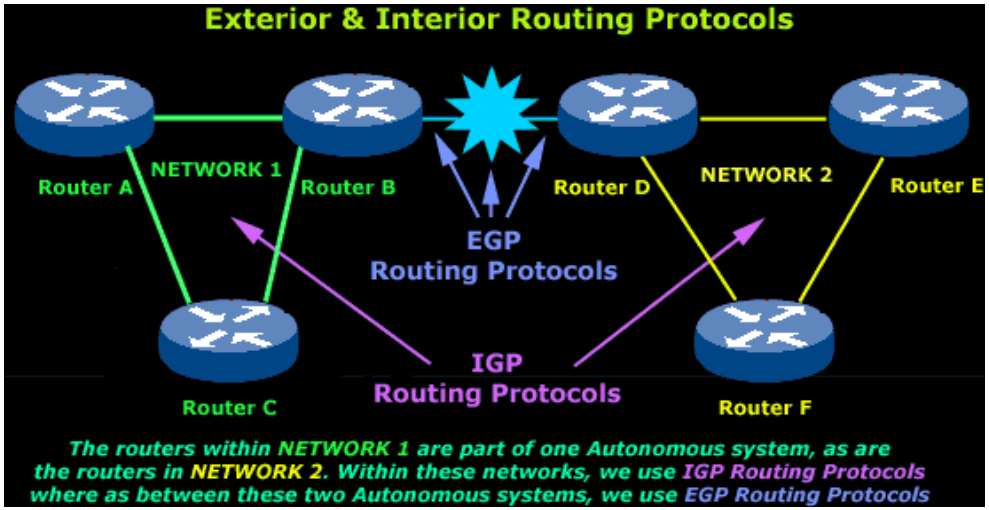
CIS 3210
VLANs



Definition: VLAN

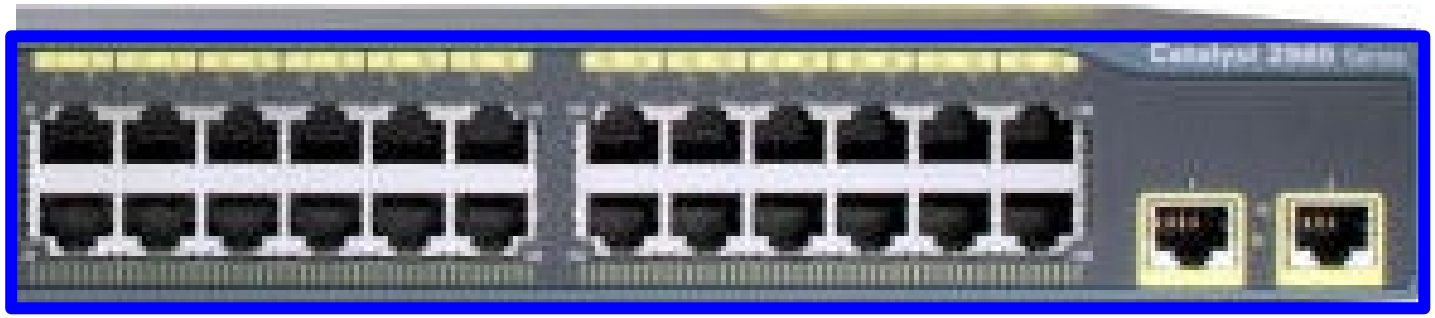
*"A VLAN is a virtual LAN that **logically** segments switched networks based on **functions**, **project teams**, or **applications** of the organization regardless of the physical location or connections to the network."*

TO CLEAR A SWITCH

- ALWAYS DO THE FOLLOWING TO CLEAR A SWITCH!!

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

S1# erase startup-config
Erasing the nvram filesystem will remove all configuration files!
  Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
S1# reload
Proceed with reload? [confirm]
```

Default VLAN Assignment

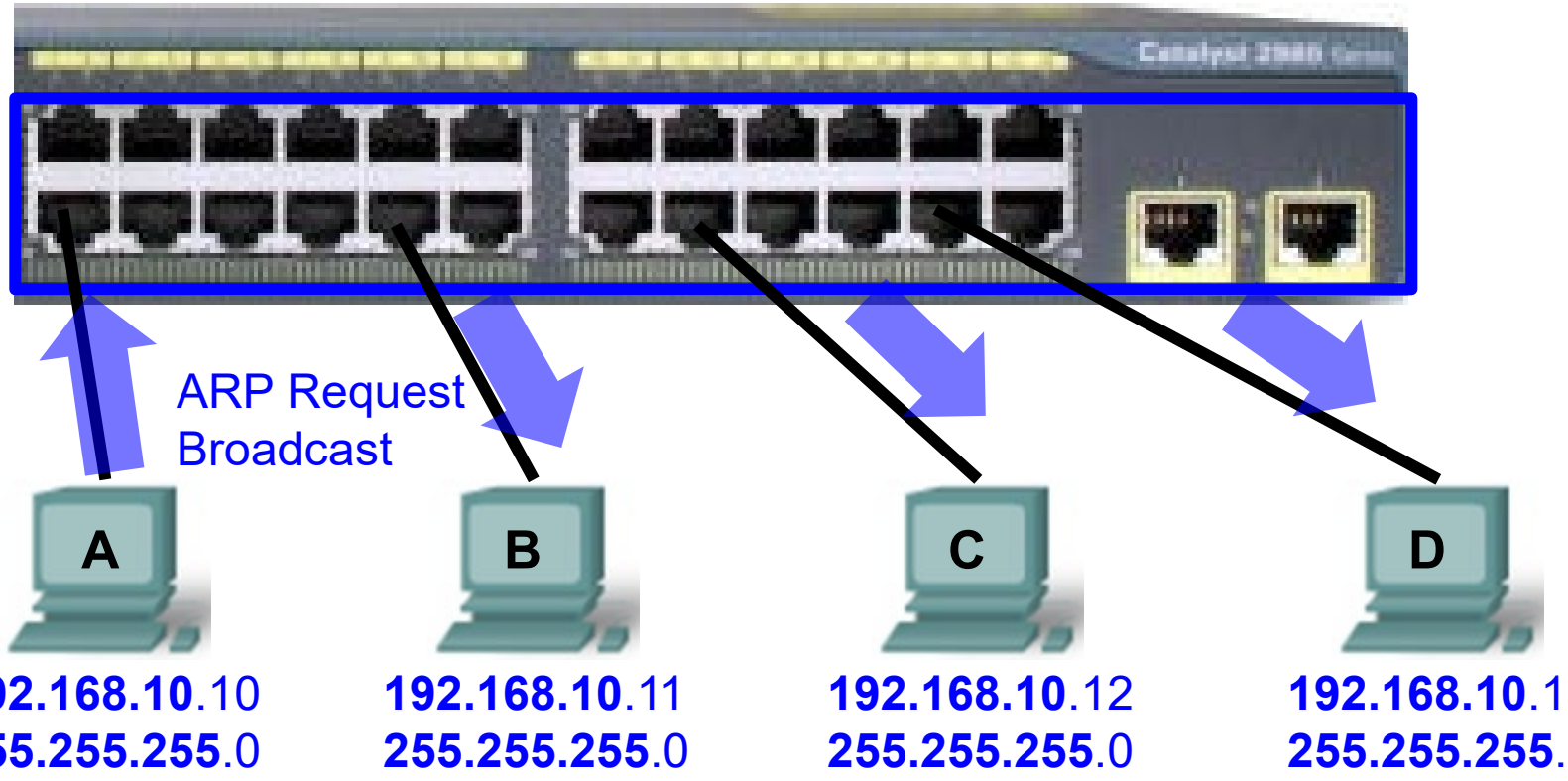


Default: All ports in the same VLAN (subnet)

