Ethernet Switching

DOMAIN 2.0

MODULE 9

Ethernet Switching Topics

Ethernet Basics

Switching Overview

VLANs

VLAN Trunking

VLAN Routing

Contention Management

Switchport Configuration

Ethernet Basics

What is Ethernet?

Most common Layer 2 wired LAN protocol

Uses source and destination MAC addresses

Can be carried on twisted pair, coax, or fiber optic cable

Uses CSMA/CD for contention management

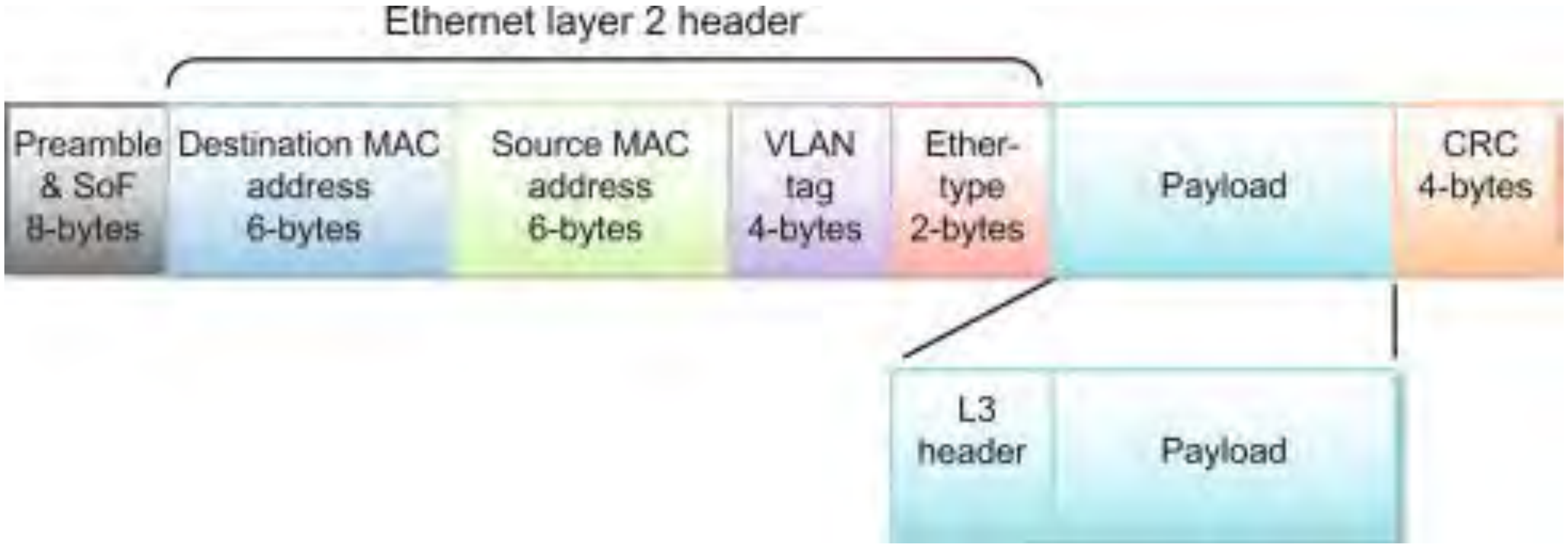
Minimum length of 64 bytes

Default maximum transmission unit size (MTU) of 1500 bytes

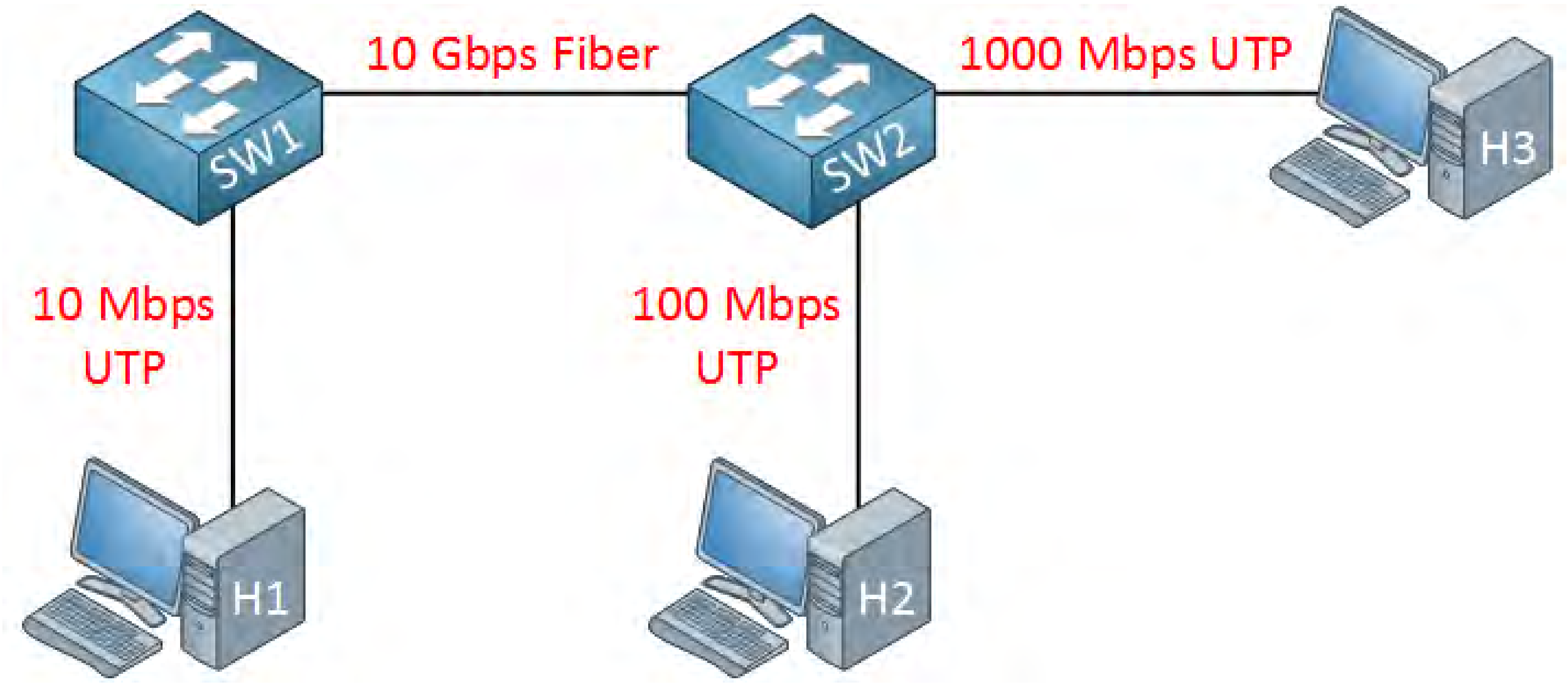
Can be modified up to 9000 bytes (jumbo frames) for special purpose

- Better performance for an iSCSI SAN
- Requires switches and NICs that support jumbo frames

Ethernet Header



Ethernet Example



Switching Overview

What is a Switch?

Layer 2 device that makes forwarding decisions based on Layer 2 (MAC) addresses

Learns the MAC address of devices plugged into it

Builds a temporary table (in memory) associating MAC addresses with switchports

Has high port density (many ports)

Some models provide Power-over-Ethernet (PoE) on ports for phones, WAPs, cameras, etc.

MAC Address Table

Built dynamically on a switch

- Whenever devices transmit, the switch notes the source MAC and adds it to the table
- Table is stored in the switch's RAM
- If a hub, uplink, or trunk link is attached to a port, that port will have multiple MAC addresses associated with it

Displays the current mapping of MAC addresses to switchports

Switch uses it to make forwarding decisions at Layer 2

If the destination MAC address is not in the table:

- The switch floods the frame out all ports (except the port it came in on)

Can be cleared manually or by rebooting the switch

Do not mistake a MAC address table for an arp cache!

- A MAC table maps source MAC addresses to switchports
- An ARP cache maps MAC addresses to destination IP addresses

Switching Modes

Store and Forward

- Buffer the entire frame
- Run a CRC check on frame to make sure it’s not damaged
- Discard frame if damaged
- Forward to destination if ok

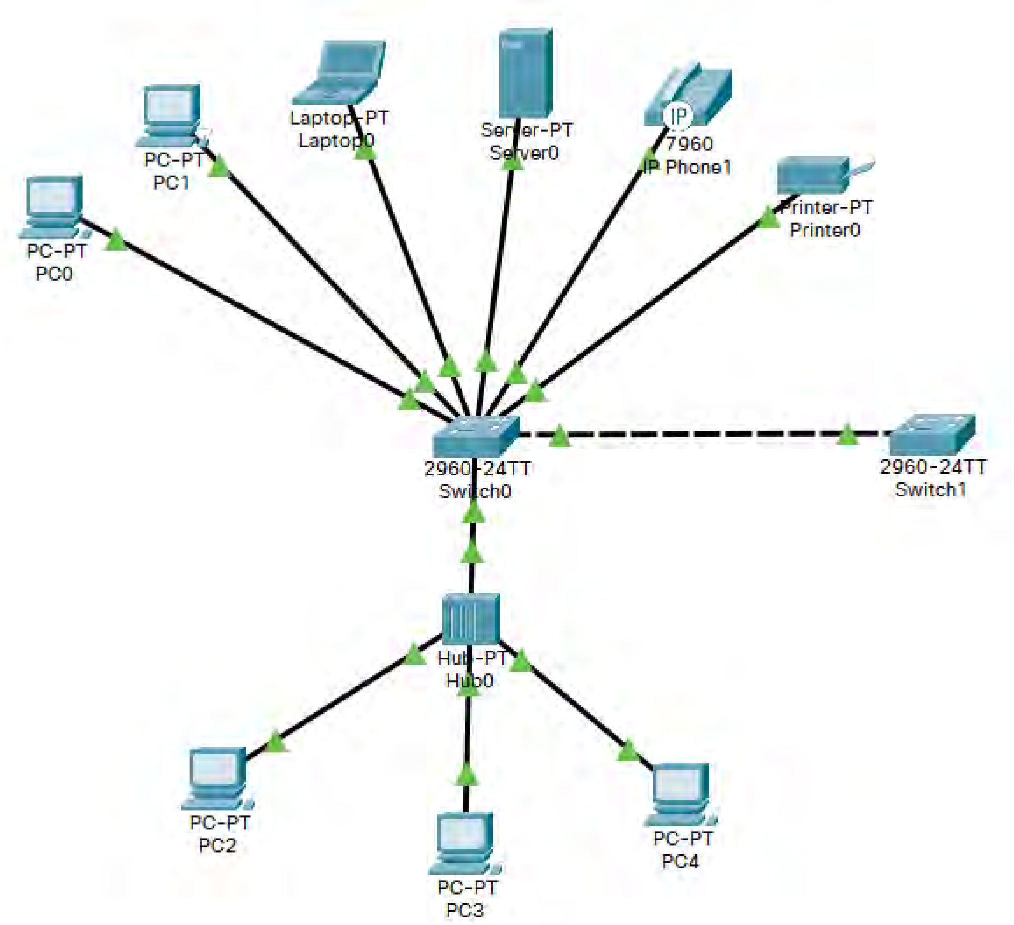
Fragment Free

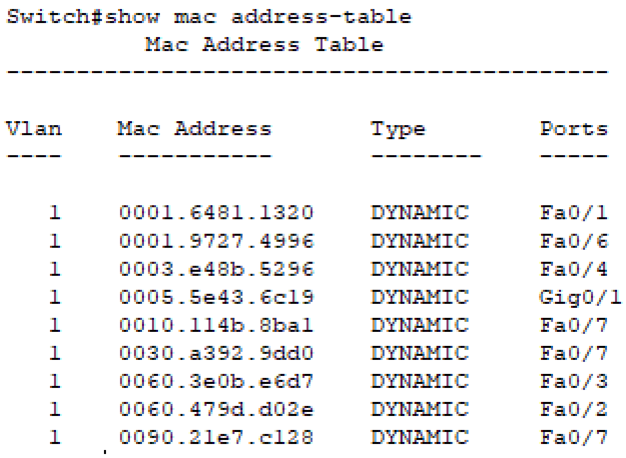
- Validate the first 64 bytes of the frame as it comes in
- The first 64 bytes is the most likely time a collision will occur
- If a collision occurs, the colliding nodes will stop transmitting
- But you still have a runt frame on the segment
- If first 64 bytes are ok, forward as the rest of the frame comes into the switch

Cut-through

- Do not check the frame at all
- Immediately start to forward as it comes in
- Trade accuracy for performance

