Virtual LANs

VLAN introduction

- 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

- Broadcast traffic in LANs is sent to all devices on LAN

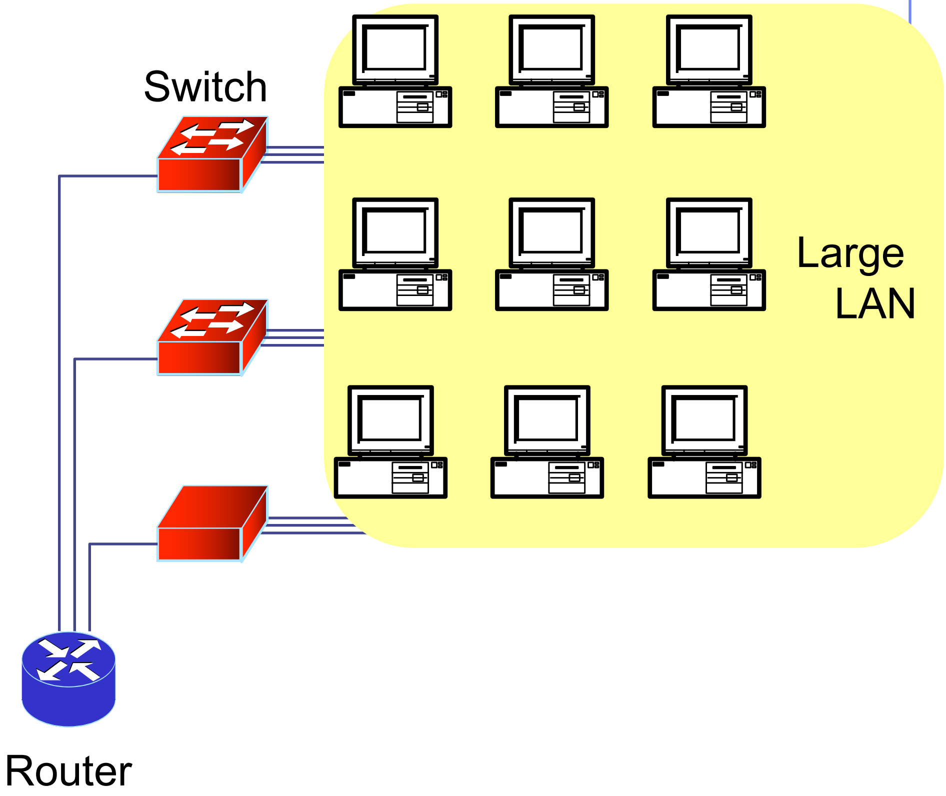
  → becomes a problem in large LANs

Traditional solution:

- Interconnect LANs by IP routers
- However, LAN membership of host is tied to local switch

Better solution: VLANs

- VLANs separate broadcast domain from location of hosts
- Used to partition large LANs
- Interconnected by IP routers
- Can run separate spanning tree in each VLAN



VLAN Introduction

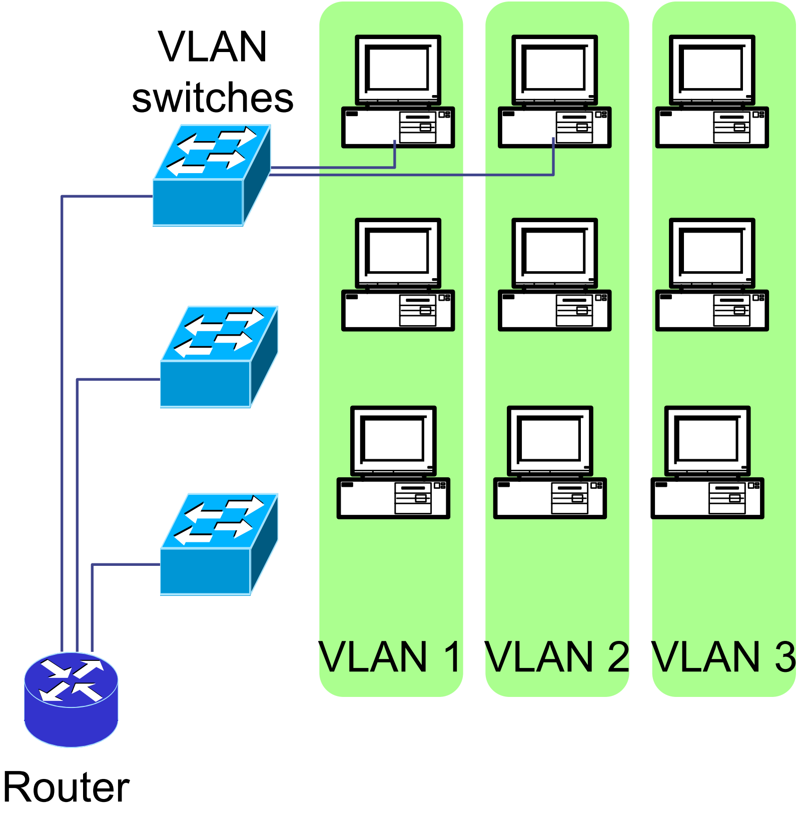
- Broadcast traffic in LANs is sent to all devices on LAN
  → becomes a problem in large LANs

Traditional solution:

- Interconnect LANs by IP routers
- However, LAN membership of host is tied to local switch

Better solution: VLANs

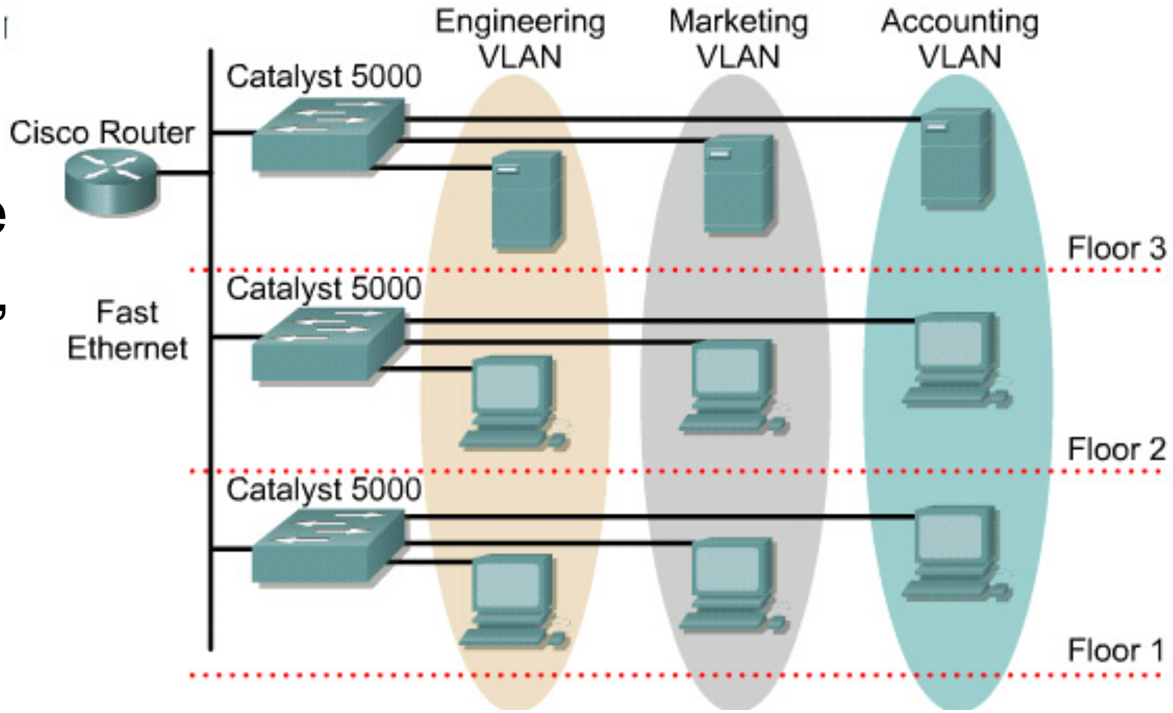
- VLANs separate broadcast domain from location of hosts
- Used to partition large LANs
- Interconnected by IP routers
- Can run separate spanning tree in each VLAN



VLAN introduction

- 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.

- Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.