```
Switch# show vlan

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
                                                 Gig0/1, Gig0/2
<output omitted>
```

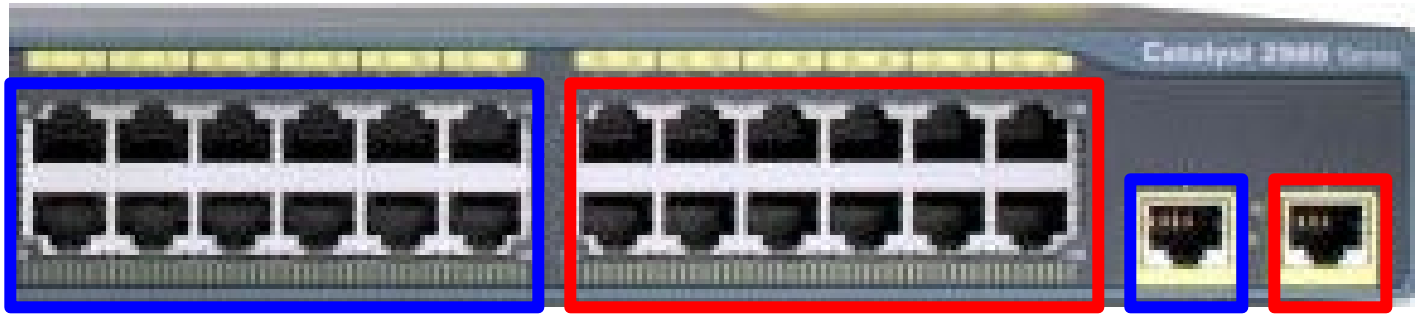
Default VLAN Assignment

Default: All ports in the same VLAN



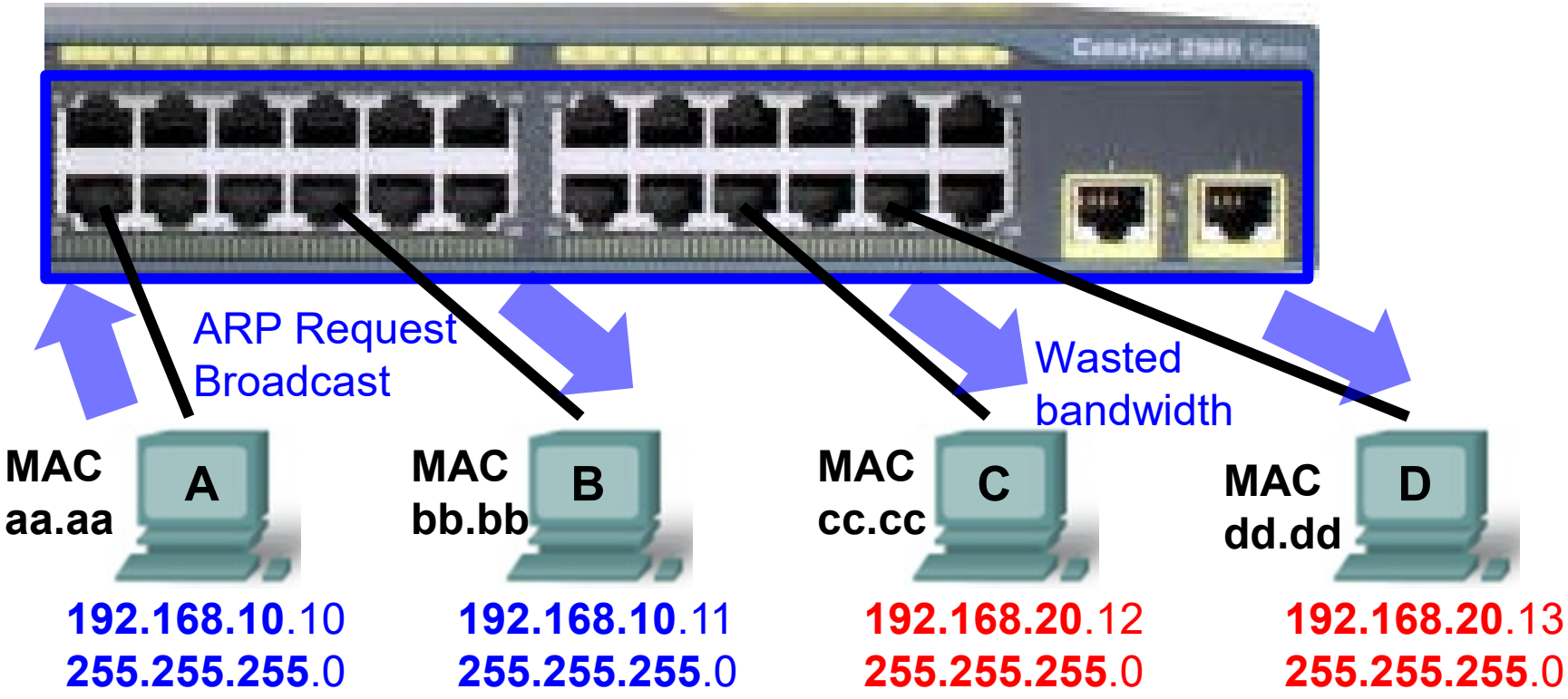
- Hosts can communicate with each other because:
  - Same IP subnet
  - Switch ports are on the same VLAN (subnet)
- Can A, B, C and D ping each other?
- If A did an ARP request for B, who would see this Ethernet broadcast?

VLAN Definitions



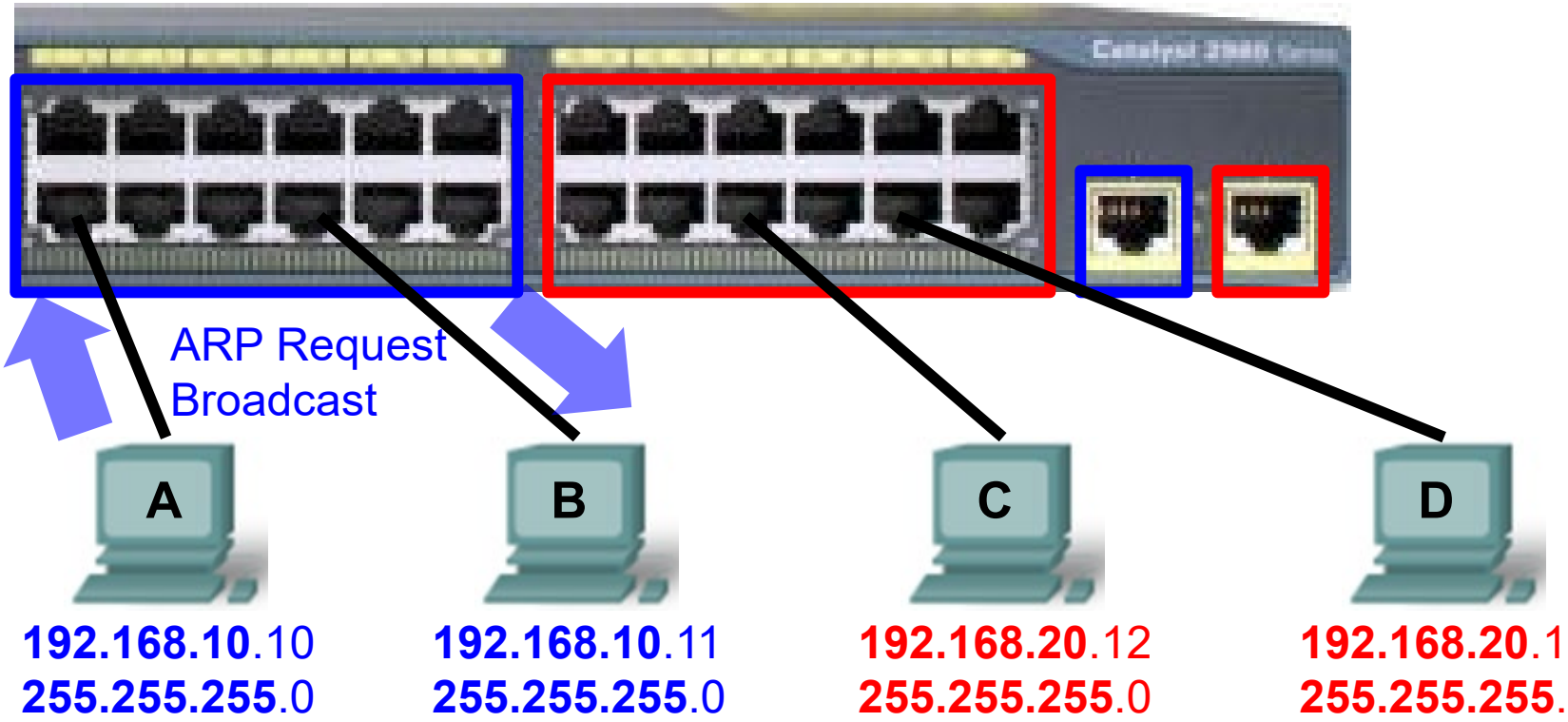
- A VLAN is a logical partition of a Layer 2 network.
- Multiple partitions can be created, allowing for multiple VLANs to co-exist.
- Each VLAN is a broadcast domain, usually with its own IP network.
- VLANs are mutually isolated and packets can only pass between them via a router.
- The partitioning of the Layer 2 network takes place inside a Layer 2 device, usually via a switch.
- The hosts grouped within a VLAN are unaware of the VLAN's existence.

A single VLAN (“no VLANs”) means no segmentation

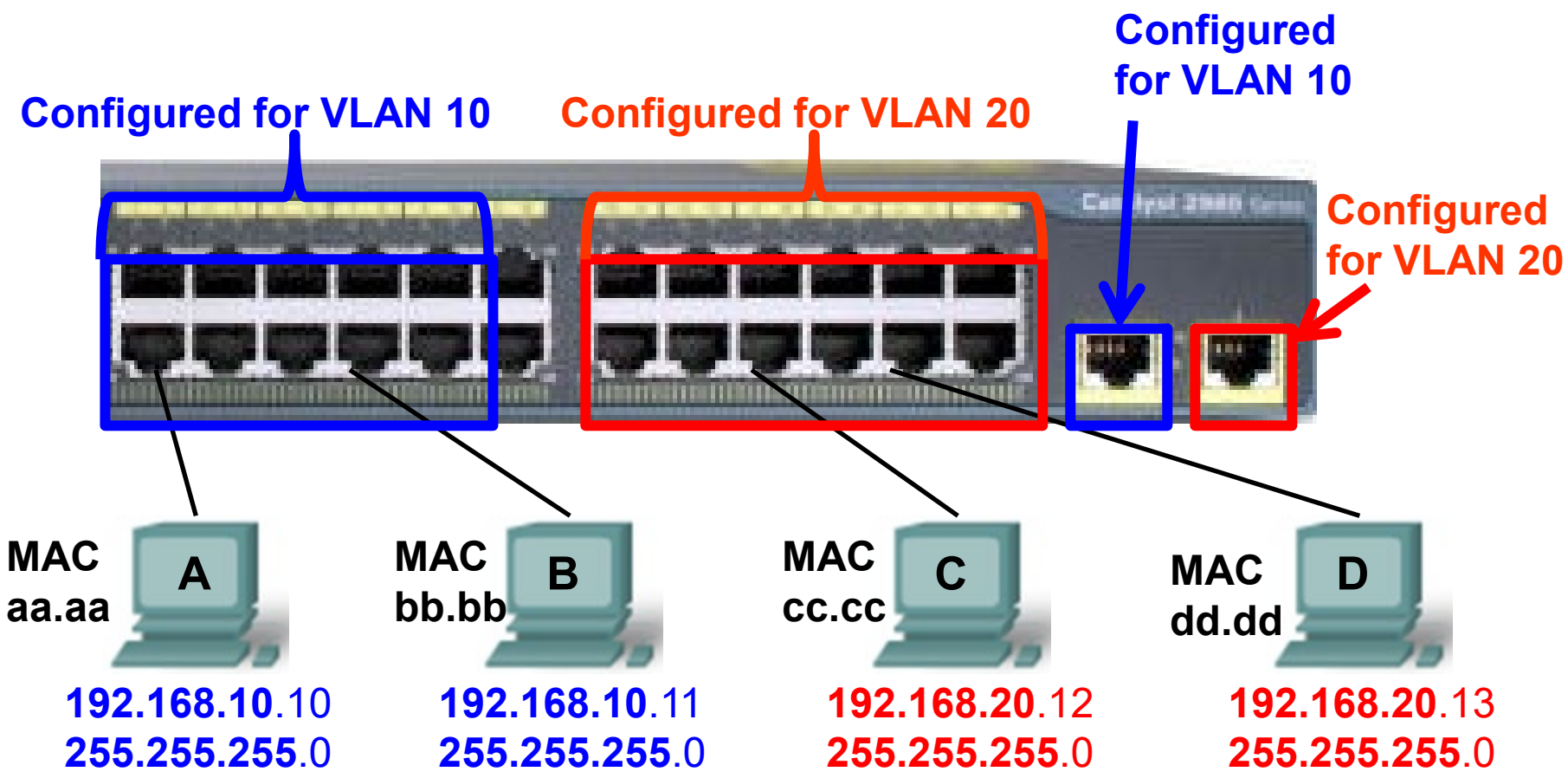


