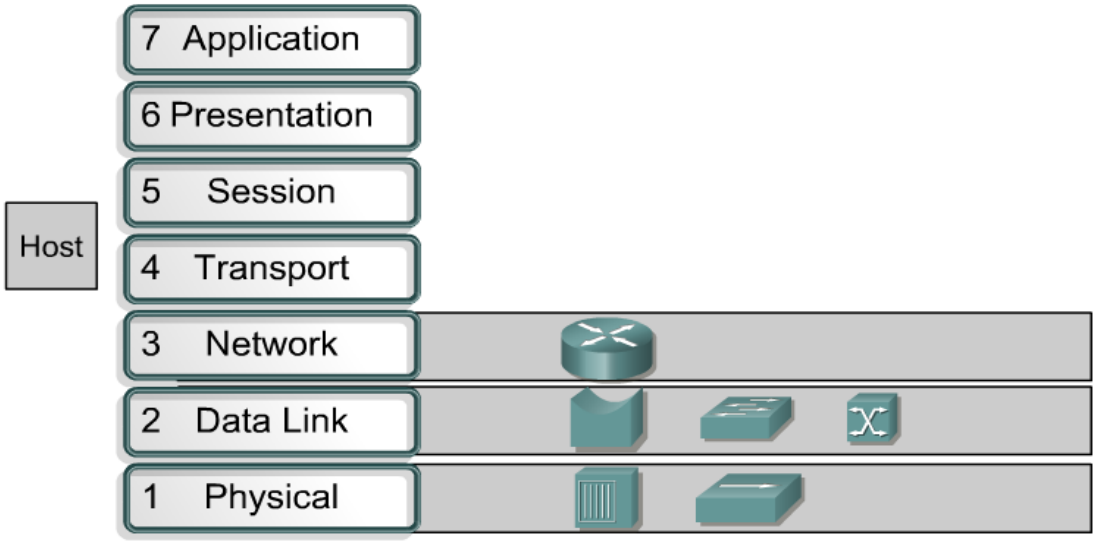
Waterford Institute of Technology

Richard Frisby

rfrisby@wit.ie

Office : 324

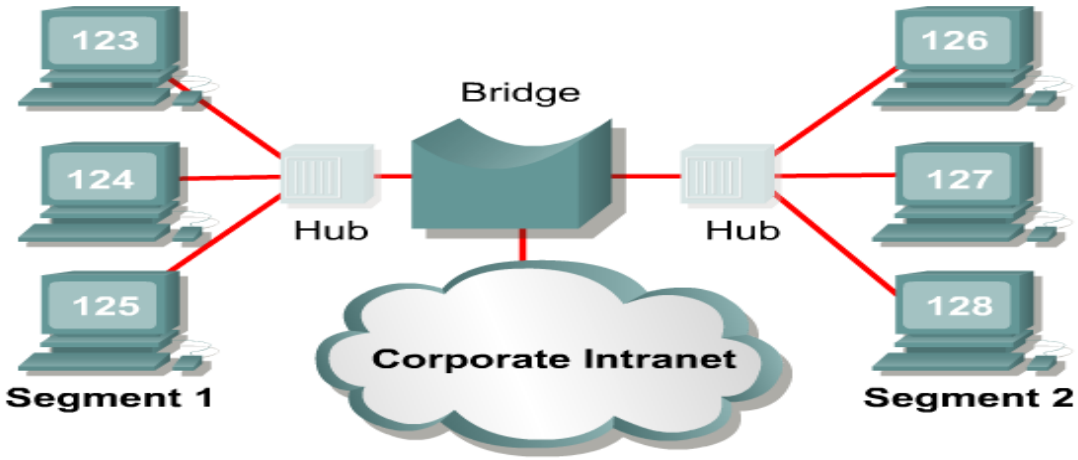
Overview/Revision



Routers
Switches, Bridges
Hub, Repeaters

- Ethernet networks used to be built using **repeaters**.
- When the performance of these networks began to suffer because too many devices shared the same segment, network engineers added bridges to create multiple collision domains.
- As networks grew in size and complexity, the **bridge evolved into the modern switch**, allowing microsegmentation of the network.
- Today's networks typically are built using **switches and routers**, often with the routing and switching function in the same device.

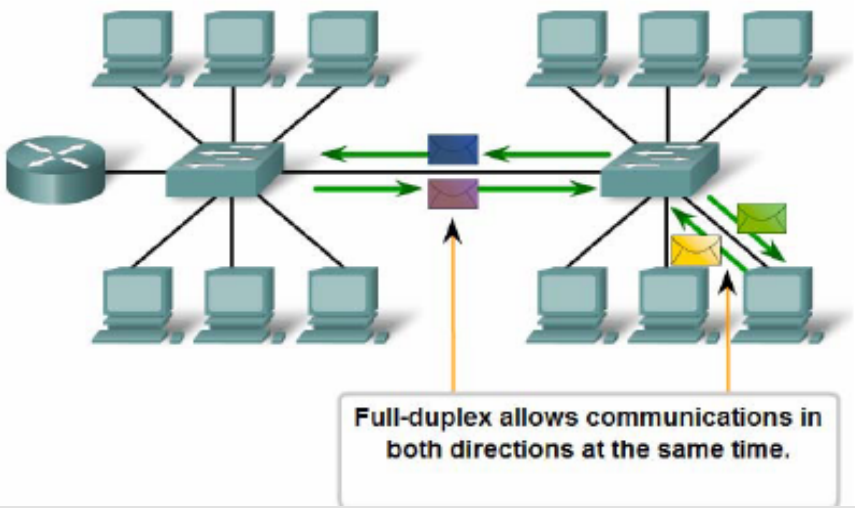
Bridges



- A bridge is a Layer 2 device used to divide, or segment, a network.
- A bridge is capable of collecting and selectively passing data frames between two network segments.
- Bridges do this by learning the MAC address of all devices on each connected segment. Using this information, the bridge builds a bridging table and forwards or blocks traffic based on that table.
- This results in smaller collision domains and greater network efficiency.
- Bridges do **NOT** restrict **broadcast** traffic.

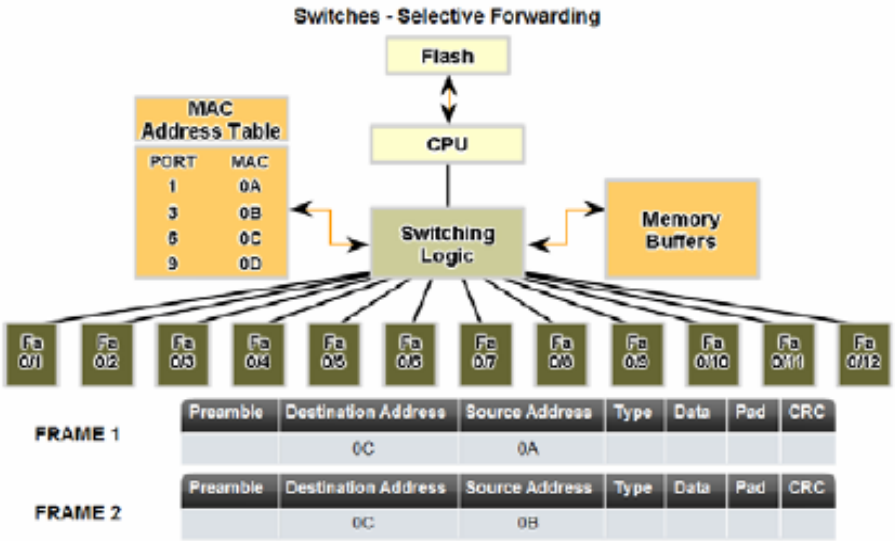
Ethernet using Switches

- Switches allow the **segmentation** of the LAN into separate **collision domains**.
- **Dedicated Bandwidth**: Each node has the full media bandwidth available in the connection between the node and the switch.
- **Collision-Free Environment**: A dedicated point-to-point connection to a switch also removes any media contention between devices, allowing a node to operate with few or no collisions.
- **Full-Duplex Operation**: Switching also allows a network to operate as a full-duplex Ethernet environment.



Switches – Selective Forwarding

- Ethernet switches forward frames using a momentary point-to-point connecti between the transmitting and receiving nodes.
- The connection is made only long enough to forward a single frame.
- During this instant, the two nodes have a full bandwidth connection between them and represent a logical point-to-point connection.
- **Store and forward** switching, the switch receives entire frame, checks FSC for errors, and forwards the frame to the appropriate port for the destination node.
- For each incoming frame, the destination MAC address is compared to the list of addresses in the MAC table (switch table, bridge table, bridging table).
- If a match is found, the port number in the table that is paired with the MAC address is used as the exit port for the frame.



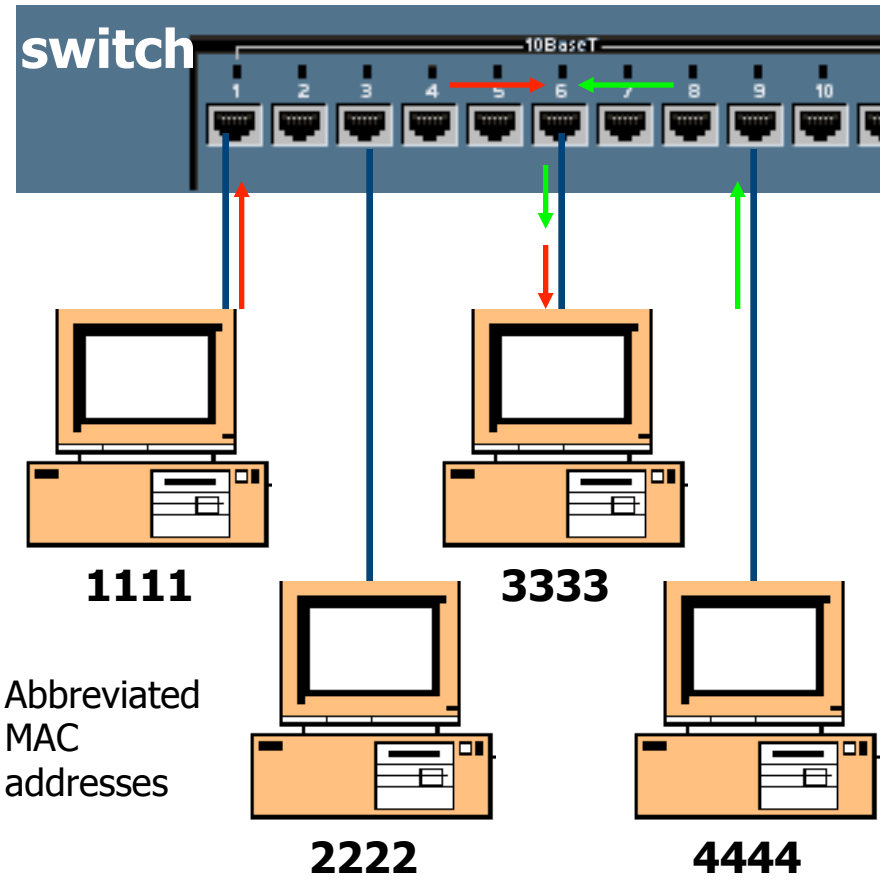
Switches – Operation

- To accomplish their purpose, Ethernet LAN switches use five basic operations: Learning, Aging, Flooding, Selective Forwarding, Filtering
- **Learning**: The switch creates a new entry in the MAC table using the source MAC address and pairs the address with the port on which the entry arrived. The switch now can use this mapping to forward frames to this node.
- **Aging**: The entries in the MAC table acquired by the Learning process are time stamped. This timestamp is used as a means for removing old entries.
- **Flooding**: If the switch does not know to which port to send a frame because the destination MAC address is not in the MAC table, the switch sends the frame to all ports except the port on which the frame arrived.
- **Selective forwarding**: When a frame arrives at the switch for which the switch has already learned the MAC address, this address is matched to an entry in the MAC table and the frame is forwarded to the corresponding port.
- **Filtering**: A frame is filtered (not forwarded) if the destination MAC address on the same port as the incoming frame.