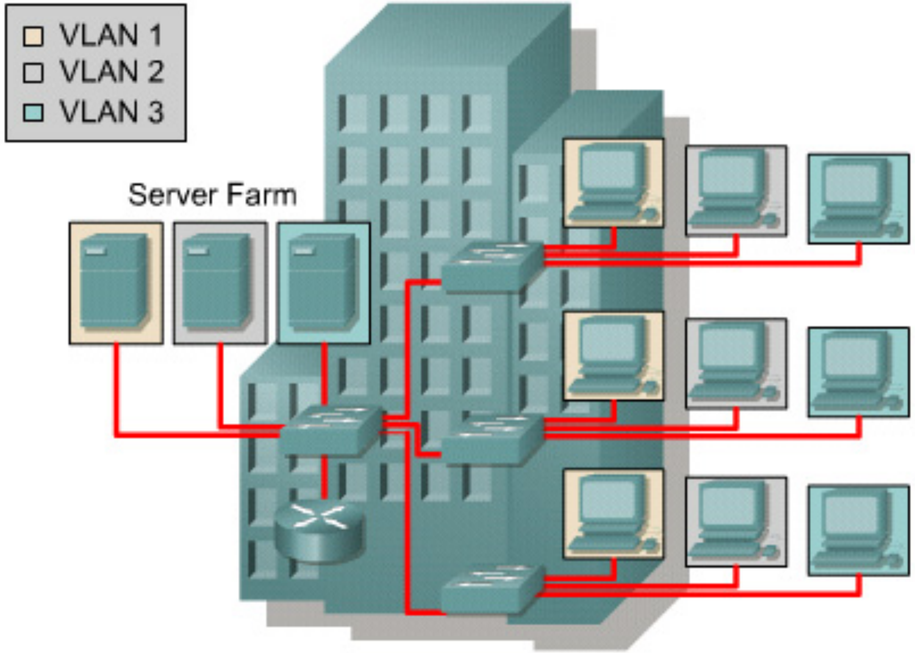


VLAN introduction

- VLANs address scalability, security, and network 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

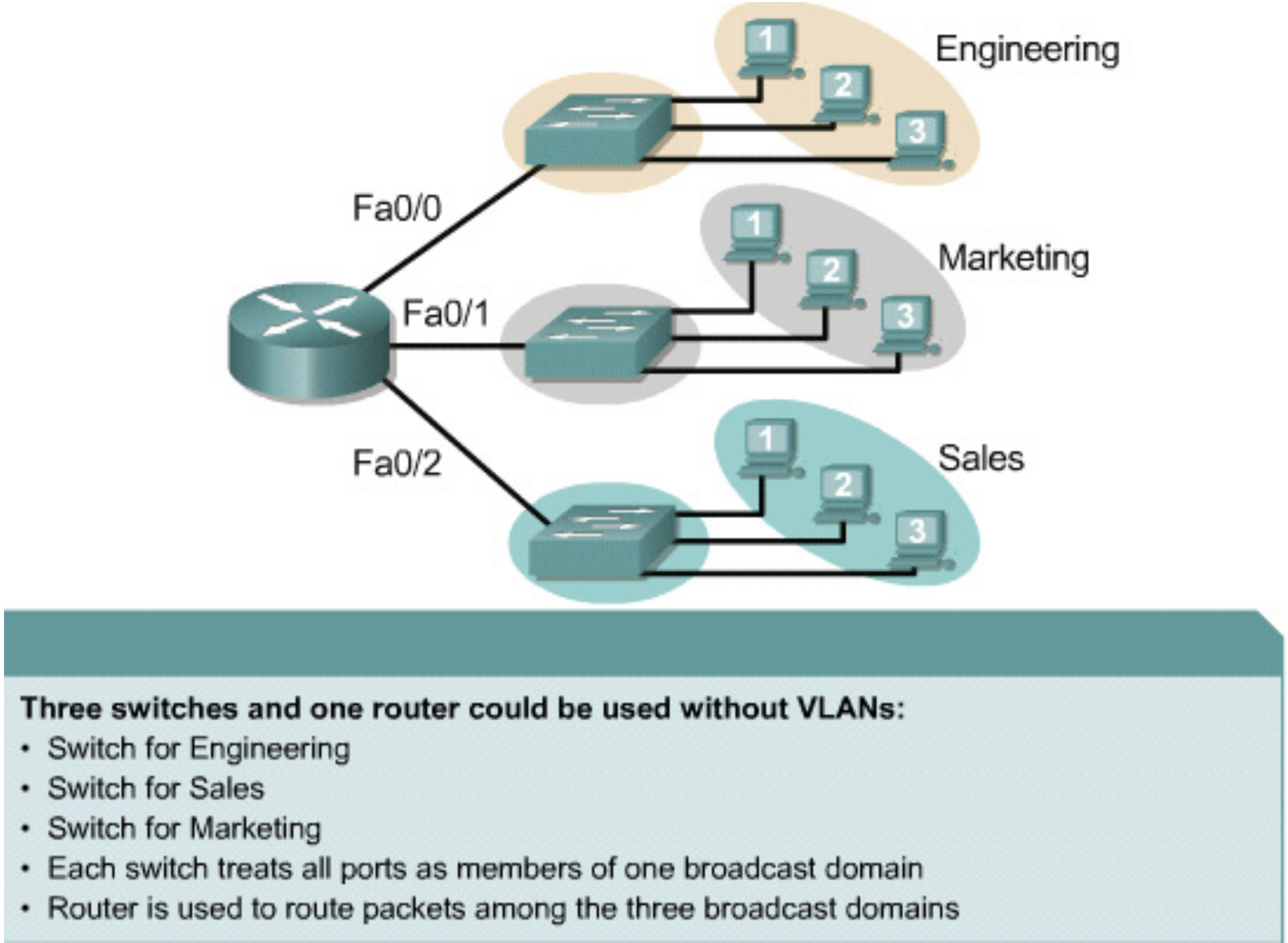
- A VLAN is a broadcast domain created by one or more switches.



- A switch creates a broadcast domain
- VLANs help manage broadcast domains
- VLANs can be defined on port groups, users, or protocols
- LAN switches and network management software provide a mechanism to create VLANs

Broadcast domains with VLANs and routers

- Layer 3 routing allows the router to send packets to the three different broadcast domains.



Three switches and one router could be used without VLANs:

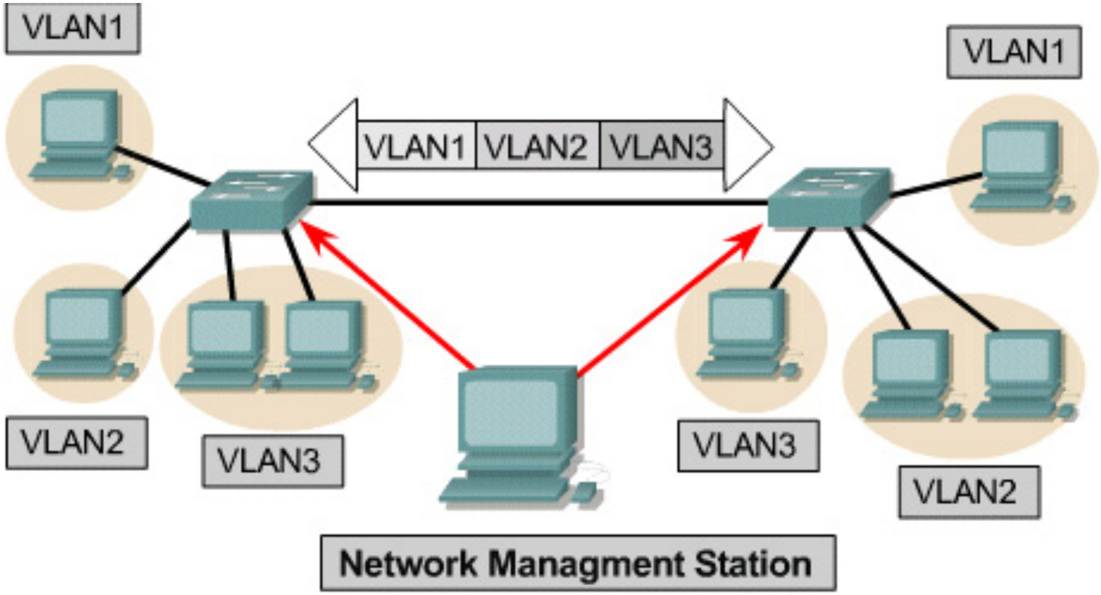
- Switch for Engineering
- Switch for Sales
- Switch for Marketing
- Each switch treats all ports as members of one broadcast domain
- Router is used to route packets among the three broadcast domains

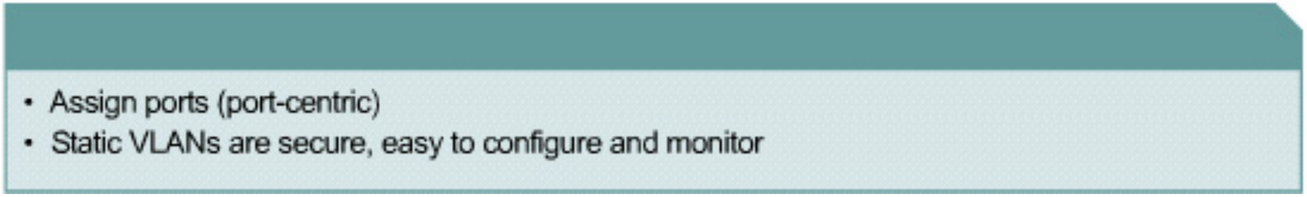
Broadcast domains with VLANs and routers

- 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.

VLAN operation

- Each switch port could 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.