- Who can A Ping? B ping? C ping? D ping?
- If A did an ARP request for B, who would see this Ethernet broadcast?
- If C did an ARP request for D, who would see this Ethernet broadcast?
- Remember: ARP requests are only when the source IP address and the destination IP address are on the SAME SUBNET.

VLANs provide segmentation into several bcast domains

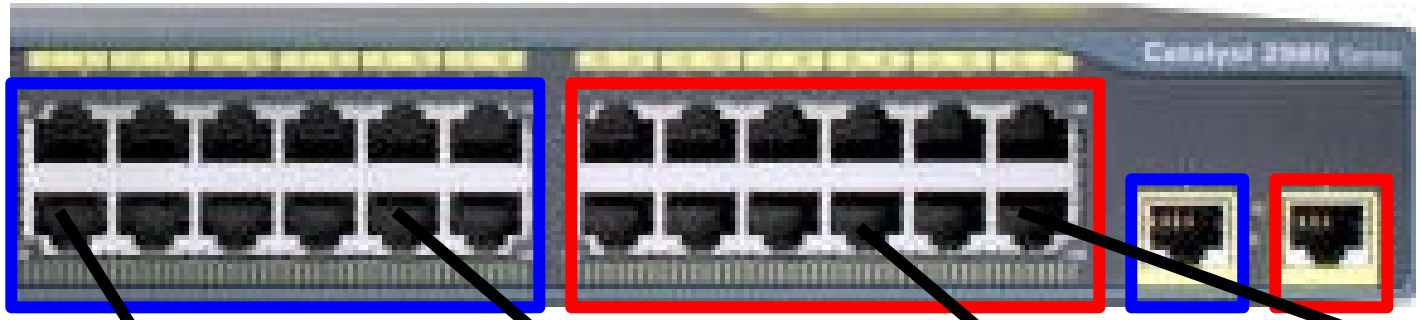


- Who can A Ping? B ping? C ping? D ping?
- If A did an ARP request for B, who would see this Ethernet broadcast?
- If C did an ARP request for D, who would see this Ethernet broadcast?
- Remember: ARP requests are only when the source IP address and the destination IP address are on the SAME SUBNET.



- VLANs are configured on the switch port
- IP Addresses and subnet masks are configured on the devices that connect to the switch ports.
- VLAN on the switch must match the IP network address of the device.

AFTER CONFIGURATION



A

B

C

D

192.168.10.10
255.255.255.0

192.168.10.11
255.255.255.0

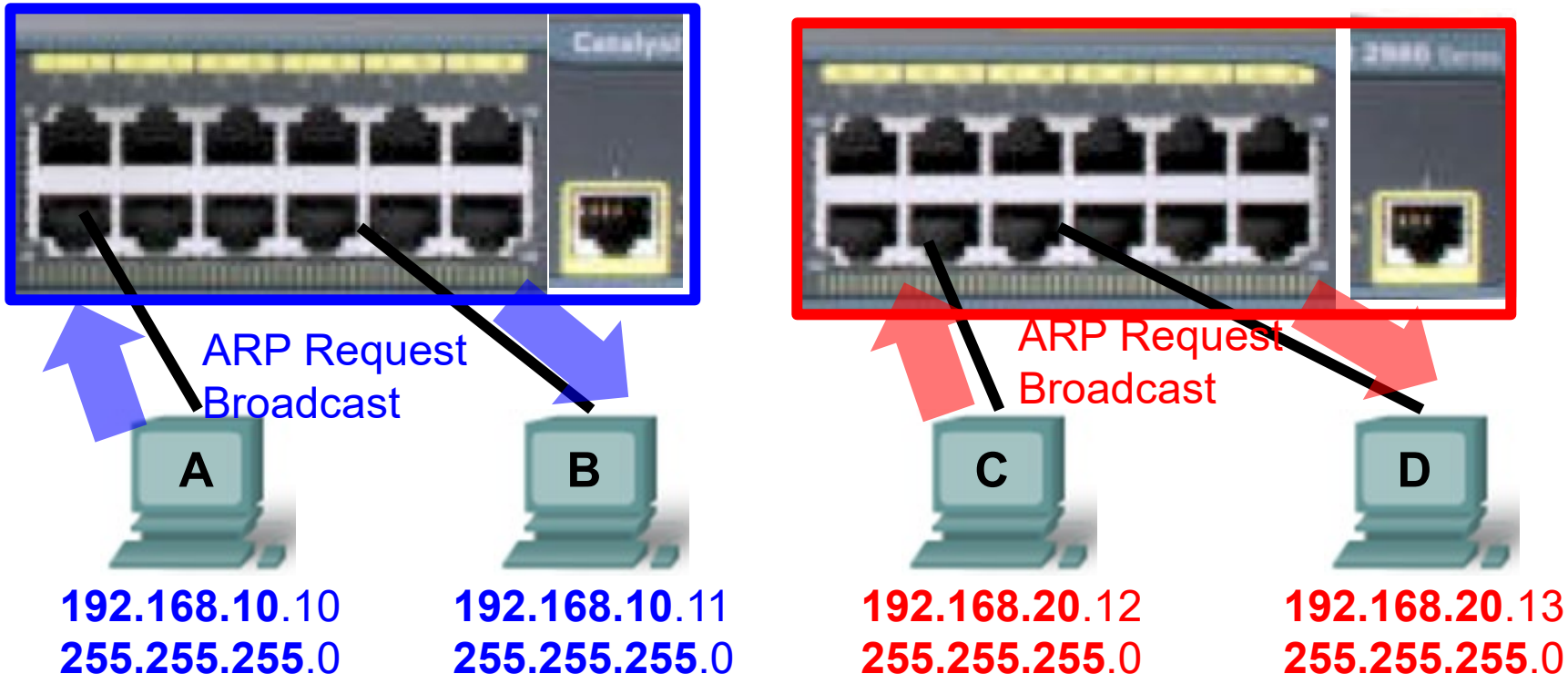
192.168.20.12
255.255.255.0

192.168.20.13
255.255.255.0

