南京大學 软件学院
NANJING UNIVERSITY · SOFTWARE INSTITUTE

LAN Switching and VLAN

Cisco Systems
Empowering the Internet Generation℠

Table of Contents

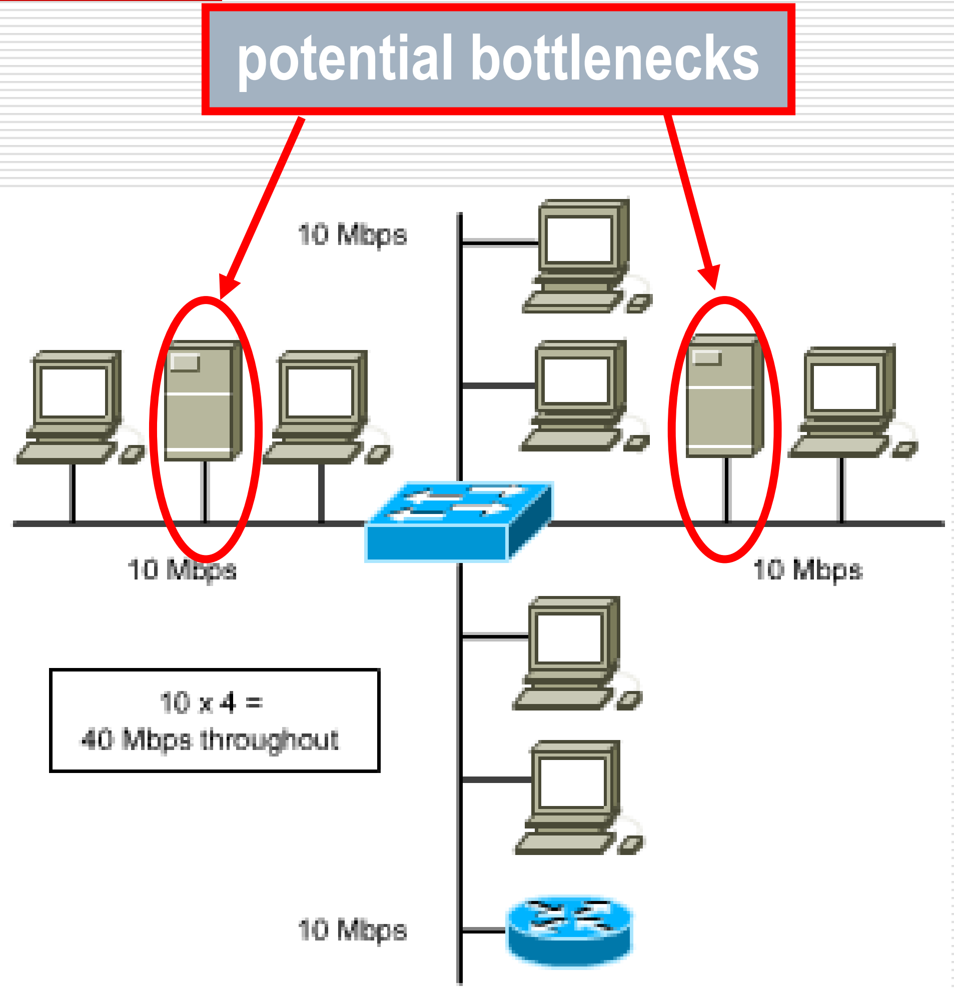
- Switching
- The Spanning-Tree Protocol
- VLAN
  - Introduction of VLAN
  - VLAN Architecture
  - VLAN Implementation
  - Routing Between VLANs

Switch Operation

- Switches perform two basic functions:
  - Building and maintaining switching tables (similar to a bridge table) based on MAC addresses
  - Switching frames out the interface to the destination

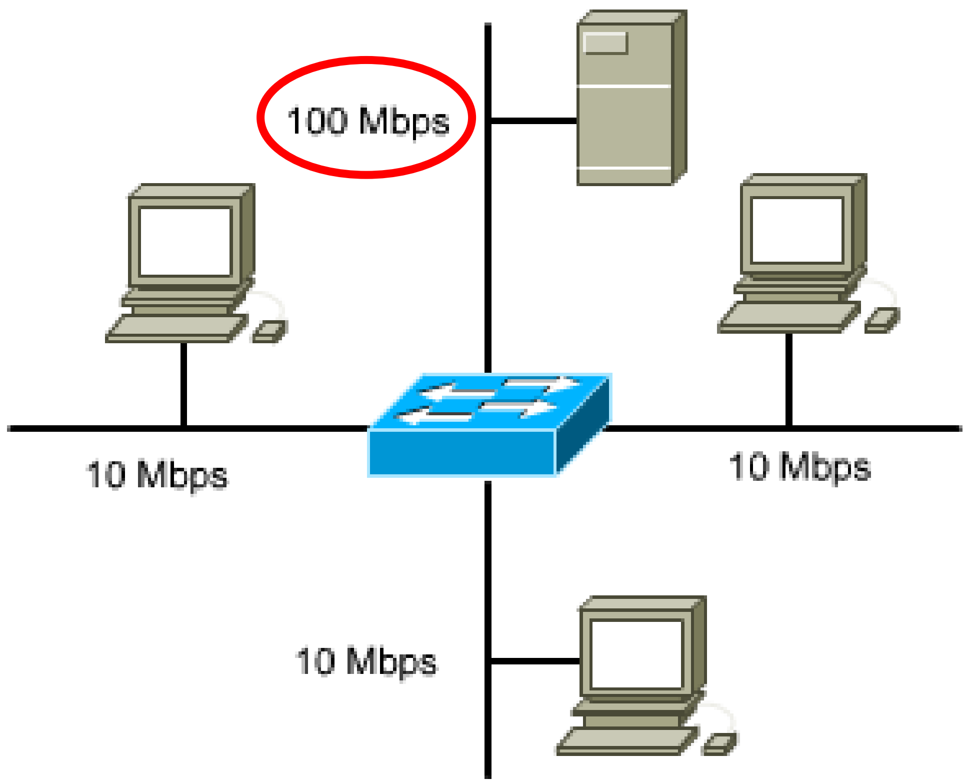
Symmetric Switching

- symmetric switching provides switched connections between ports with the same bandwidth (10/10 Mbps or 100/100 Mbps)
- can cause bottlenecks as users try to access servers on other segments.



Asymmetric Switching

- asymmetric switching reduces the likelihood of a potential bottleneck at the server by attaching the segment with the server to a higher bandwidth port (100 Mbps)
- asymmetric switching requires memory buffering in the switch



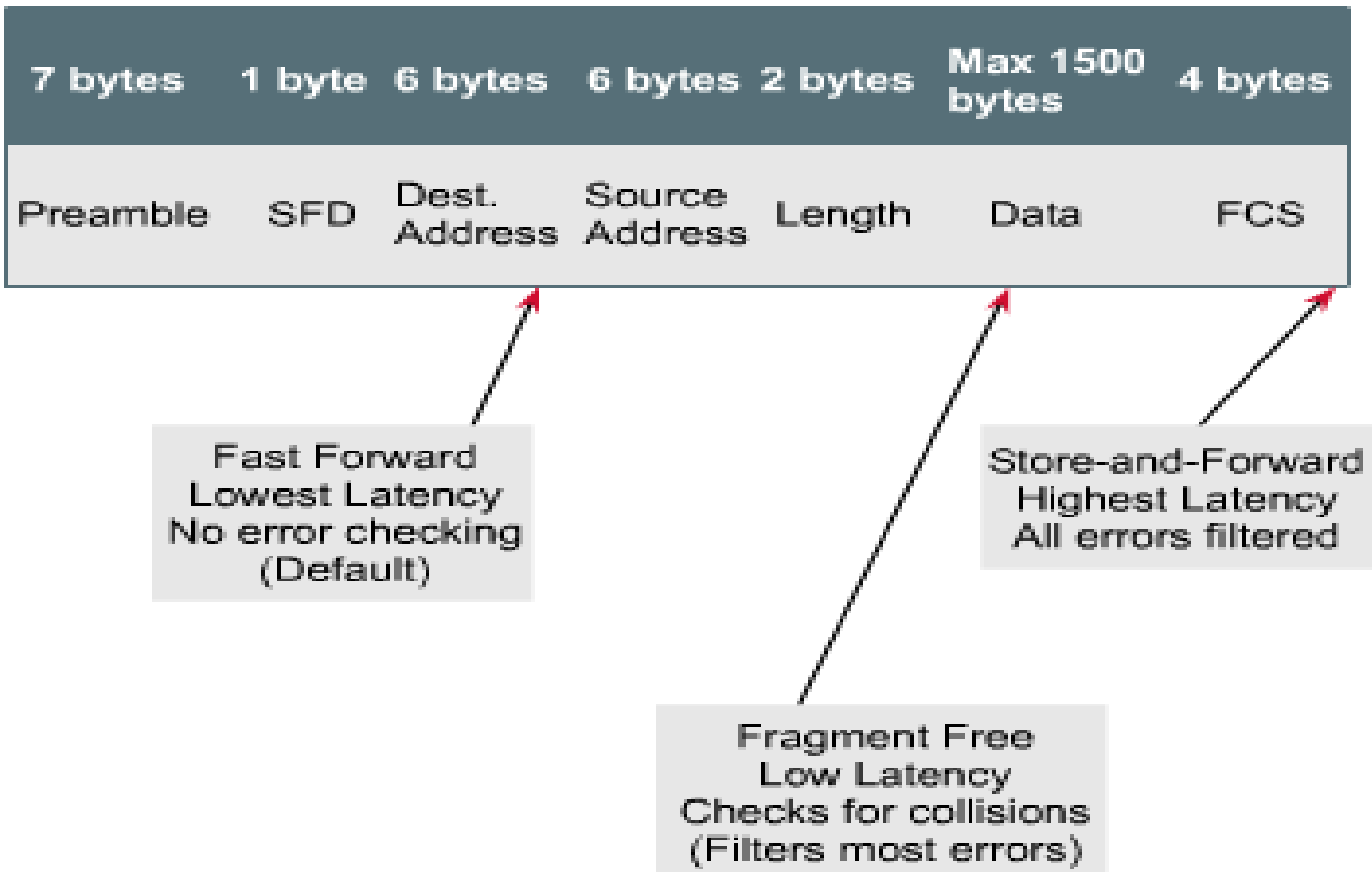
Memory Buffering

- Area of memory in a switch where destination and transmission data are stored until it can be switched out the correct port.
  - Port-based memory buffering
    - packets are stored in a queue on each port
    - possible for one packet to delay transmission of other packets because of a busy destination port
  - Shared memory buffering
    - common memory buffering shared by all ports
    - allows packets to be RX on one port and TX out another port without changing it to a different queue.