Layer 2 and Layer 3 Switching

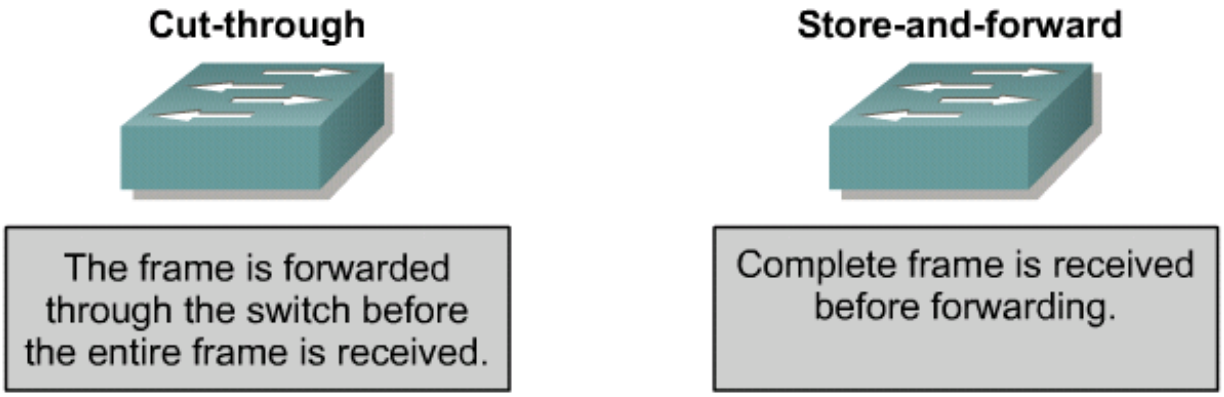
- Switching is the process of receiving an incoming frame on one interface and delivering that frame out another interface. Routers use Layer 3 switching to route a packet. Switches use Layer 2 switching to forward frames.
- A layer 3 switch is typically a layer 2 switch that includes a routing process, I.e. does routing.
- Layer 3 switching has many meanings and in many cases is just a marketing term !!
- Layer 2 switching looks at a destination MAC address in the frame header and forwards the frame to the appropriate interface or port based on the MAC address in the switching table. The switching table is contained in Content Addressable Memory (CAM). If the Layer 2 switch does not know where to send the frame, it broadcasts the frame out all ports to the network. When a reply is returned, the switch records the new address in the CAM.
- Layer 3 switching is a function of the network layer. The Layer 3 header information is examined and the packet is forwarded based on the IP address.
- Traffic flow in a switched or flat network is inherently different from the traffic flow in a routed or hierarchical network. Hierarchical networks offer more flexible traffic flow than flat networks.

Memory buffering



- An Ethernet switch may use a buffering technique to store and forward frames.
- Buffering may also be used when the destination port is busy.
- The area of memory where the switch stores the data is called the memory buffer.
- This memory buffer can use two methods for forwarding frame:
  - **port-based memory buffering**
  - **shared memory buffering**
- In port-based memory buffering frames are stored in queues that are linked to specific incoming ports.
- Shared memory buffering deposits all frames into a common memory buffer which all the ports on the switch share.

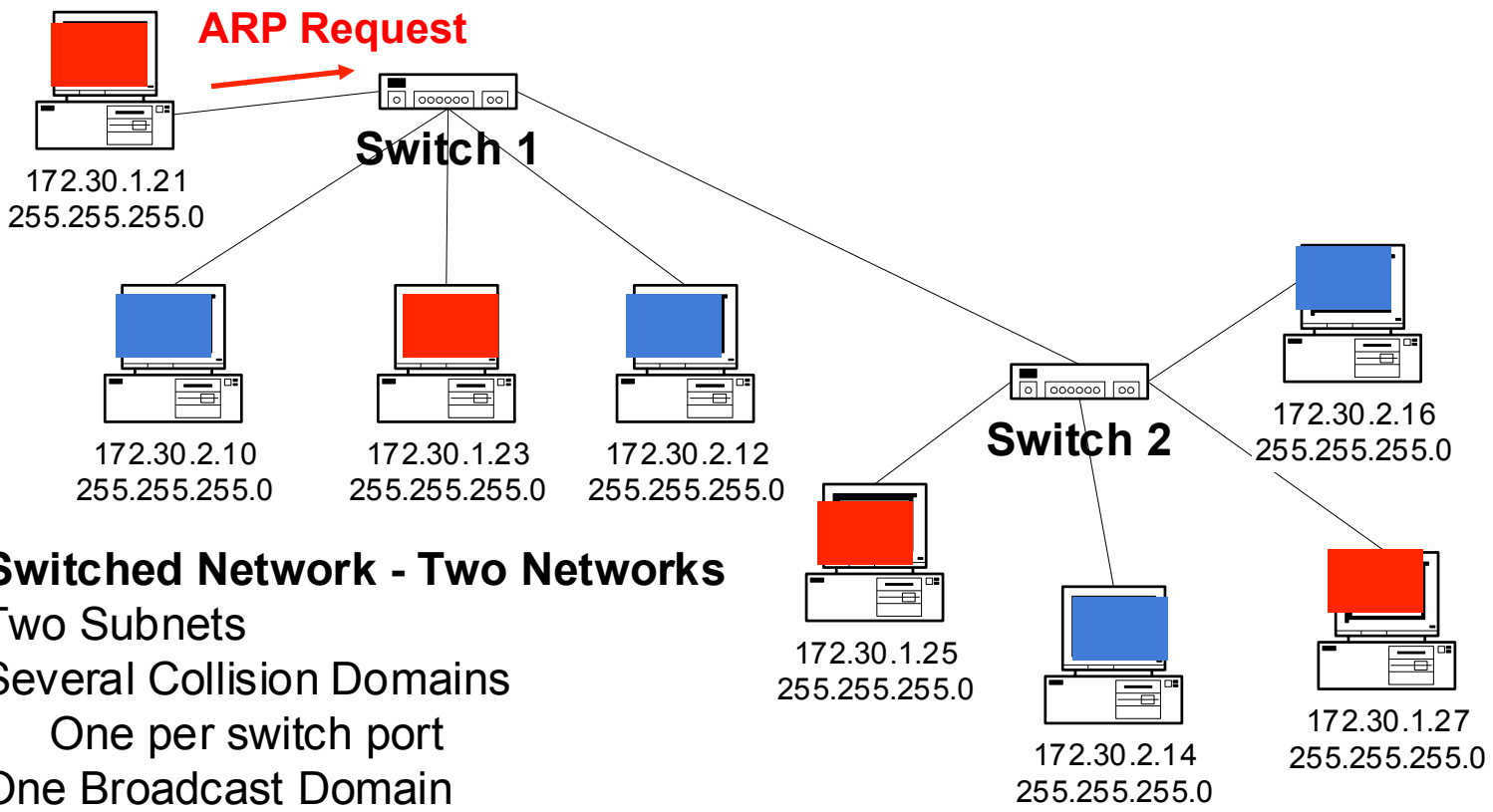
Two Switching Methods



Cut-through – The frame is forwarded through the switch before the entire frame is received. At a minimum the frame destination address must be read before the frame can be forwarded. This mode decreases the latency of the transmission, but also reduces error detection.

Store-and-forward – The entire frame is received before any forwarding takes place. The destination and source addresses are read and filters are applied before the frame is forwarded. Latency occurs while the frame is being received. Latency is greater with larger frames because the entire frame must be received before the switching process begins. The switch is able to check the entire frame for errors, which allows more error detection.

Switched Network with Multiple Subnets

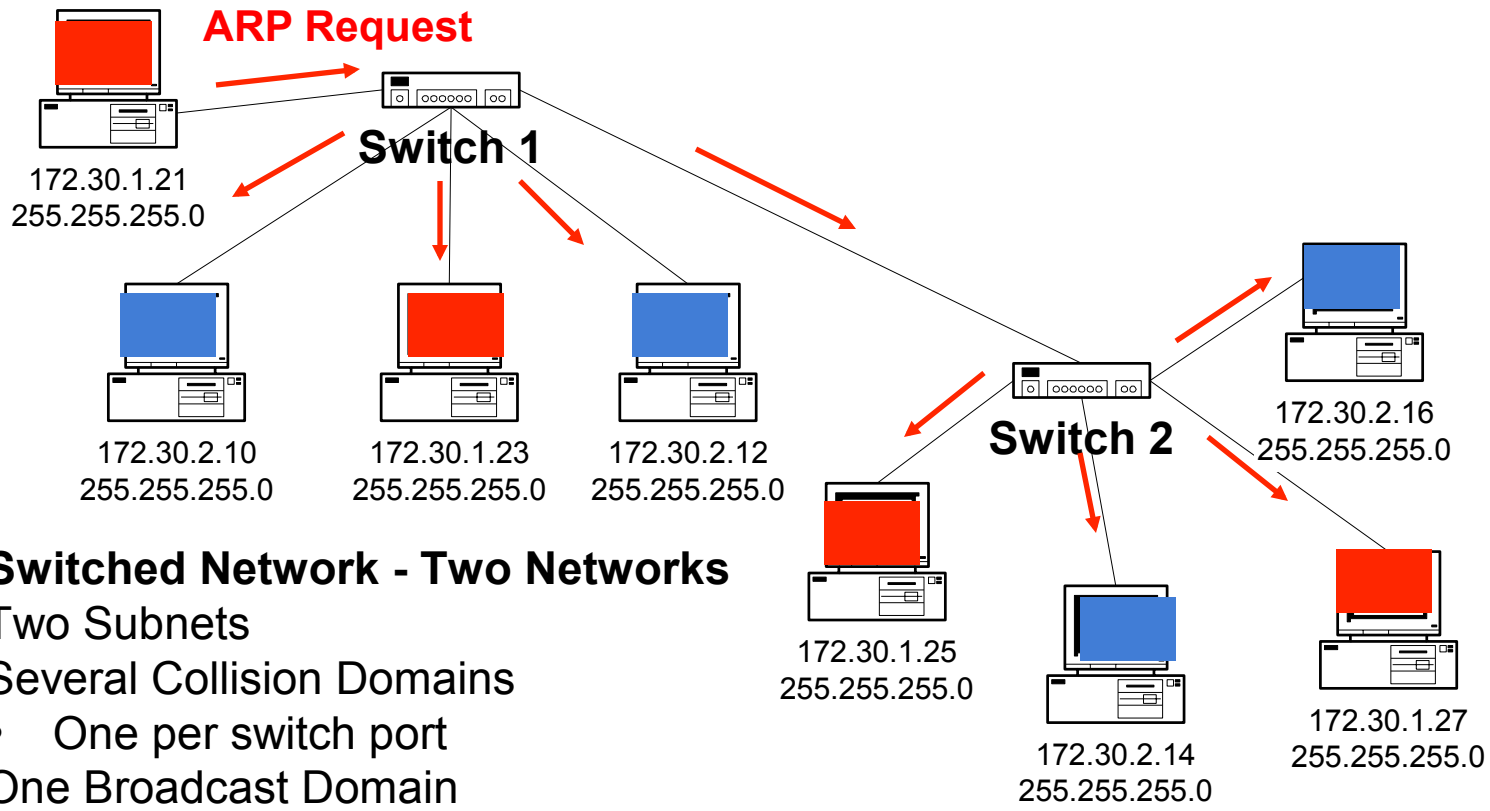


All Switched Network - Two Networks

- Two Subnets
- Several Collision Domains
  - One per switch port
- One Broadcast Domain

- What are the issues?
- Can data travel within the subnet? Yes
- Can data travel between subnets? No, need a router!
- What is the impact of a layer 2 broadcast, like an ARP Request?

Switched Network with Multiple Subnets

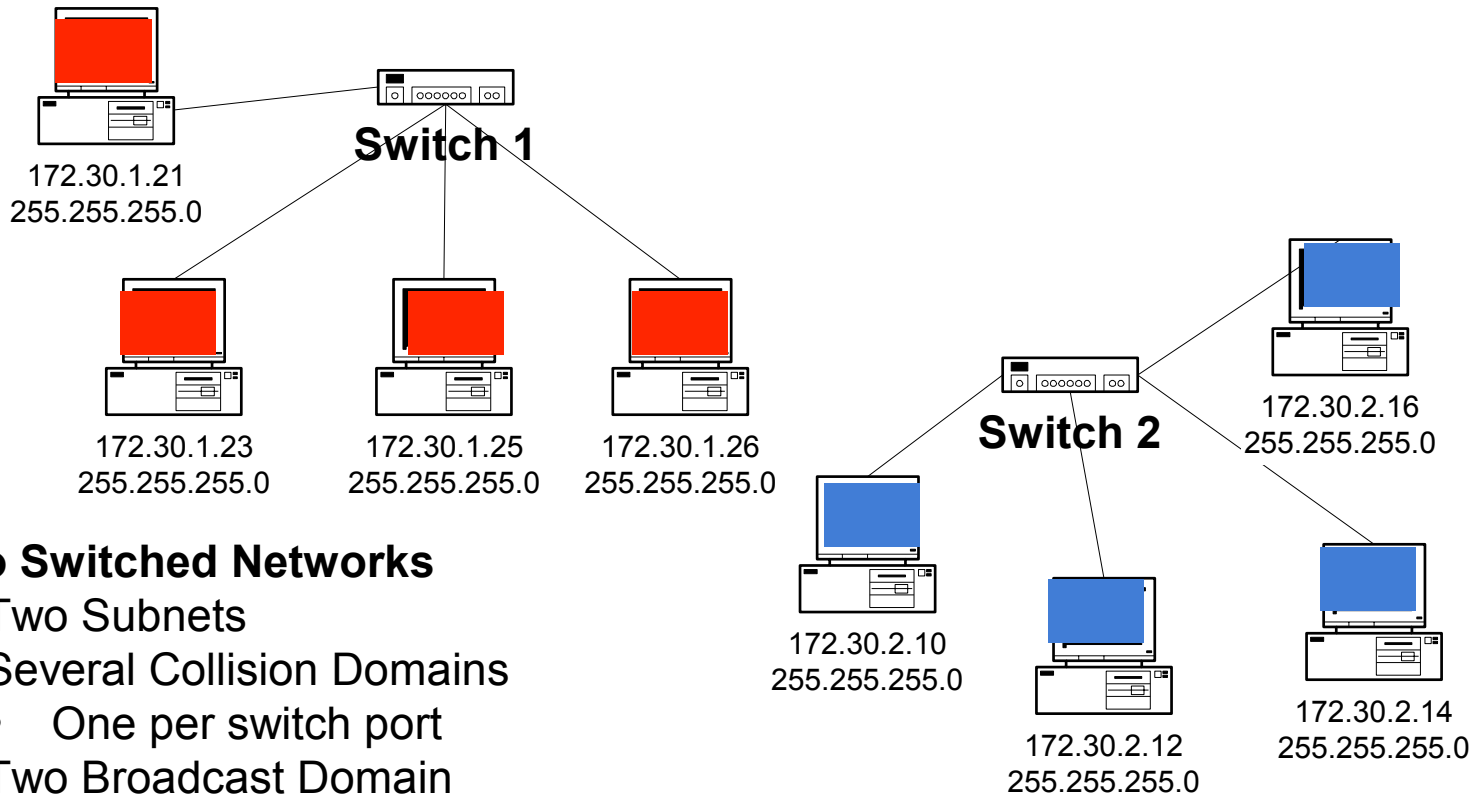


All Switched Network - Two Networks

- Two Subnets
- Several Collision Domains
  - One per switch port
- One Broadcast Domain

- All devices see the ARP Request, even those on the other subnets that do not need to see it.
- One broadcast domain means the switches flood all broadcast out all ports, except the incoming port.
- Switches have no idea of the layer 3 information contained in the ARP Request.This consumes bandwidth on the network and processing cycles on the hosts.