```
Switch# show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
10                                     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,
                                                 Gig0/1

20                                     active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24,
                                                 Gig0/2
```

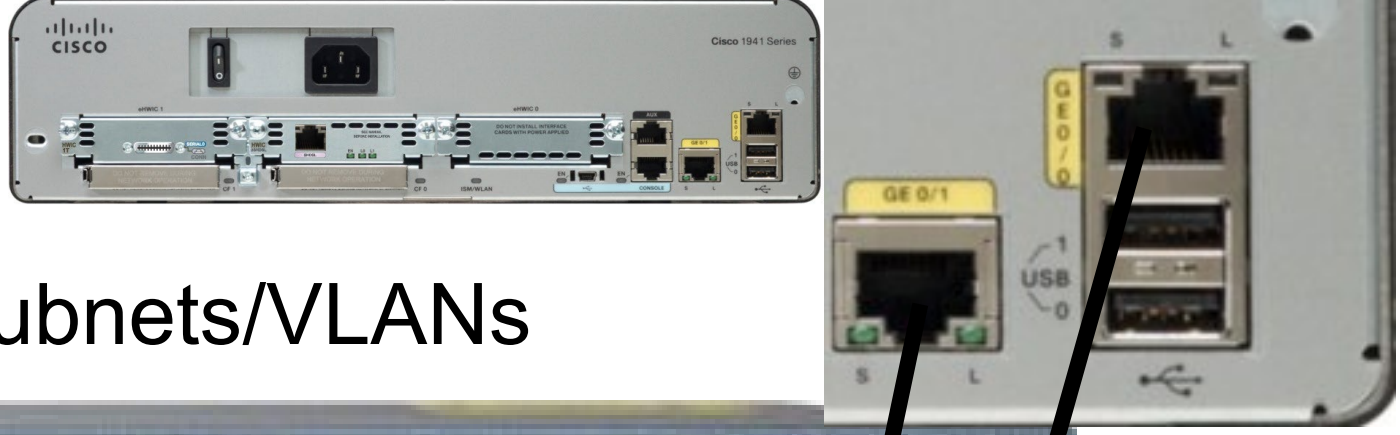
VLANs give proper segmentation – Like having separate switches

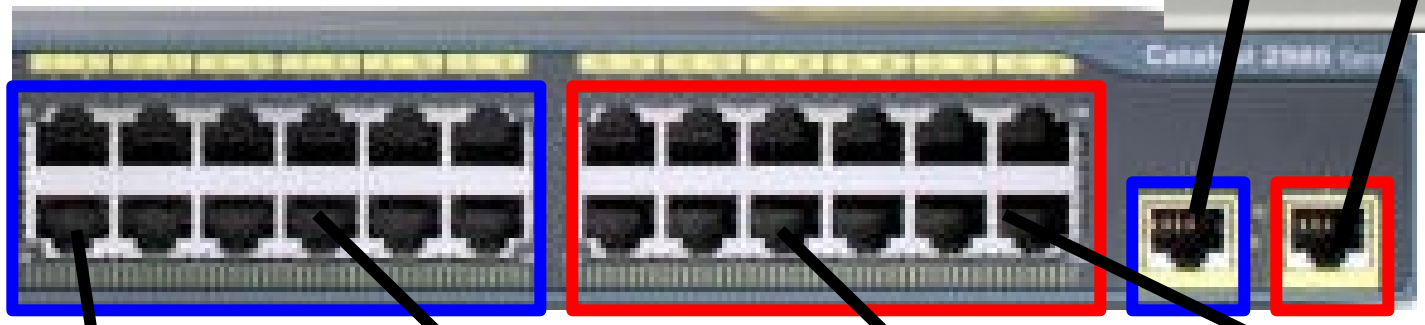
VLANs do **not** have to be configured contiguously on the switch.



- VLANs segment switches in to different VLANs or Subnets
- Think of it like having separate switches
- Who can A Ping? B ping? C ping? D ping?
- If A did an ARP request for B, who would see this Ethernet broadcast?
- If C did an ARP request for D, who would see this Ethernet broadcast?

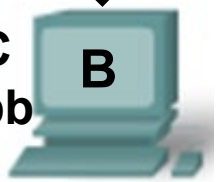
Router and subnets/VLANs





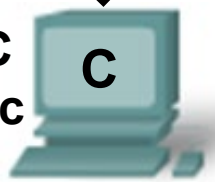
MAC aa.aa

192.168.10.10
255.255.255.0



MAC bb.bb

192.168.10.11
255.255.255.0



MAC cc.cc

192.168.20.12
255.255.255.0

MAC dd.dd

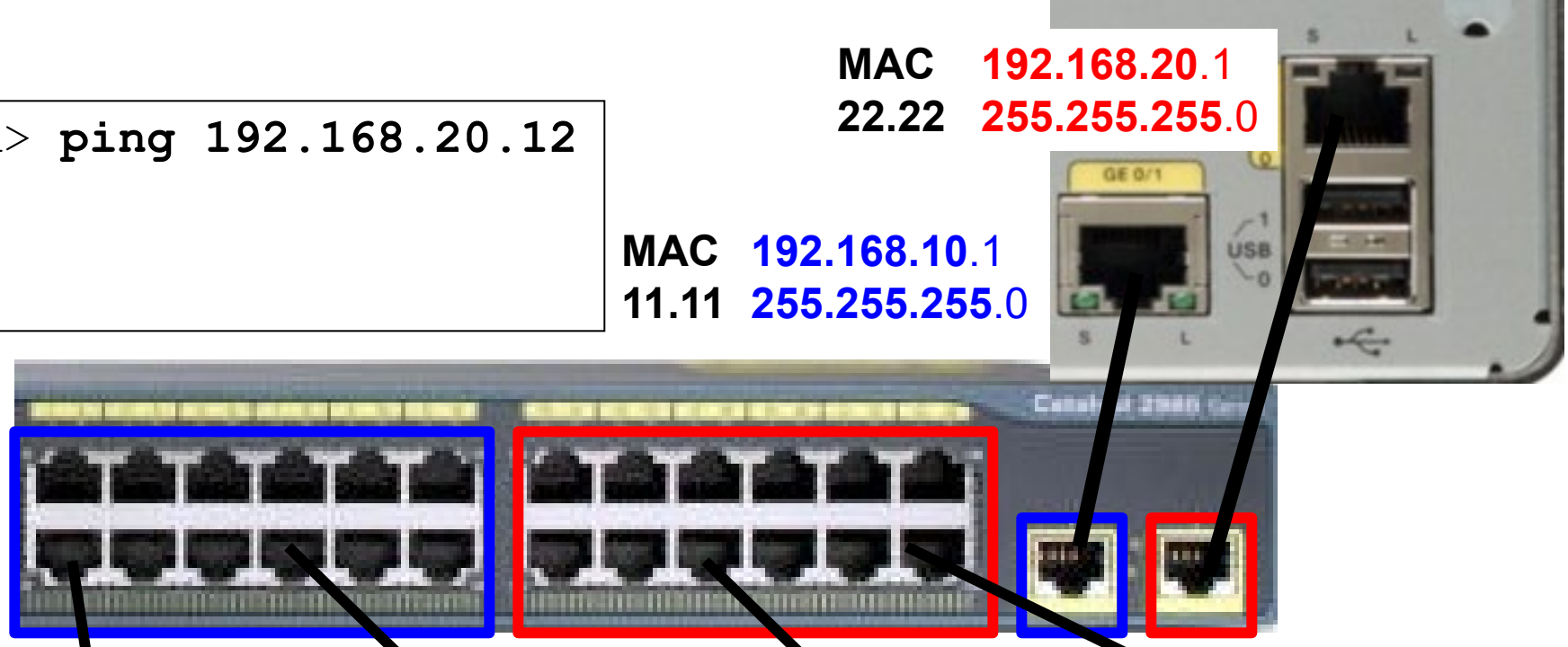
192.168.20.13
255.255.255.0

- Router is required to connect (route) between subnets/VLANs