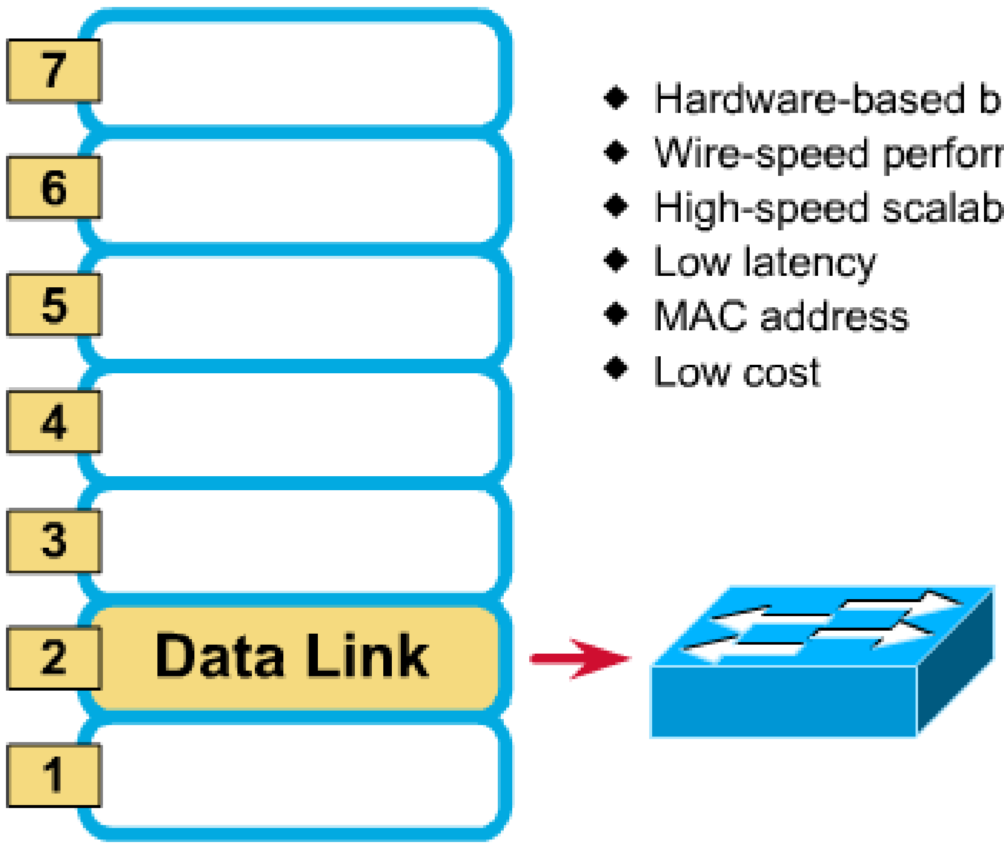
Switching Methods

- Store-and-Forward
  - The switch receives the entire frame, calculating the CRC at the end, before sending it to the destination
- Cut-through
  - A switch adds latency. It can be reduced by using cut-through switching method
  - Fast forward switching--only checks the destination MAC before immediately forwarding the frame
  - Fragment Free--reads the first 64 bytes to reduce errors before forwarding the frame

Two Switching Methods

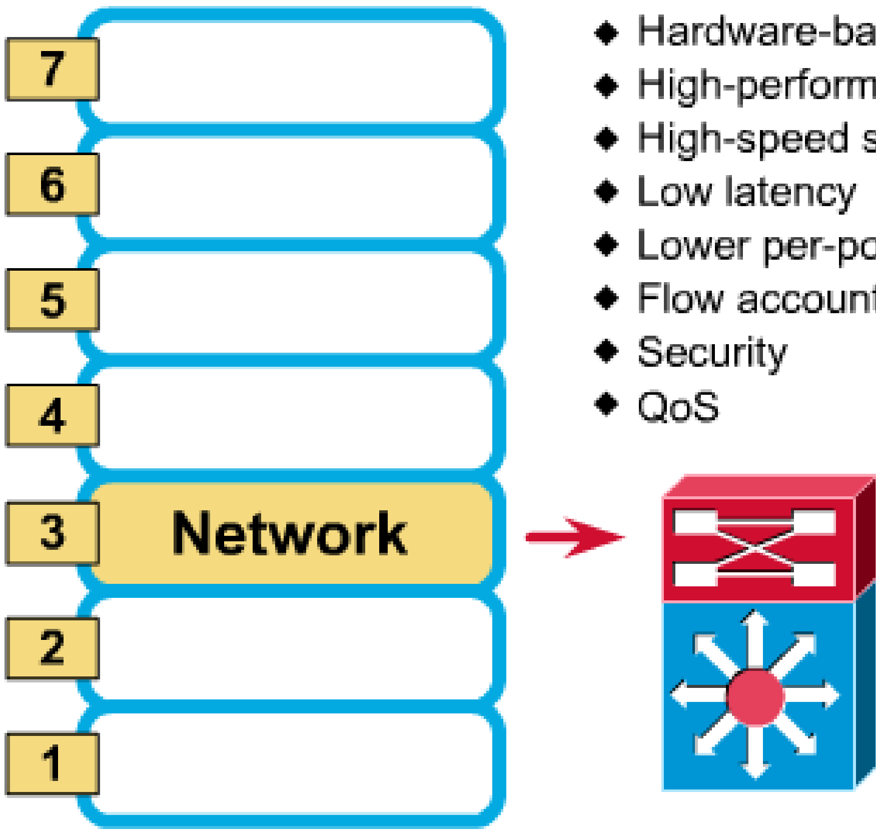


Layer 2 Switching



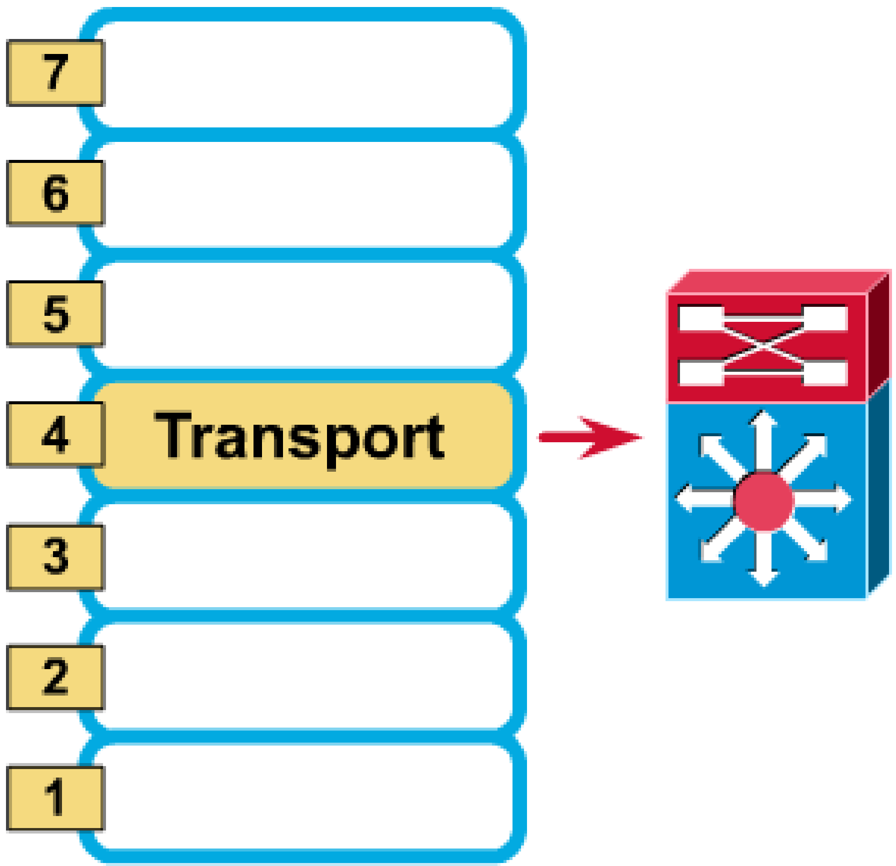
- Hardware-based bridging
- Wire-speed performance
- High-speed scalability
- Low latency
- MAC address
- Low cost

Layer 3 Switching



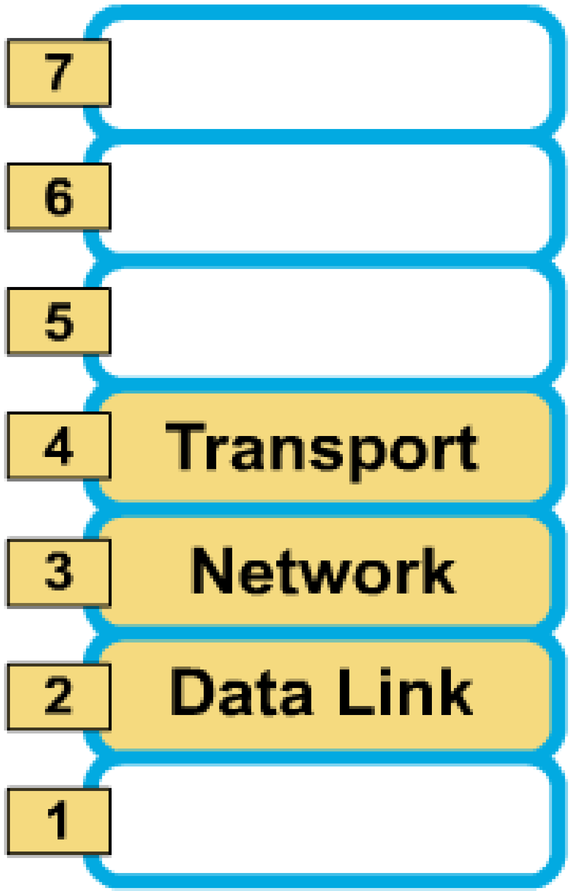
- Hardware-based packet forwarding
- High-performance packet switching
- High-speed scalability
- Low latency
- Lower per-port cost
- Flow accounting
- Security
- QoS

Layer 4 Switching



- Based on Layer 3
- Based on application-related information
- TCP fields
- UDP fields
- QoS
- Granular Traffic Control

Multilayer Switching



- Combines functionality of:
- -Layer 2 switching
  -Layer 3 switching
  -Layer 4 switching
- High-speed scalability
- Low latency

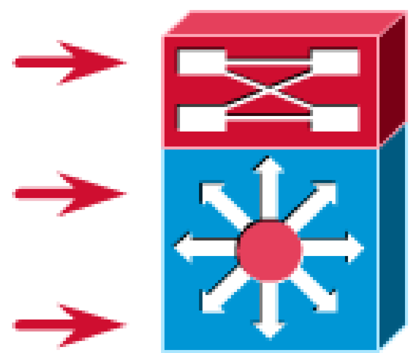


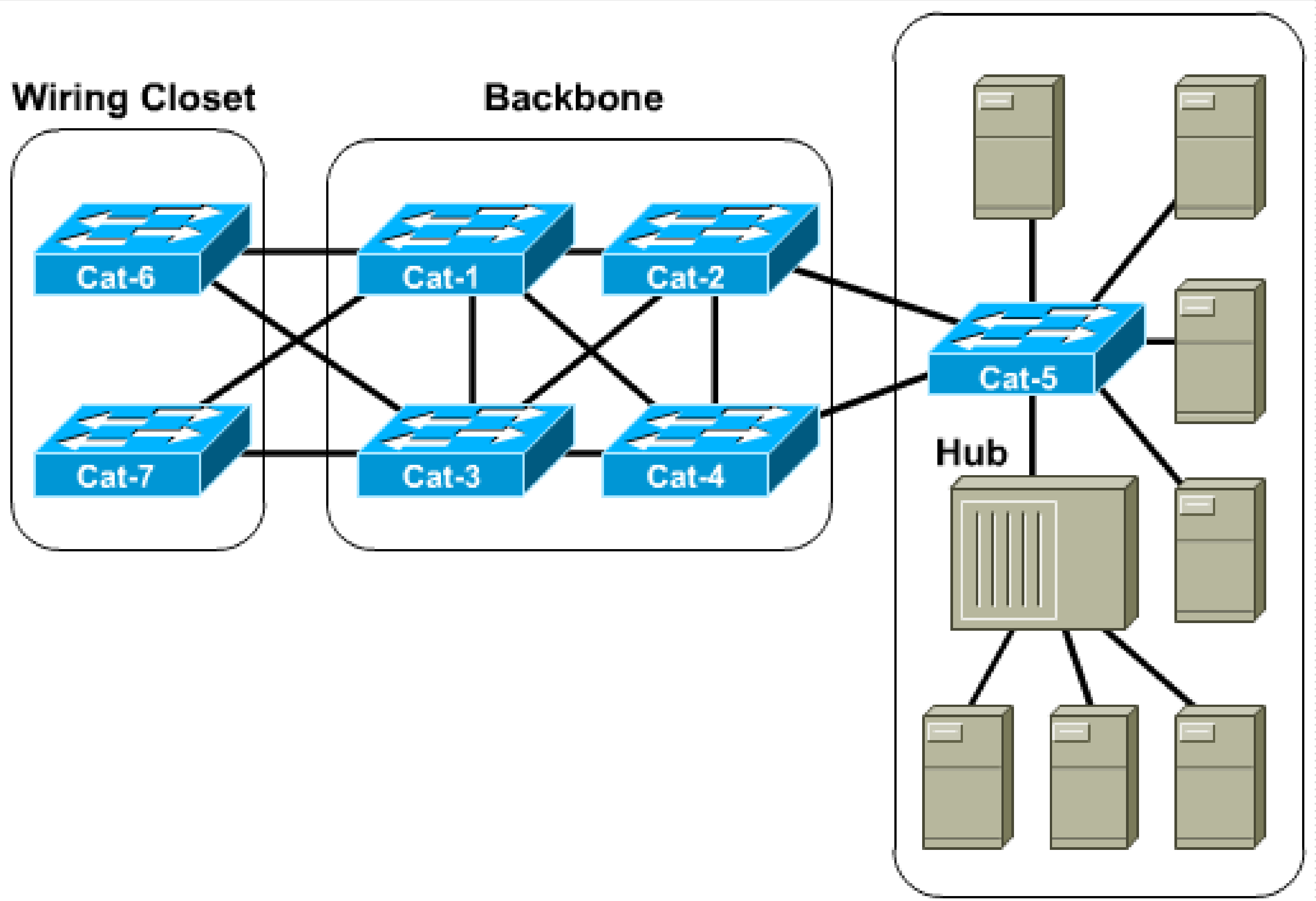
Table of Contents

Bridging Loops

- Loops may occur in a network for a variety of reasons.
  - Usually loops in networks are the result of a deliberate attempt to provide redundancy.
  - Can also occur by configuration error
    - Two primary reasons loops can be absolutely disastrous in a bridged network:
      - broadcast loops
      - bridge-table corruption