MAC Address Table Examples

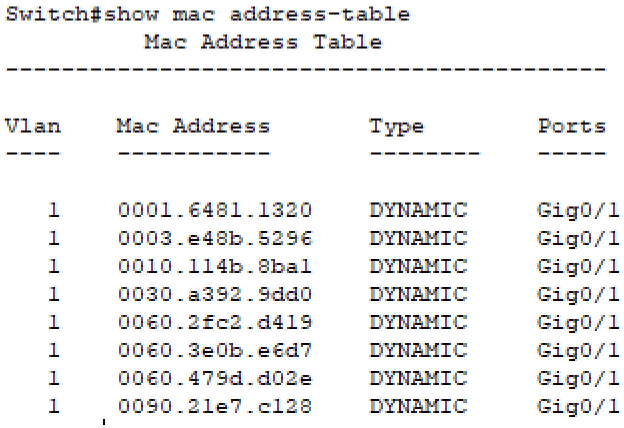




```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.6481.1320    DYNAMIC     Fa0/1
   1    0001.9727.4996    DYNAMIC     Fa0/6
   1    0003.e48b.5296    DYNAMIC     Fa0/4
   1    0005.5e43.6c19    DYNAMIC     Gig0/1
   1    0010.114b.8ba1    DYNAMIC     Fa0/7
   1    0030.a392.9dd0    DYNAMIC     Fa0/7
   1    0060.3e0b.e6d7    DYNAMIC     Fa0/3
   1    0060.479d.d02e    DYNAMIC     Fa0/2
   1    0090.21e7.c128    DYNAMIC     Fa0/7
```



```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.6481.1320    DYNAMIC     Gig0/1
   1    0003.e48b.5296    DYNAMIC     Gig0/1
   1    0010.114b.8ba1    DYNAMIC     Gig0/1
   1    0030.a392.9dd0    DYNAMIC     Gig0/1
   1    0060.2fc2.d419    DYNAMIC     Gig0/1
   1    0060.3e0b.e6d7    DYNAMIC     Gig0/1
   1    0060.479d.d02e    DYNAMIC     Gig0/1
   1    0090.21e7.c128    DYNAMIC     Gig0/1
```

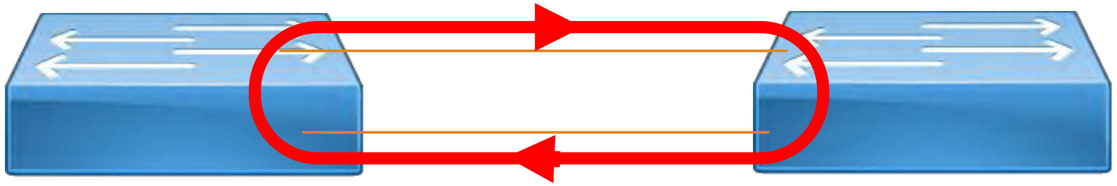
Switching Loop

Occurs on a network when there is a redundant link between switches

Switches by their nature flood broadcasts, multicasts, and unknown unicasts out all ports (except the port it was received on)

Loops cause broadcast storms:

1. A host sends a Layer 2 broadcast (such as an ARP or DHCP discover)
2. The switch repeats the broadcast out all other ports, including the redundant link to the other switch
3. The other switch in turn repeats the broadcast out all its ports, including the first link to the first switch
4. The process repeats endlessly



Spanning Tree Protocol (STP)

Important

IEEE 802.1d

Used to eliminate switching loops

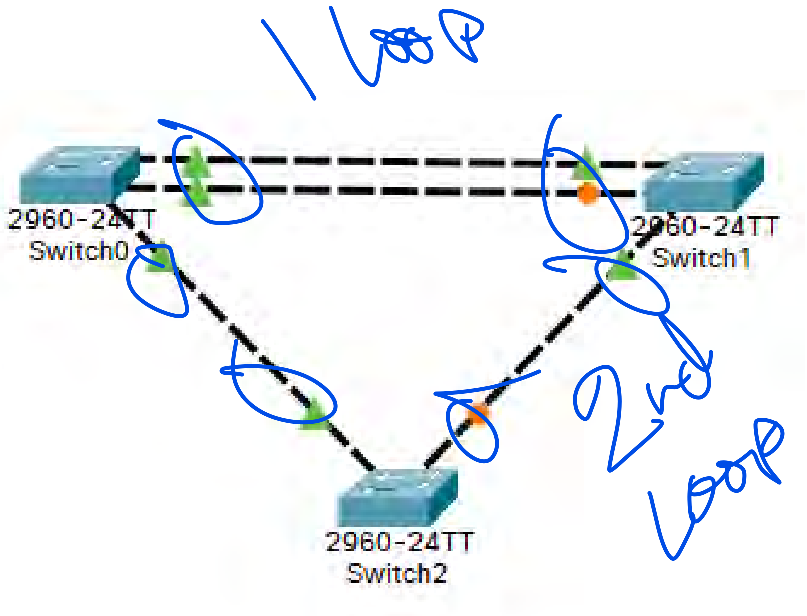
Switches self-organize to identify redundant links
- Switches elect a “Root Bridge” among them as a focal point
- Switch with the lowest Bridge Priority and/or MAC address wins “election”

The Root sends out Root Bridge Protocol Data Units (Root BPDUs)
- Root BPDUs are forwarded by all other switches out all other ports

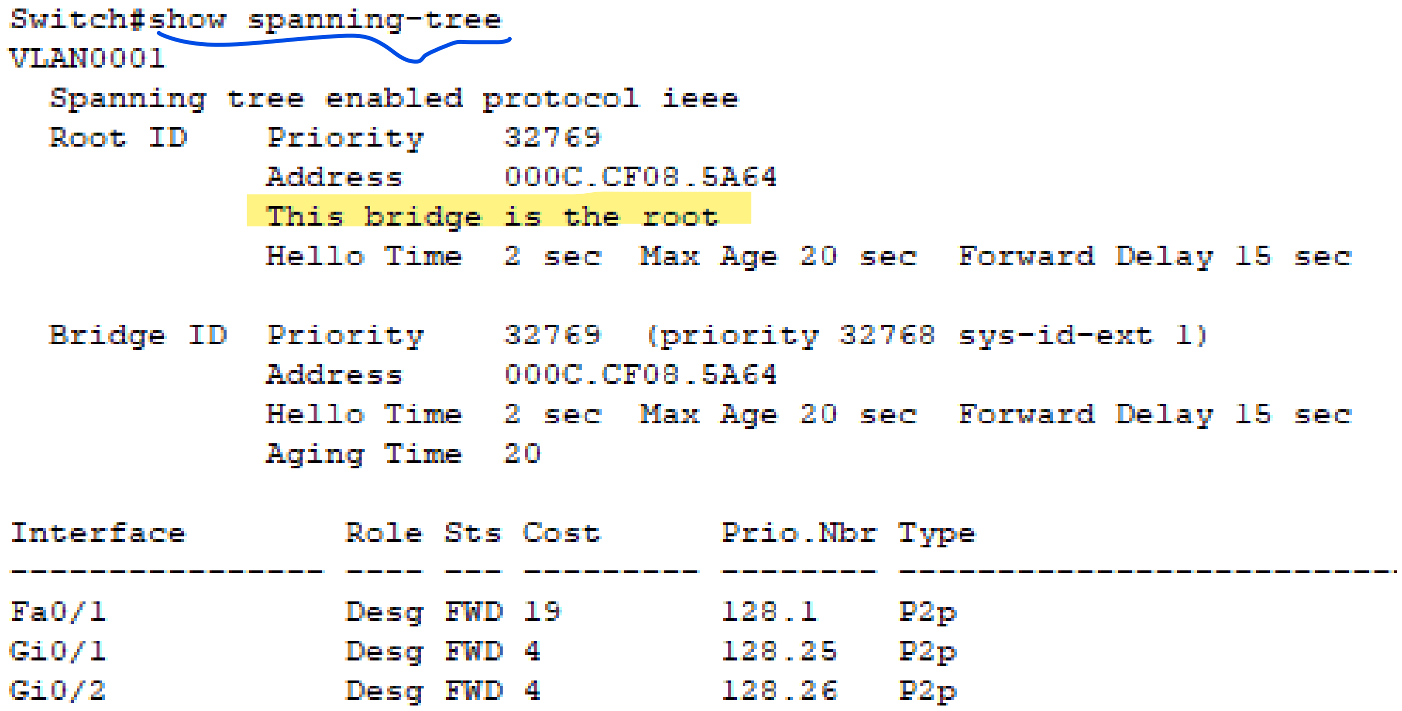
If a switch receives the same Root BPDU from two or more different ports, it knows there is a redundancy
- Redundant links are put in a blocking state
- Link speed, port number, and priority can all be used to determine which port will be blocked
- If the active link goes down, the blocked port takes over and begins forwarding traffic

Replaced with newer/better performing versions (Rapid STP, Per-VLAN Spanning Tree (PVST), PVST+)

STP Example



Switch0



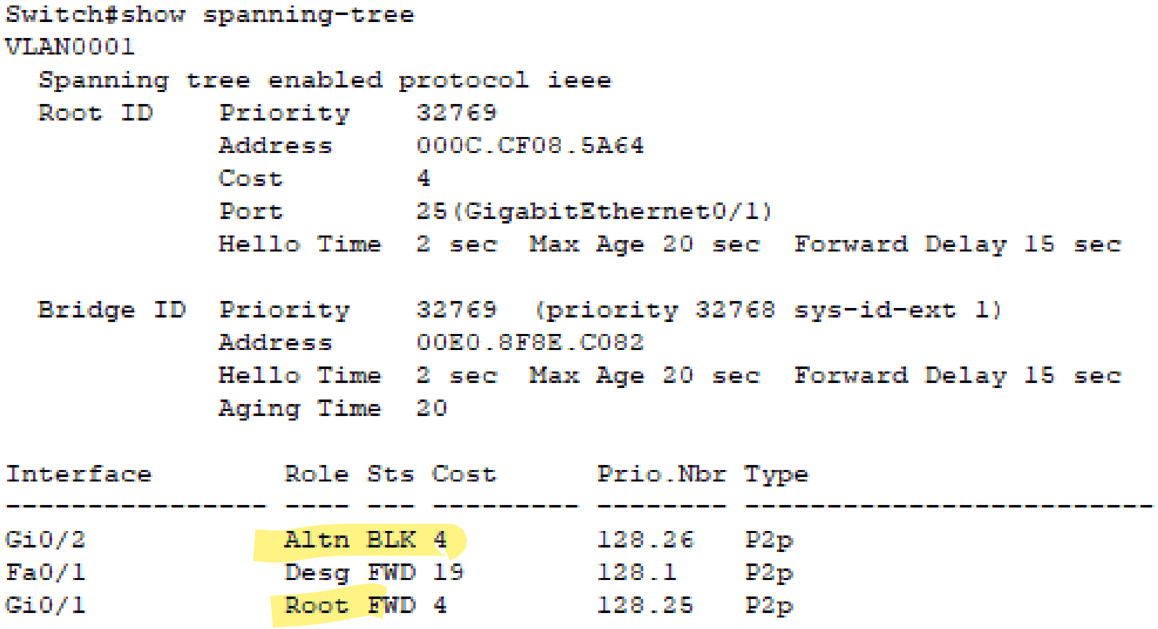
```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000C.CF08.5A64
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000C.CF08.5A64
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

STP Example (cont'd)

Switch1

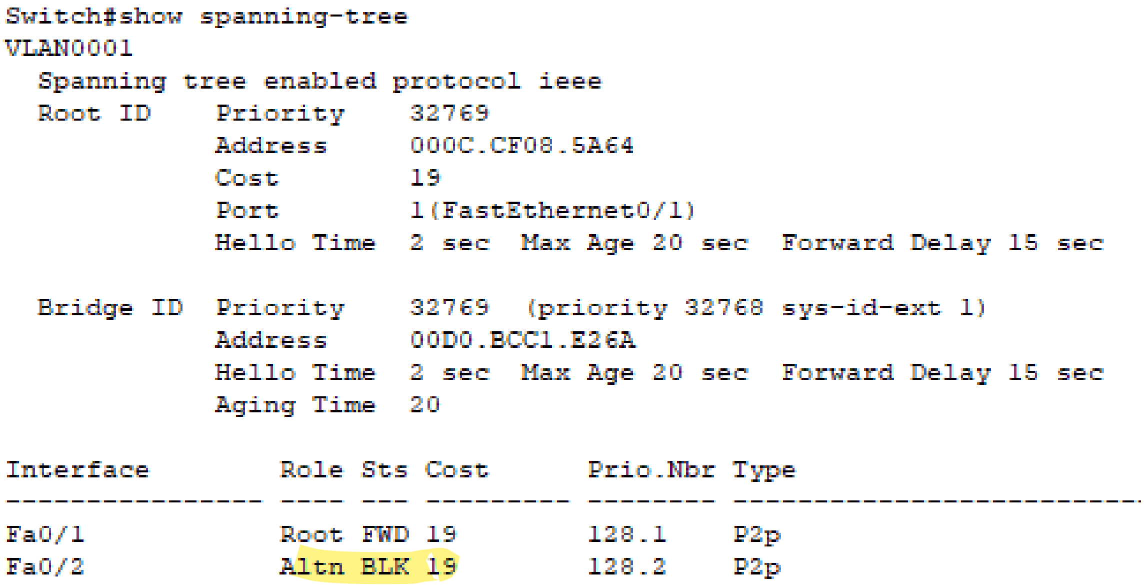