One Solution: Physically separate the subnets

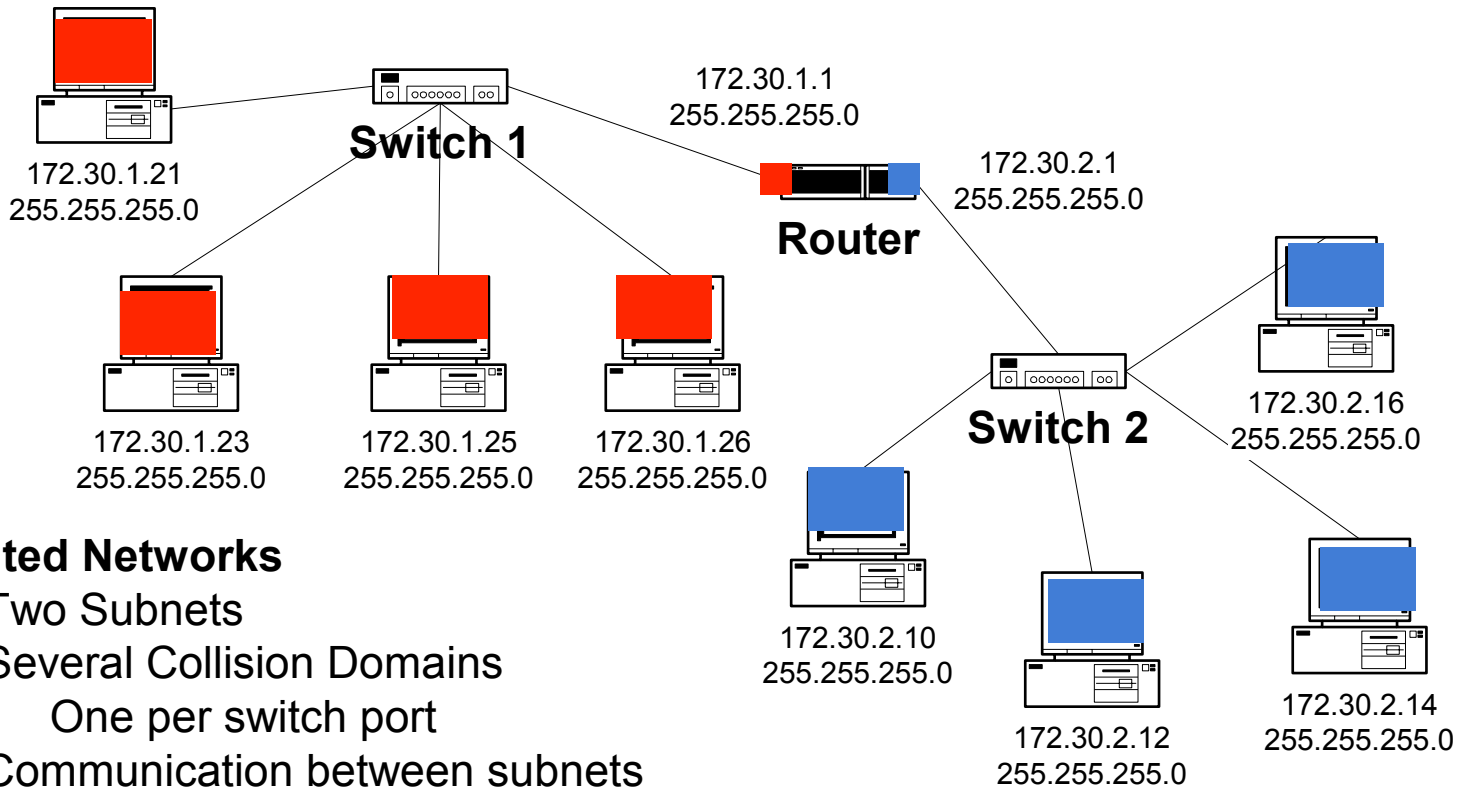


Two Switched Networks

- Two Subnets
- Several Collision Domains
  - One per switch port
- Two Broadcast Domain

- But still no data can travel between the subnets.
- How can we get the data to travel between the two subnets?

Another Solution: Use a Router



Routed Networks

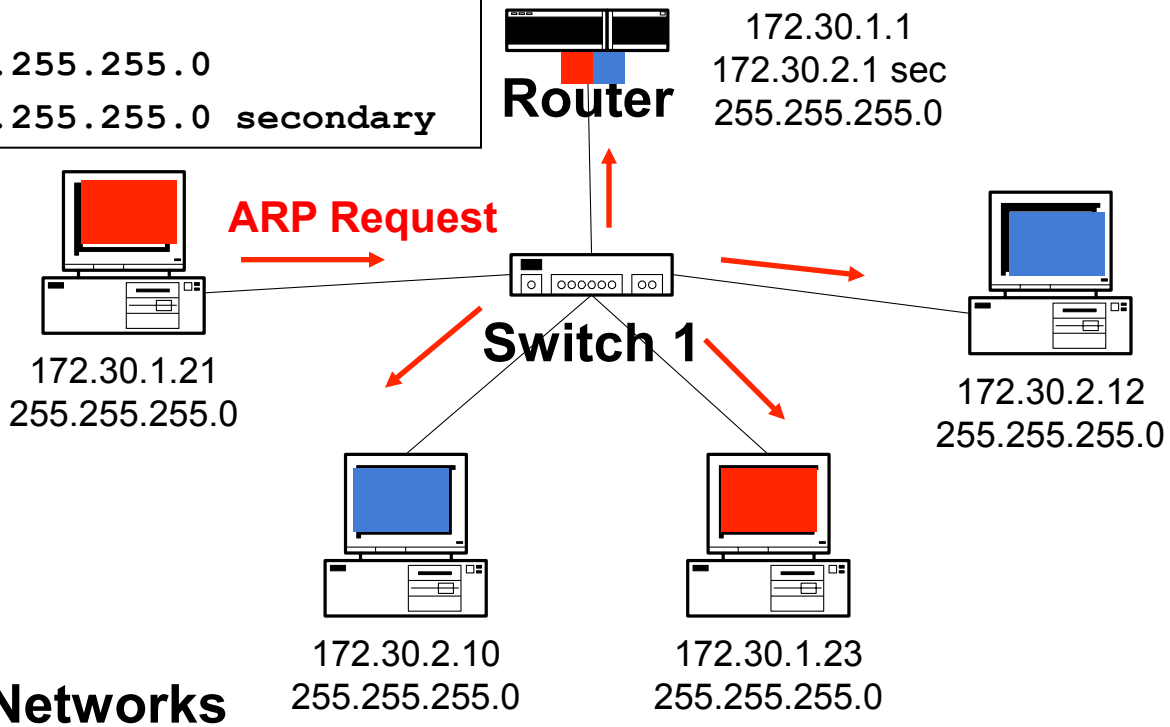
- Two Subnets
- Several Collision Domains
  - One per switch port
- Communication between subnets

- Two separate broadcast domains, because the router will not forward the layer 2 broadcasts such as ARP Requests.

Another solution config : Router-on-a-stick or One-Arm-Router

```
interface e 0
ip address 172.30.1.1 255.255.255.0
ip address 172.30.2.1 255.255.255.0 secondary
```

Secondary addresses can be used when the router does not support sub-interfaces.



Routed Networks

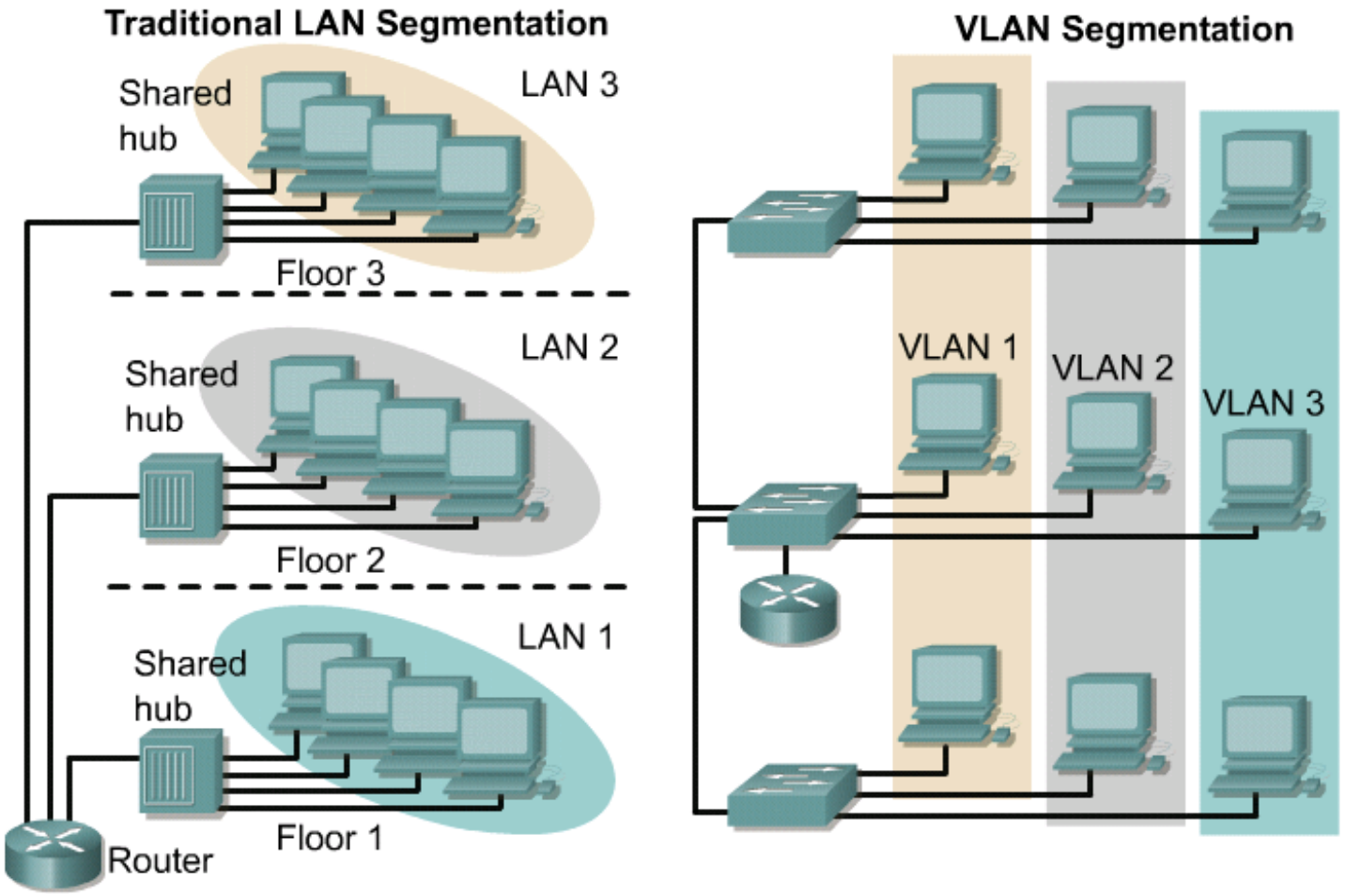
- Two Subnets
- Communication between subnets

- When a single interface is used to route between subnets or networks, this is know as a router-on-a-stick.
- To assign multiple ip addresses to the same interface, secondary addresses or subinterfaces are used.

Virtual LANs Overview

- A VLAN is a logical grouping of devices or users. These devices or users can be grouped by function, department, or application despite the physical LAN segment location.
- Devices on a VLAN are restricted to only communicating with devices that are on their own VLAN. Just as routers provide connectivity between different LAN segments, routers provide connectivity between different VLAN segments.
- VLANs increase overall network performance by logically grouping users and resources together. Businesses often use VLANs as a way of ensuring that a particular set of users are logically grouped regardless of the physical location. Therefore, users in the Marketing department are placed in the Marketing VLAN, while users in the Engineering Department are placed in the Engineering VLAN.
- VLANs can enhance scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- VLANs are powerful tools for network administrators when properly designed and configured. However, improperly configured VLANs can make a network function poorly or not function at all. Understanding how to implement VLANs on different switches is important when designing a network.