NANJING UNIVERSITY

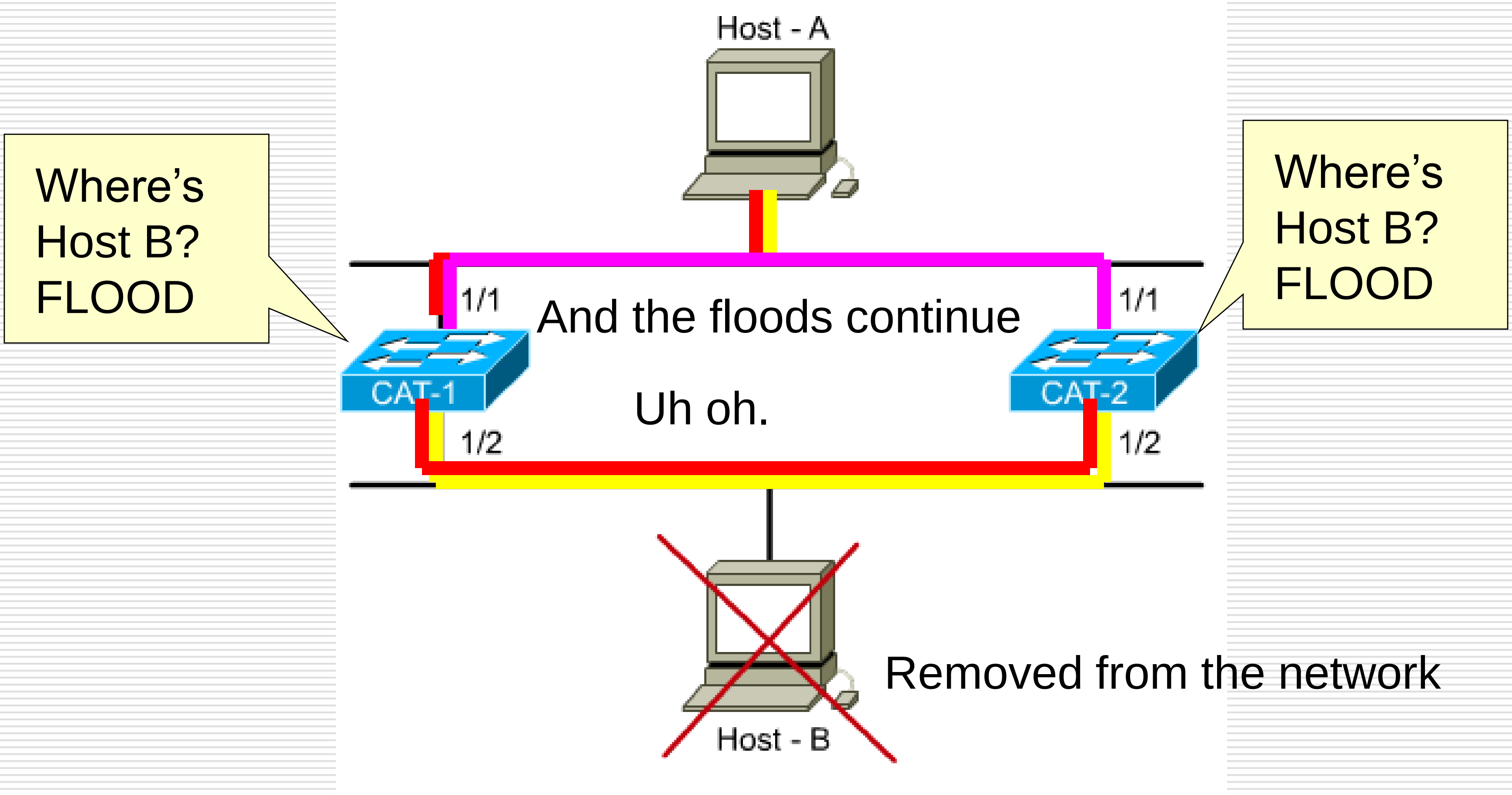
Redundancy Creates Loops



L2 Loops

- Broadcasts and Layer 2 loops can be a dangerous combination.
- Ethernet frames have no TTL field
- After an Ethernet frame starts to loop, it will probably continue until someone shuts off one of the switches or breaks a link
- The switches will flip flop the bridging table entry for Host A (creating extremely high CPU utilization).

L2 Loops - Flooded unicast frames



Overview of STP

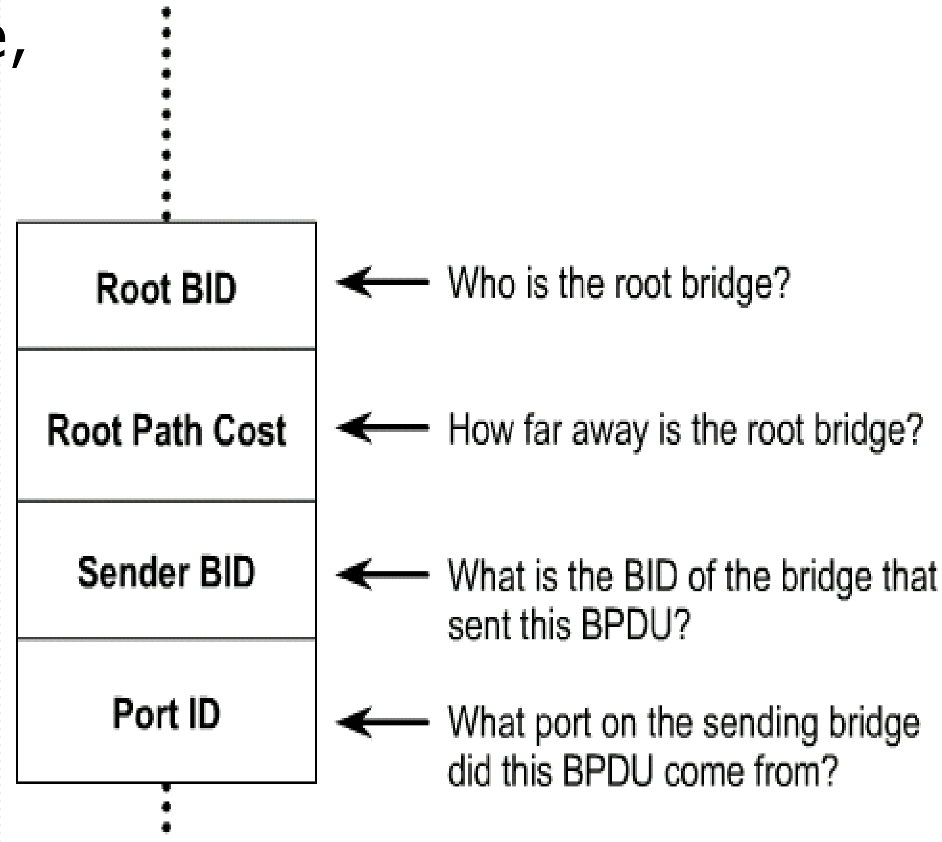
- Elements of the Spanning Tree Protocol
  - Main function: allow redundant paths in a switched/bridged network without incurring latency from the effects of loops.
  - STP prevents loops by calculating a stable spanning-tree network topology
  - Spanning-tree frames (called bridge protocol data units--BPDUs) are used to determine the spanning-tree topology

STP Decision Sequence

- Spanning Tree always uses the same four-step decision sequence:
  - Lowest root BID (Bridge Identification)
  - Lowest path cost to root bridge
  - Lowest sender BID
  - Lowest port ID

BPDUs

- STP establishes a root node, called the root bridge
- The resulting tree originates from the root bridge.
- Redundant links that are not part of the shortest path tree are blocked.
- Data frames received on blocked links are dropped.
- The message that a switch sends, allowing the formation of a loop free logical topology, is BPDU



BPDUs are switch-to-switch traffic; they do not carry end-user traffic.

Bridge Identification/BID

- A Bridge ID (BID): 8 bytes
  - The high-order BID subfield(2 bytes): bridge priority
    - 2^{16} possible values: 0-65,535 (default: 32,768)
    - Typically expressed in a decimal format
  - The low-order subfield(6 bytes): a MAC address assigned to the switch
    - Expressed in hexadecimal format
- *STP cost values:* ***lower costs are better.***

Electing the Root Switch

- The switches elect a single root switch by looking for the switch with the lowest BID (often referred to as a root war).
- If all the switches are using the default bridge priority of 32,768, the lowest MAC address serves as the tie-breaker.

Path Cost

Bandwidth	STP Cost
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

Bridges use the concept of cost to evaluate how close they are to other bridges.

Five STP States

- States are established by configuring each port according to policy
- Then the STP modifies the states based on traffic patterns and potential loops
- The default order of STP states are:
  - Blocking--no frames forwarded, BPDUs heard
  - Listening--no frames forwarded, listening for data frames
  - Learning--no frames forwarded, learning addresses
  - Forwarding--frames forwarded, learning addresses
  - Disabled--no frames forwarded, no BPDUs heard

blocking
20s
15s
15s
forwarding

Initial STP Convergence

- When the network first starts, all the bridges flood the network with a mix of BPDU information.
- Immediately, they apply the decision sequence allowing them to hone in on the set of BPDUs that form a single spanning tree for the entire network.

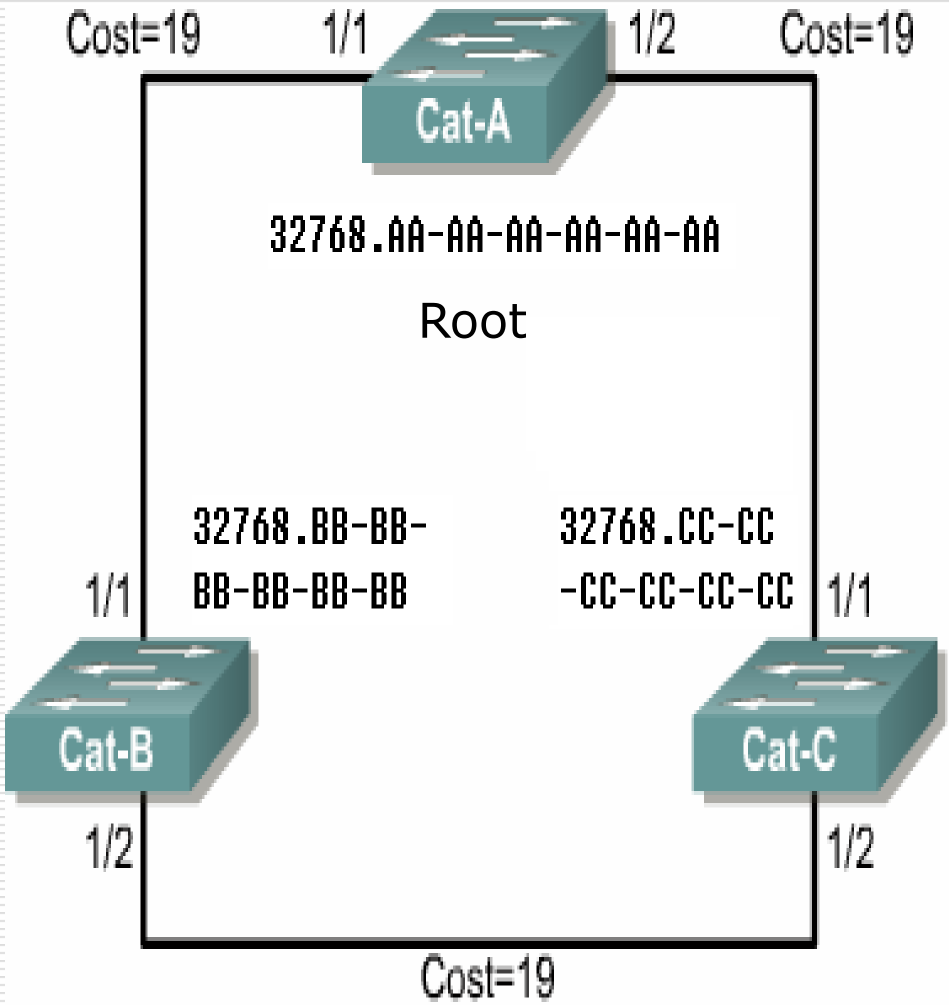
(Step 1) *Root switch decision:* A single root bridge is elected to act as the central point of this network