```
PCA> ping 192.168.20.12
```

MAC 22.22 192.168.20.1 255.255.255.0

MAC 11.11 192.168.10.1 255.255.255.0



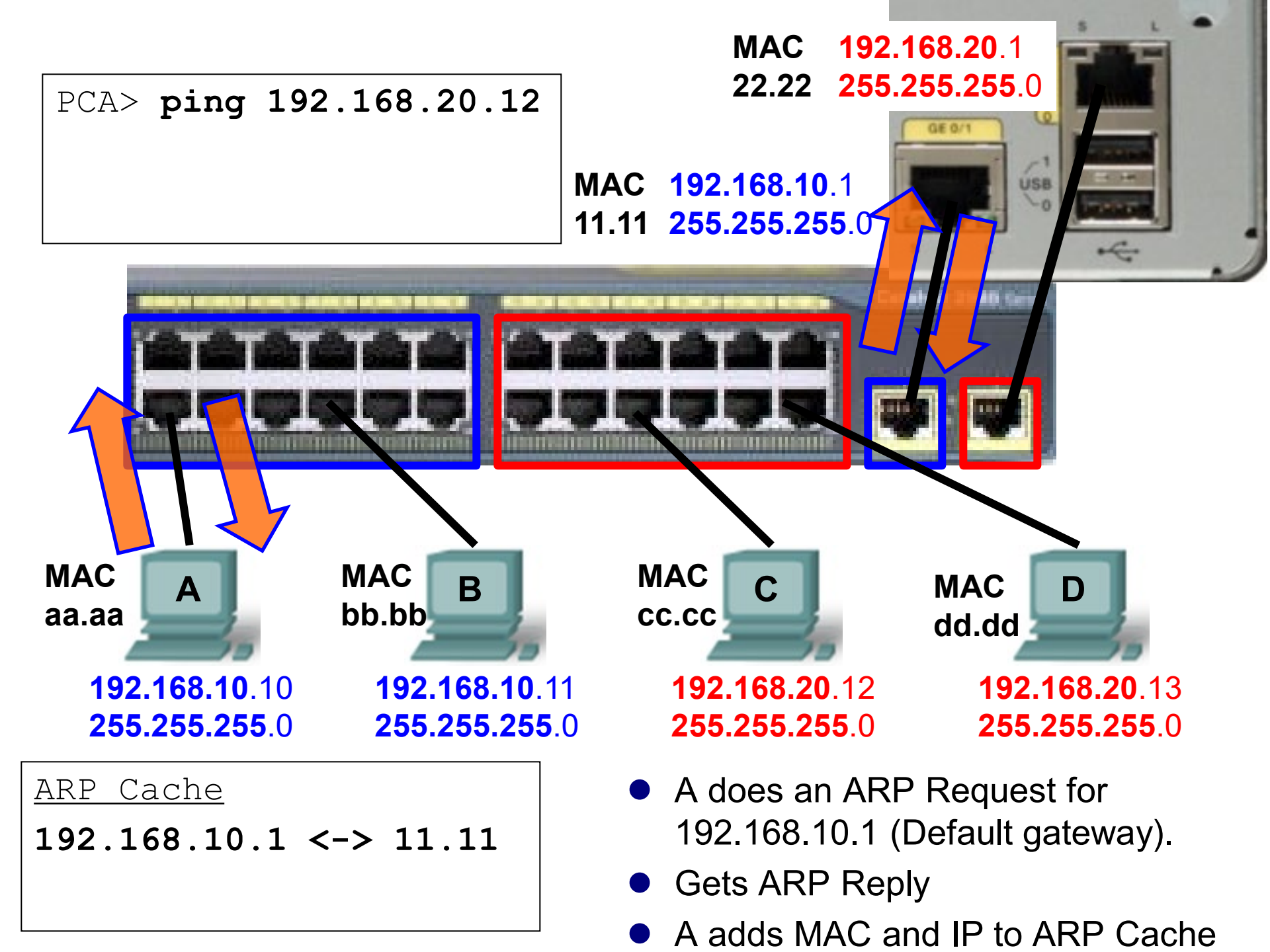
MAC aa.aa — A — 192.168.10.10 255.255.255.0

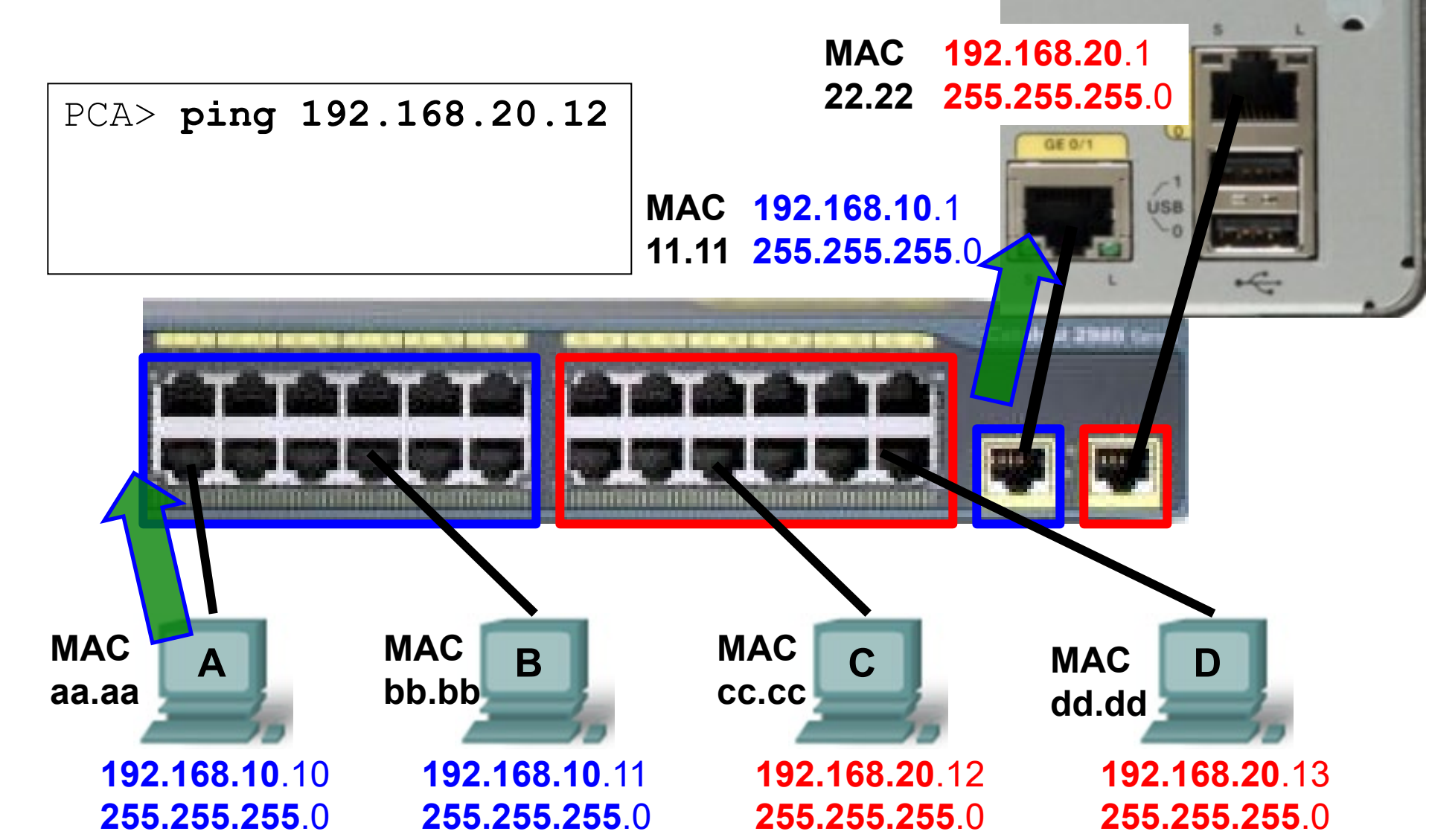
MAC bb.bb — B — 192.168.10.11 255.255.255.0

MAC cc.cc — C — 192.168.20.12 255.255.255.0

MAC dd.dd — D — 192.168.20.13 255.255.255.0

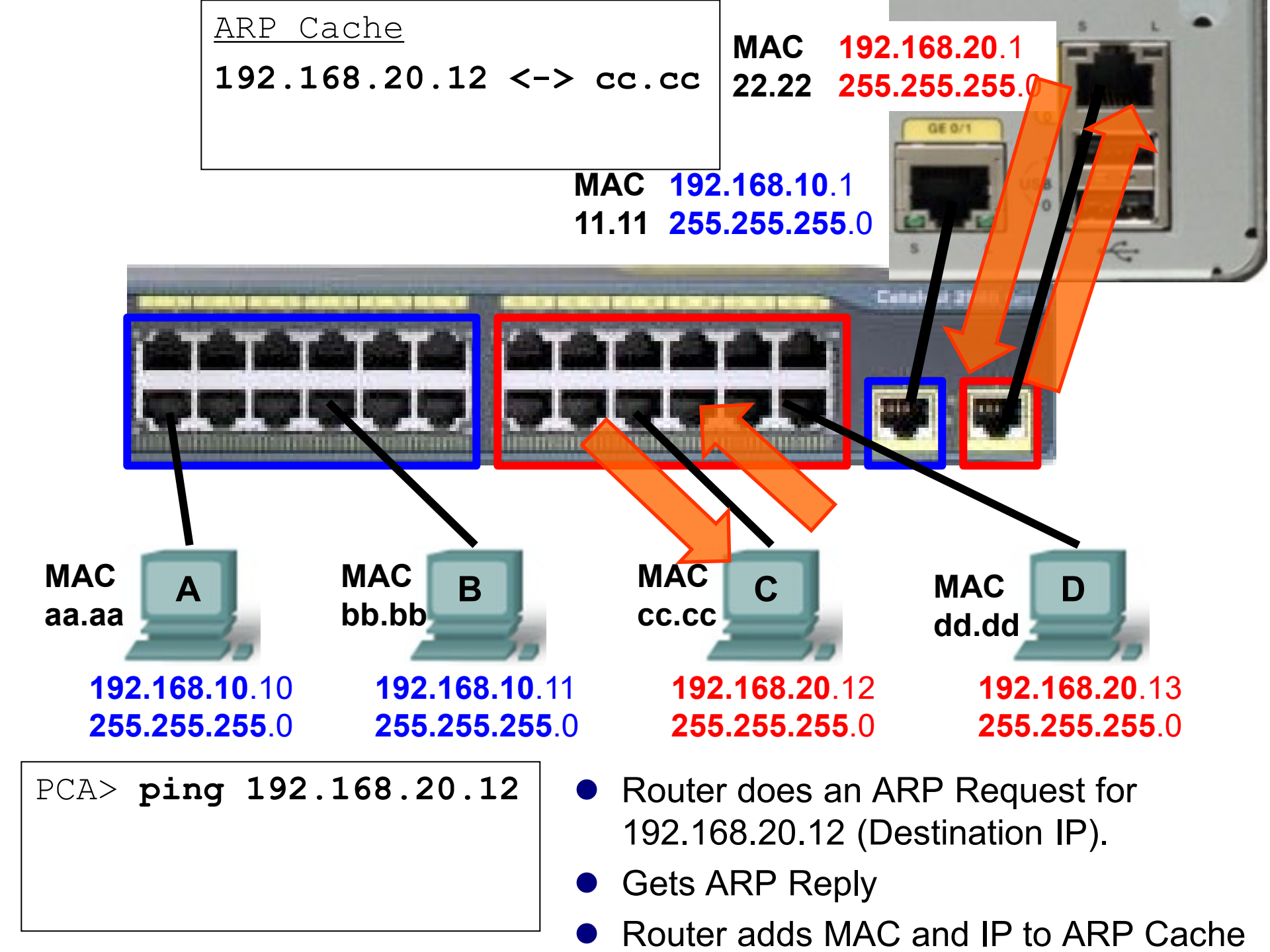
- Router is required to connect (route) between subnets/VLANs
- In this example, a single router with two IP addresses, one on each subnet, is connected to the switch.
- Each of the router's interfaces is connected to a proper VLAN port on the switch to match it's IP subnet. (Just like the host computers!)