VLAN Introduction



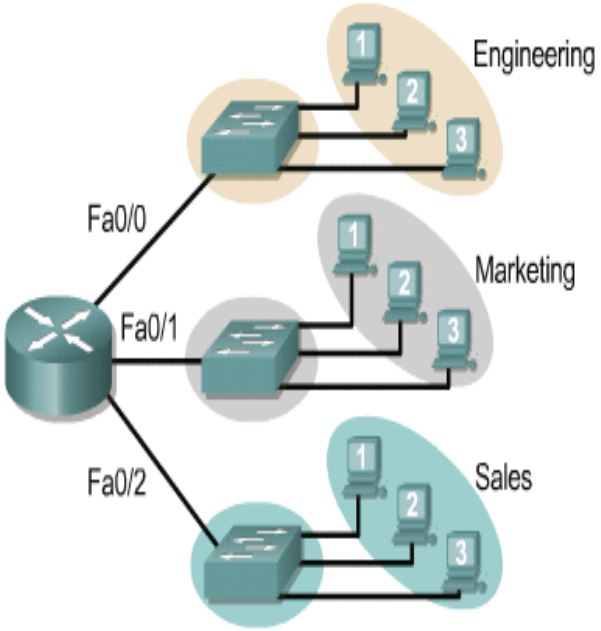
VLAN Introduction

- VLANs logically segment switched networks
- Configuration or reconfiguration of VLANs is done through software. Physically connecting or moving cables and equipment is unnecessary when configuring VLANs.
- A workstation in a VLAN group is restricted to communicating with file servers in the same VLAN group. VLANs function by logically segmenting the network into different broadcast domains so that packets are only switched between ports that are designated for the same VLAN.
- VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations. VLANs address scalability, security, and network management.

Broadcast Domains with VLANs and Routers

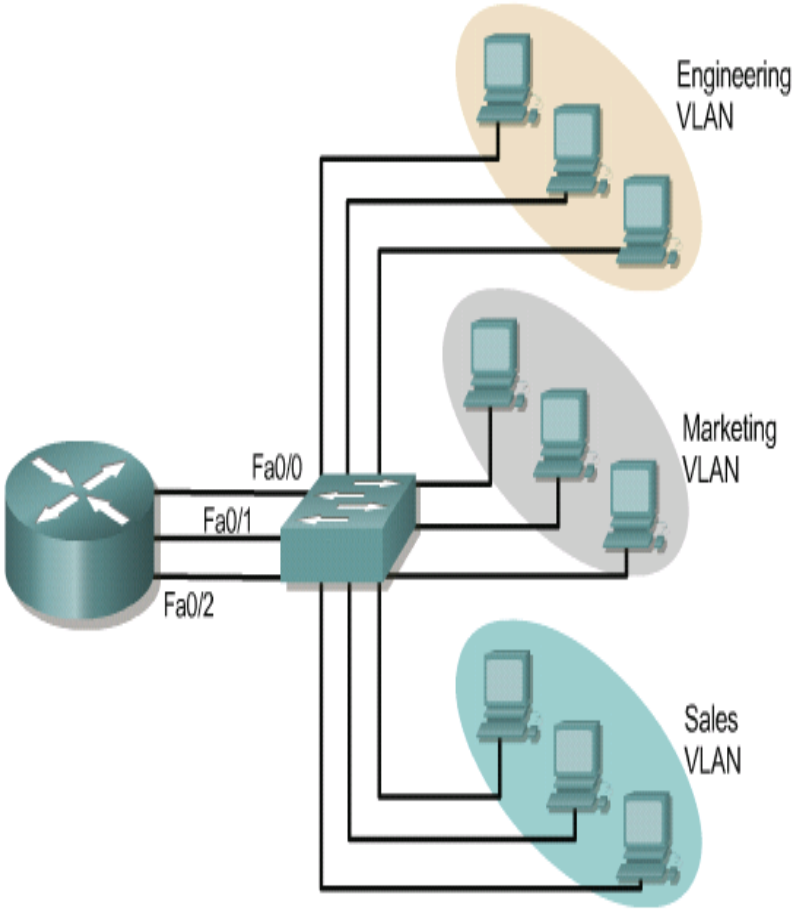
- A VLAN is a broadcast domain created by one or more switches.
- If Workstation 1 on the Engineering VLAN wants to send frames to Workstation 2 on the Sales VLAN, the frames are sent to the Fa0/0 MAC address of the router. Routing occurs through the IP address on the Fa0/0 router interface for the Engineering VLAN.
- If Workstation 1 on the Engineering VLAN wants to send a frame to Workstation 2 on the same VLAN, the destination MAC address of the frame is the MAC address for Workstation 2.
- Implementing VLANs on a switch causes the following to occur:
  - The switch maintains a separate bridging table for each VLAN.
  - If the frame comes in on a port in VLAN 1, the switch searches the bridging table for VLAN 1.
  - When the frame is received, the switch adds the source address to the bridging table if it is currently unknown.
  - The destination is checked so a forwarding decision can be made.
  - For learning and forwarding the search is made against the address table for that VLAN only.

Broadcast Domains with VLANs and Routers

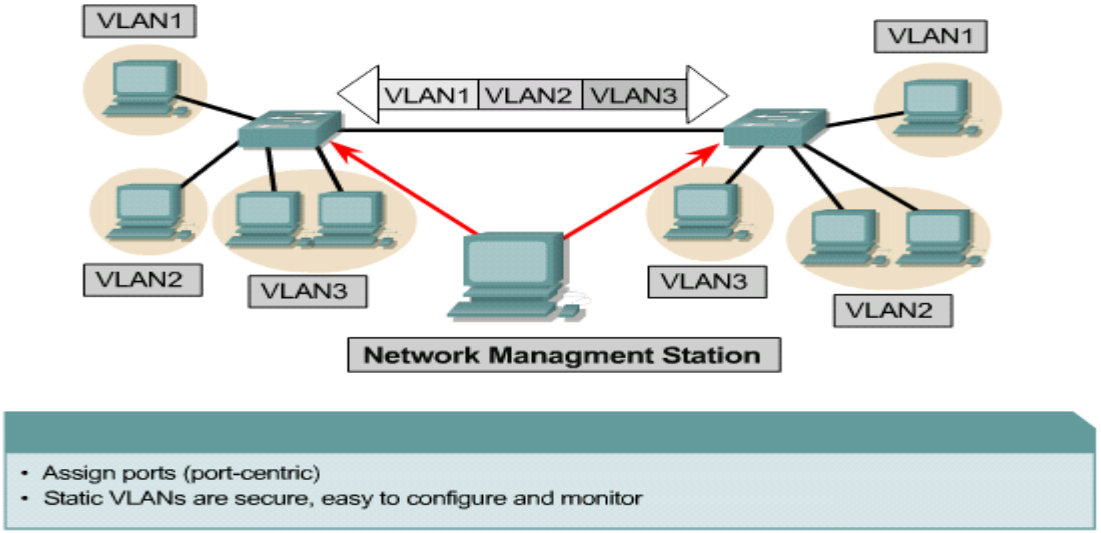


Three switches and one router could be used without VLANs:

- Switch for Engineering
- Switch for Sales
- Switch for Marketing
- Each switch treats all ports as members of one broadcast domain
- Router is used to route packets among the three broadcast domains



Static VLANs



- **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 on Cisco switches is always VLAN 1 and may not be deleted."
- All other ports on the switch may be reassigned to alternate VLANs.

Types of VLANs

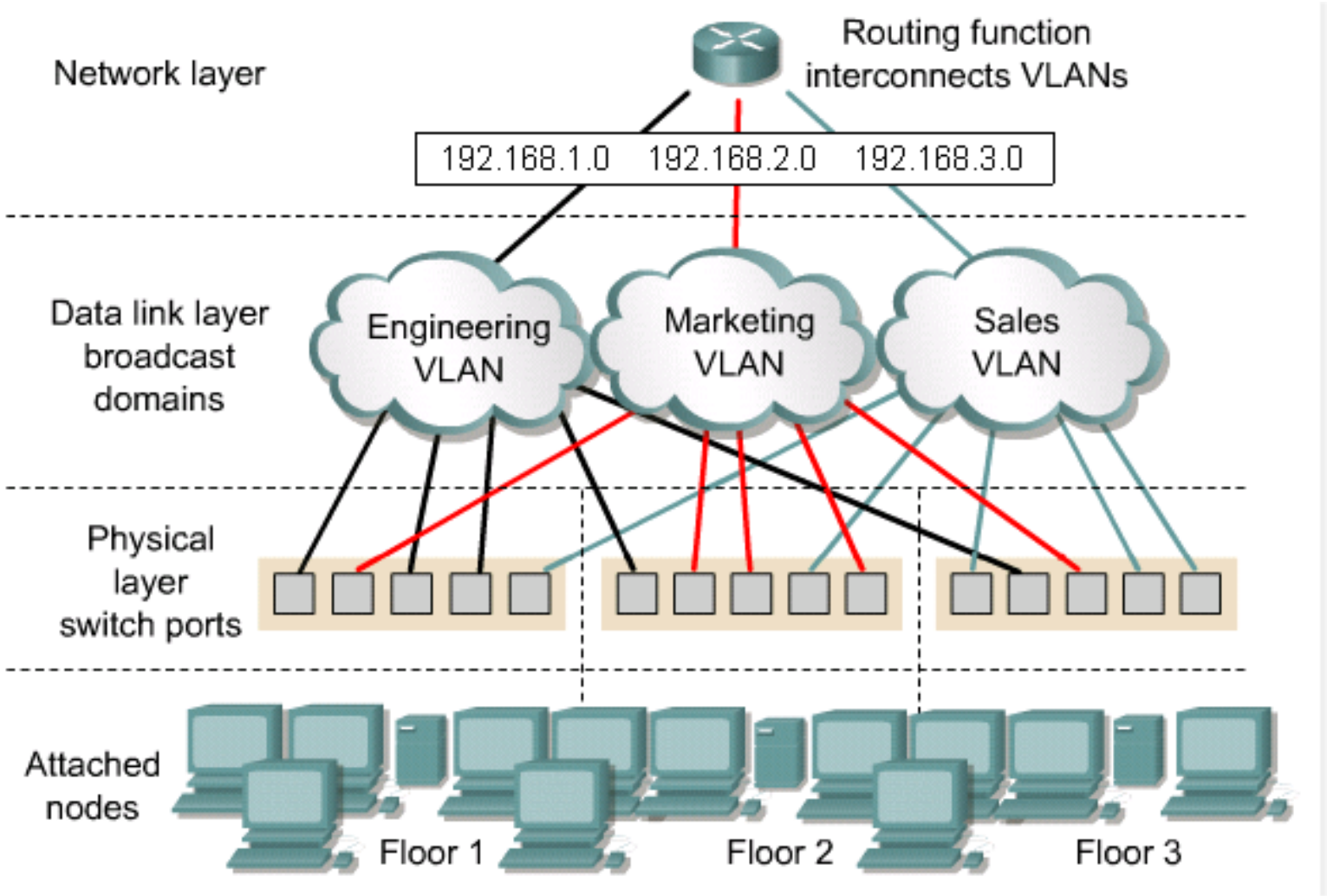
VLAN 1

```
Switch# show vlan brief

VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------
1    default              active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                    Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                    Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                    Gi0/1,  Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
```

- All ports assigned to VLAN 1 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.

VLAN Operation



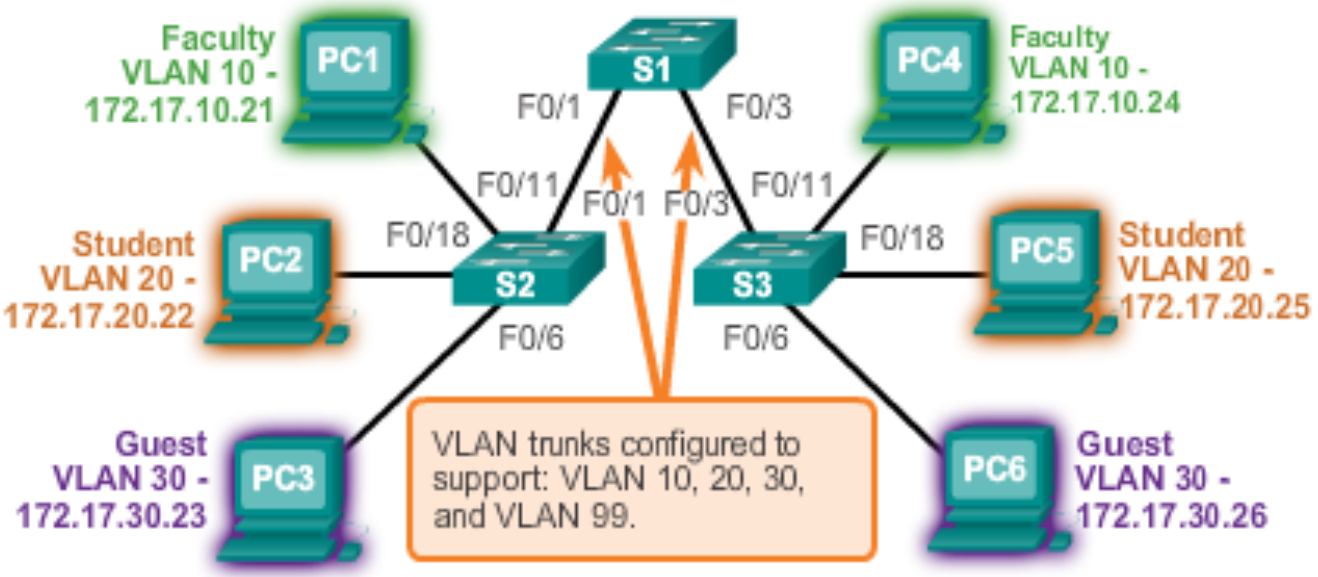
VLAN Trunks

- A VLAN trunk carries more than one VLAN.
- A VLAN trunk is usually established between switches so same-VLAN devices can communicate, even if physically connected to different switches.
- A VLAN trunk is not associated to any VLANs; neither is the trunk ports used to establish the trunk link.
- Cisco IOS supports IEEE802.1q, a popular VLAN trunk protocol.