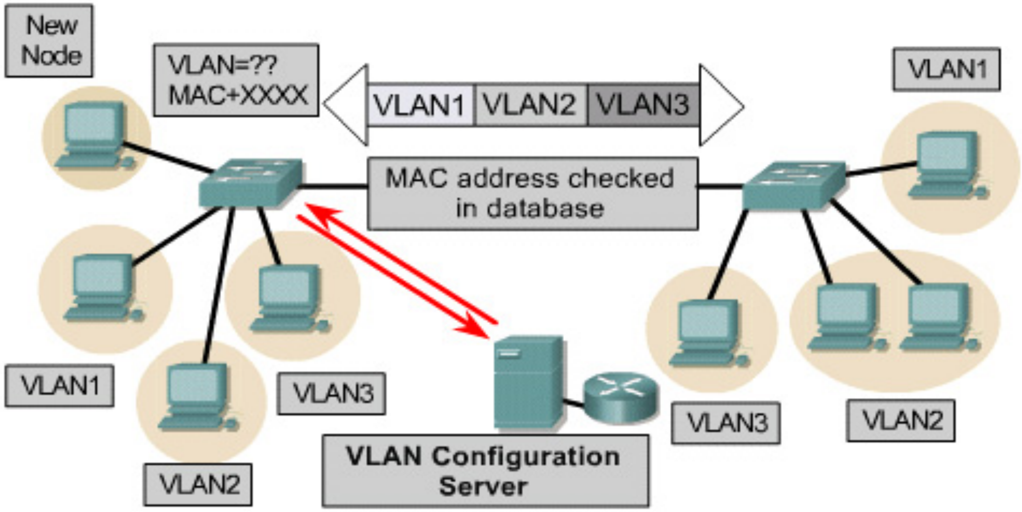
- Assign ports (port-centric)
- Static VLANs are secure, easy to configure and monitor

VLAN operation

- Users attached to the same shared segment, share the bandwidth of that segment.
- Each additional user attached to the shared medium means less bandwidth and deterioration of network performance.
- VLANs offer more bandwidth to users than a shared network.
- 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. All other ports on the switch may be reassigned to alternate VLANs.

VLAN operation

- 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.

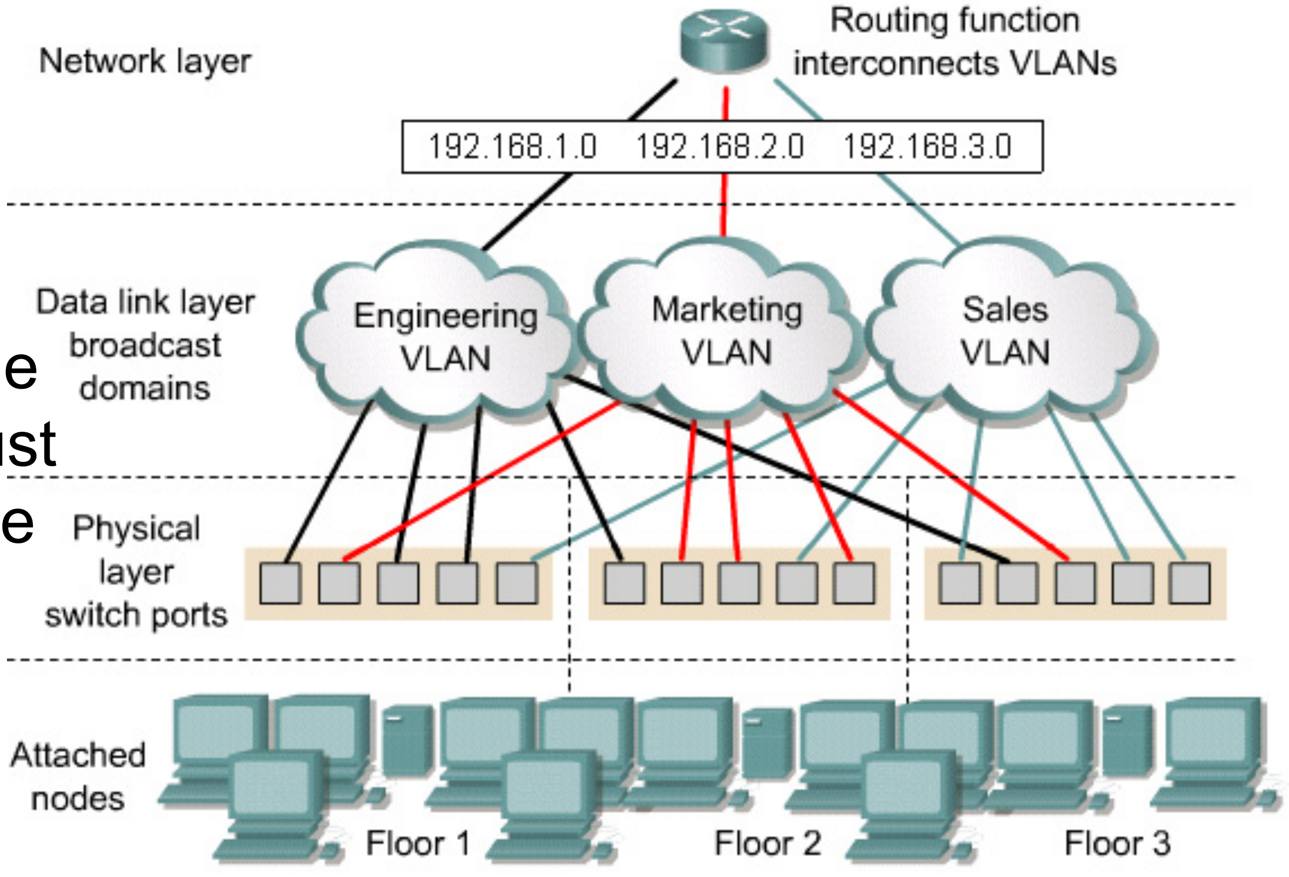


- VLANs assigned using centralized VLAN management application
- VLANs based on MAC address, logical address, or protocol type
- Less administration in wiring closet
- Notification when unrecognized user is added to network

VLAN operation

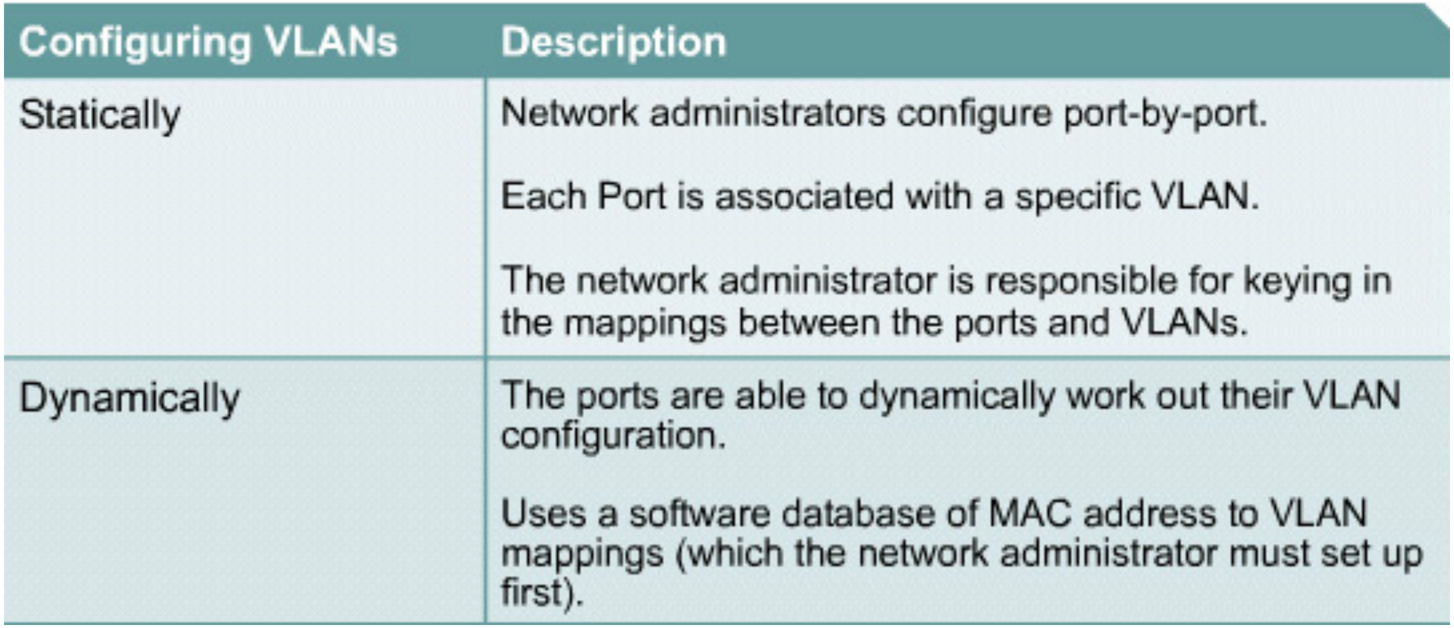
- In port-based or port-centric VLAN membership, the port is assigned to a specific VLAN membership independent of the user or system attached to the port.