PCA> ping 192.168.20.12
MAC 192.168.20.1
22.22 255.255.255.0
MAC 192.168.10.1
11.11 255.255.255.0
MAC
aa.aa
A
MAC
bb.bb
B
MAC
cc.cc
C
MAC
dd.dd
D
192.168.10.10
255.255.255.0
192.168.10.11
255.255.255.0
192.168.20.12
255.255.255.0
192.168.20.13
255.255.255.0
ARP Cache
192.168.10.1 <-> 11.11
A does an ARP Request for 192.168.10.1 (Default gateway).
Gets ARP Reply
A adds MAC and IP to ARP Cache



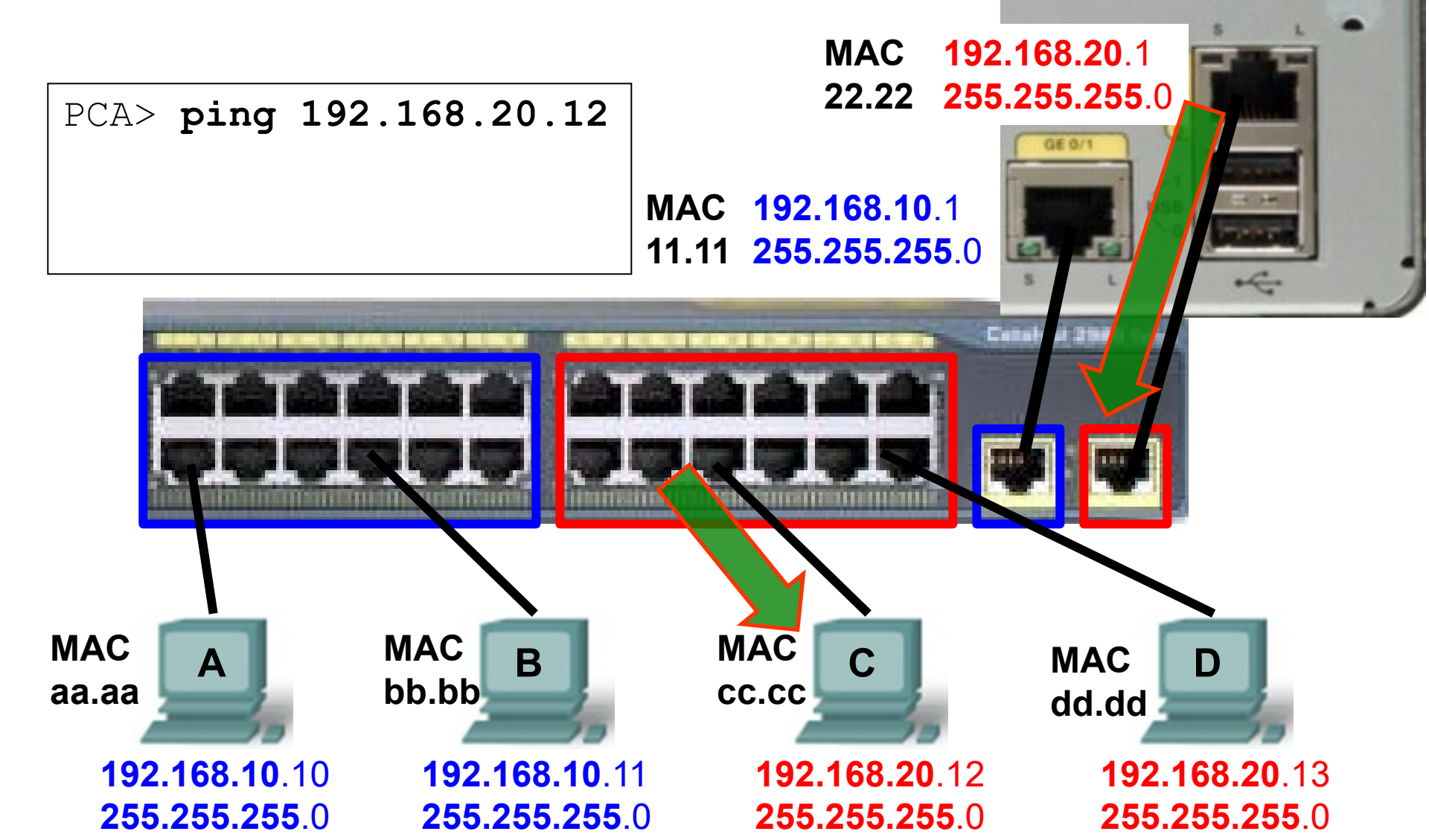
Destination Address	Source Address	Type	IP (ICMP)	FCS
11.11	aa.aa		DA 192.168.20.12	

- A sends Ethernet frame to default gateway, the router