VLAN Trunks (cont.)

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.



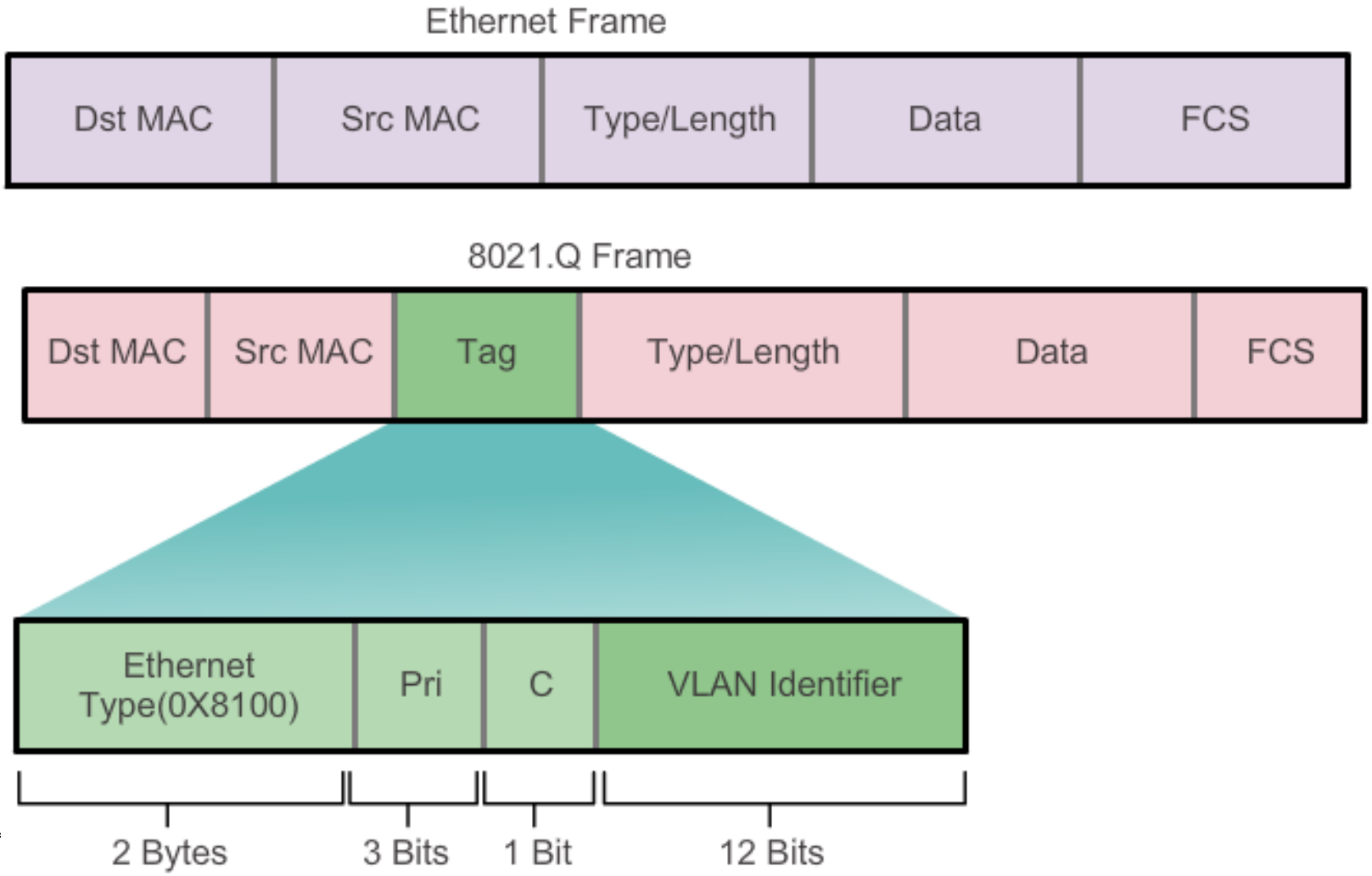
Controlling Broadcast Domains with VLANs

- VLANs can be used to limit the reach of broadcast frames.
- A VLAN is a broadcast domain of its own.
- A broadcast frame sent by a device in a specific VLAN is forwarded within that VLAN only.
- VLANs help control the reach of broadcast frames and their impact in the network.
- Unicast and multicast frames are forwarded within the originating VLAN.

Tagging Ethernet Frames for VLAN Identification

- Frame tagging is the process of adding a VLAN identification header to the frame.
- It is used to properly transmit multiple VLAN frames through a trunk link.
- Switches tag frames to identify the VLAN to that they belong. Different tagging protocols exist; IEEE 802.1Q is a vey popular example.
- The protocol defines the structure of the tagging header added to the frame.
- Switches add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through nontrunk ports.
- When properly tagged, the frames can transverse any number of switches via trunk links and still be forwarded within the correct VLAN at the destination.

Tagging Ethernet Frames for VLAN Identification



Benefits of VLANs

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.
- Shrink Broadcast Domains
- Improve security.

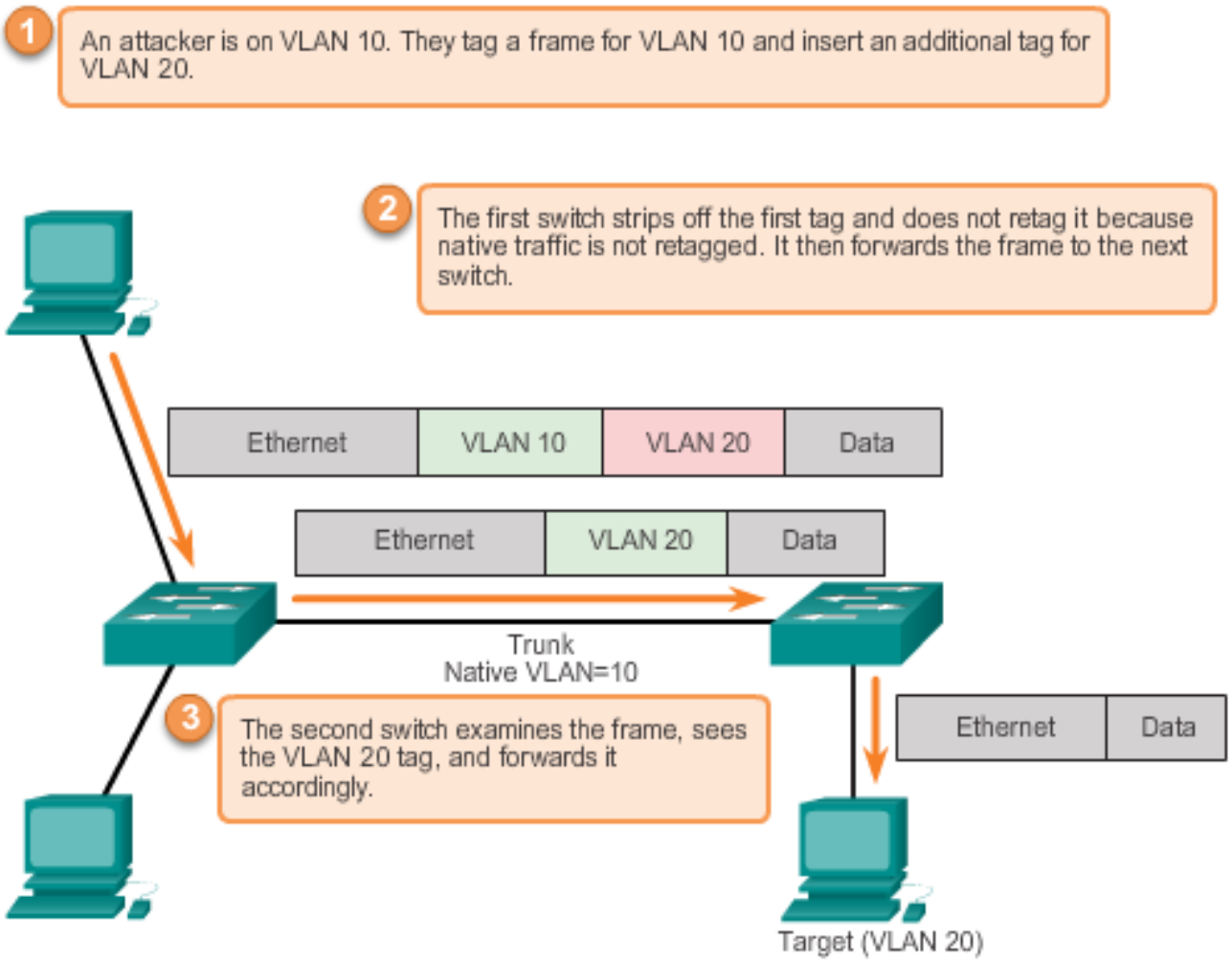
Switch Spoofing Attack

- There are a number of different types of VLAN attacks in modern switched networks; VLAN hopping is one example.
- The default configuration of the switch port is dynamic auto.
- By configuring a host to act as a switch and form a trunk, an attacker could gain access to any VLAN in the network.
- Because the attacker is now able to access other VLANs, this is called a VLAN hopping attack.
- To prevent a basic switch spoofing attack, turn off trunking on all ports, except the ones that specifically require trunking.

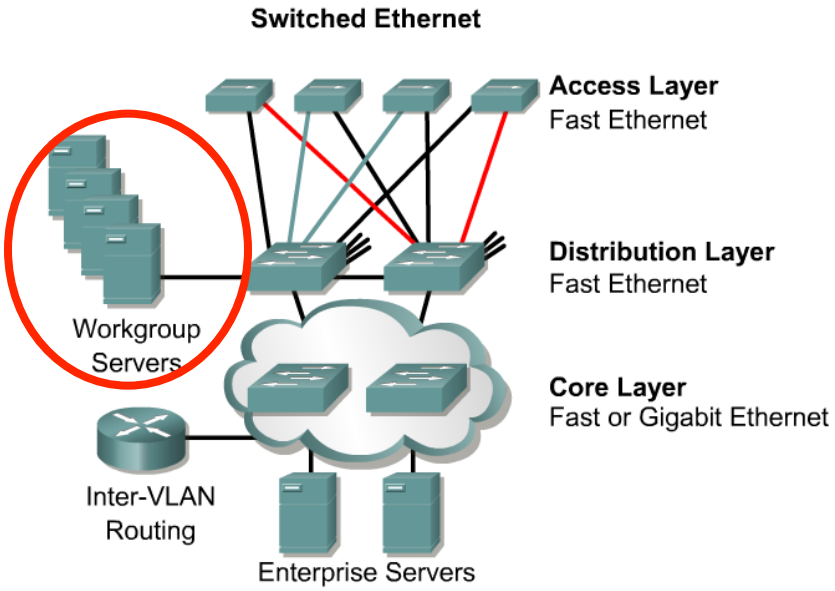
Double-Tagging Attack

- Double-tagging attack takes advantage of the way that hardware on most switches de-encapsulate 802.1Q tags.
- Most switches perform only one level of 802.1Q de-encapsulation, allowing an attacker to embed a second, unauthorized attack header in the frame.
- After removing the first and legit 802.1Q header, the switch forwards the frame to the VLAN specified in the unauthorized 802.1Q header.
- The best approach to mitigating double-tagging attacks is to ensure that the native VLAN of the trunk ports is different from the VLAN of any user ports.

Double-Tagging Attack (cont.)