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



VLAN operation

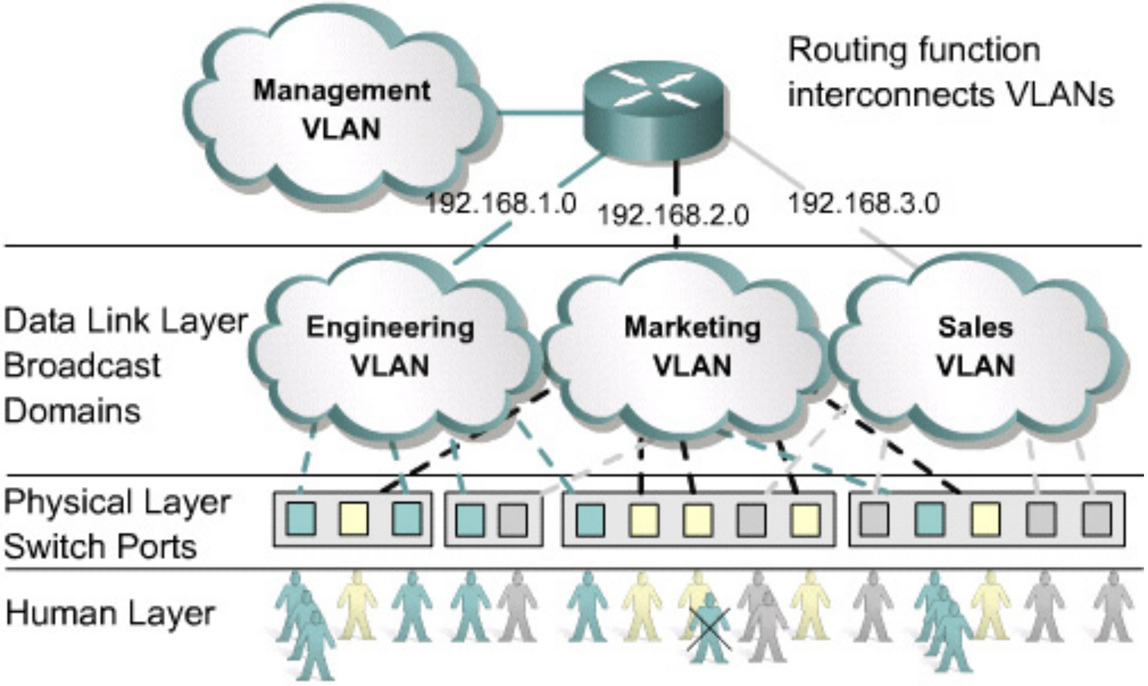
- Network administrators are responsible for configuring VLANs both manually and statically.



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).

Benefits of VLANs

- The key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically.



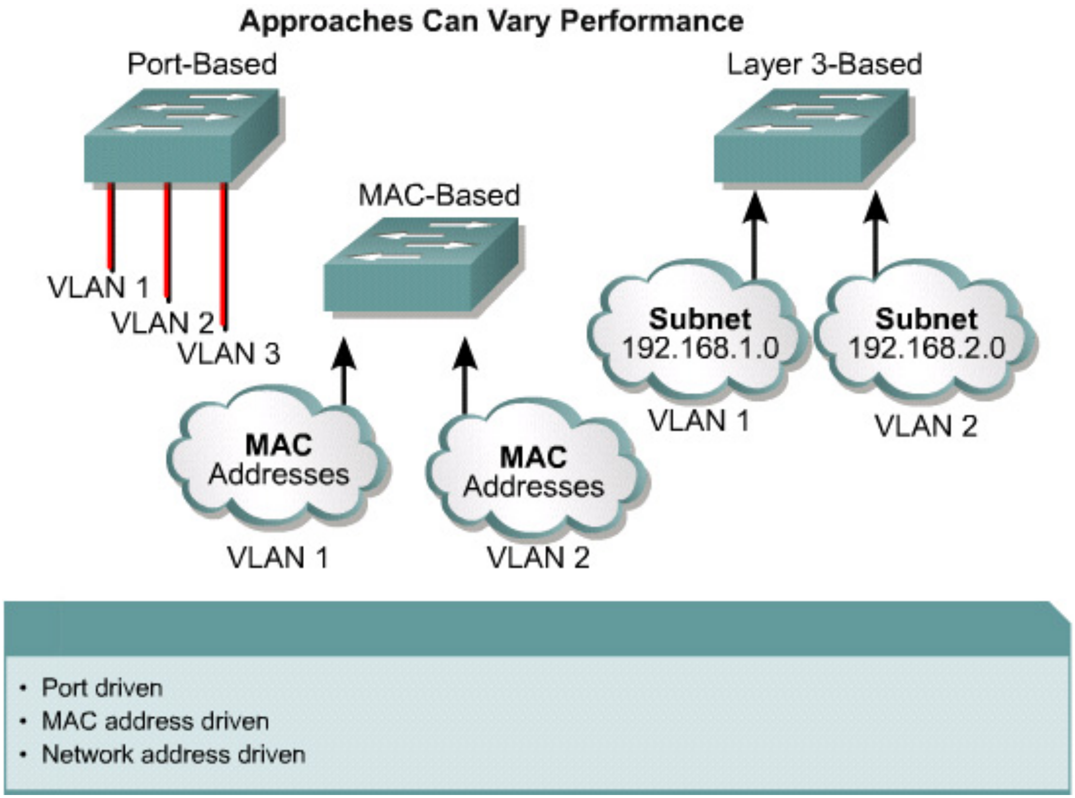
All users attached to the same switch port must be in the same VLAN.

VLAN types

- There are three basic VLAN memberships for determining and controlling how a packet gets assigned: -
  - Port-based VLANs
  - MAC address based
  - Protocol based VLANs
- The frame headers are encapsulated or modified to reflect a VLAN ID before the frame is sent over the link between switches.
- Before forwarding to the destination device, the frame header is changed back to the original format.

VLAN types

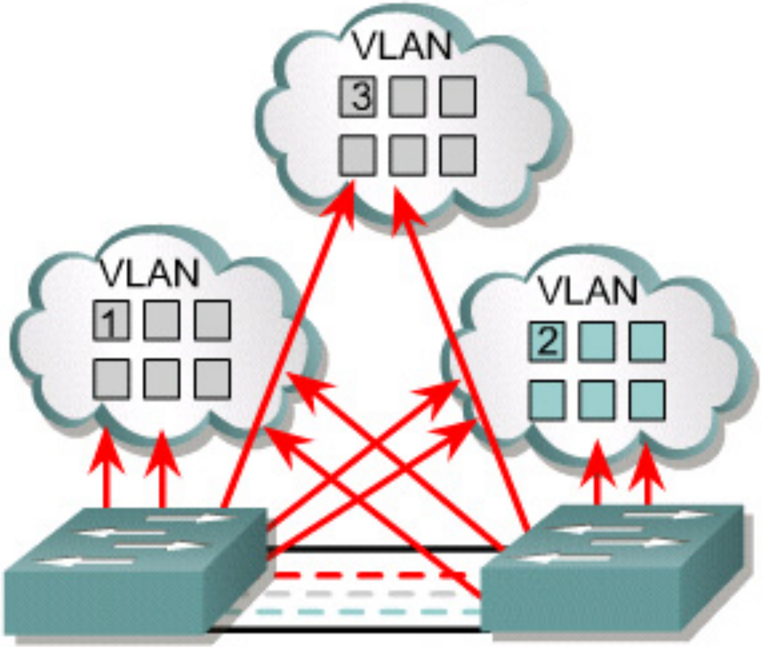
- Port-based VLANs
- MAC address based VLANs
- Protocol based VLANs