```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000C.CF08.5A64
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.8F8E.C082
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Gi0/2            Altn BLK 4         128.26   P2p
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/1            Root FWD 4         128.25   P2p
```

Switch2



```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000C.CF08.5A64
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.BCC1.E26A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
```

VLANs

Virtual Local Area Network (VLAN)

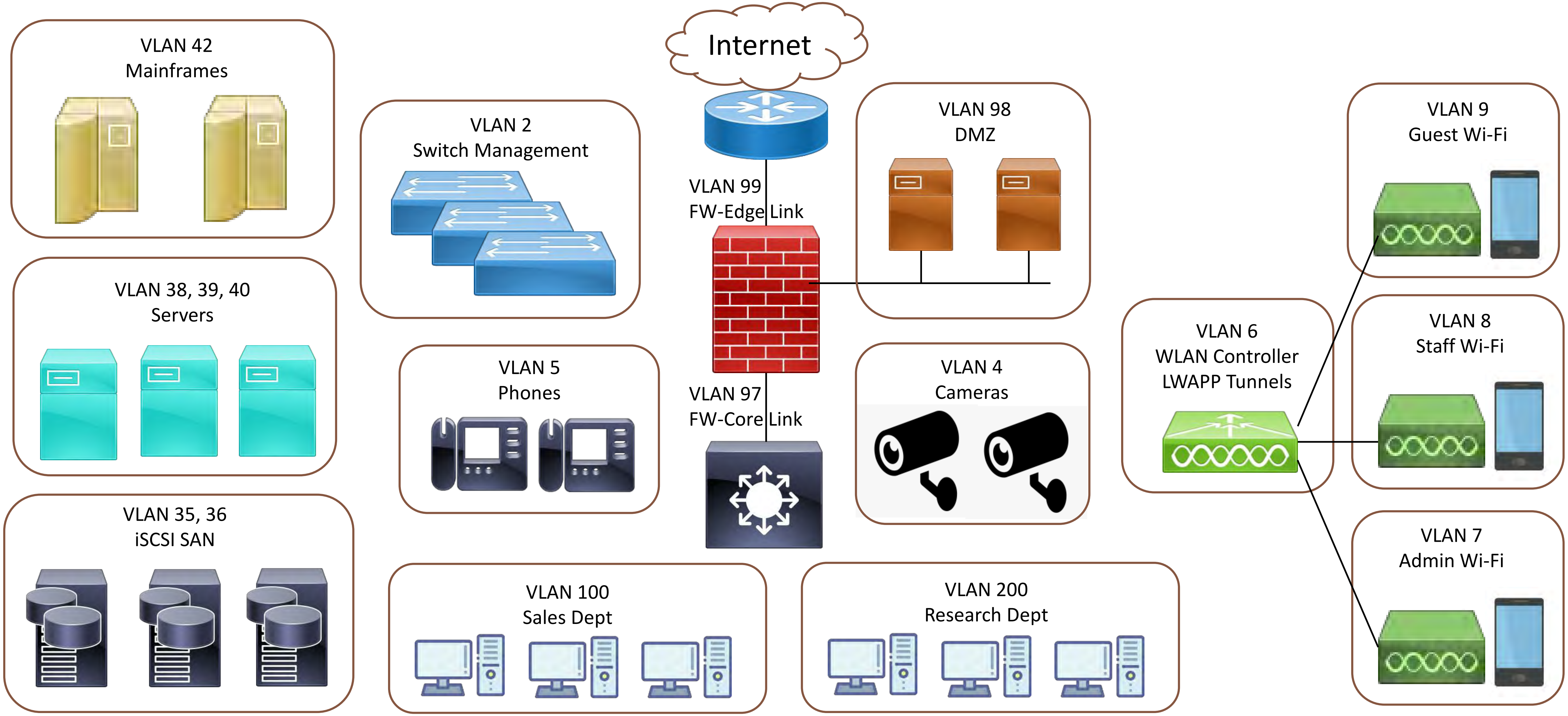
Grouping of switch ports to create a separate network segment

- Logically divides a switch into multiple switches
- Typically used to separate departments, rooms, device types, or security levels
- Traffic stays limited to within the VLAN
- Each VLAN is a broadcast domain

Each VLAN should be assigned its own subnet ID

- Nodes in the VLAN should be configured for that subnet
- VLANs cannot talk to each other unless traffic is routed between VLANs by a router

Common VLAN Usage Example



Configuring VLANs

You create the VLAN on the switch, then add physical ports to the VLAN

- The switchports in one VLAN do NOT need to be physically near each other
- You could have switchports in other rooms or buildings on the LAN belong to the same VLAN
- You can easily change a port's VLAN membership

Switch ports generally only belong to one VLAN at a time

- Exception: when an IP phone connects to the network through a PC
- Switch port has one VLAN for the phone, one VLAN for the PC (data)

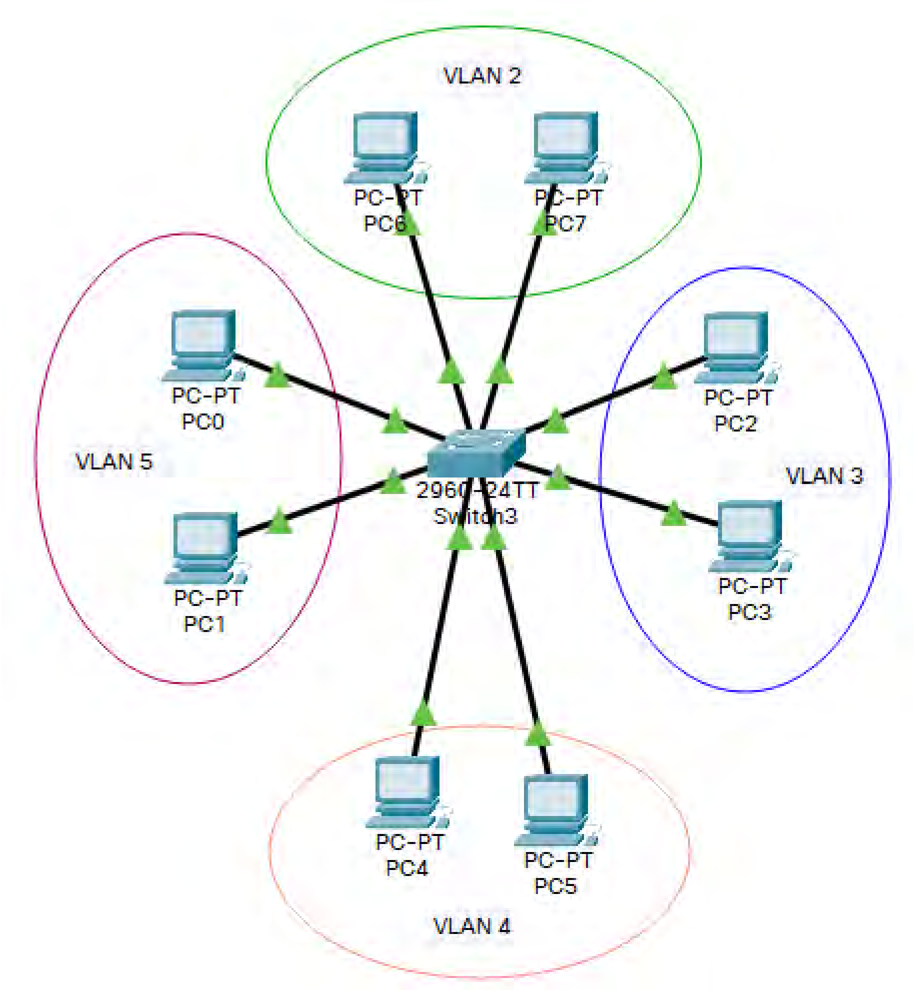
Initially, all switch ports are in the same default VLAN (usually VLAN 1)

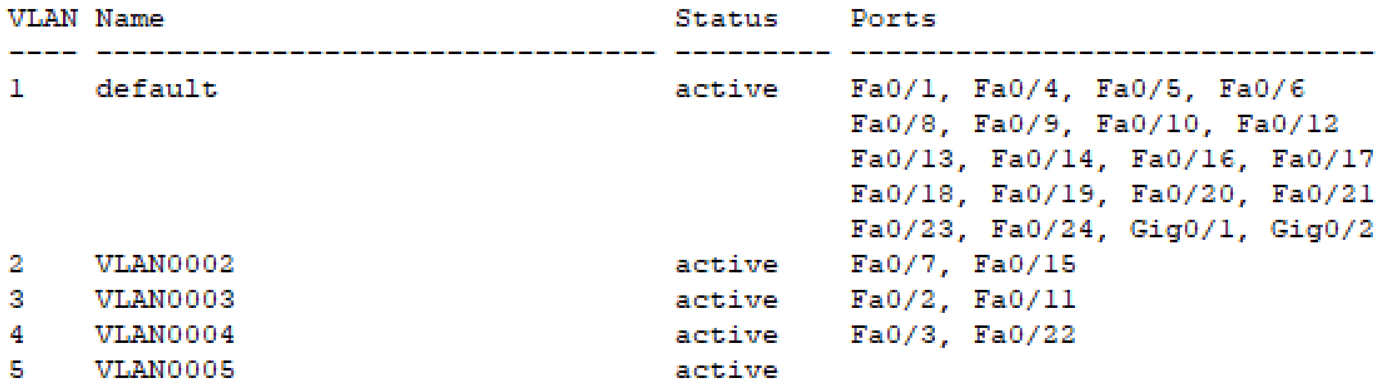
If you configure a port to join a particular VLAN and then unjoin the port, it reverts back to the default VLAN

If you delete the VLAN without unjoining the ports from it, those ports become "orphaned" and (usually) go into a blocking state

- They stop forwarding traffic

VLAN Example