```
PCA> ping 192.168.20.12
```

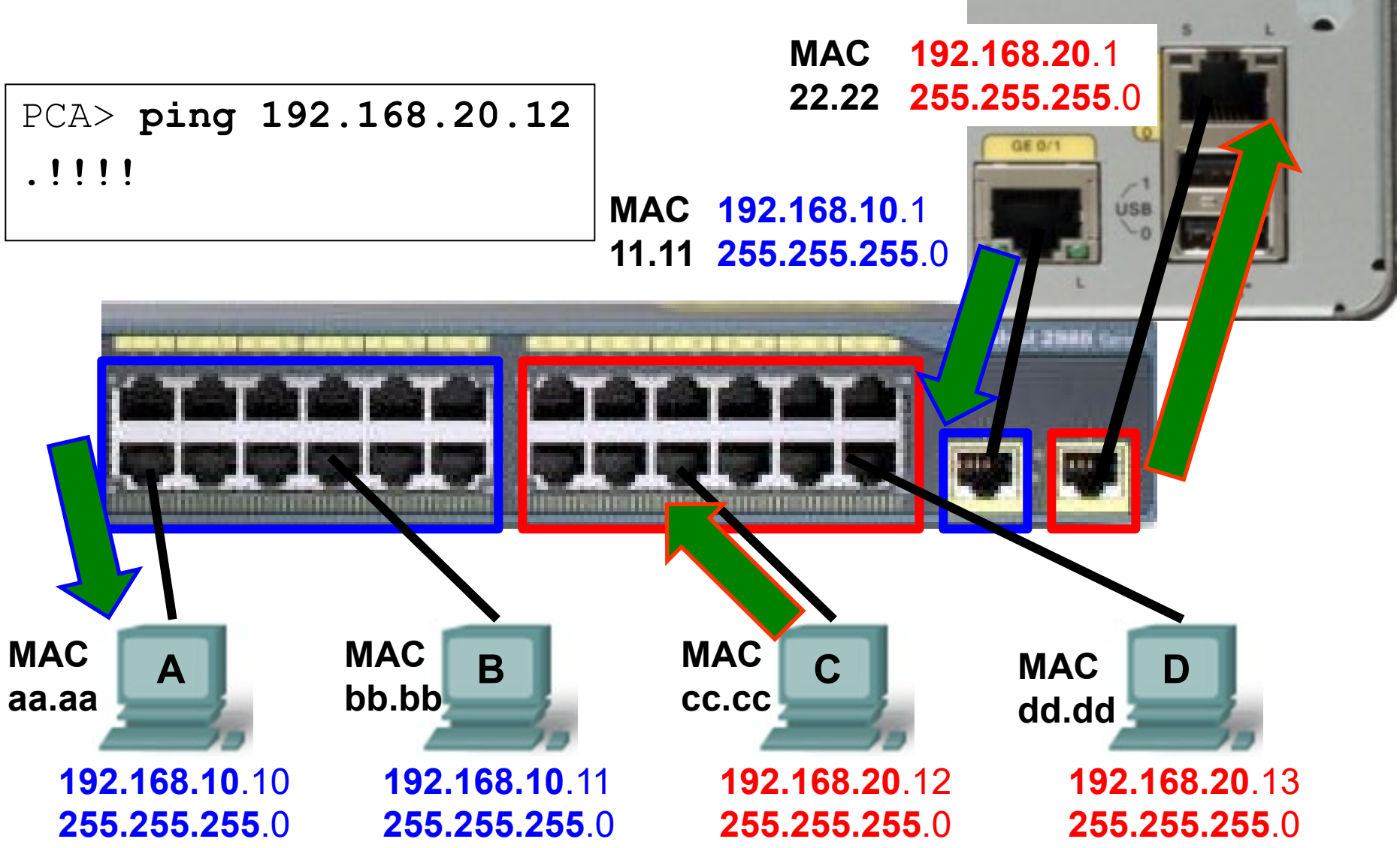
- Router does an ARP Request for 192.168.20.12 (Destination IP).
- Gets ARP Reply
- Router adds MAC and IP to ARP Cache



Destination Address	Source Address	Type	IP (ICMP)	FCS
cc.cc	22.22		DA 192.168.20.12	

- Router sends Ethernet frame to final destination, PC-C