- Port driven
- MAC address driven
- Network address driven

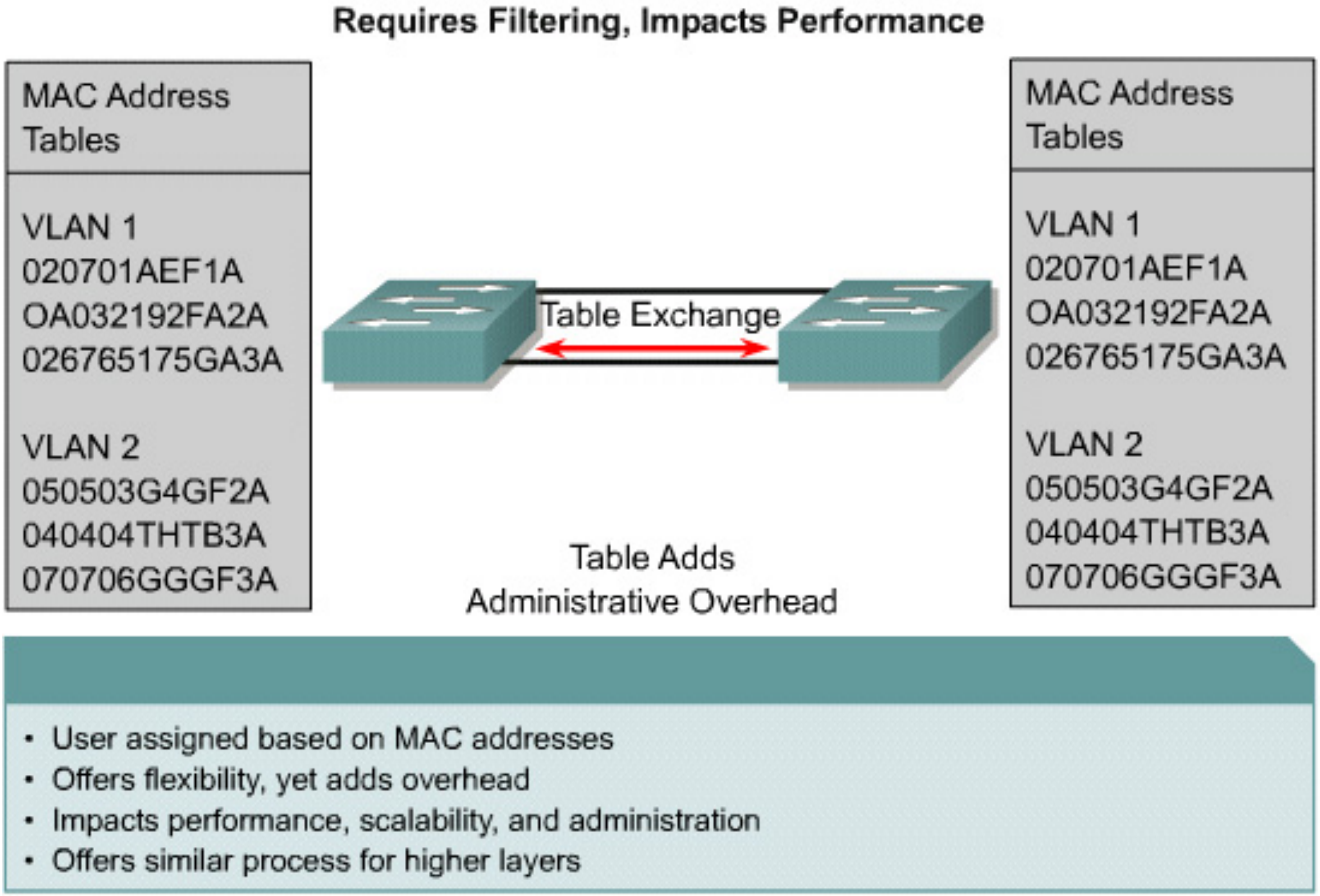
Membership by Port

Maximizes Forwarding Performance



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

Membership by MAC-Addresses



Requires Filtering, Impacts Performance

MAC Address Tables

VLAN 1
020701AEF1A
OA032192FA2A
026765175GA3A

VLAN 2
050503G4GF2A
040404THTB3A
070706GGGF3A

MAC Address Tables

VLAN 1
020701AEF1A
OA032192FA2A
026765175GA3A

VLAN 2
050503G4GF2A
040404THTB3A
070706GGGF3A

Table Adds
Administrative Overhead

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

VLAN types

- The number of VLANs in a switch vary depending on several factors:
  - Traffic patterns
  - Types of applications
  - Network management needs
  - Group commonality

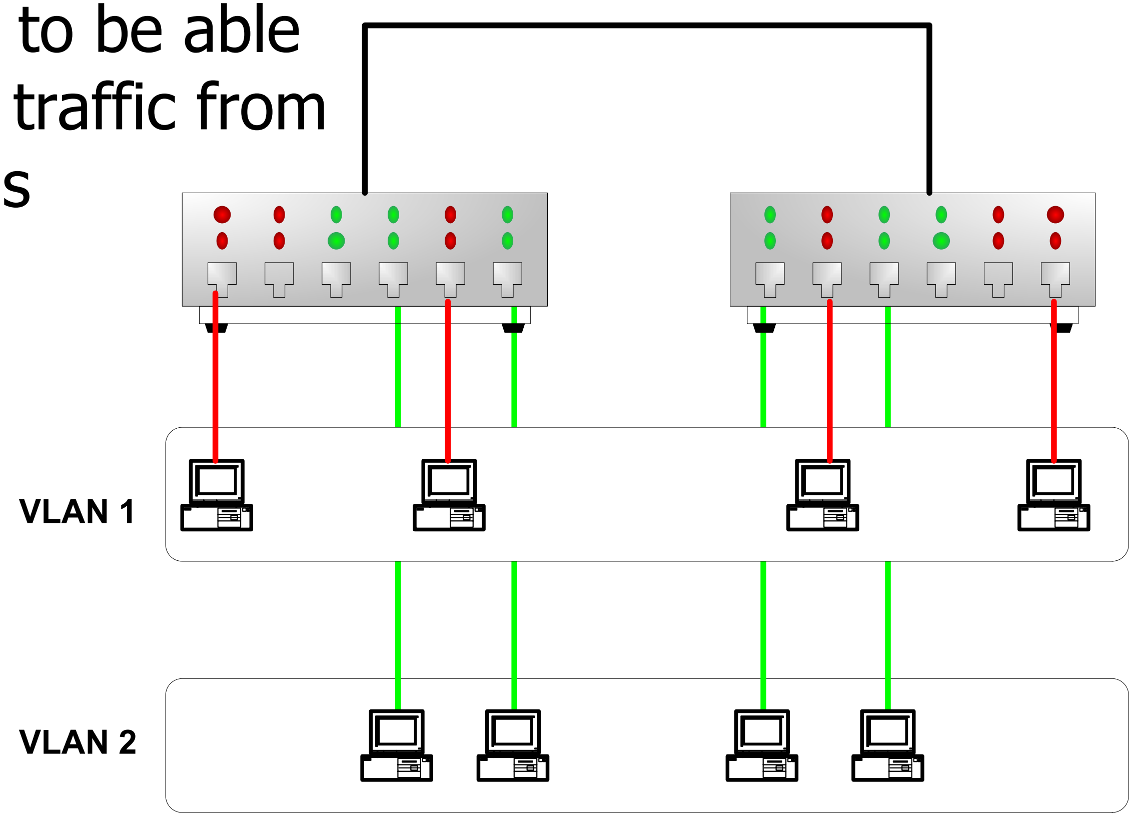
VLAN types

- An important consideration in defining the size of the switch and the number of VLANs is the IP addressing scheme.
- Because a one-to-one correspondence between VLANs and IP subnets is strongly recommended, there can be no more than 254 devices in any one VLAN.
- It is further recommended that VLANs should not extend outside of the Layer 2 domain of the distribution switch.

VLANs across multiple switches

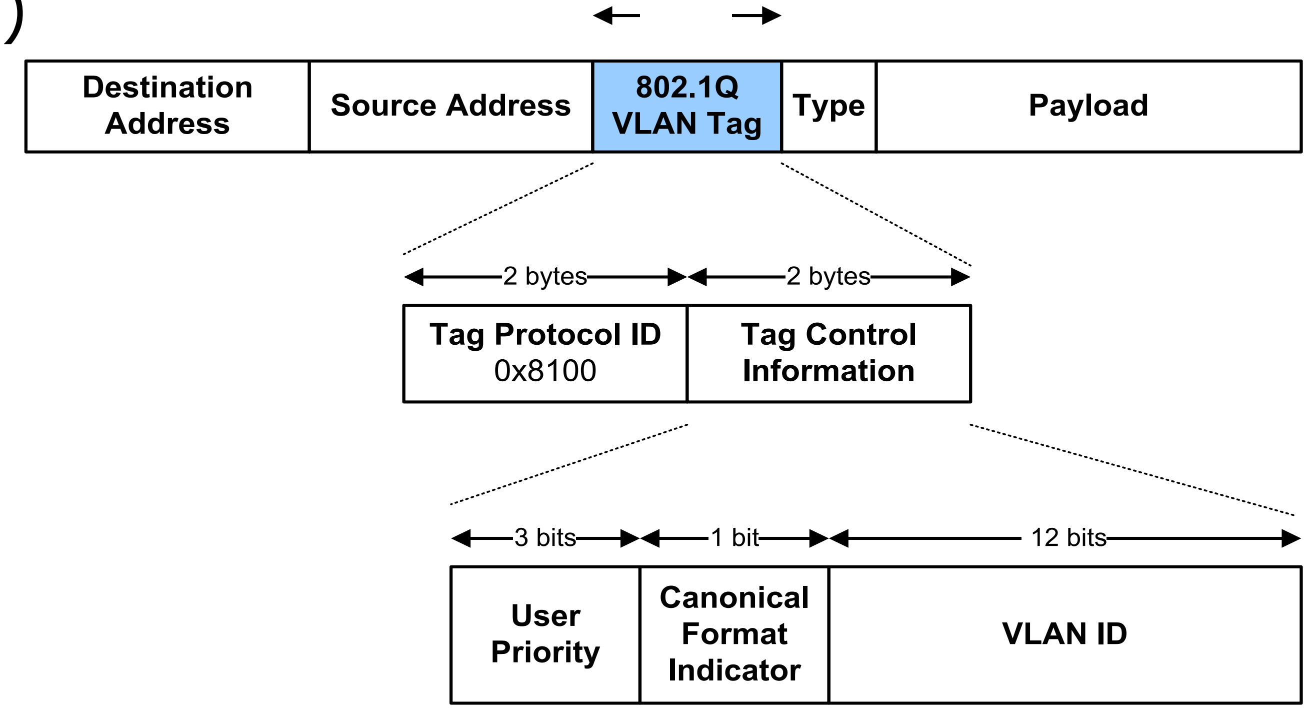
- If VLANs span multiple switches, then the traffic between the switches belongs to different VLANs
- Switches need to be able to demultiplex traffic from different VLANs

→ VLAN tags



IEEE 802.1Q: VLAN Tagging

- For VLAN traffic between LAN switches, add a tag to Ethernet frames that identifies the LAN
- Tag can be transparent to endsystems (by stripping off VLAN tag)