(Step 2) *Electing the root ports:* All the remaining bridges calculate a set of root ports

(Step 3) *Electing the designated ports:* All the remaining bridges calculate a set of designated ports

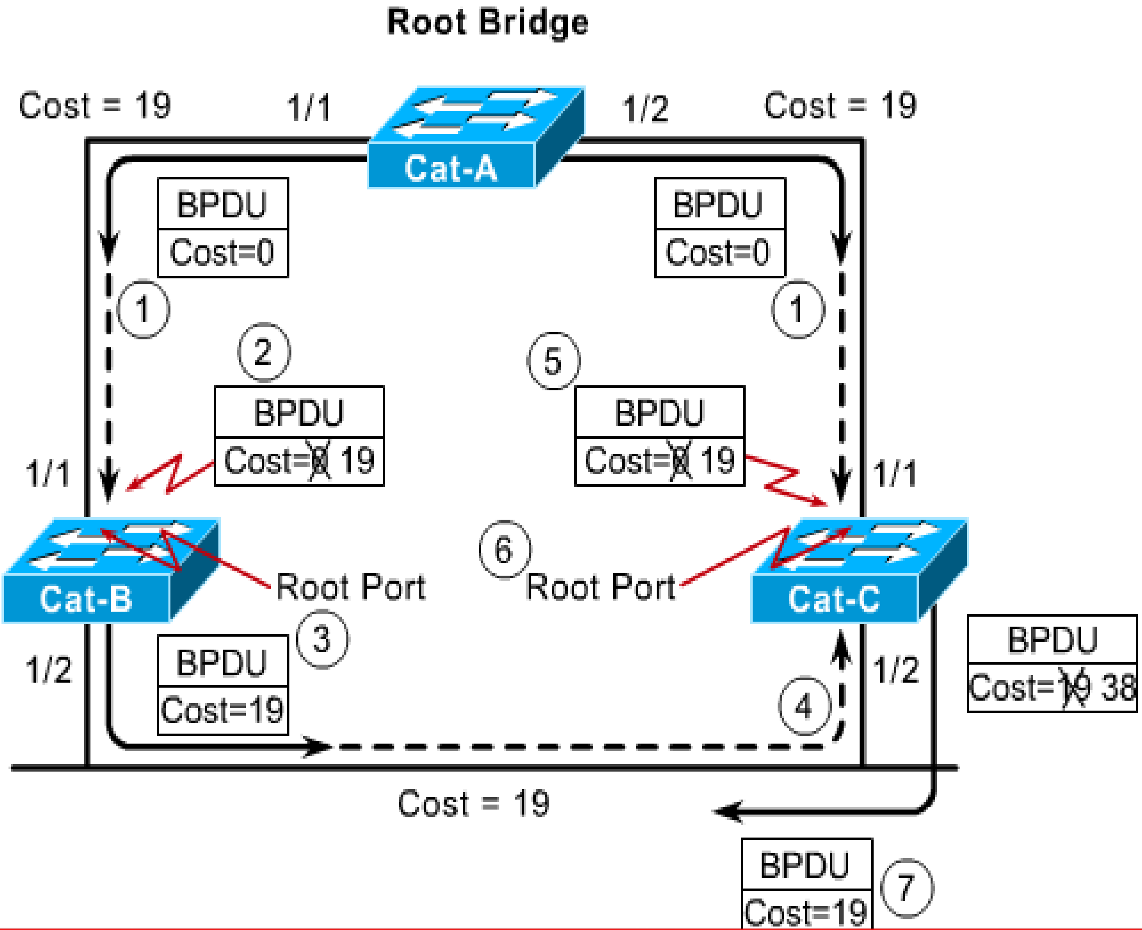
Step1: Root Switch Decision

- Announce itself as the root
- Checking all BPDUs received on the port as well as the BPDU that would be sent on that port
- For each arrived BPDU, if it is lower in value than the existing BPDU saved for the port
  - The old value is replaced
  - The sender of BPDU is accepted as the new root



Step2: Electing the Root Ports

- Every non-root bridge must select one root port.
  - The root port of a bridge is the port that is closest to the root bridge.
  - The root path cost is the cumulative cost of all links to the root bridge.



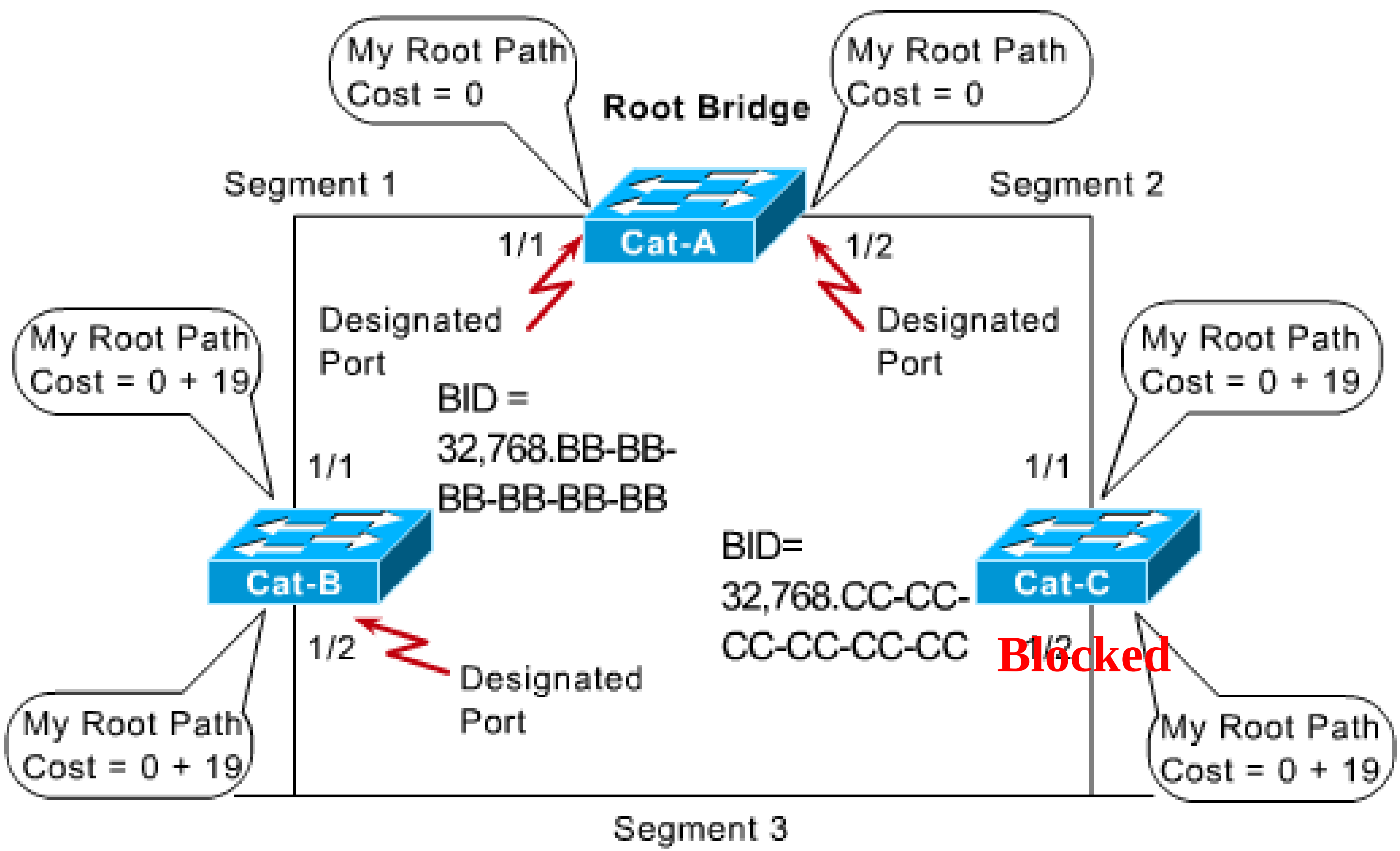
STP costs are incremented as BPDUs are received on a port, not as they are sent out a port.

Step3: Electing Designated Ports(I)

- Each segment has one designated port
  - Functions as the single bridge /switch port that both sends and receives traffic to and from that segment and the root bridge.
- The bridge/switch containing the designated port for a given segment is referred to as the *designated bridge* for that segment.
- All the bridges/switches will block the non-designated ports on them

Every active port on the root bridge becomes a designated port

Step3: Electing Designated Ports(II)