```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
2    VLAN0002                         active    Fa0/7, Fa0/15
3    VLAN0003                         active    Fa0/2, Fa0/11
4    VLAN0004                         active    Fa0/3, Fa0/22
5    VLAN0005                         active
```

VLAN Trunking

VLAN Trunking

Used to extend VLANs to other switches

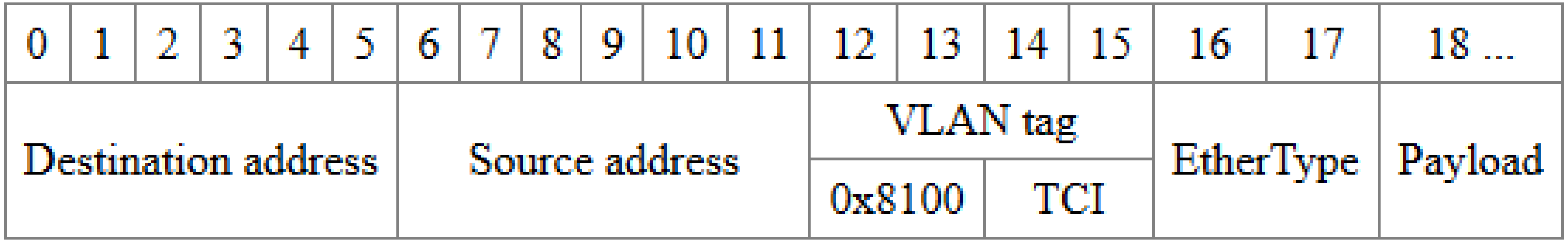
- Trunk links carry traffic from all VLANs from one switch to another

A broadcast in a VLAN will extend across the trunk link to all switches and their ports that use that VLAN

IEEE 802.1Q (“dot 1 q”) is the most common VLAN trunking protocol

802.1Q VLAN frames are distinguished from ordinary Ethernet frames

- 4-byte VLAN tag is inserted into the Ethernet header



<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18 ...</td></tr>
<tr><td colspan="6" rowspan="2">Destination address</td><td colspan="6" rowspan="2">Source address</td><td colspan="4">VLAN tag</td><td colspan="2" rowspan="2">EtherType</td><td rowspan="2">Payload</td></tr>
<tr><td colspan="2">0x8100</td><td colspan="2">TCI</td></tr>
</table>

Trunk Link vs Uplink

Do not confuse the two!

An uplink is just a cable connecting two switches

- Used to add more devices to a single switch port
- All devices belong to the same VLAN
- Requires no special configuration

A trunk link is an uplink that has been configured to carry traffic from all VLANs from one switch to the next

- A trunk port tags outgoing frames with their respective VLAN ID
- Trunk links extend VLANs across multiple switches
- Requires ports on both sides of the link to be configured as trunk ports

VLAN Tagging

A tag inserted into the Ethernet header identifies which VLAN a particular frame belongs to

- The sending switch applies the VLAN tag to the frame before transmitting it
- The receiving switch then knows which VLAN that frame belongs to
- Tags are only meaningful on a trunk link

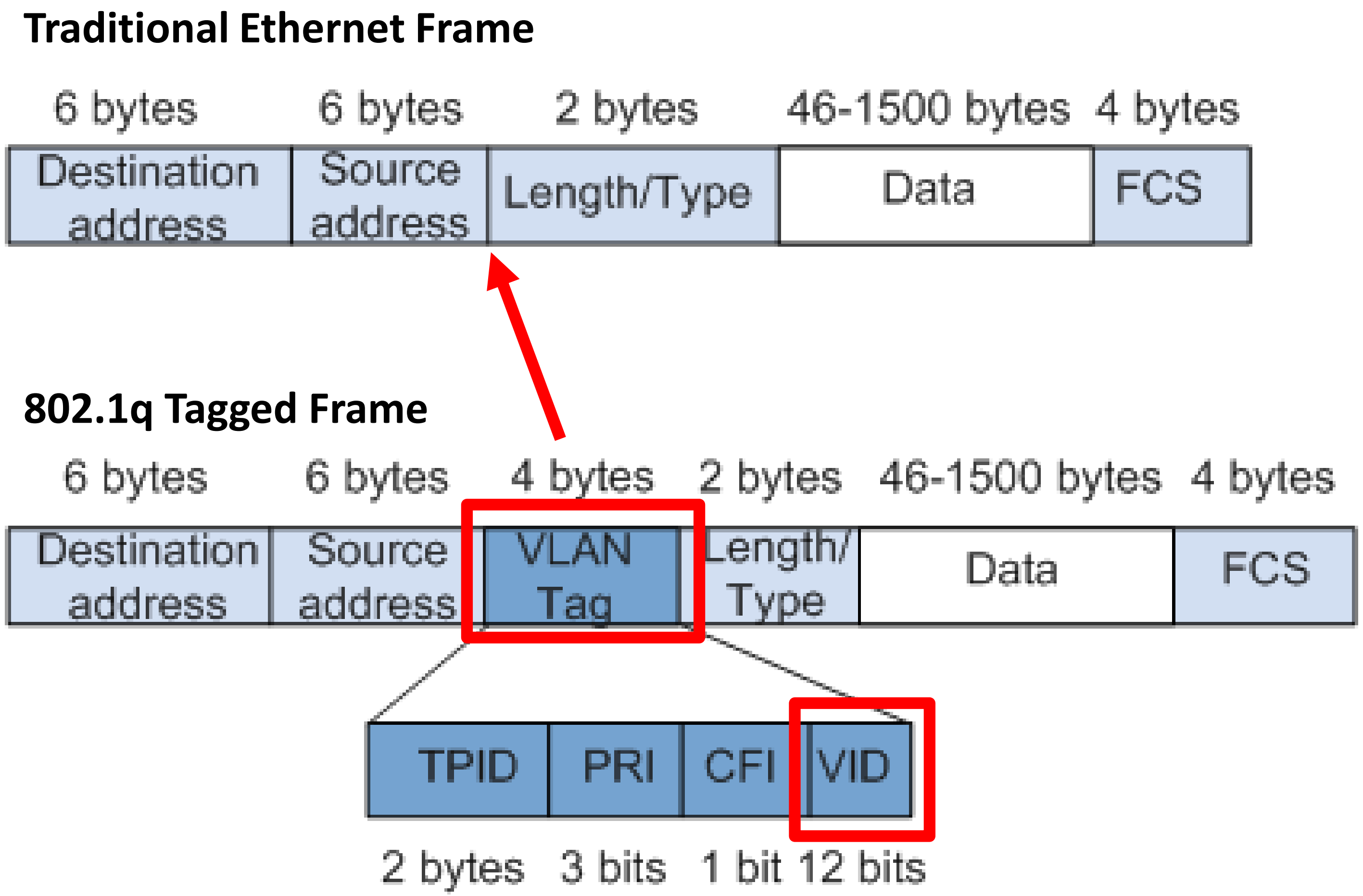
Ports that computers, phones, and end devices are plugged into do not tag their frames

- The end devices have no knowledge of the VLAN
- Ports meant for end devices are configured as “access” ports
- Access ports do not use VLAN tags

Default VLAN 1 traffic is untagged (per 802.1q)

- This makes it possible to connect the two switches using a multi-access device such as a hub
- The hub (and any other devices plugged into it) treat the switch traffic as normal Ethernet
- They ignore any VLAN tagging

VLAN Tagging in Ethernet Header



Traditional Ethernet Frame