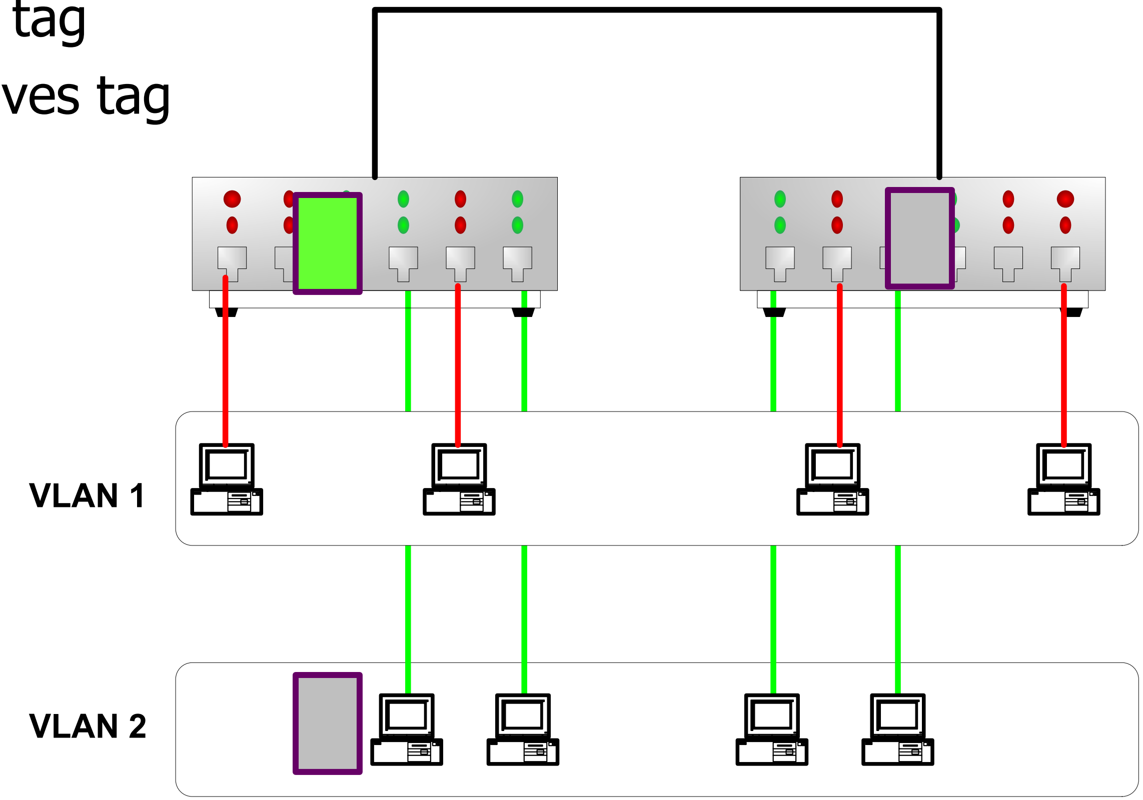
802.1Q Tag Fields

- **Tag Protocol Identifier:**
  - Value 0x8100 identifies 802.1Q tag
- **User Priority:**
  - Can be used by sender to prioritize different types of traffic (e.g., voice, data)
  - 0 is lowest priority
- **Canonical Format Indicator:**
  - Used for compatibility between different types of MAC protocols
- **VLAN Identifier (VID):**
  - Specifies the VLAN (1 – 4094)
  - 0x000 indicates frame does not belong to a VLAN
  - 0xfff is reserved

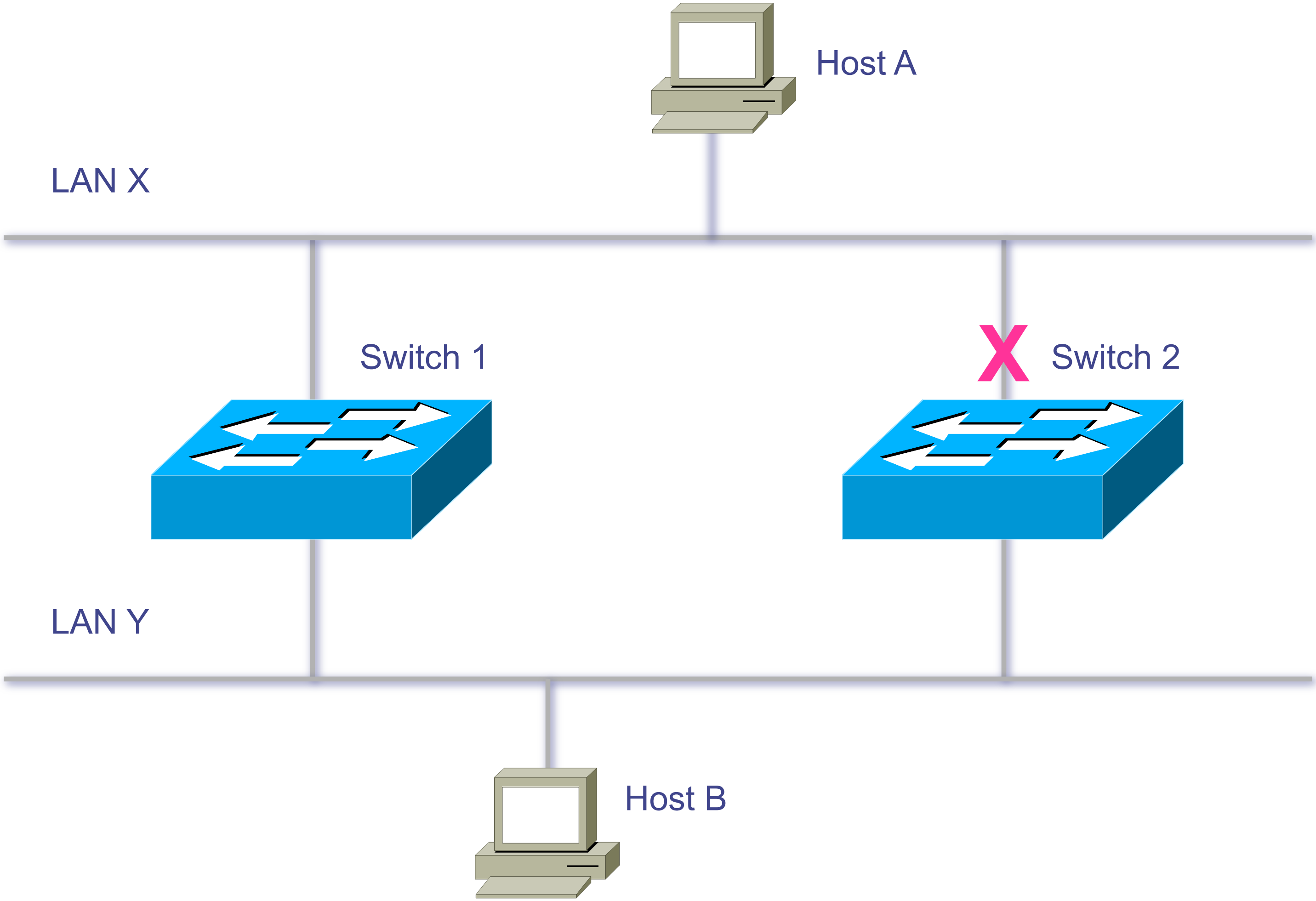
VLANs Tags

Normal operation:

- Sender sends frame
- First switch adds tag
- Last switch removes tag



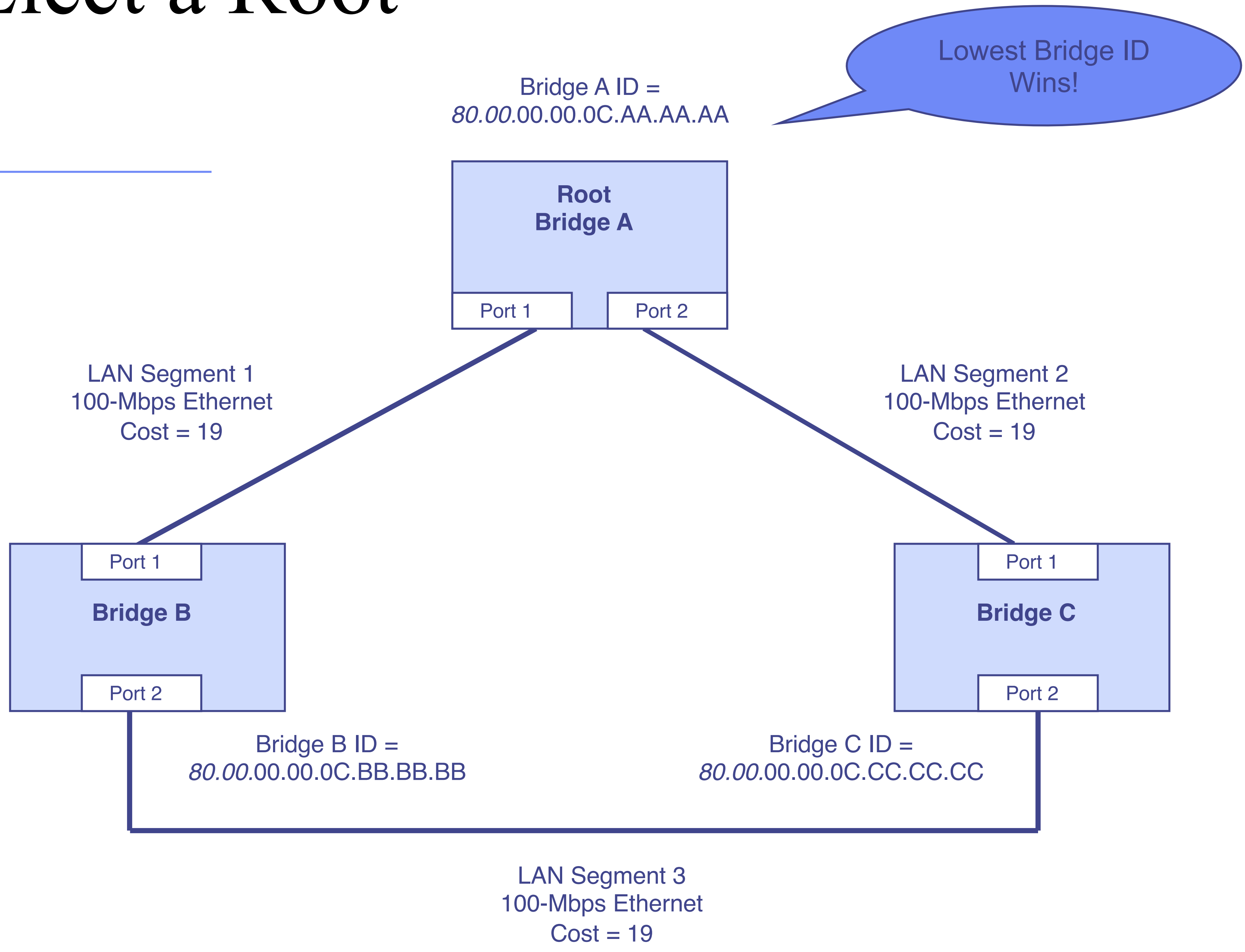
Bridges and Switches use Spanning-Tree Protocol (STP) to Avoid Loops