An Example of STP

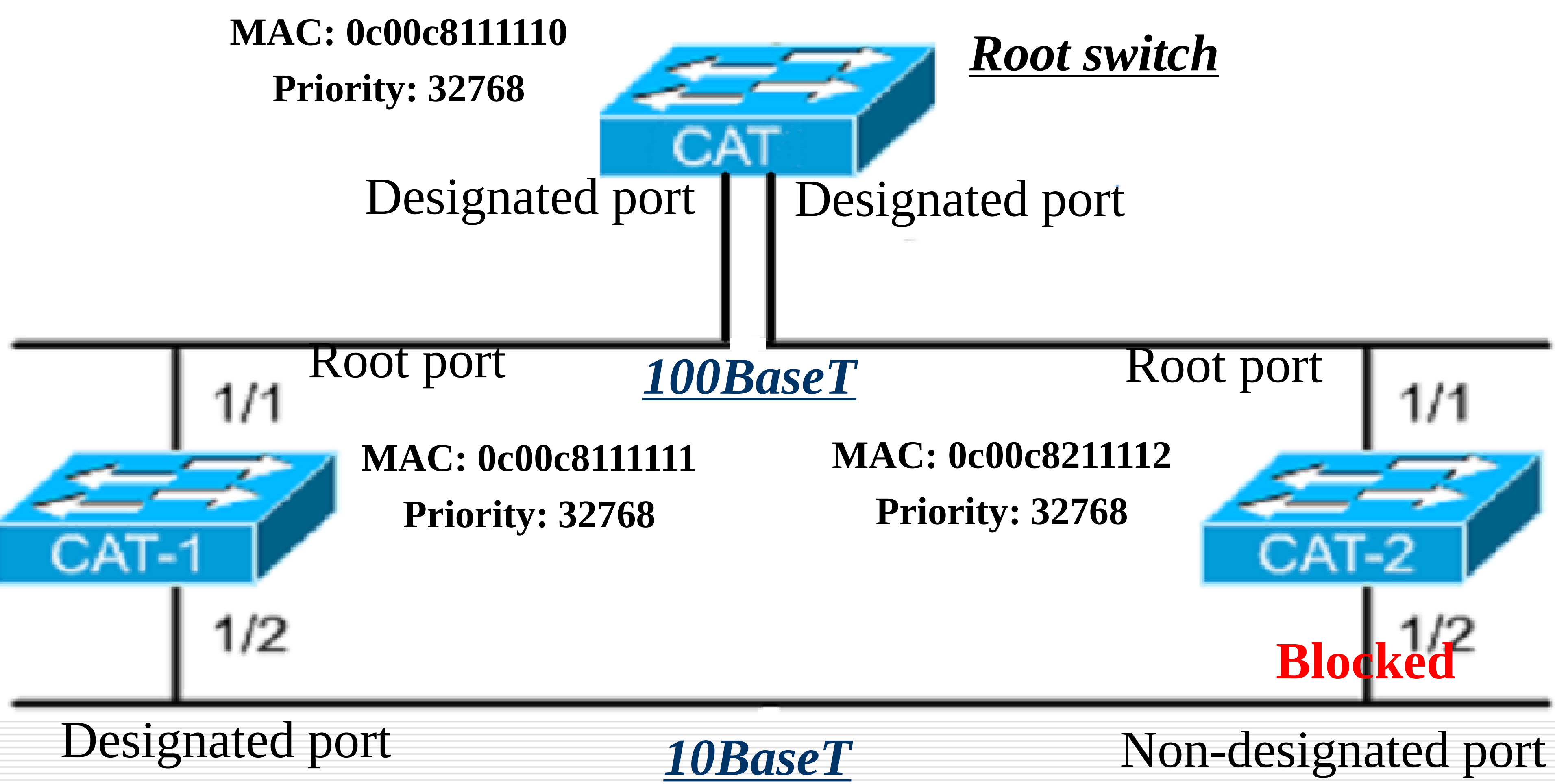


Table of Contents

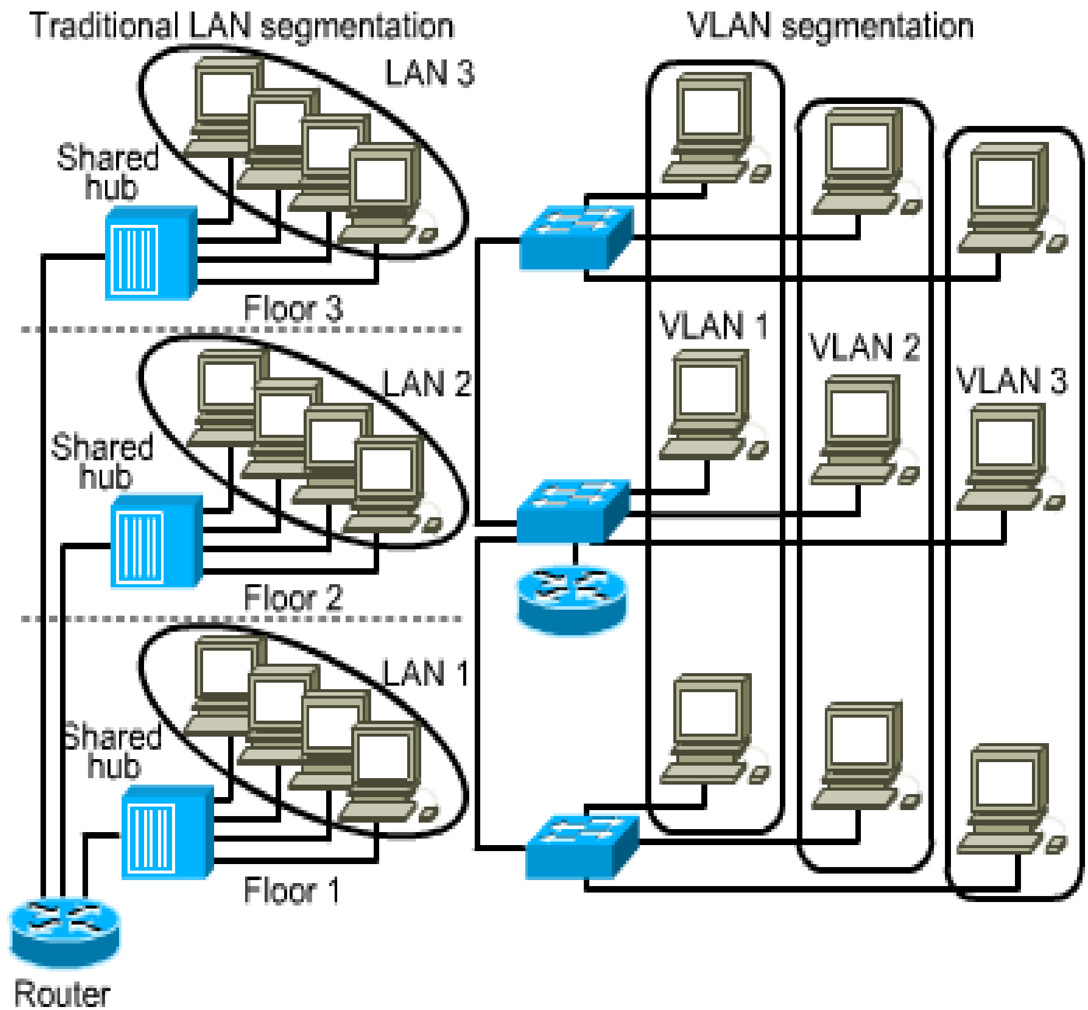
- Switching
- The Spanning-Tree Protocol
- VLAN
  - Introduction of VLAN
  - VLAN Architecture
  - VLAN Implementation
  - Routing Between VLANs

Existing Shared LAN Configurations

- In a typical shared LAN...
  - Users are grouped physically based on the hub they are plugged into
  - Routers segment the LAN and provide broadcast firewalls
- In VLANs...
  - you can group users logically by function, department or application in use
  - configuration is done through proprietary software

Differences between LANs & VLANs

- VLANs...
  - work at Layer 2 & 3
  - control network broadcasts
  - allow users to be assigned by net admin.
  - provide tighter network security. How?



VLANs (IEEE 802.1q)

- Characteristics
  - A logical grouping of network devices or users that are not restricted to a physical switch segment.
  - The devices or users in a VLAN can be grouped by function, department, application, and so on, regardless of their physical segment location.
  - A VLAN creates a single broadcast domain that is not restricted to a physical segment and is treated like a subnet.
  - VLAN setup is done in the switch by the network administrator using the vendor's software.

南京大學
NANJING UNIVERSITY

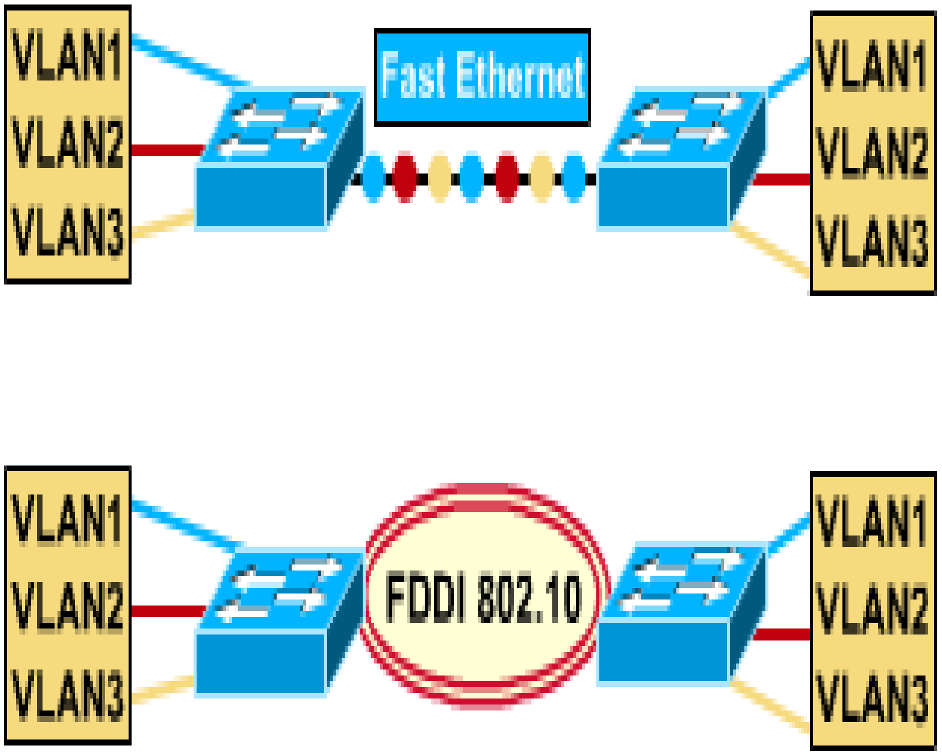
Grouping Users

- VLANs can logically segment users into different subnets (broadcast domains)
- Broadcast frames are only switched between ports on the switch or switches with the same VLAN ID.
- Users can be logically group via software based on:
  - port number
  - MAC address
  - protocol being used
  - application being used

Table of Contents

VLANs Across the Backbone

- VLAN configuration needs to support backbone transport of data between interconnected routers and switches.
- The backbone is the area used for inter-VLAN communication
- The backbone should be high-speed links, typically 100Mbps or greater

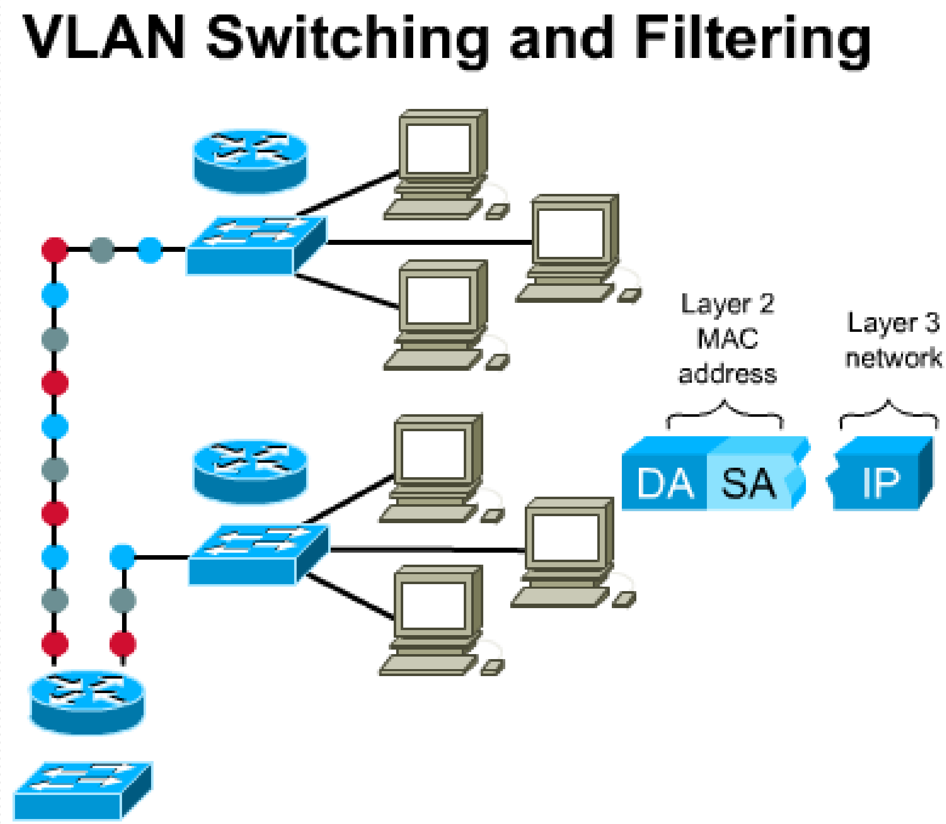


Router’s Role in a VLAN

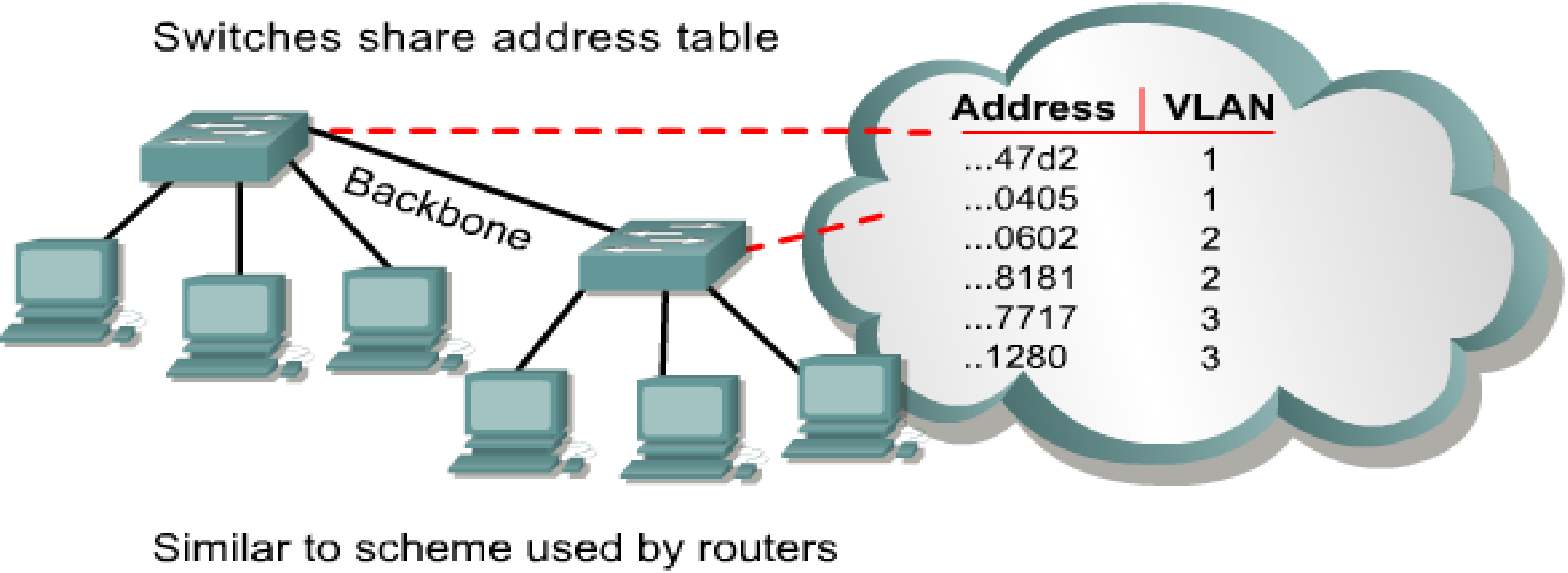
- A router provides connection between different VLANs
- For example, you have VLAN1 and VLAN2.
  - Within the switch, users on separate VLANs cannot talk to each other (benefit of a VLAN!)
  - However, users on VLAN1 can email users on VLAN2 but they need a router to do it.