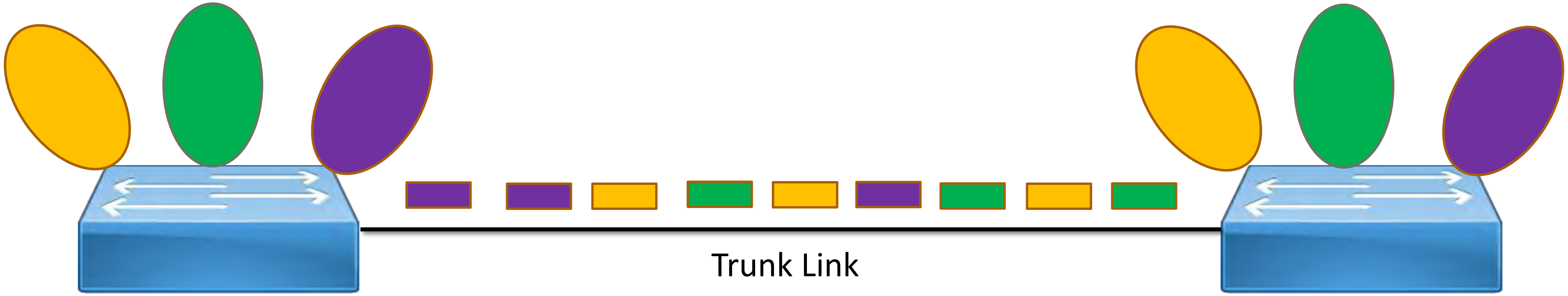
6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes
Destination address	Source address	Length/Type	Data	FCS

802.1q Tagged Frame

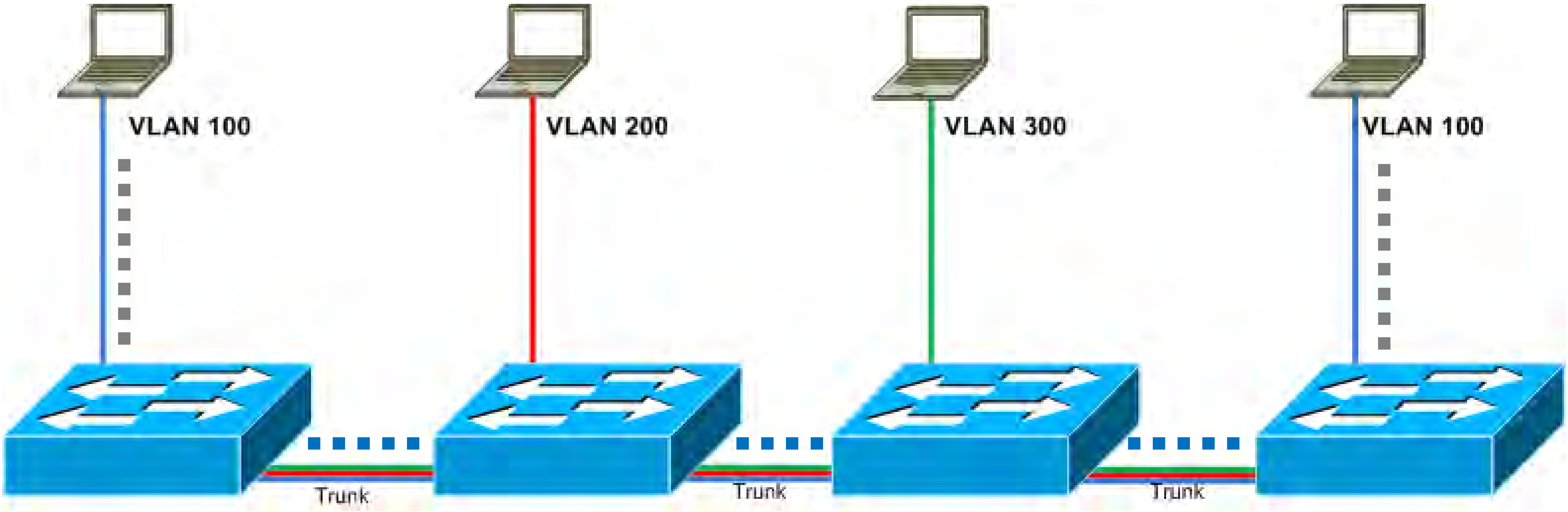
6 bytes	6 bytes	4 bytes	2 bytes	46-1500 bytes	4 bytes
Destination address	Source address	VLAN Tag	Length/ Type	Data	FCS

TPID	PRI	CFI	VID
2 bytes	3 bits	1 bit	12 bits

VLAN Tagging Example



VLAN Tagging Example #2



VLAN Routing

Why Route Between VLANs?

Ports and devices belonging to one VLAN cannot communicate with ports and devices belonging to another VLAN

Sometimes you will want to allow devices on one VLAN to communicate with devices on another VLAN

- You have placed servers or other popular destinations together in a single VLAN
- As administrator, you want to be able to remotely manage devices in other VLANs

How to Route Between VLANs

You must use a router to move traffic between VLANs

Well-designed VLANs include these characteristics:

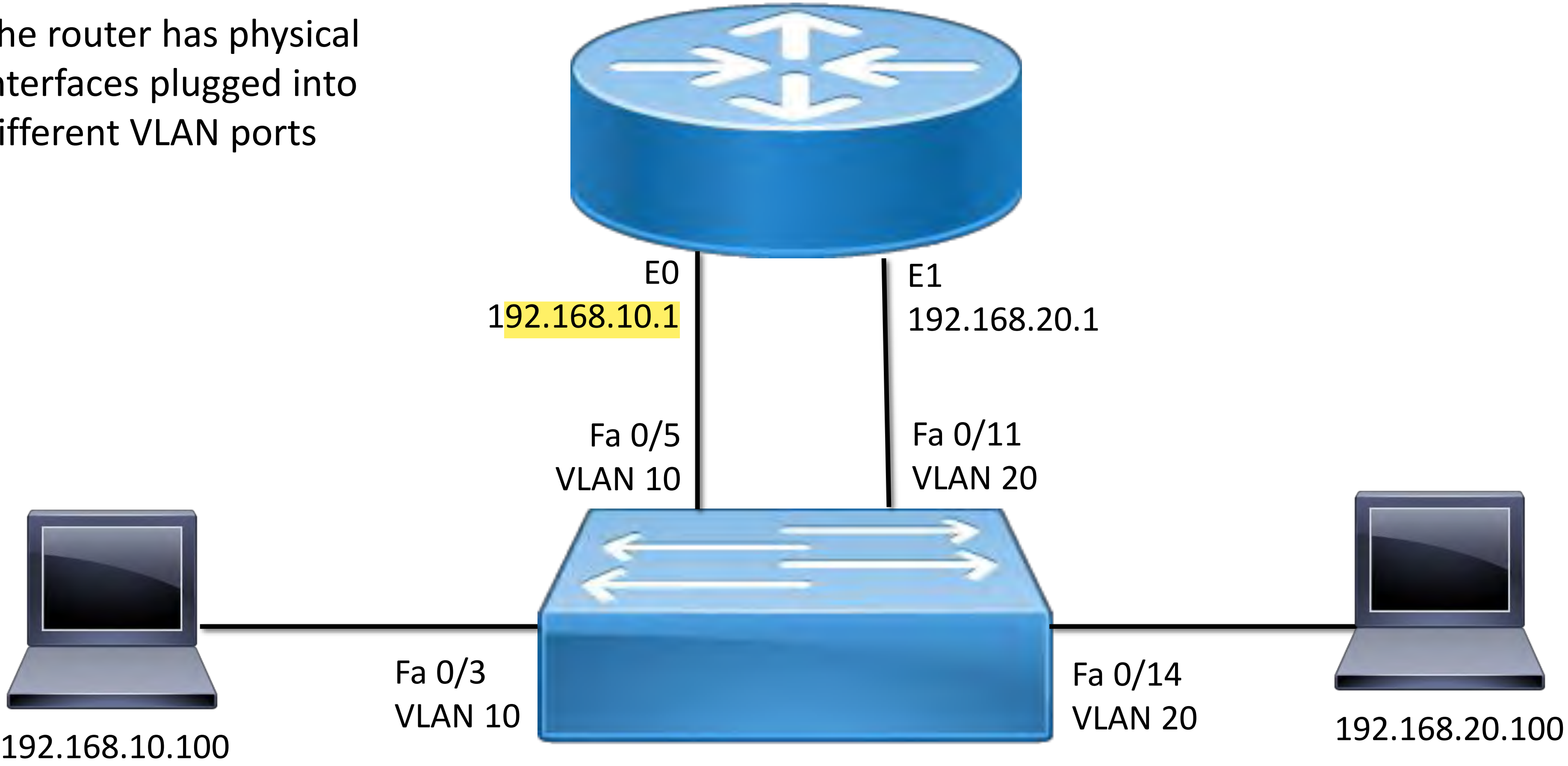
- Each VLAN has its own subnet ID
- All devices in a VLAN belong to the same subnet

VLAN routing can be done the following ways:

- The router has physical connections to each VLAN
- The router interface is configured as a trunk port, then divided into sub-interfaces (one for each VLAN)
- The router is actually a software process inside a multilayer switch
  - You need to create a VLAN interface for each VLAN that needs to be routed
  - Each VLAN interface must be configured with an IP address, as the default gateway for that VLAN
  - All devices on the VLAN must be configured to use that VLAN interface as their default gateway

The Worst Way to Route Between VLANs

The router has physical interfaces plugged into different VLAN ports



Router On A Stick

Some routers allow a port to be configured as a VLAN trunk link

- This configuration is known as "router on a stick"
- On Cisco routers, the port must be Fast Ethernet speed or higher

The physical interface is "divided" into multiple logical sub-interfaces

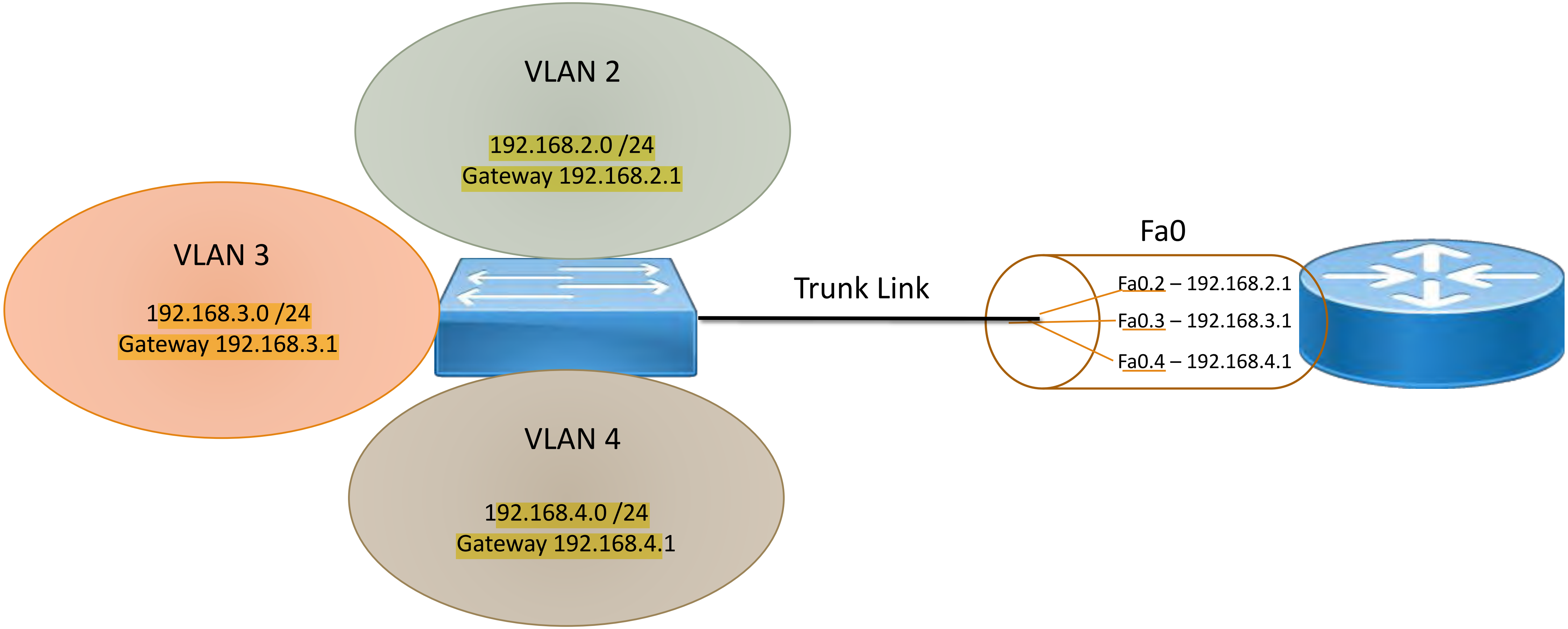
- The physical interface should not be given an IP address or VLAN ID
- The sub-interfaces are configured with the appropriate IP address and VLAN ID
- Each sub-interface becomes the default gateway for that VLAN
- It is common to name the sub-interface after its associated VLAN ID

The switch sends tagged traffic down to the trunk link to the router

The router reads the destination IP address

- It routes the frame to the correct sub-interface
  - It overwrites the Layer 2 header to include the correct destination VLAN