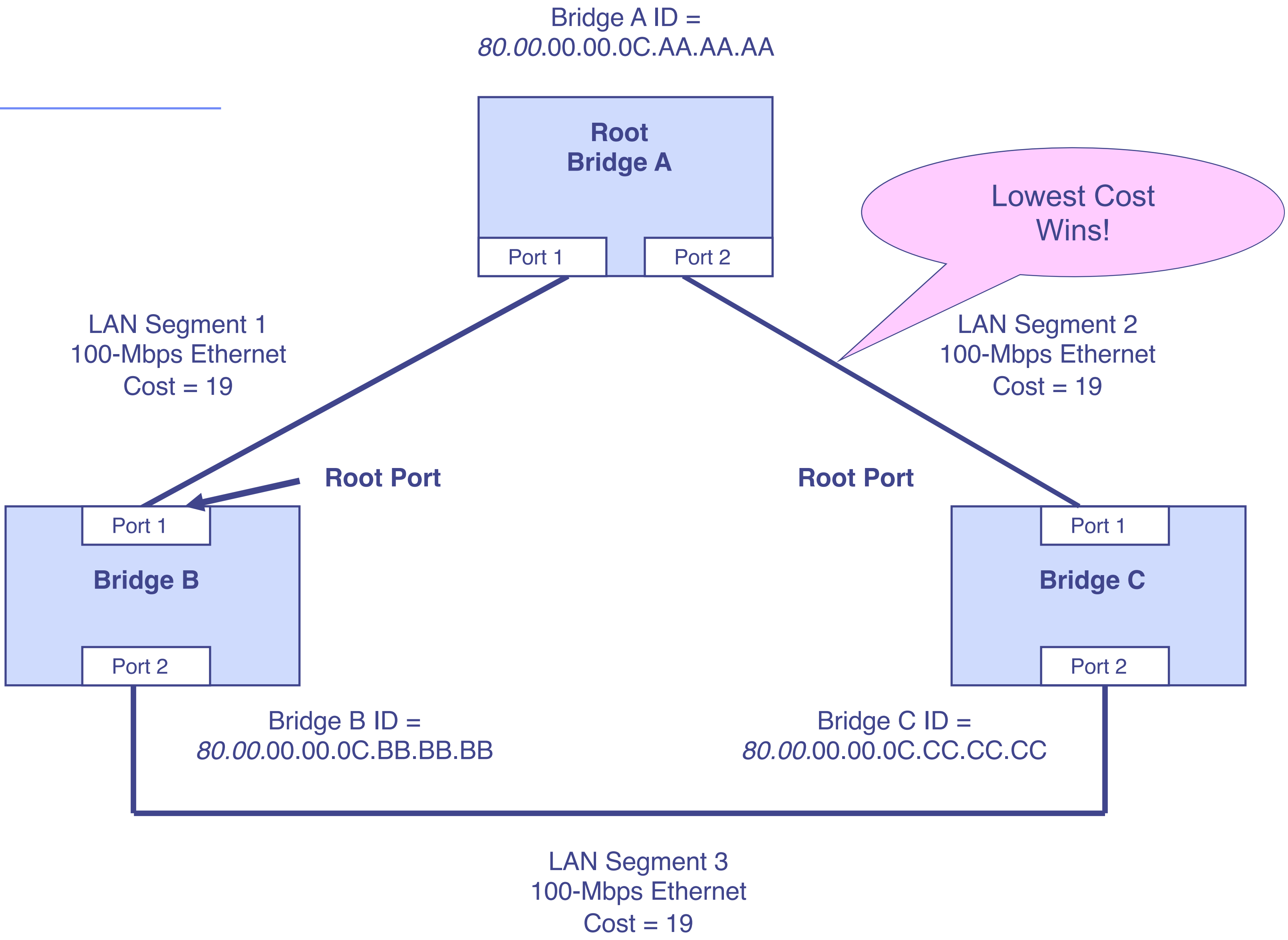
Bridges (Switches) Running STP

- Participate with other bridges in the election of a single bridge as the Root Bridge.
- Calculate the distance of the shortest path to the Root Bridge and choose a port (known as the Root Port) that provides the shortest path to the Root Bridge.
- For each LAN segment, elect a Designated Bridge and a Designated Port on that bridge. The Designated Port is a port on the LAN segment that is closest to the Root Bridge. (All ports on the Root Bridge are Designated Ports.)
- Select bridge ports to be included in the spanning tree. The ports selected are the Root Ports and Designated Ports. These ports forward traffic. Other ports block traffic.

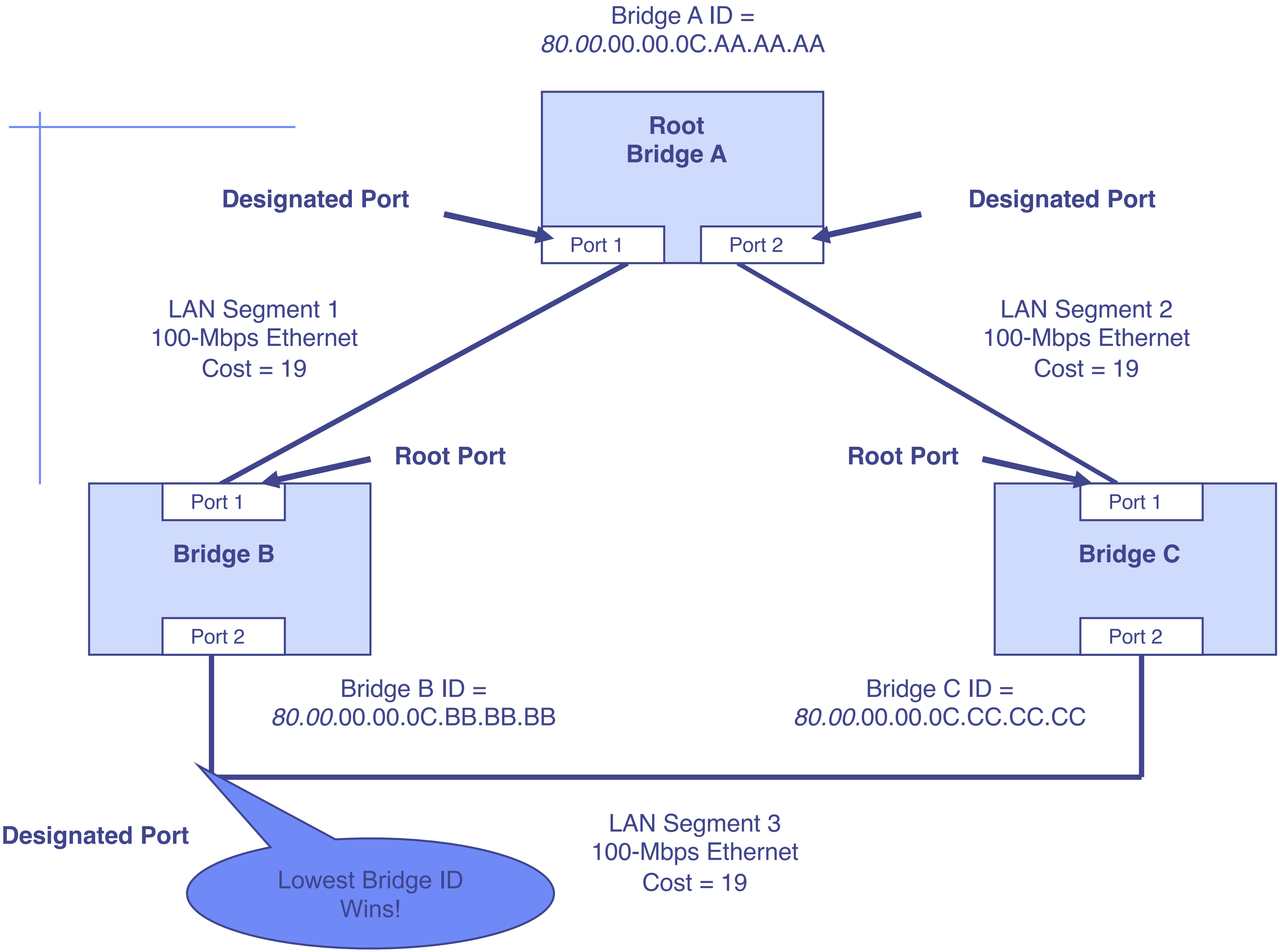
Elect a Root


Lowest Bridge ID Wins!
Bridge A ID = *80.00.*00.00.0C.AA.AA.AA
Root Bridge A
Port 1
Port 2
LAN Segment 1
100-Mbps Ethernet
Cost = 19
LAN Segment 2
100-Mbps Ethernet
Cost = 19
Port 1
Bridge B
Port 2
Port 1
Bridge C
Port 2
Bridge B ID = *80.00.*00.00.0C.BB.BB.BB
Bridge C ID = *80.00.*00.00.0C.CC.CC.CC
LAN Segment 3
100-Mbps Ethernet
Cost = 19