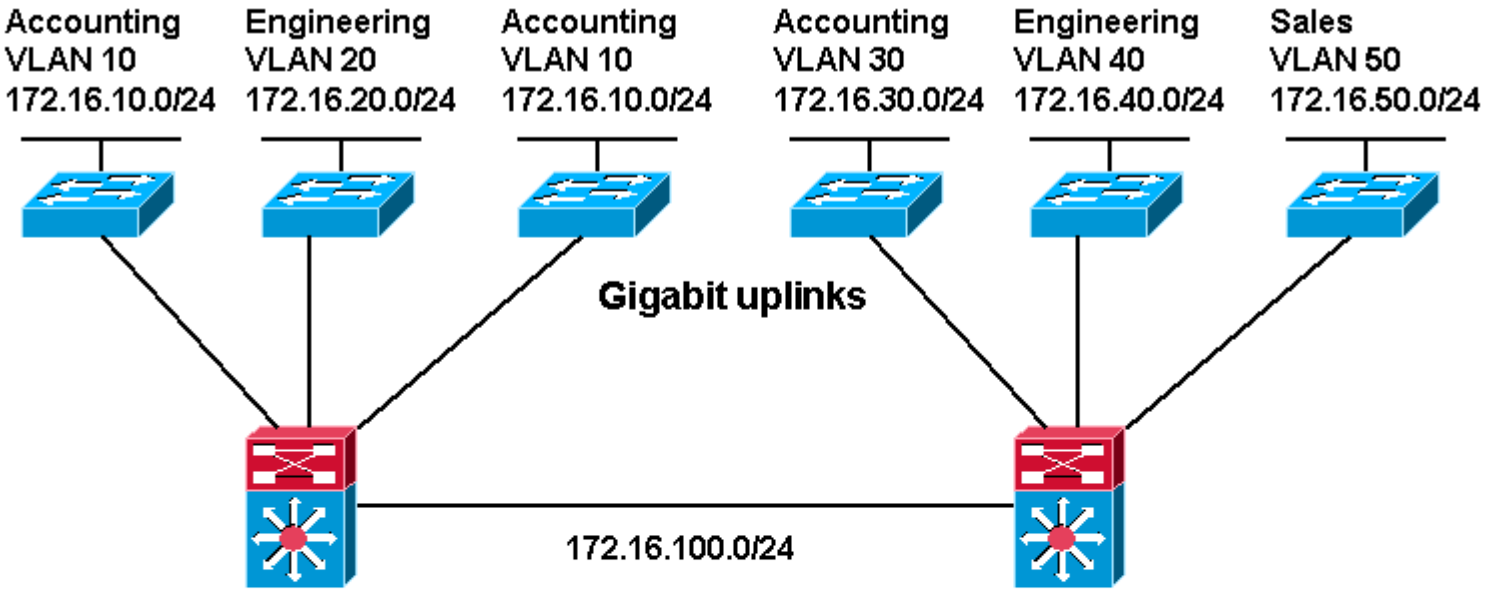
Geographic or Local VLANs



- 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

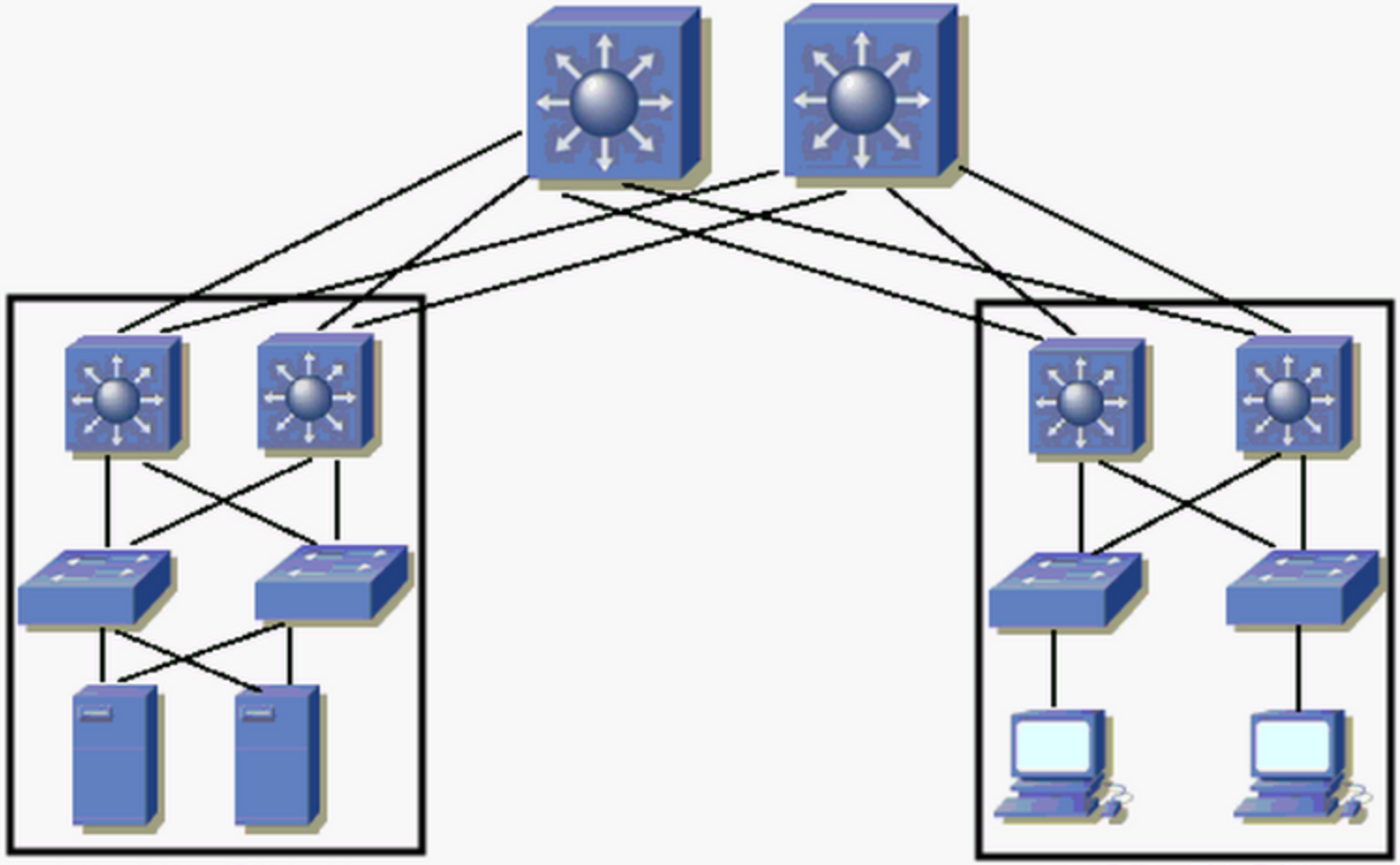
This model is the recommended method.



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

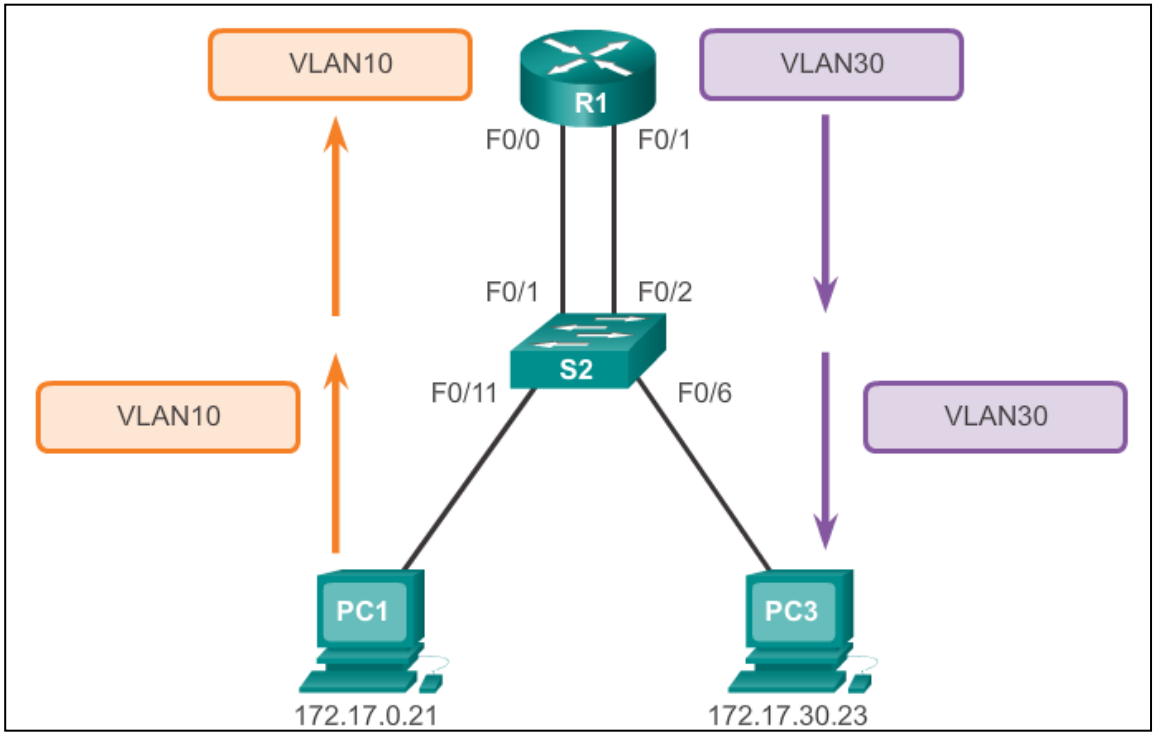
An Ideal Design: Local VLANs



- LOCAL VLANS DO NOT EXTEND BEYOND THE DISTRIBUTION
- LOCAL VLAN TRAFFIC ROUTED TO OTHER DESTINATIONS

What is Inter-VLAN routing?

- Layer 2 switches cannot forward traffic between VLANs without the assistance of a router.
- Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another, using a router.



Legacy Inter-VLAN Routing

In the past:

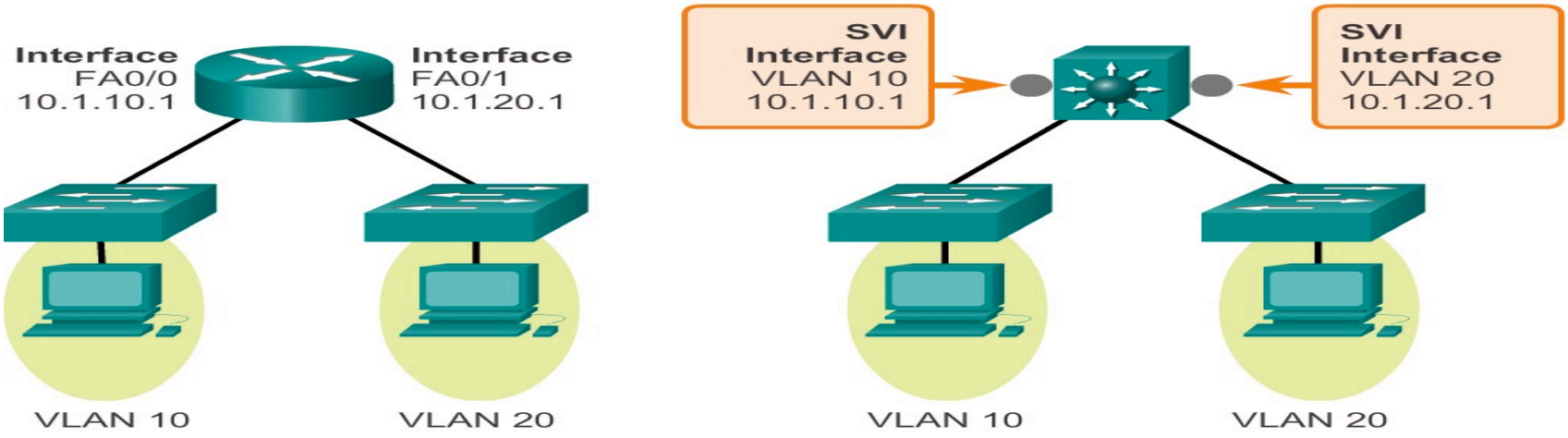
- Actual routers were used to route between VLANs.
- Each VLAN was connected to a different physical router interface.
- Packets would arrive on the router through one through interface, be routed and leave through another.
- Because the router interfaces were connected to VLANs and had IP addresses from that specific VLAN, routing between VLANs was achieved.
- Large networks with large number of VLANs required many router interfaces.

Router-on-a-Stick Inter-VLAN Routing

- The router-on-a-stick approach uses a different path to route between VLANs.
- One of the router's physical interfaces is configured as a 802.1Q trunk port so it can understand VLAN tags.
- Logical subinterfaces are created; one subinterface per VLAN.
- Each subinterface is configured with an IP address from the VLAN it represents.
- VLAN members (hosts) are configured to use the subinterface address as a default gateway.
- Only one of the router's physical interface is used.

Switch Virtual Interface (SVI)

- An SVI is a virtual interface that is configured within a multilayer switch. An SVI can be created for any VLAN that exists on the switch. An SVI is considered to be virtual because there is no physical port dedicated to the interface. It can perform the same functions for the VLAN as a router interface would, and can be configured in much the same way as a router interface (i.e., IP address, inbound/outbound ACLs, etc.). The SVI for the VLAN provides Layer 3 processing for packets to or from all switch ports associated with that VLAN.