- The frame is sent back to the switch on the same trunk link
  - The switch forwards the frame out the correct port on the new VLAN

Router on a Stick Example



Best Way to Route Between VLANs

A multilayer switch is configured with logical VLAN interfaces

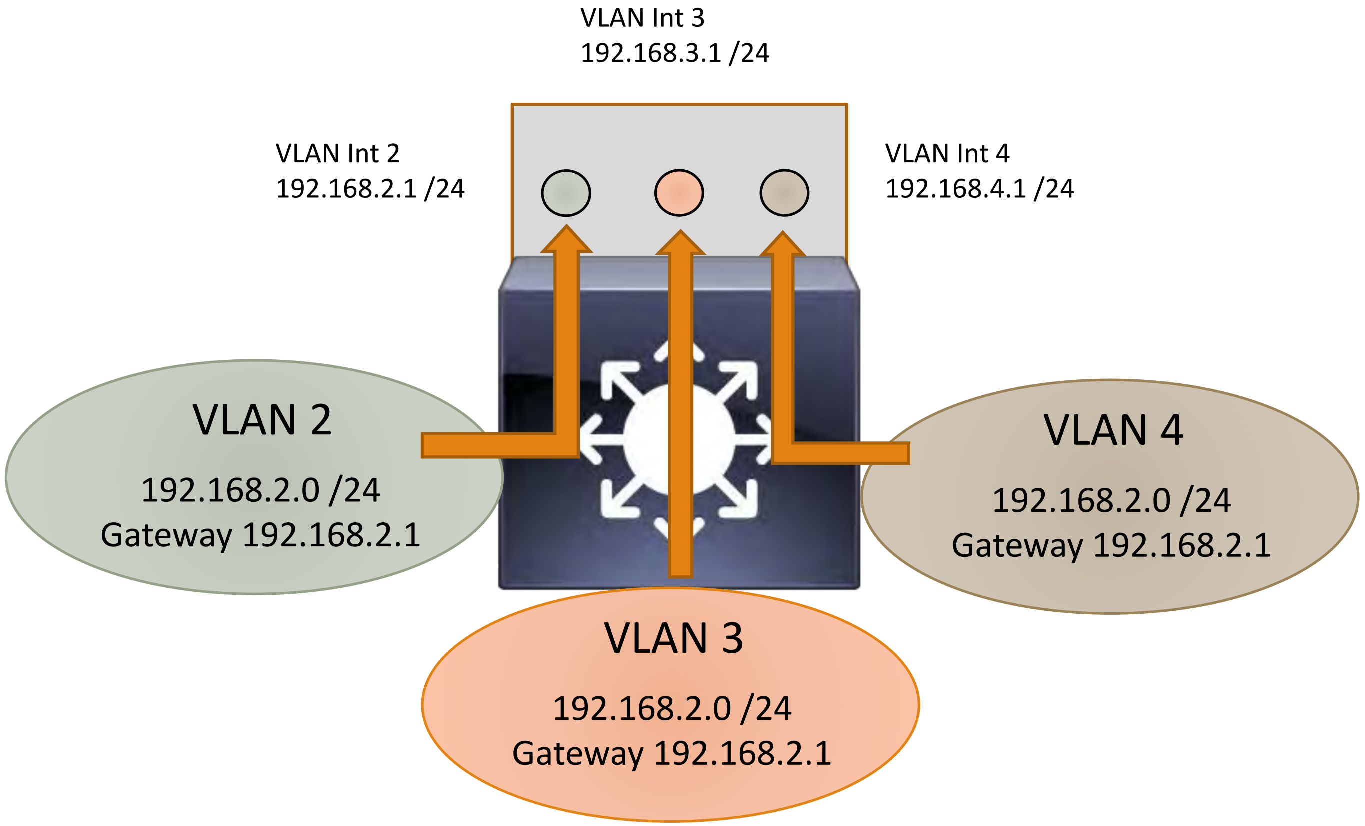
- VLAN interfaces are configured with the VLAN ID and IP address

The VLAN interfaces route between VLANs on the backplane of the switch

VLAN interfaces stay "up" so long as at least one VLAN member port is active

A trunk link can serve as the member port to keep all VLAN interfaces up

VLAN interfaces can only route between Ethernet segments



Contention Management

What is Network Contention?

Multiple nodes try to use the network at the same time

Contention leads to collisions

Contention needs to be managed

CSMA/CD

Carrier Sense Multiple Access with Collision Detection

The LAN access method used in Ethernet networks

When a device wants to gain access to the network, it checks to see if the network is free

- Network is not free, the device waits a random amount of time before retrying
- Network is free and two devices access the line at exactly the same time, their signals collide and both stop and wait a random amount of time before retrying
- When the line is free that last transmission is resent

Collision Domain

A network segment where collisions can occur:

- Hub
- Coax bus

A *collision* occurs when two devices send a frame at the same time on the same network segment

If frames collide both devices must send the frames again

A collision is the most common cause of runt frames being on the segment

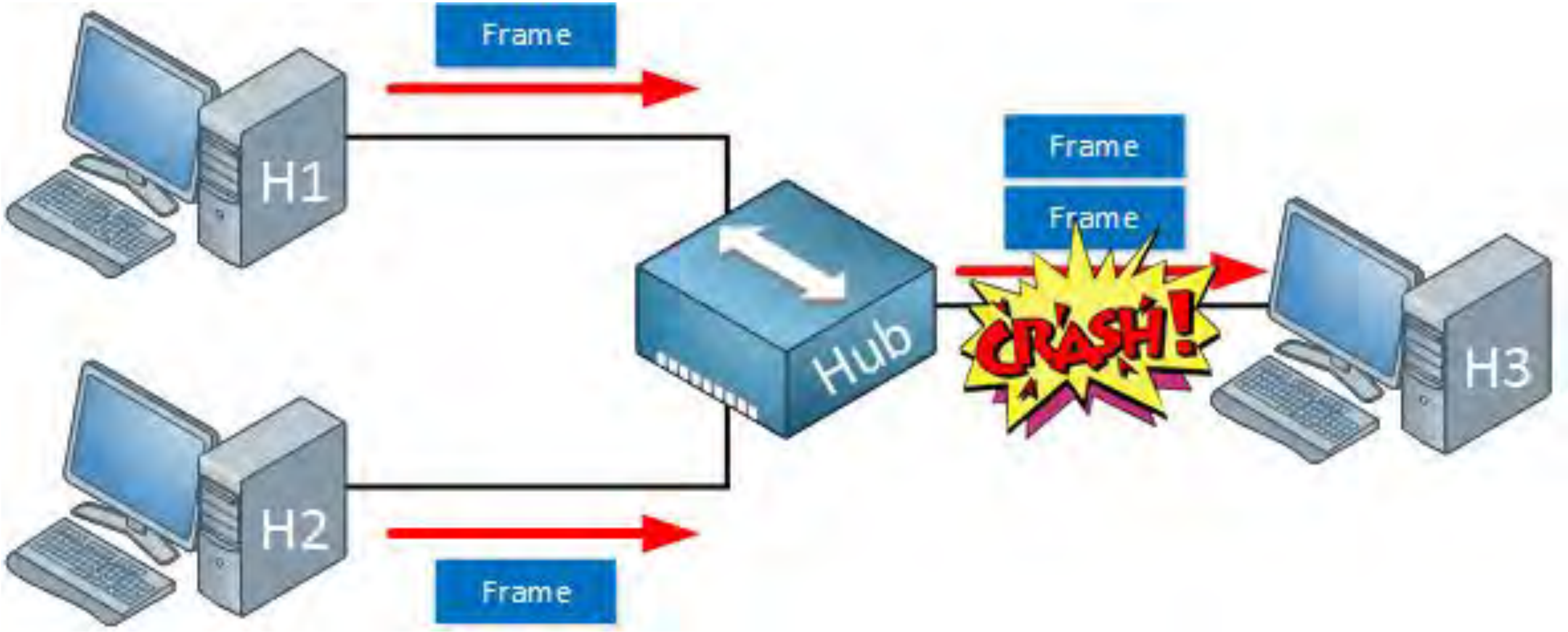
Partial frames might inadvertently be “attached” to another frame, causing a “jumbo” frame

- Do not mistake for deliberately configured 9000 byte jumbo frames used in SANs

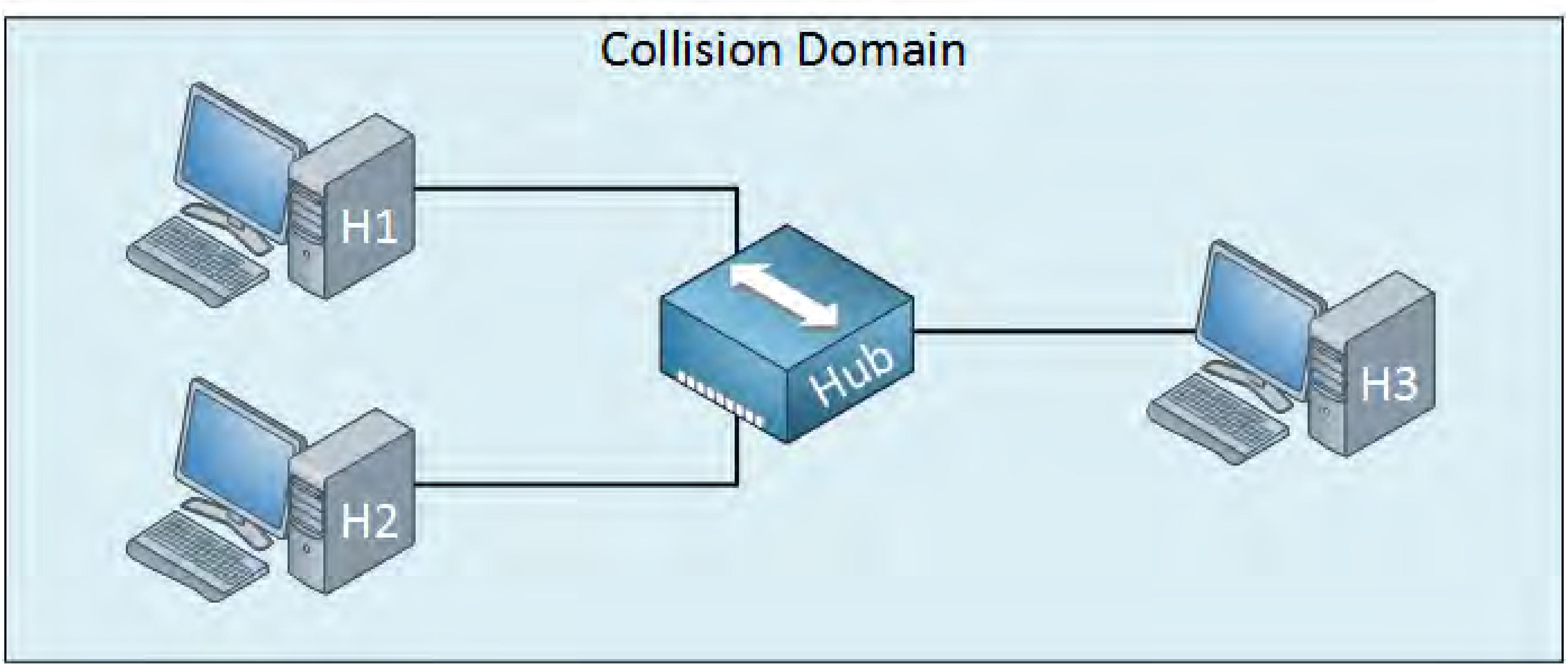
Very inefficient on a contention-based network like Ethernet

Switch ports divide the network segment into collision domains

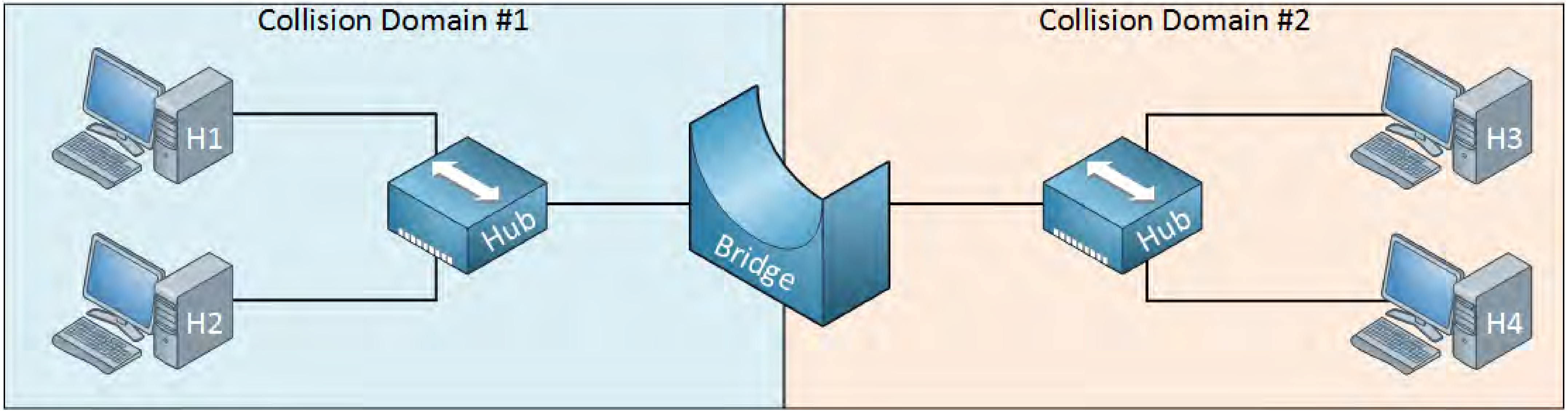
Collision Example



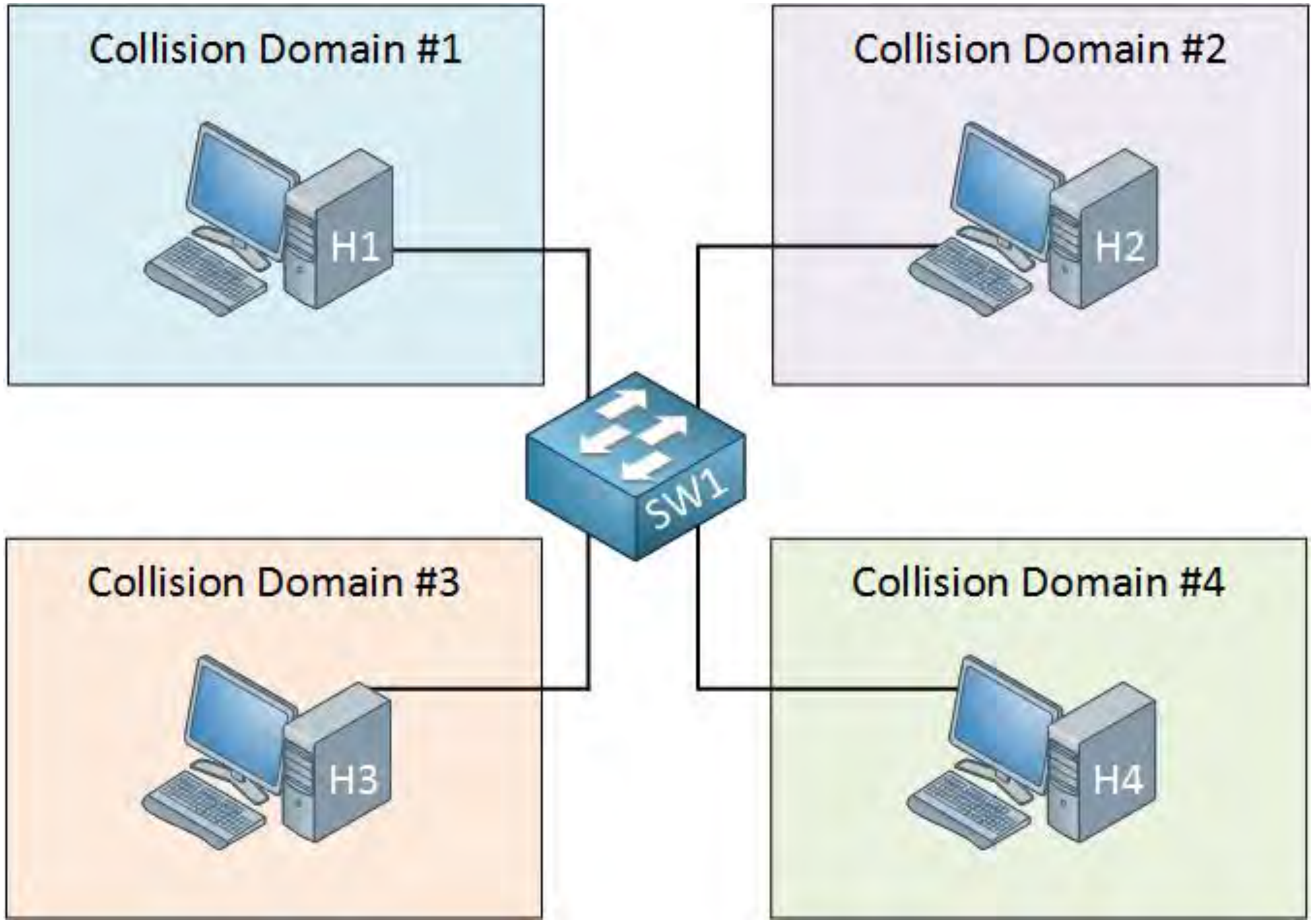
Collision Domain Example



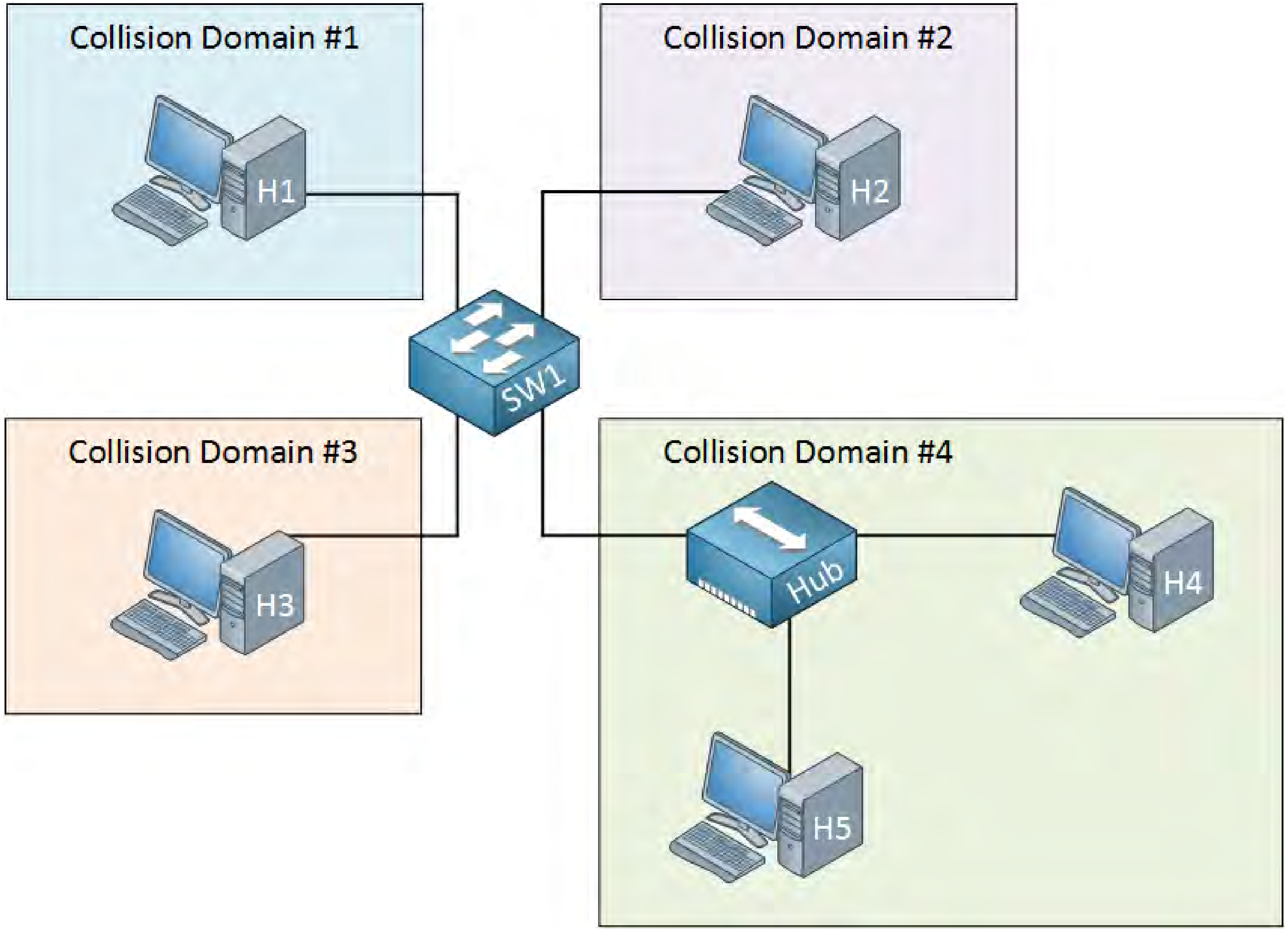
Collision Domain Example #2



Collision Domain Example #3



Collision Domain Example #4



Broadcast Domain D → important

A network segment where Layer 2 (ARP) broadcasts are allowed to propagate

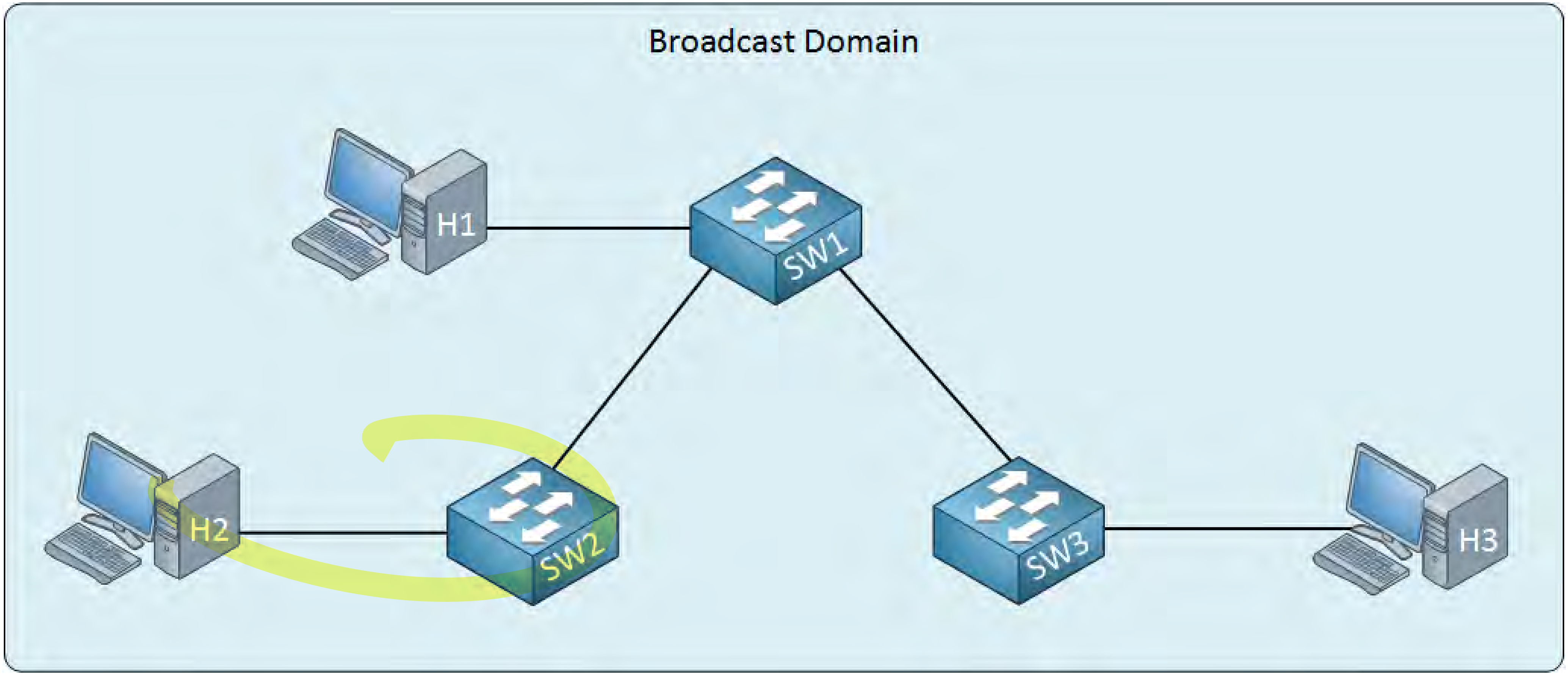
Includes all switch ports in a single VLAN / LAN segment

- Even across multiple switches