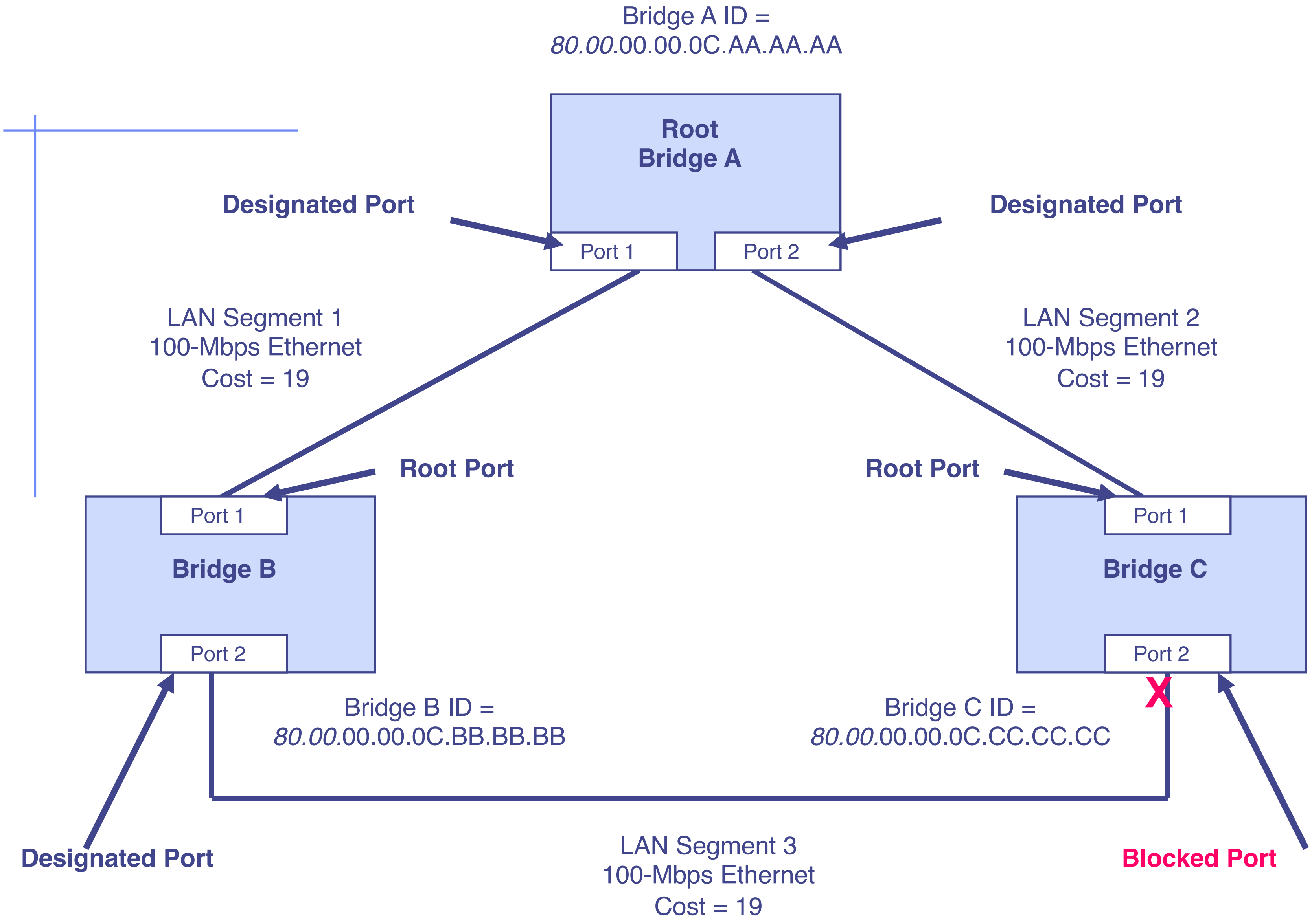
Determine Root Ports



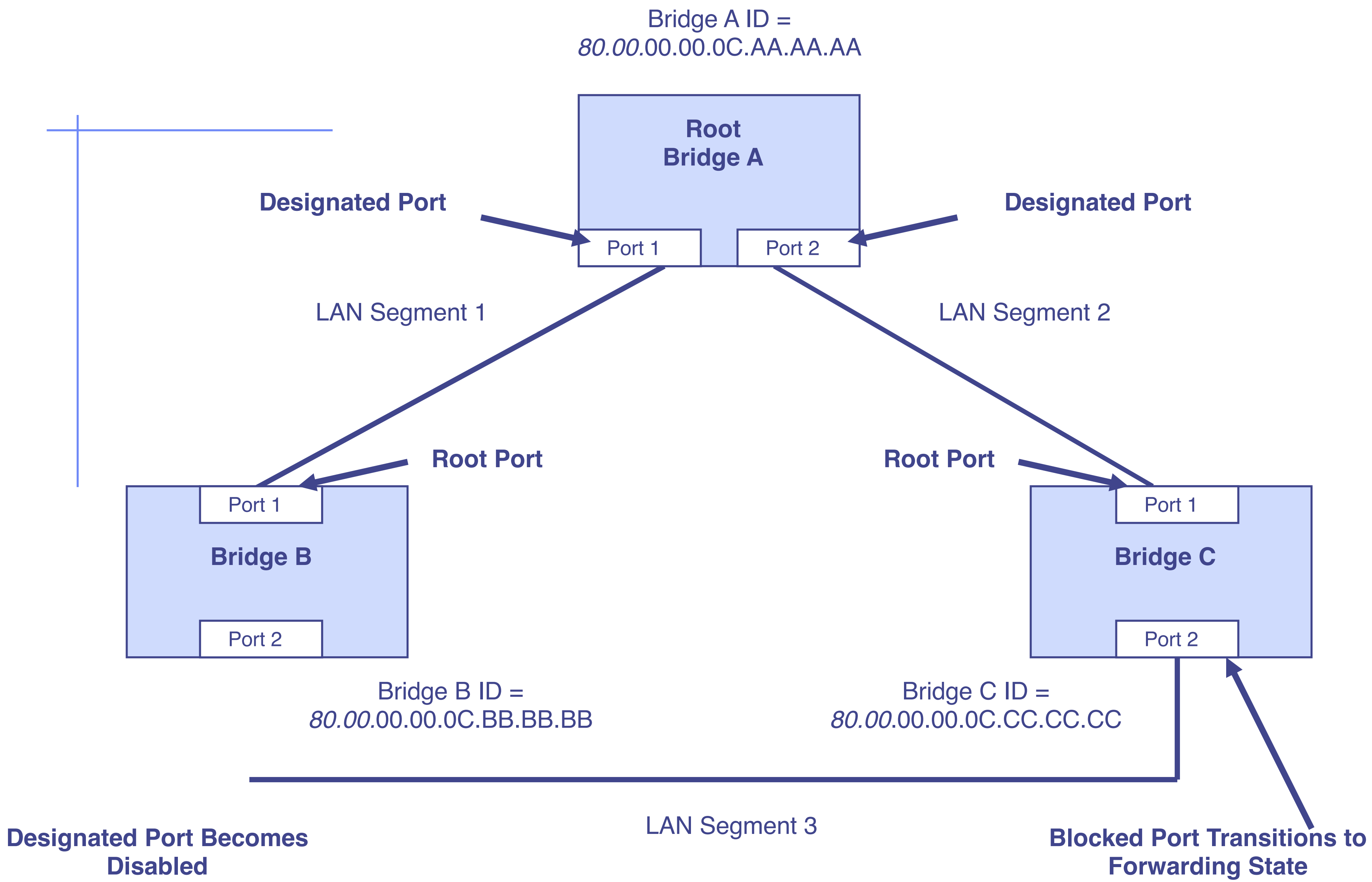
Determine Designated Ports



Prune Topology into a Tree!



React to Changes



Scaling the Spanning Tree Protocol

- Keep the switched network small
  - It shouldn't span more than seven switches
- Use BPDU skew detection on Cisco switches
- Use IEEE 802.1w
  - Provides rapid reconfiguration of the spanning tree
  - Also known as RSTP