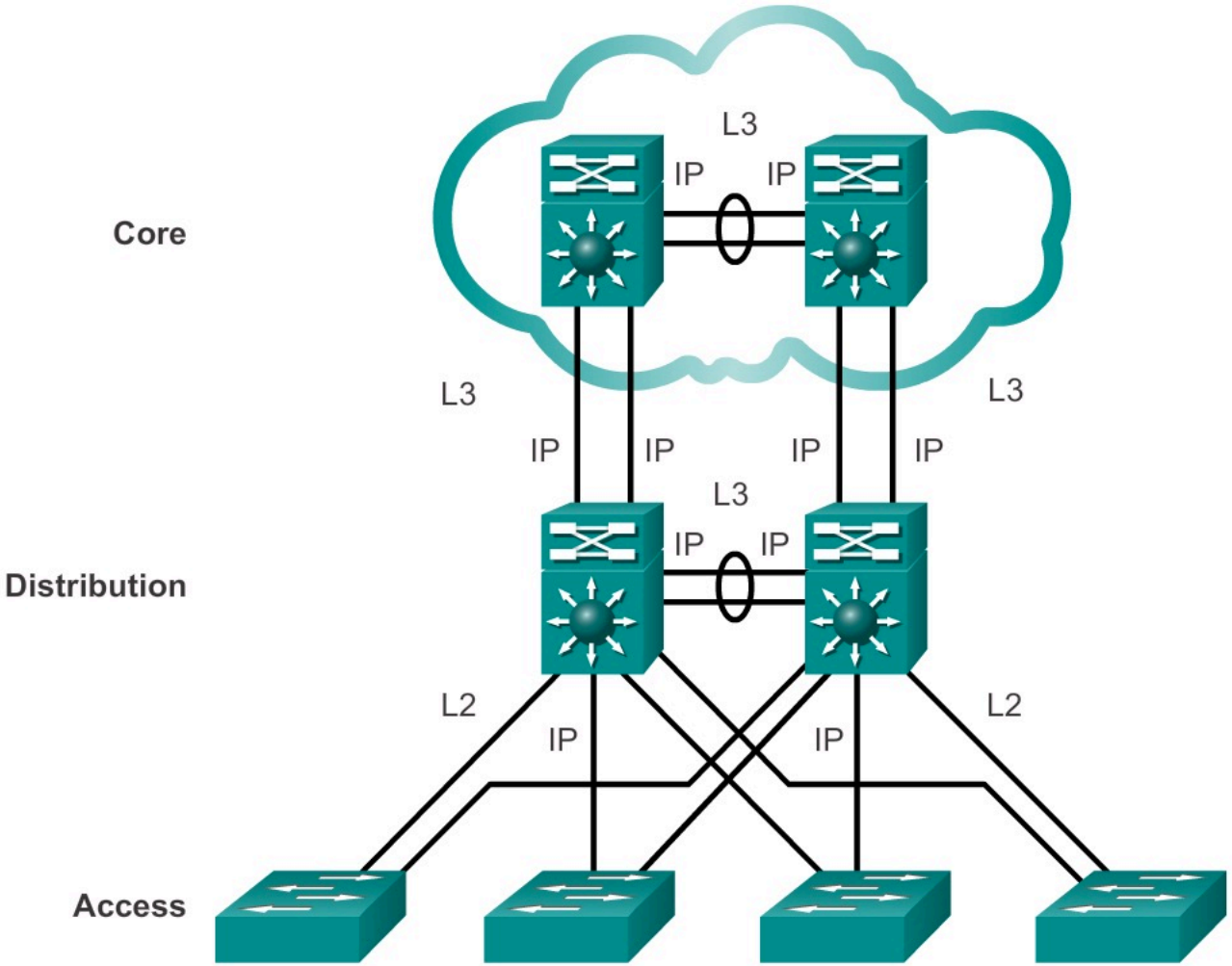
Multilayer Switch Inter-VLAN Routing

- Multilayer switches can perform Layer 2 and Layer 3 functions, replacing the need for dedicated routers.
- Multilayer switches support dynamic routing and inter-VLAN routing.
- The multilayer switch must have IP routing enabled.
- A switch virtual interface (SVI) exists for VLAN 1 by default. On a multilayer switch, a logical (layer 3) interface can be configured for any VLAN.
- The switch understands network-layer PDUs; therefore, can route between its SVIs, just as a router routes between its interfaces.
- With a multilayer switch, traffic is routed internal to the switch device.
- This routing process is a suitable and scalable solution.

Inter-VLAN Routing with Switch Virtual Interfaces

- Today's routing has become faster and cheaper and can be performed at hardware speed.
- Routing can be transferred to core and distribution devices with little to no impact on network performance.
- Many users are in separate VLANs, and each VLAN is usually a separate subnet. This implies that each distribution switch must have IP addresses matching each access switch VLAN.
- A routed port is a physical port that acts similarly to an interface on a router. Unlike an access port, a routed port is not associated with a particular VLAN.
- Layer 3 (routed) ports are normally implemented between the distribution and the core layer. This model is less dependent on spanning tree, because there are no loops in the Layer 2 portion of the topology.

Switched Network Design



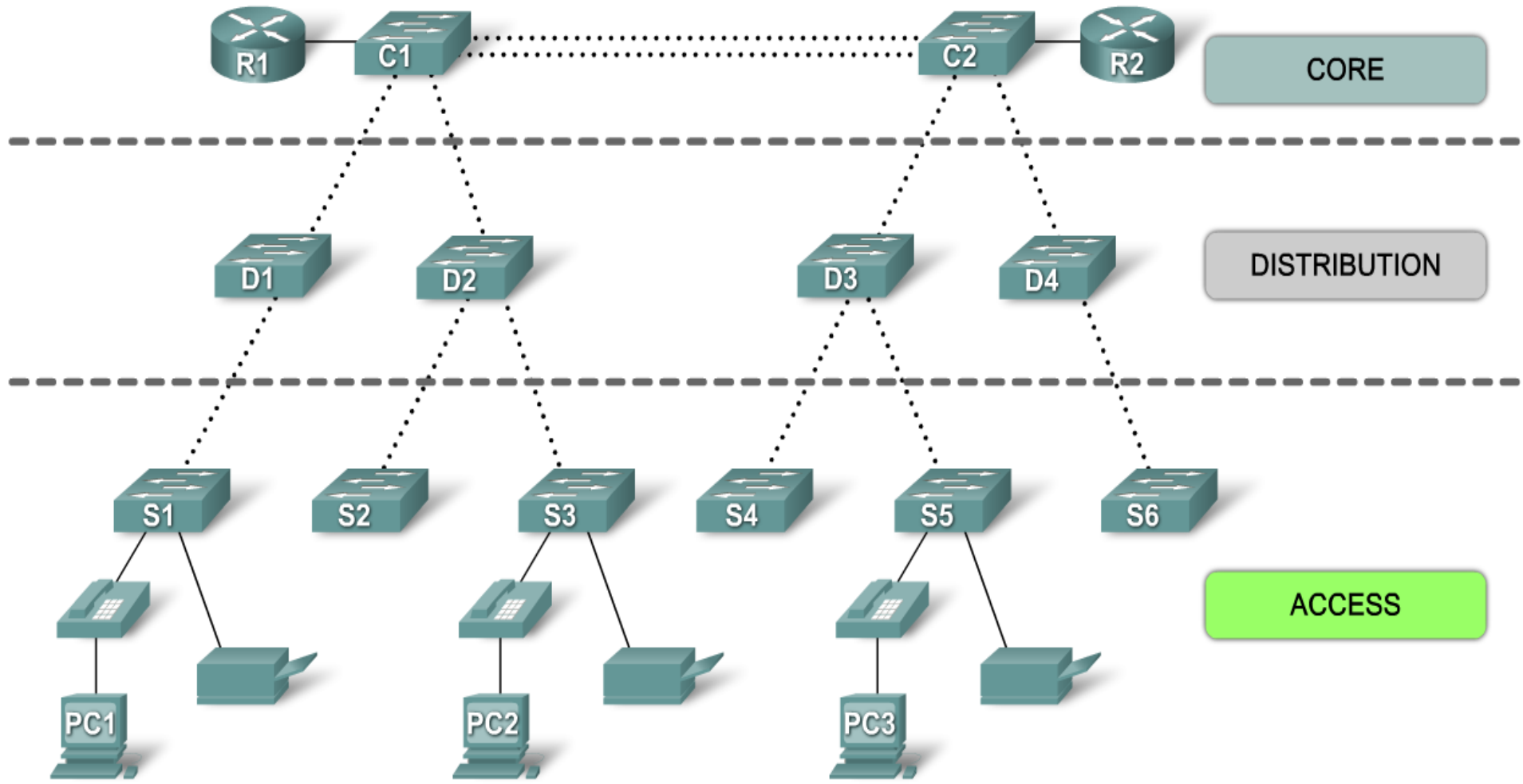
Inter-VLAN Routing with SVIs (Cont.)

- By default, an SVI is created for the default VLAN (VLAN 1). This allows for remote switch administration.
- Any additional SVIs must be created by the administrator.
- SVIs are created the first time the VLAN interface configuration mode is entered for a particular VLAN SVI.
- Enter the **`interface vlan 10`** command to create an SVI named VLAN 10.
- The VLAN number used corresponds to the VLAN tag associated with data frames on an 802.1Q encapsulated trunk.
- When the SVI is created, ensure that the specific VLAN is present in the VLAN database.

Inter-VLAN Routing with SVIs

- SVIs advantages include:
  - Much faster than router-on-a-stick, because everything is hardware-switched and routed.
  - No need for external links from the switch to the router for routing.
  - Not limited to one link. Layer 2 EtherChannels can be used between the switches to get more bandwidth.
  - Latency is much lower, because it does not need to leave the switch.

The Hierarchical Network Model



Benefits of a Hierarchical Network

Scalability

- Hierarchical networks can be expanded easily

Redundancy

- Redundancy at the core and distribution level ensure path availability

Performance

- Link aggregation between levels and high-performance core and distribution level switches allow for near wire-speed throughout the network

Security

- Port security at the access level and policies at the distribution level make the network more secure

Manageability

- Consistency between switches at each level makes management more simple

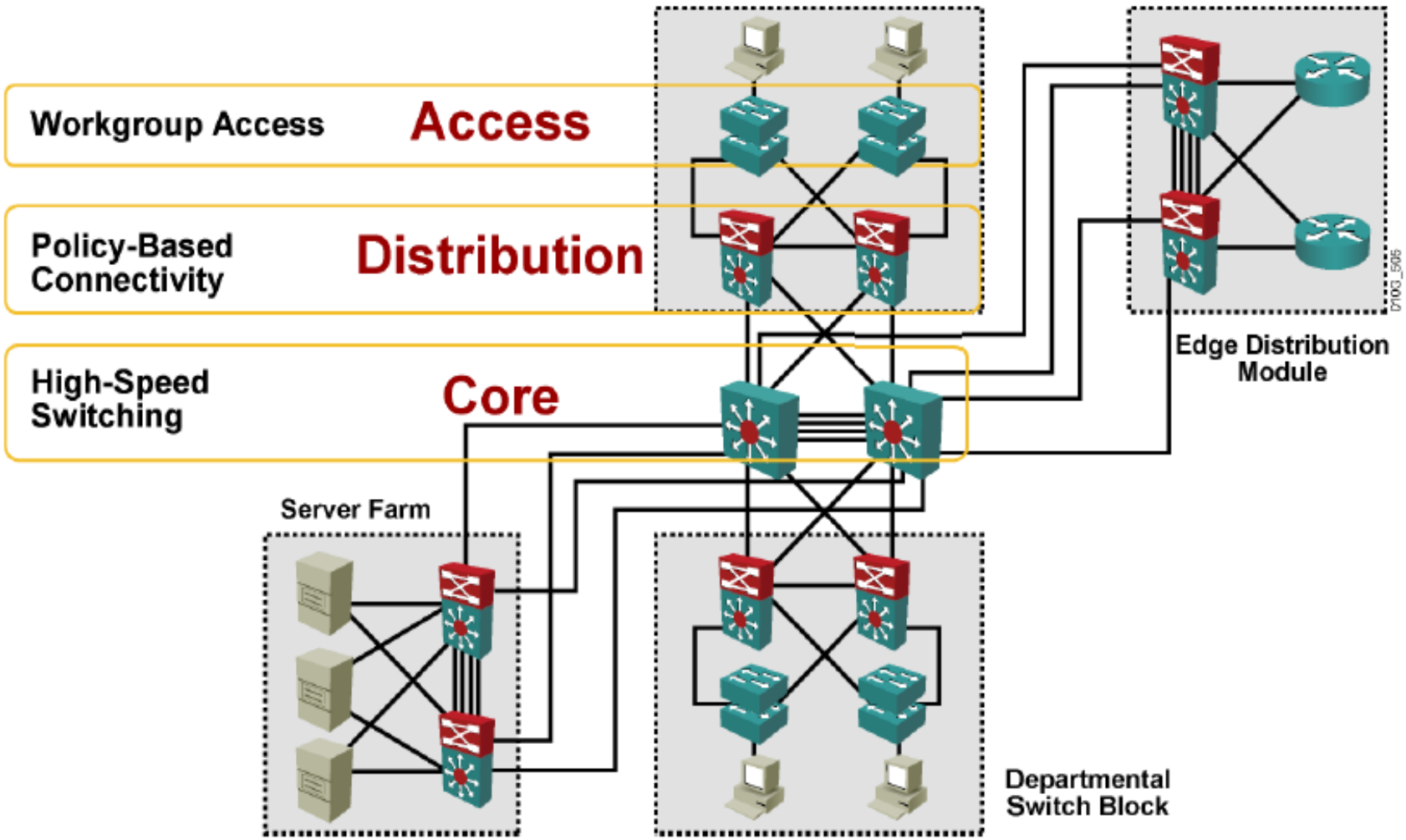
Maintainability

- The modularity of hierarchical design allows for the network to scale without becoming overly complicated