- Switches will propagate ARPs across trunk links and non-trunking simple uplinks

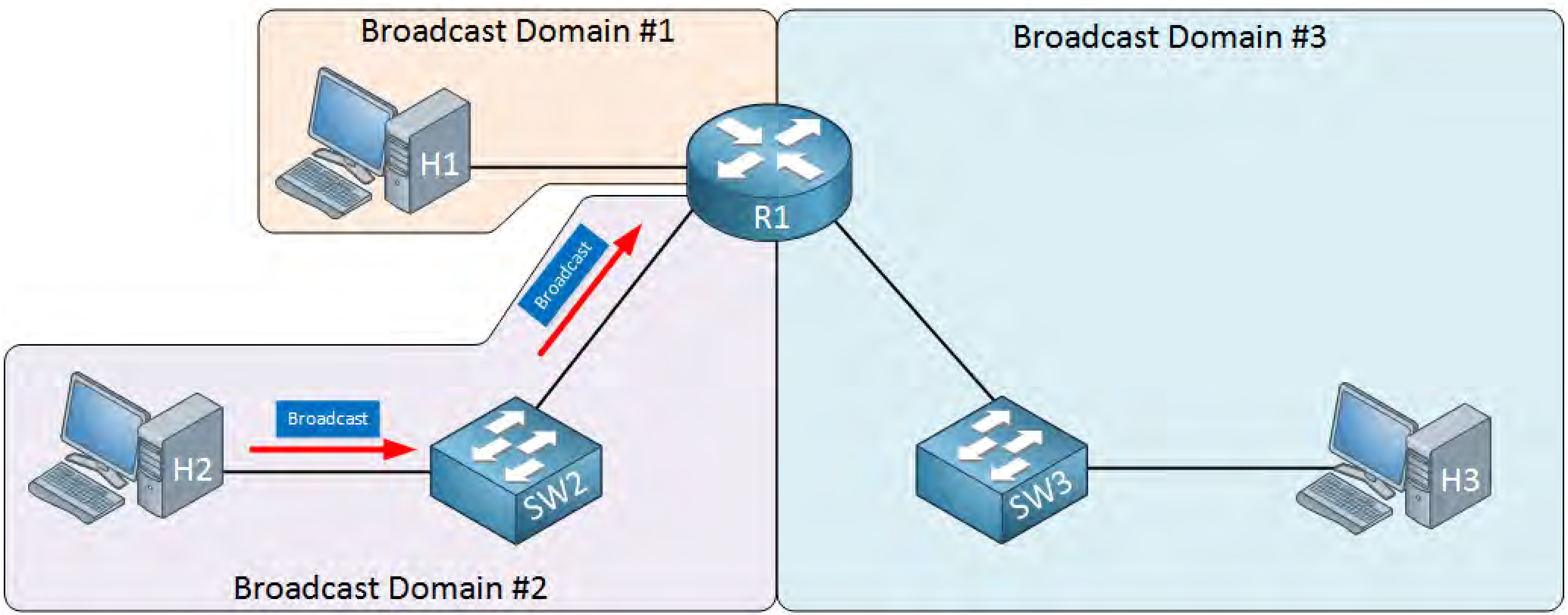
Routers and VLANs divide the segment into broadcast domains

A broadcast domain will also contain at least one collision domain

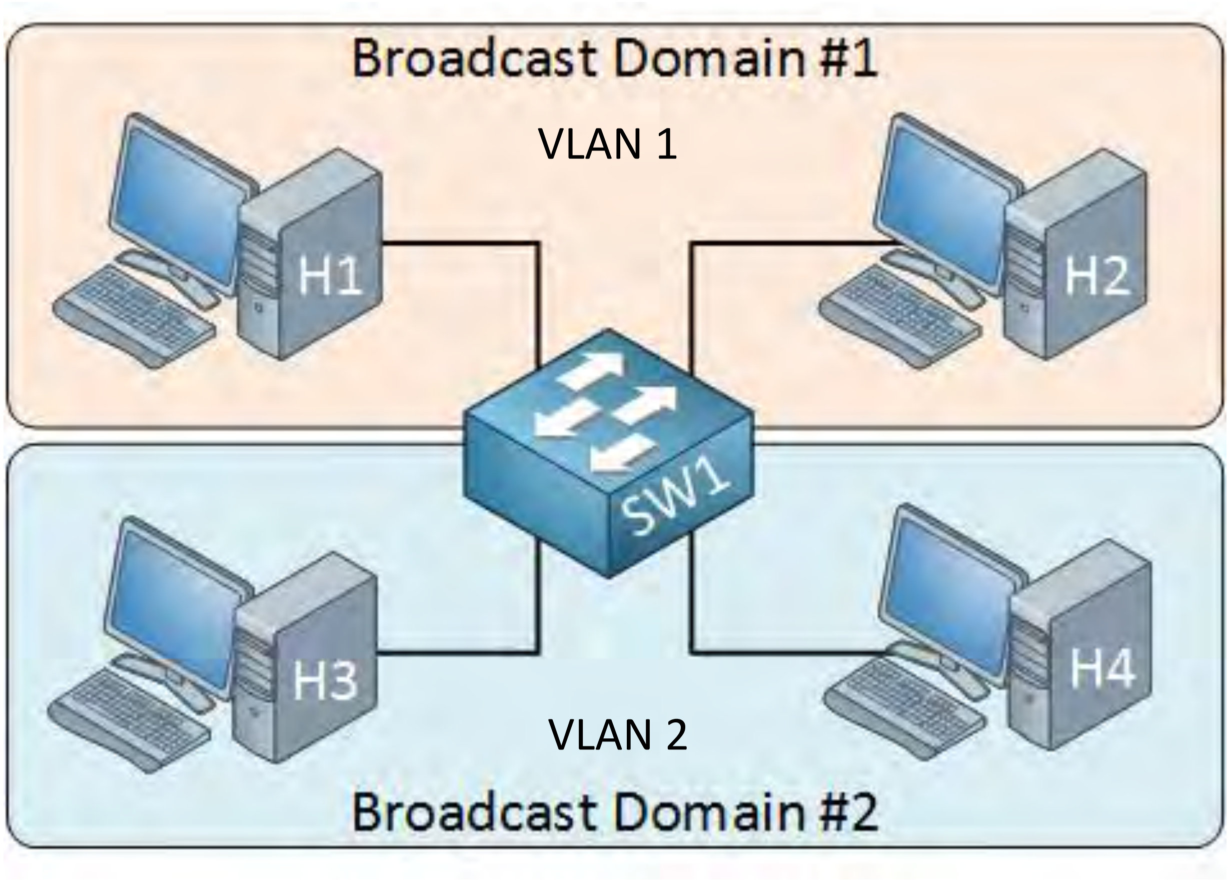
Broadcast Domain Example



Broadcast Domain Example #2



Broadcast Domain Example #3



Switchport Configuration

Common Port Configurations

Speed
- 10 / 100 / 1000 / etc.
- Auto - Device and switchport will negotiate the fastest speed both support

Duplex
- Full
  - Both sides can transmit simultaneously
  - Requires two separate conductors/wire pairs (Tx and Rx)
- Half
  - Devices must take turns transmitting
- Auto – Device and switchport will attempt to negotiate full duplex if possible

Mode
- Access – port is for end devices
- Trunk – port connects to another switch to extend VLAN

Switchport Modes

Each port on a switch can be configured for one of two modes

You can change the mode on a port as necessary

Access Port	Trunk Port
Connects to an end device	Connects to another switch
Belongs to one VLAN*	Used by all VLANs
Frames transmitted out the port are not tagged	Frames transmitted out the port are “tagged” with the VLAN they belong to
You can use an uplink (regular crossover cable) to plug a hub into the port to add more devices to the port**	After connecting the switches with a crossover cable, you configure the ports on both sides for trunking

* Some switches allow you to create a second “phone” VLAN on the same port

  You then plug the PC into the switchport, and the phone into the PC

** You can also plug in another switch so long as it is not configured with any VLANs

Additional Port Configurations

Configuration	Description
Port Mirroring	All traffic on this port is copied to another port Admin puts a protocol analyzer or sniffer on the mirrored port to monitor traffic
Port Security	Admin can restrict the port to allow only a specific MAC address(es) If the user plugs in an “illegal” device, the switch can drop unauthorized frames or even shut down the port
Jumbo Frames	Configure specific switchports to allow Ethernet frame size up to 9000 bytes Useful for iSCSI or other links where you are trying to increase performance
Port Aggregation Link Aggregation Control Protocol (LACP)	802.3ad Allows switches with multiple links to negotiate and bundle the links together The member links are treated by Spanning Tree as a single link

Auto-medium-dependent Interface Crossover (MDI-X)

The transmit wires of one device should connect to the receive wires of the other device