How Frames are Used in a VLAN

- Switches make filtering and forwarding decisions based on data in the frame.
- There are two techniques used.
  - Frame Filtering--examines particular information about each frame (MAC address or layer 3 protocol type)
  - Frame Tagging--places a unique identifier in the header of each frame as it is forwarded throughout the network backbone.



Frame Filtering

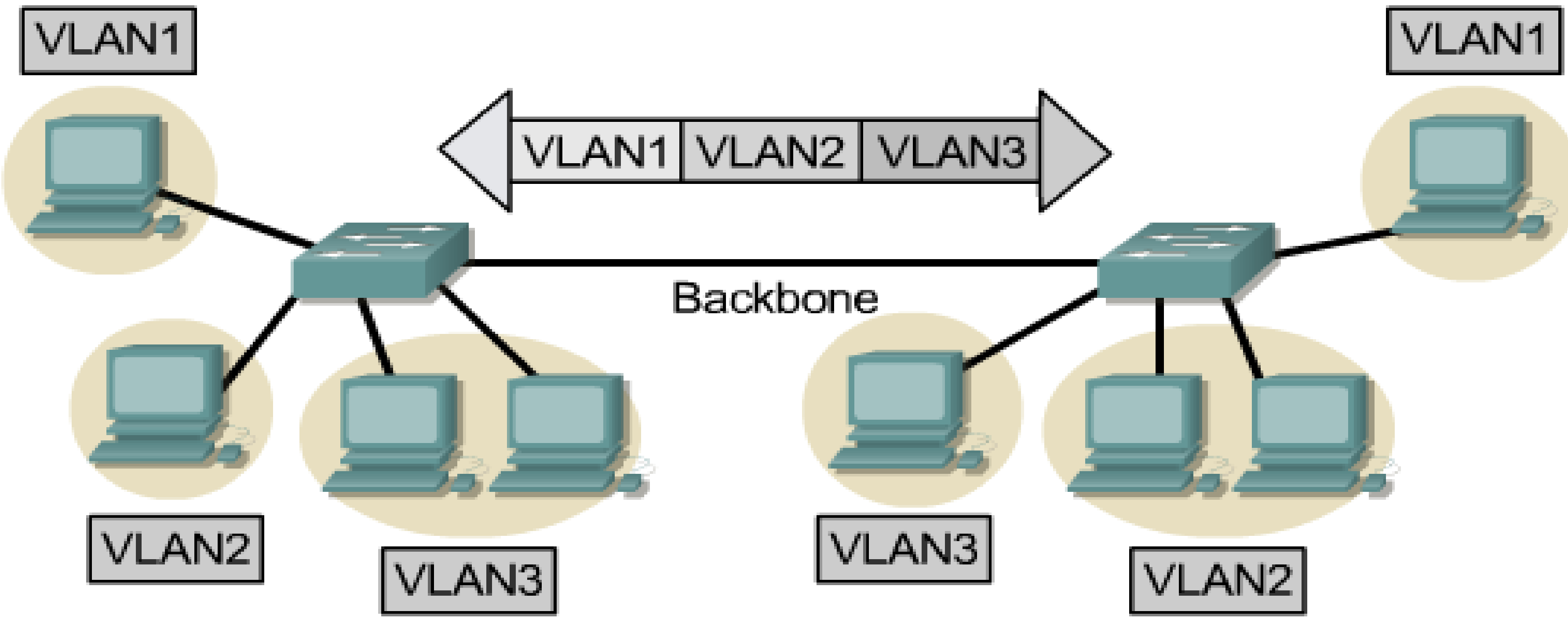


A filtering table is developed for each switch. Switches share address table information. Table entries are compared with the frames. Switch takes appropriate action.

Frame Tagging

- Frame tagging implementation process:
  - Places a VLAN identifier in the header of each frame as it is forwarded throughout the network backbone.
  - The identifier is understood and examined by each switch.
  - When the frame exits the network backbone, the switch removes the identifier before the frame is transmitted to the target end station.
- Frame tagging functions at Layer 2 and requires little processing or administrative overhead.

Frame Tagging



Frame Tagging– IEEE802.1Q and ISL

- IEEE802.1Q
  - IEEE Standard, insert a label of VLAN to the header to identify the VLAN belonging to. (Frame Tagging)。
- ISL(Inter-Switch Link)
  - Cisco proprietary. ISL add a header of 26 bytes in front of the data frame, and appends a CRC(4 byte) at the end.

Name	Encapsulation	Label	Media
802.1Q	No	Yes	Ethernet
ISL	Yes	No	Ethernet

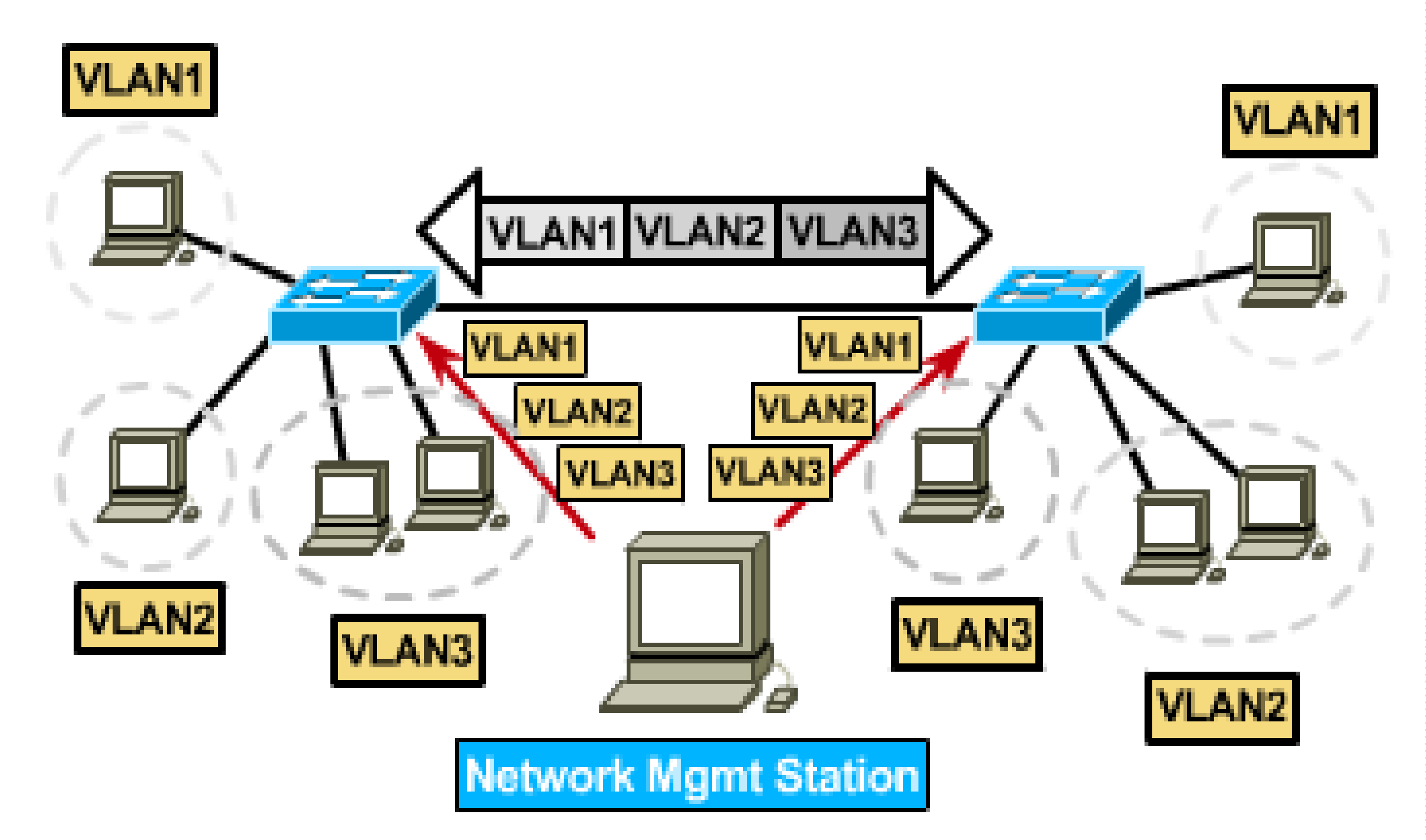
Table of Contents

- Switching
- The Spanning-Tree Protocol
- VLAN
  - Introduction of VLAN
  - VLAN Architecture
  - VLAN Implementation
  - Routing Between VLANs

Ports, VLANs, and Broadcasts

- Three methods for implementing VLANs
  - Static
  - Dynamic
- Each switched port can be assigned to a VLAN. This...
  - ensures ports that <u>do not</u> share the same VLAN <u>do not</u> share broadcasts.
  - ensures ports that <u>do</u> share the same VLAN <u>will share</u> broadcasts.

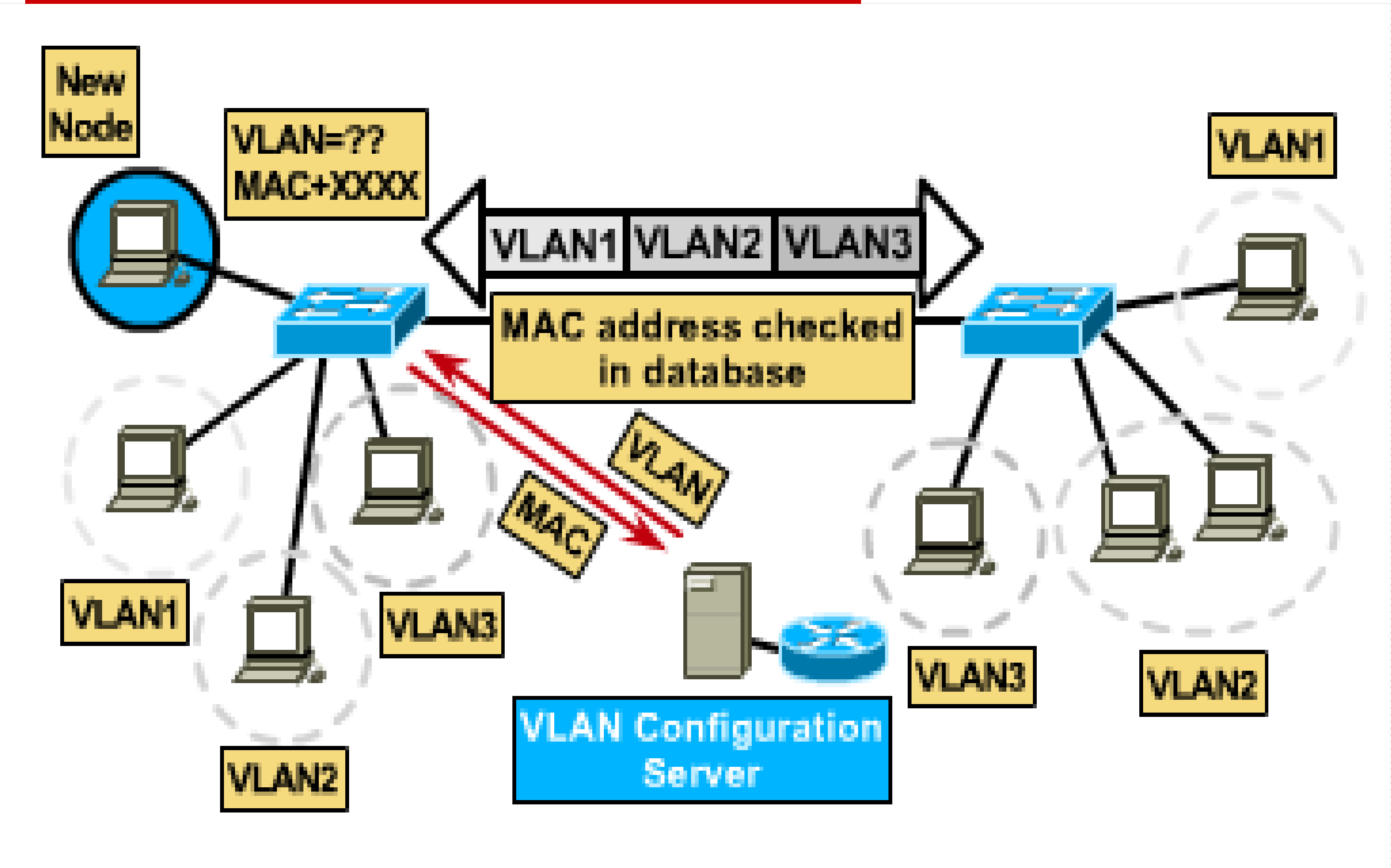
Static VLANs



Static VLANs

- Defined
  - Static VLANs are when ports on a switch are administratively assigned to a VLAN
- Benefits
  - secure, easy to configure and monitor
  - works well in networks where moves are controlled