Hierarchical Network Design

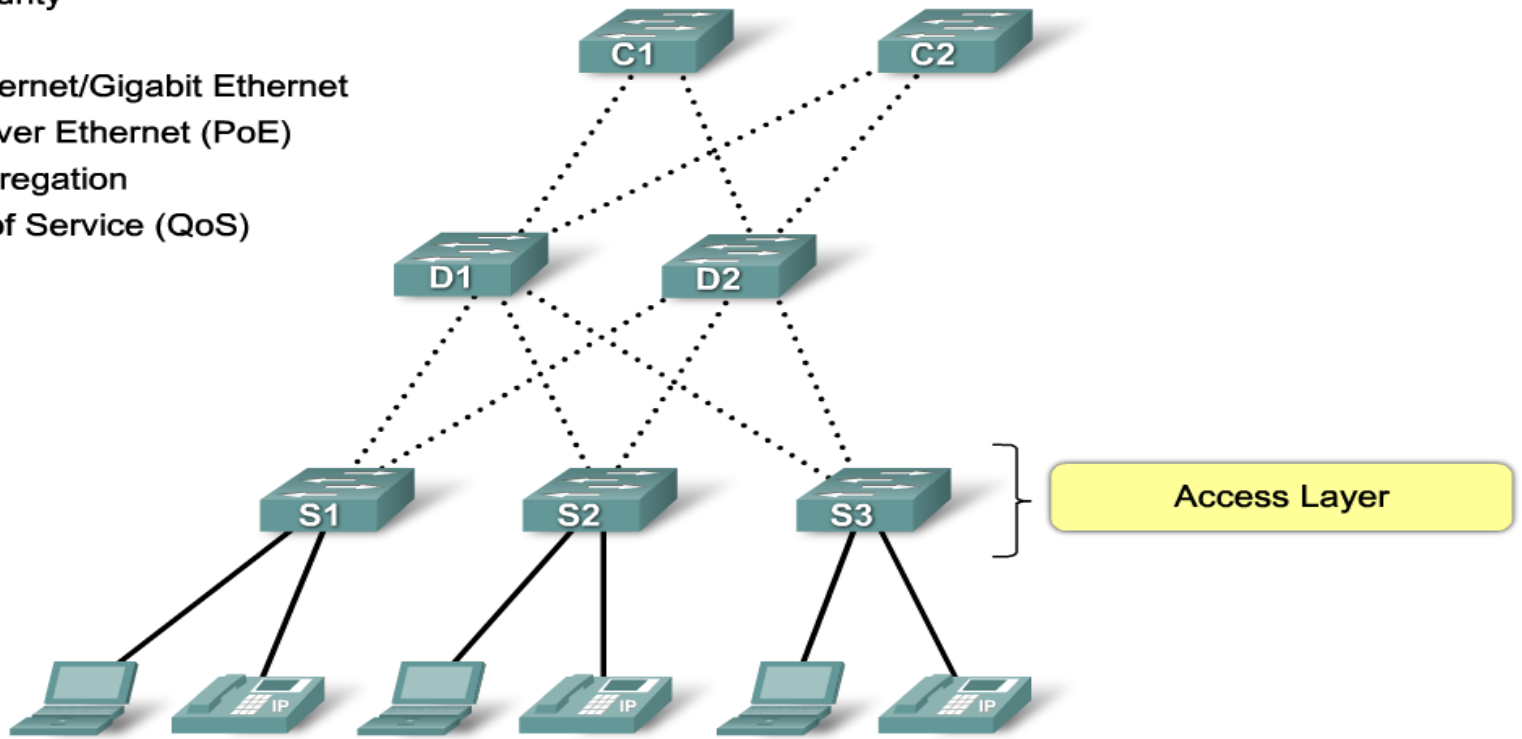
- The main purpose of the access layer is to provide a means of connecting devices to the network and controlling which devices are allowed to communicate on the network.
- The access layer interfaces with end devices, such as PCs, printers, and IP phones, to provide access to the rest of the network. The access layer can include routers, switches, bridges, hubs, and wireless access points (AP).
- The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. The distribution layer controls the flow of network traffic using policies and delineates broadcast domains by performing routing functions between virtual LANs (VLANs) defined at the access layer.
- The core layer of the hierarchical design is the high-speed backbone of the internetwork. The core layer is critical for interconnectivity between distribution layer devices, so it is important for the core to be highly available and redundant. The core area can also connect to Internet resources. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly.

Network Design - Hierarchical Campus Model



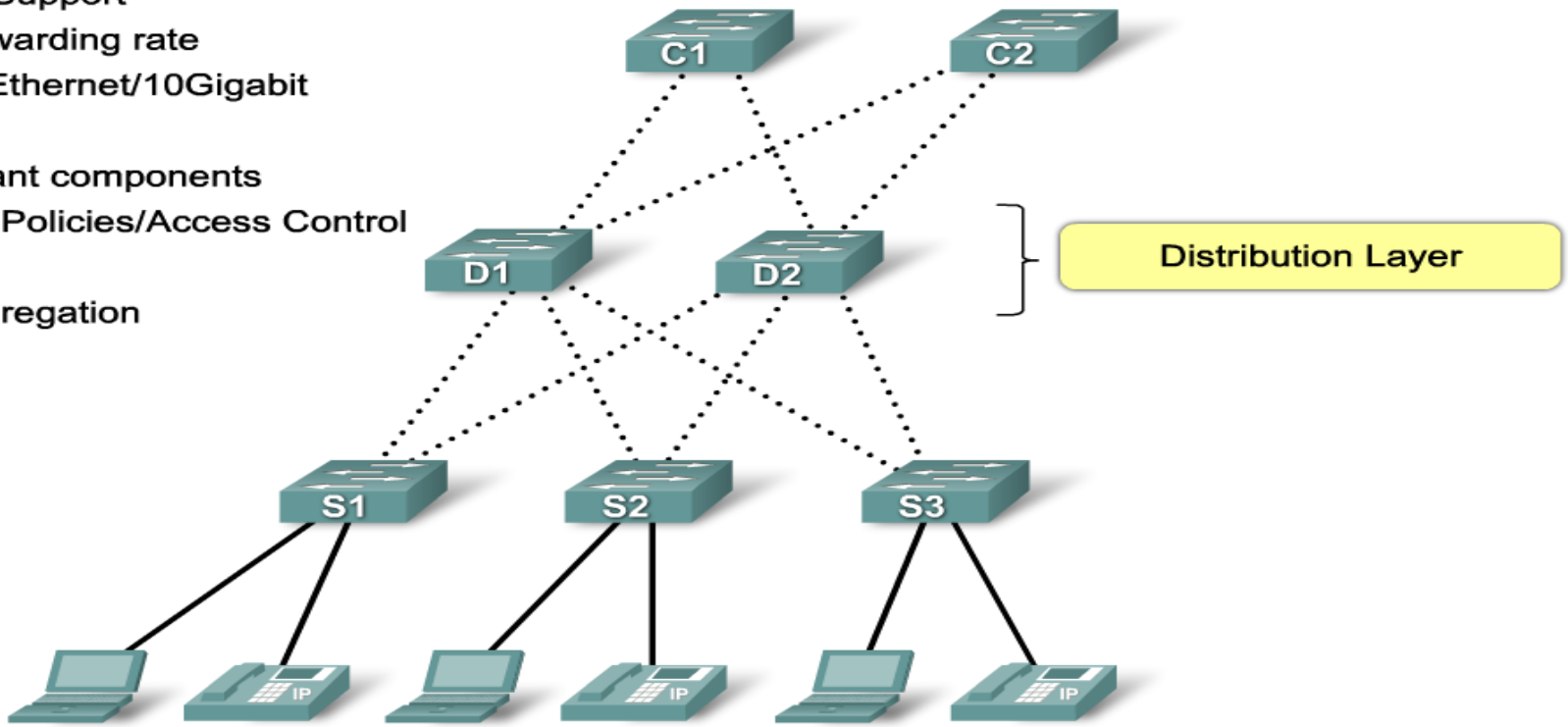
Access Layer Switch Features

- Port security
- VLANs
- Fast Ethernet/Gigabit Ethernet
- Power over Ethernet (PoE)
- Link aggregation
- Quality of Service (QoS)



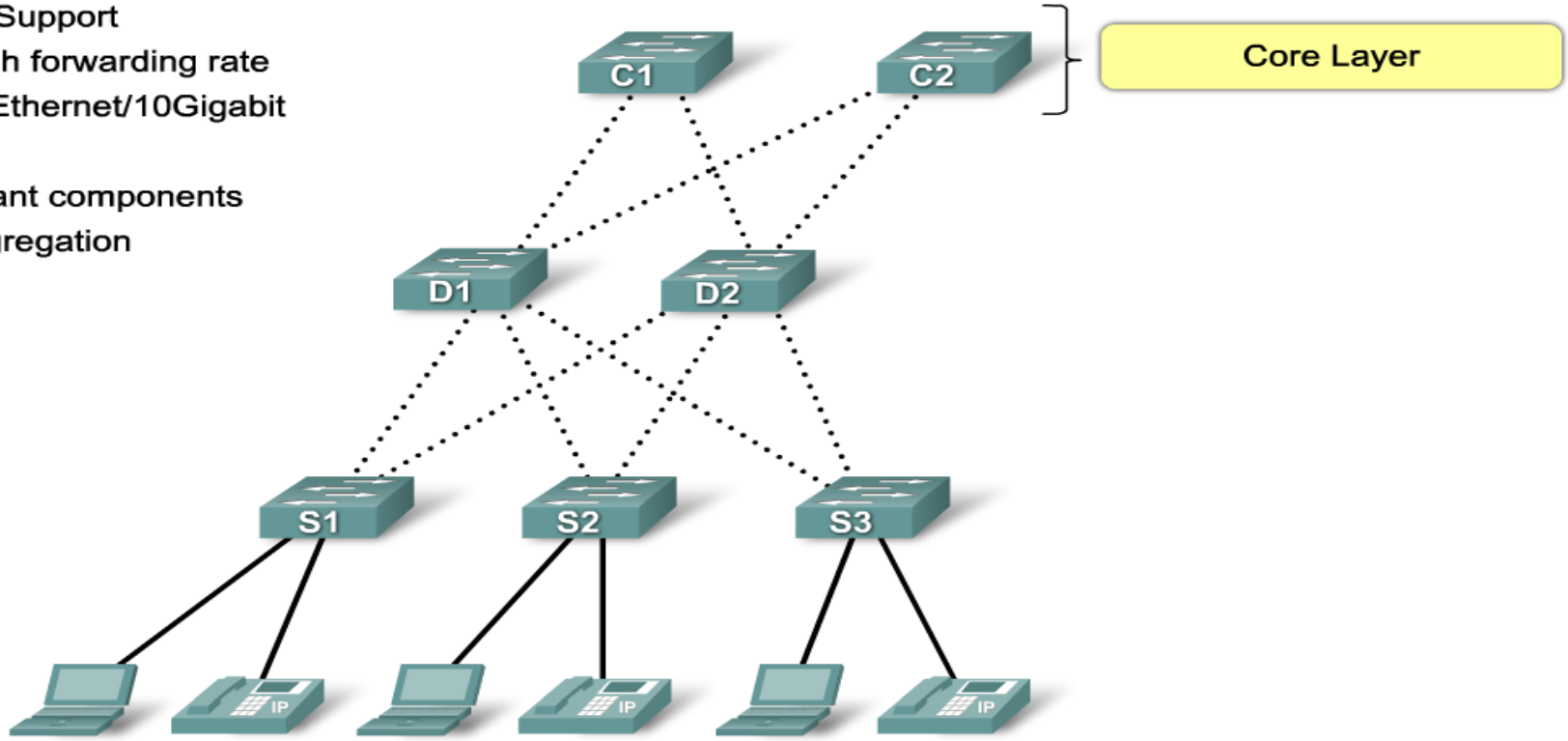
Distribution Layer Switch Features

- Layer 3 Support
- High forwarding rate
- Gigabit Ethernet/10Gigabit Ethernet
- Redundant components
- Security Policies/Access Control Lists
- Link Aggregation
- QOS



Core Layer Switch Features

- Layer 3 Support
- Very High forwarding rate
- Gigabit Ethernet/10Gigabit Ethernet
- Redundant components
- Link Aggregation
- QoS



References

- LAN Switching
  http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook#Bridging_and_Switching
- VLANs -
  http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/xcfvl.html
- Hierarchical Network Design
  http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_--_Internetworking_Design_Basics#Internetworking_Design_Basics