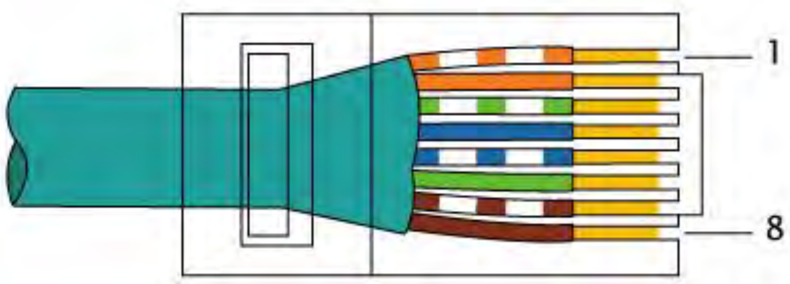
You cannot communicate if transmit is connect to transmit, or receive is connected to receive

On modern switches, the ports can detect if transmit and receive signals are connected to the wrong pins

Can automatically swap Tx and Rx ports if the wrong cable (straight-through or crossover) was used

The ports cannot correct other types of miswiring

EIA/TIA 568B RJ-45 Pinout

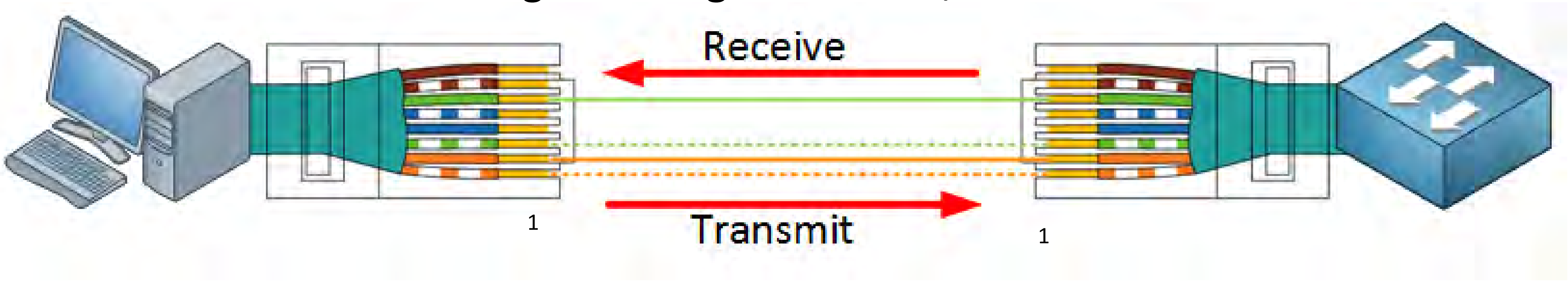


Orange pair = Tx

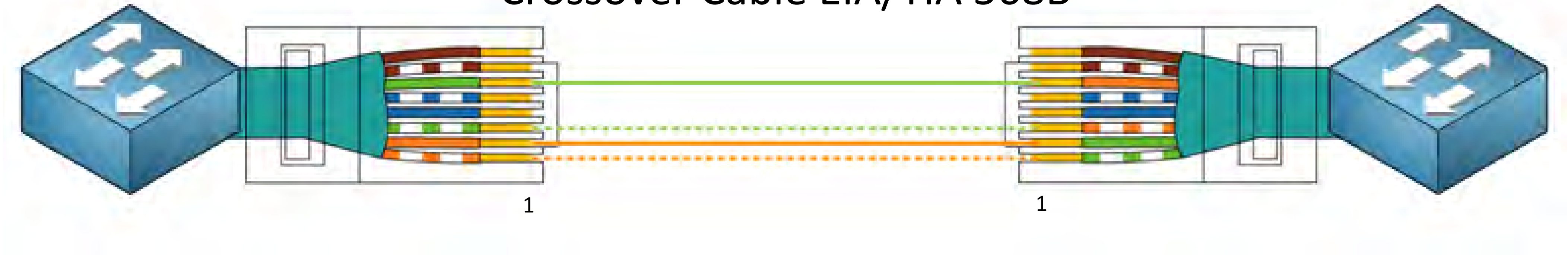
Green pair = Rx

Ethernet Straight-through and Crossover Cables

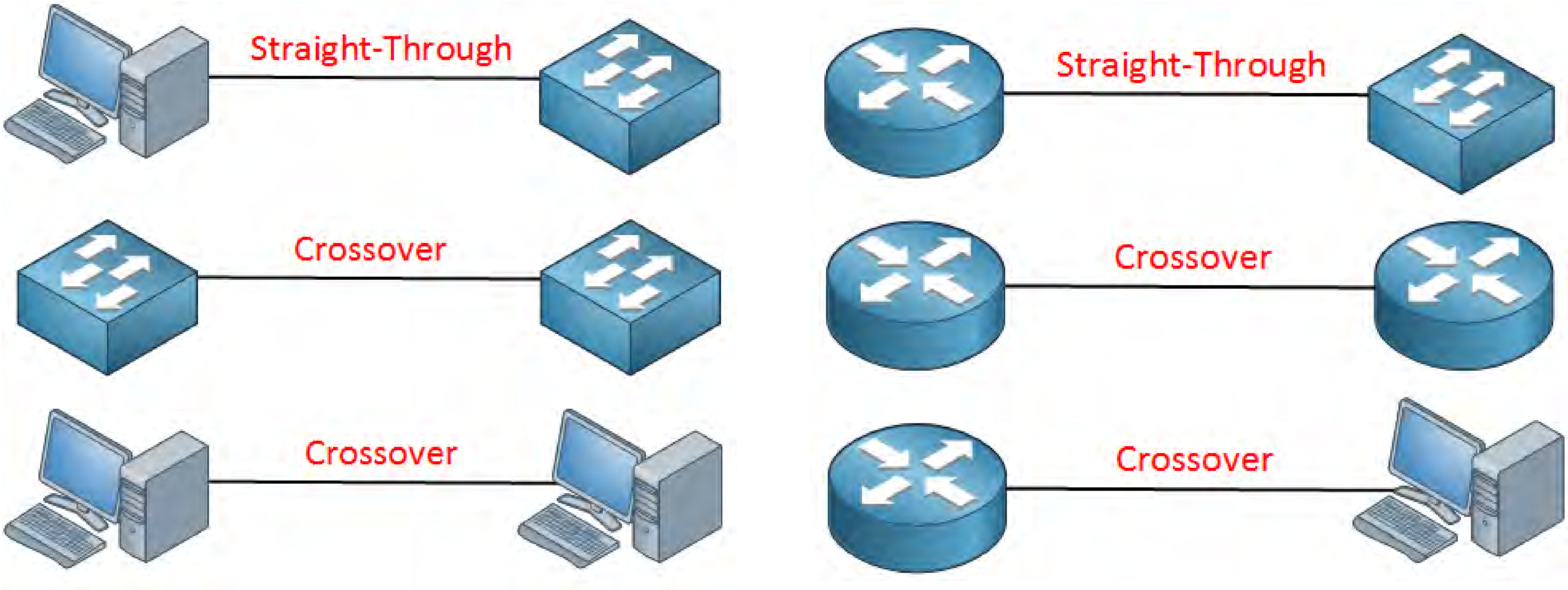
Straight-through Cable EIA/TIA 568B



Crossover Cable EIA/TIA 568B



Ethernet Straight-Through / Crossover Cable Selection



Flow Control

A predictive congestion management mechanism

Used by a switch to prevent uncontrolled packet drops

The switch PREDICTS that based on the current traffic flow, it will run out of receive buffer space in the next few frames

- It sends a PAUSE frame (request) to the sending device
- The sending device shuts up for a few milliseconds
- This is a complete halt of all traffic flow, regardless of traffic priority

This mechanism is no longer preferred

- It is better to implement and enforce true QoS
- Even better to monitor bandwidth utilization trends and increase bandwidth / offload traffic to other segments

IGMP Snooping

Configure the switch to watch for IGMP messages from clients

Identify multicast groups

Forward multicast frames out specific ports, rather than flooding

Configured at the switch level

Power over Ethernet (PoE)

Some switches can provide PoE on their ports

- Provide power to WAPs, IP phones, Cameras, PACS, alarms, etc.

Only twisted pair cable carries PoE

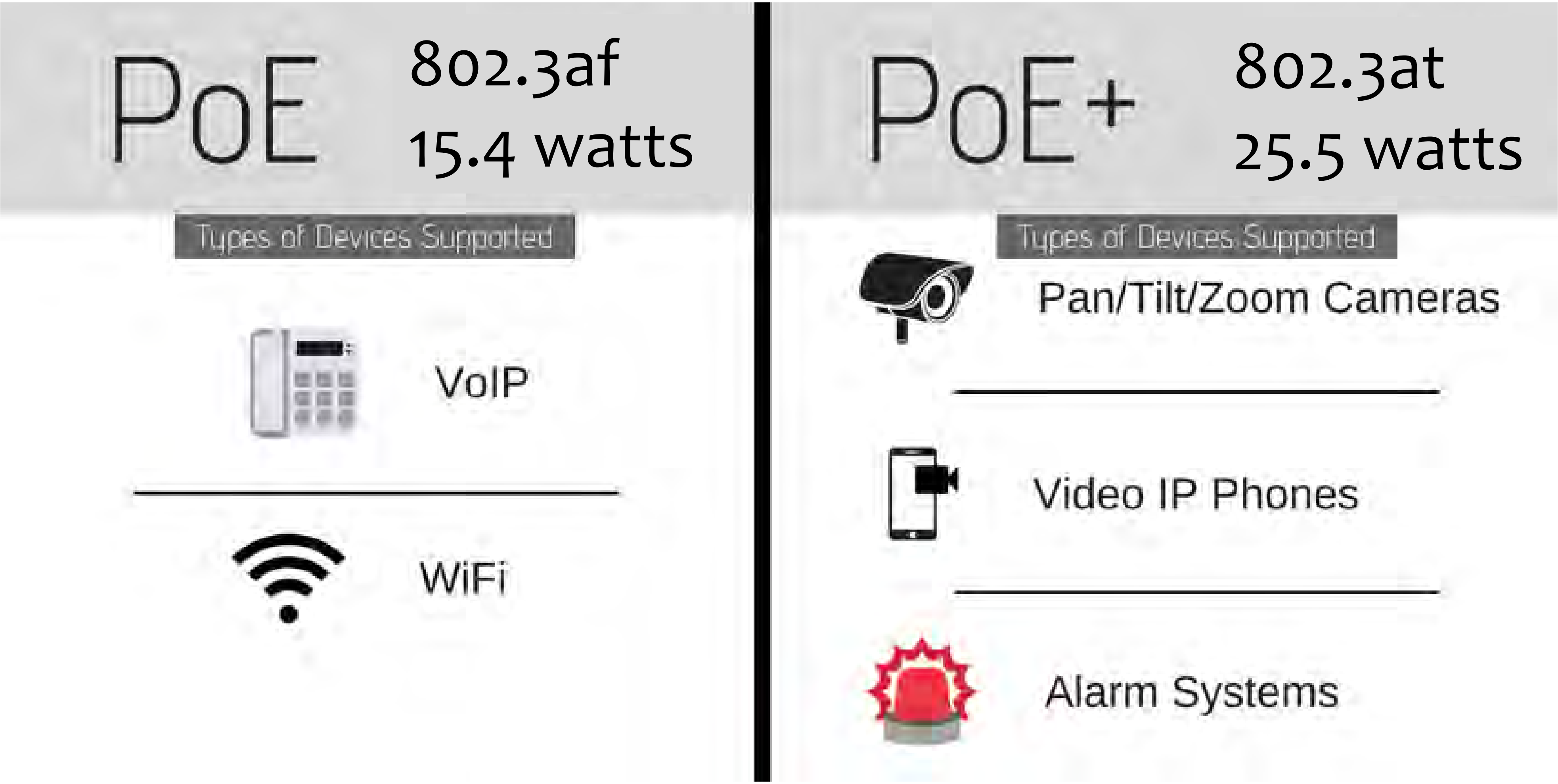
- Use CAT 6a or higher for distances over 50 meters

The PoE port must be directly connected to the PoE device

- Do not insert another switch or hub between the PoE switchport and its end device
- The intermediate device cannot "relay" power
- Most PoE switches can autosense if the end device requires PoE to automatically turn the power on or off
- If your switch does not support PoE, then use a power injector – place the injector as close as possible to the end device

Note: The average life span of a PoE switch is 3 – 5 years

Choosing Between PoE and PoE+



PoE

802.3af

15.4 watts

Types of Devices Supported

- VoIP
- WiFi

PoE+

802.3at

25.5 watts

Types of Devices Supported

- Pan/Tilt/Zoom Cameras
- Video IP Phones
- Alarm Systems