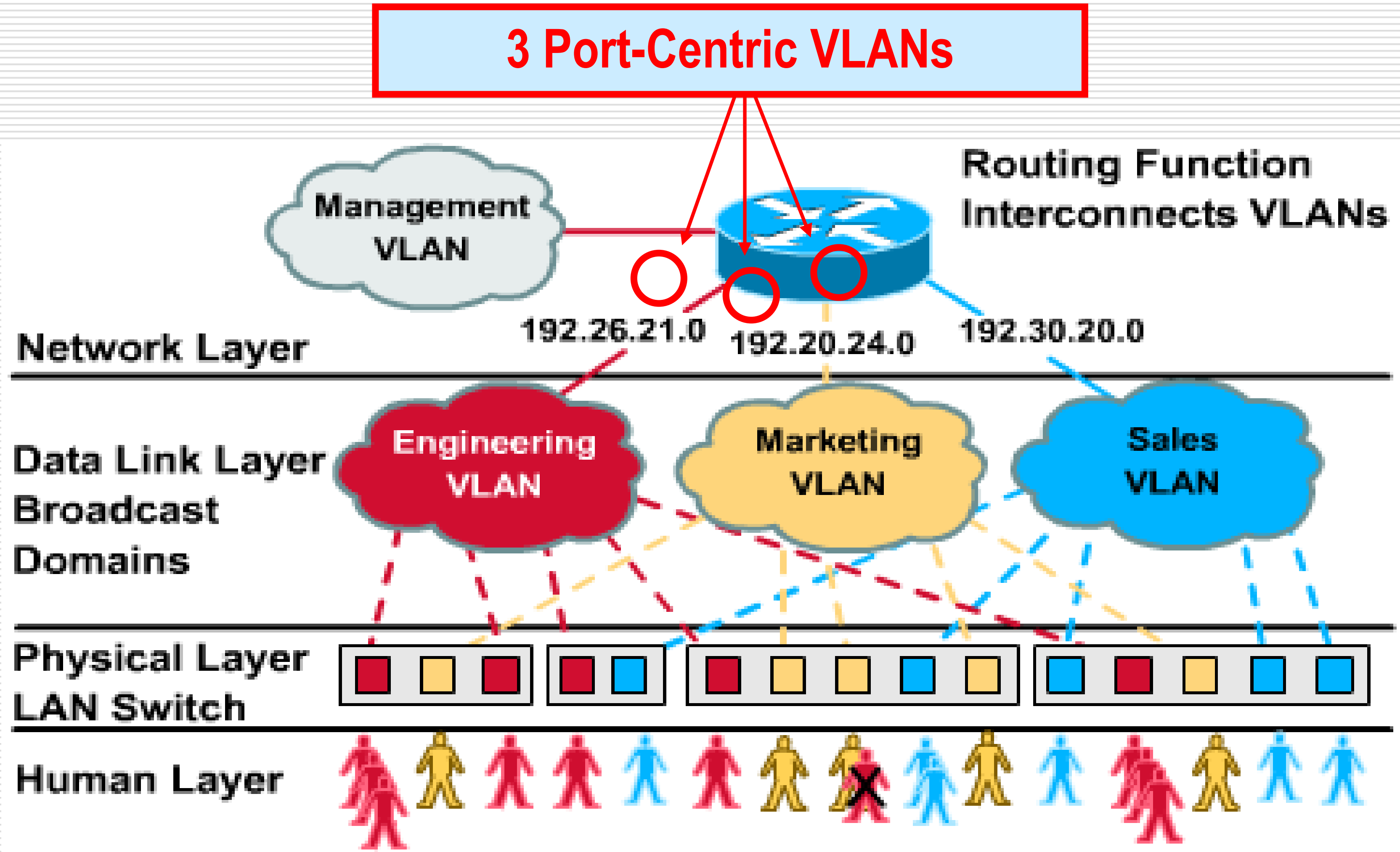
Dynamic VLANs



Dynamic VLANs

- When a station is initially connected to an unassigned port, the switch checks an entry in the table and dynamically configures the port with the right VLAN
- Benefits
  - less administration (more upfront) when users are added or move
  - centralized notification of unauthorized user

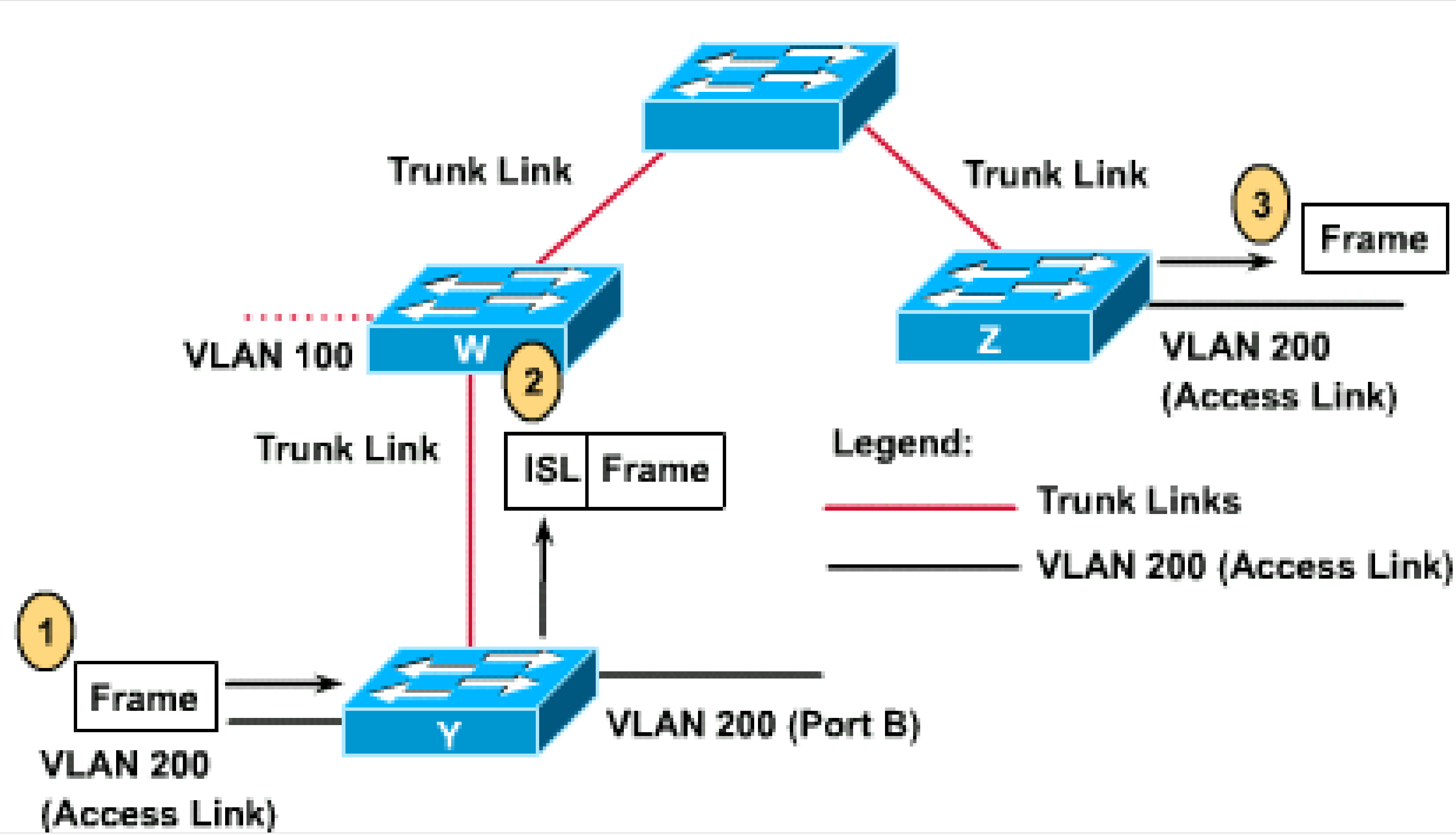
Port-Centric VLANs



Benefits of Port-Centric VLANs

- All nodes in the same VLAN are attached to the same router interface
- Makes management easier because...
  - Users are assigned by router port
  - VLANs are easy to admin.
  - provides increased security
  - packets do not “leak” into other domains

Access and Trunk Links



Access Links

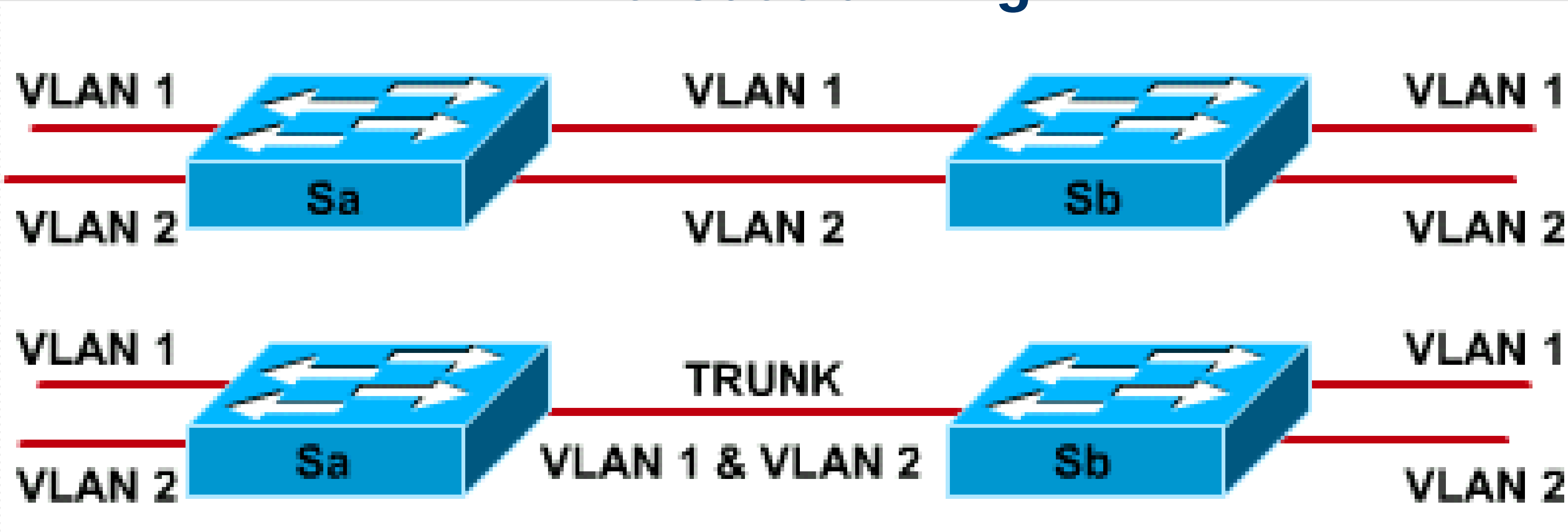
- An access link is a link on the switch that is a member of only one VLAN.
- This VLAN is referred to as the *native VLAN* of the port.
  - Any device that is attached to the port is completely unaware that a VLAN exists.

Trunk Links

- A trunk link is capable of supporting multiple VLANs.
- Trunk links are typically used to connect switches to other switches or routers.
- Switches support trunk links on both Fast Ethernet and Gigabit Ethernet ports.
- Access and trunk links exist, too

Trunk Links

Without trunking



With trunking

- **A trunk is a point-to-point link that supports several VLANs**
- **A trunk is to saves ports when creating a link between two devices implementing VLANs**

Trunk Links

- A trunk link does not belong to a specific VLAN.
  - Acts as a conduit for VLANs between switches and routers.
- The trunk link can be configured to transport all VLANs or to transport a limited number of VLANs.
- A trunk link may, however, have a native VLAN.
  - The native VLAN of the trunk is the VLAN that the trunk uses if the trunk link fails for any reason.

Configuration in Switch 29xx

- The following guidelines must be followed when configuring VLANs on Cisco 29xx switches:
  - The maximum number of VLANs is switch dependent.
  - 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.

VLAN Configuration

Step1: The steps necessary to create the VLAN. A VLAN name may also be configured, if necessary.

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

Step2: Assign the VLAN to one or more interfaces:

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

Adding a VLAN Example

cat2950#vlan database

cat2950(vlan)#vlan 9 name switchlab90

VLAN 9 added:

Name: switchlab90

cat2950(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

reset Abandon current changes and reread current database

cat2950(config)#interface fa 0/2
cat2950(config-if)# switchport access vlan 9

Verifying a VLAN

Switch# show vlan [*vlanid]*

```
cat2950#sh vlan

VLAN Name                             Status     Ports
---- -------------------------------- ---------- ------------
1   Default                          active         Fa0/1, Fa0/3
9     switchlab90                    active         Fa0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Deleting VLANs

- When a VLAN is deleted any ports assigned to that VLAN become inactive. The ports will, however, remain associated with the deleted VLAN until assigned to a new VLAN.

switch(vlan)# no vlan *vlanid* [name *vlan-name*]

```
cat2950(vlan)#no vlan 9
Deleting VLAN 9...
cat2950(vlan)#exit
APPLY completed.
Exiting....
cat2950#
```

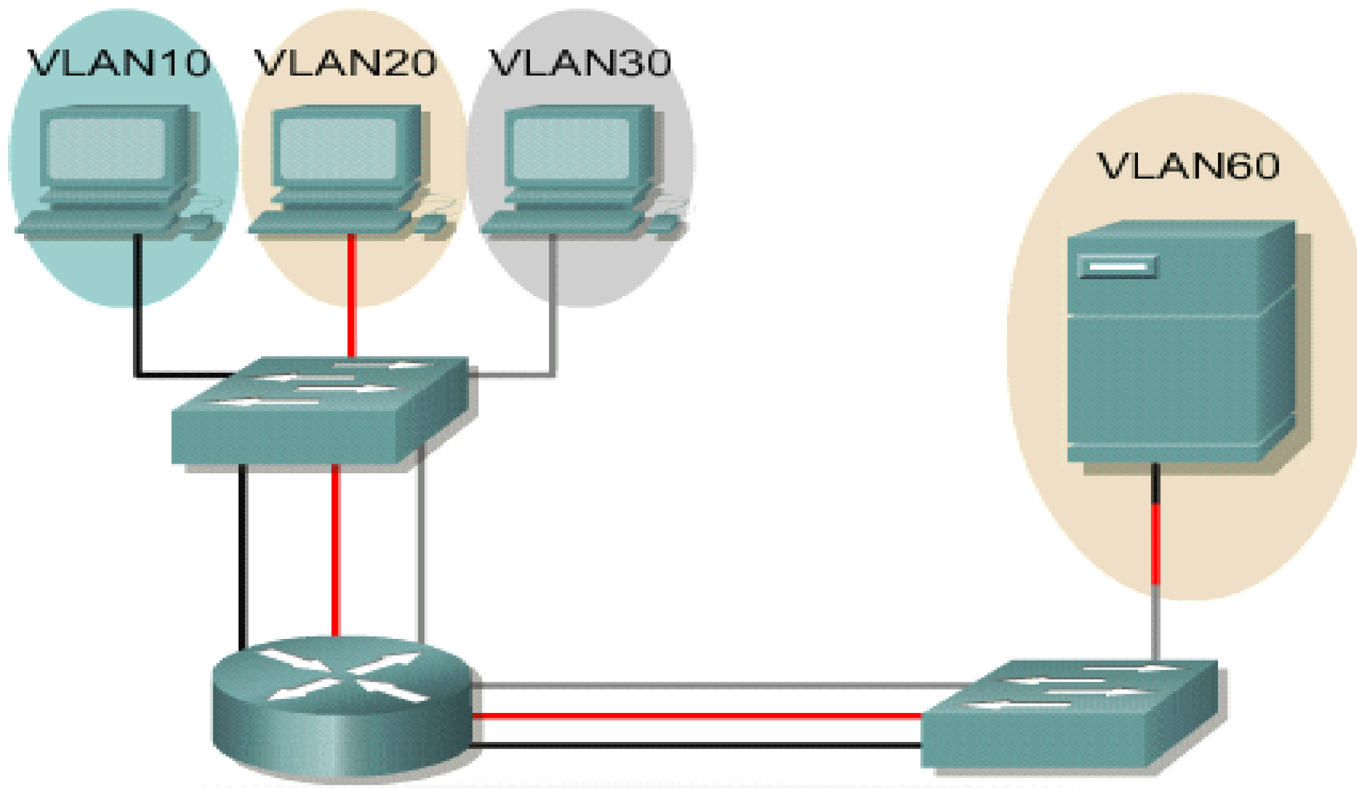
Table of Contents

Routing Between VLANs

Multiple Links

FIGURES

1
2
3



The router supports one VLAN per interface.

Routing Between VLANs

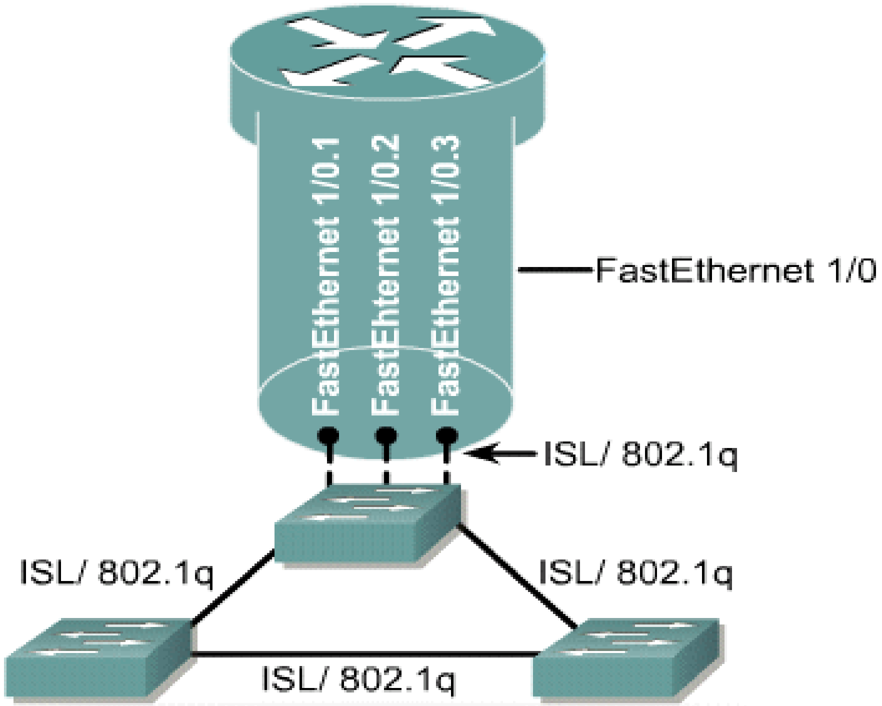
Trunk-Connected Routers

FIGURES

1

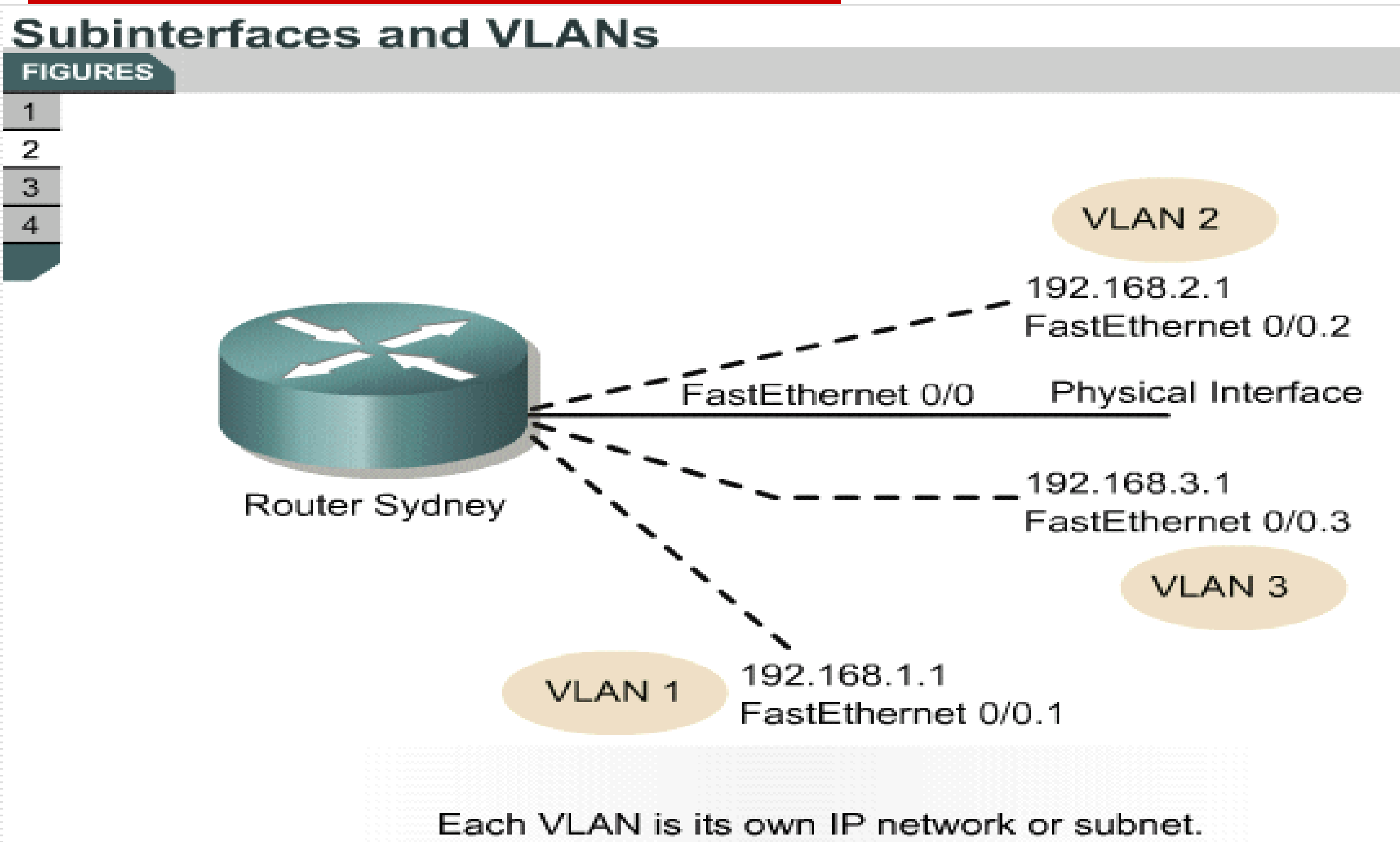
2

3



An ISL or 802.1q-enabled interface on the router connects to a trunk port on the switch.

Subinterfaces



Configuring Inter-VLAN Routing

Step1: Identify the interface.

Router(config)#interface fastethernet *port-number. subinterface-number*

Step2: Define the VLAN encapsulation.

Router(config-if)#encapsulation dot1q *vlan-number*

Step3: Assign an IP address to the interface

Router(config-if)#ip address *ip-address subnet-mask*

Configuring Inter-VLAN Routing

- Sydney(config)#interface FastEthernet 0/0
- Sydney(config-if)#full duplex
- Sydney(config-if)#no shut

- Sydney(config-if)#interface FastEthernet 0/0.1
- Sydney(config-subif)#encapsulation 802.1q 1
- Sydney(config-subif)#ip address 192.168.1.1 255.255.255.0

- Sydney(config-if)#interface FastEthernet 0/0.2
- Sydney(config-subif)#encapsulation 802.1q 20
- Sydney(config-subif)#ip address 192.168.2.1 255.255.255.0

- Sydney(config-if)#interface FastEthernet 0/0.3
- Sydney(config-subif)#encapsulation 802.1q 30
- Sydney(config-subif)#ip address 192.168.3.1 255.255.255.0

谢 谢！