```
PCA> ping 192.168.20.12
.!!!!
```



Destination Address	Source Address	Type	IP (ICMP)	FCS
22.22	cc.cc		DA 192.168.10.10	

Destination Address	Source Address	Type	IP (ICMP)	FCS
aa.aa	11.11		DA 192.168.10.10	

Benefits of VLANs

- **Security**:
  - Improved by isolating user access to sensitive data and applications.
- **Cost reduction**:
  - Reduces the need for expensive network upgrades and more efficient use of existing bandwidth and uplinks.
- **Smaller Broadcast Domains**:
  - Divide a network into smaller logical networks, resulting in lower susceptibility to broadcast storms.
- **Better performance**:
  - Divides the flat Layer 2 networks into multiple broadcast domains reducing unnecessary traffic on the network and boosts performance.
- **Improved IT staff efficiency:**
  - Makes the network easier to manage.

How many VLANs can you configure on a switch?

It depends….
on the switch and
the switch's capabilities
and what you require.

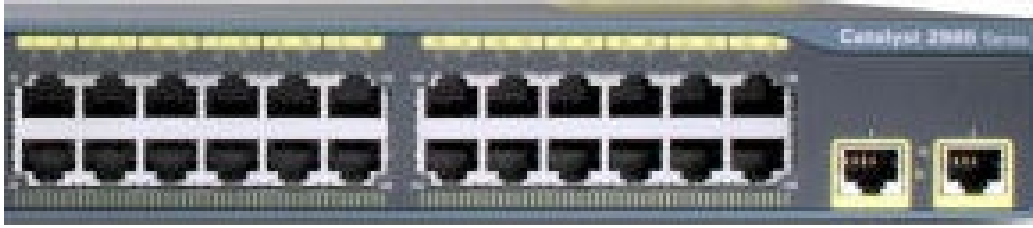
- VLAN ID

- Normal-range IDs
  - 1 – 1005
  - 1002 -1005 reserved for Token Ring and FDDI VLANs
  - 1 and 1002 to 1005 are automatically created and cannot be removed
  - Stored in the vlan.dat file in flash memory

- Extended-range IDs
  - 1006 – 4094
  - Designed for service providers
  - Have fewer options than normal range VLANs
  - Stored in the running configuration file

- A Cisco Catalyst 2960 switch supports 255 normal and extended range VLANs

Default VLAN Assignment



```
Switch# show vlan

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
                                                   Gig0/1, Gig0/2
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Switch#
```

Normal Range VLANs

```
Switch# show vlan

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
                                                 Gig0/1, Gig0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

- Used in small- and medium-sized business and enterprise networks.
  - VLAN Range: 1 – 1005
  - Reserved VLANs: VLANs 1, 1002 – 1005
  - Configurations stored in **vlan.dat** in flash memory.

- **Note:**
  - VLAN Trunking Protocol (VTP) can manage normal range VLANs.

Extended Range VLANs

- Used in Service Provider networks (great number of customers) or large, global enterprises.
  - VLAN Range: 1006 - 4094.
  - Support fewer VLAN features than normal range VLANs.
  - Saved in the running configuration file.

Catalyst 2960G-24TC

- 20 10/100/1000 ports
- 4 dual-purpose uplink ports

Catalyst 2960G-48TC

- 44 10/100/1000 ports
- 4 dual-purpose uplink ports

Catalyst 2960-24TC

- 24 10/100 ports
- 2 dual-purpose uplink ports

Catalyst 2960-48TC

- 48 10/100 ports
- 2 dual-purpose uplink ports

Catalyst 2960-24TT

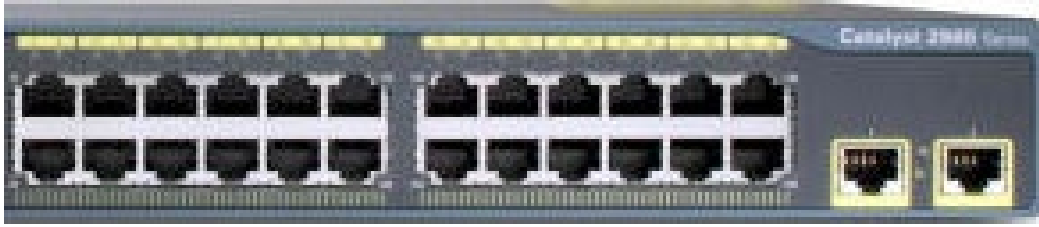
- 24 10/100 ports
- 2 10/100/1000 uplink ports

Catalyst 2960-48TT

- 48 10/100 ports
- 2 10/100/1000 uplink ports

- It can support up to 255 normal range and extended range VLANs.

Types of VLANs

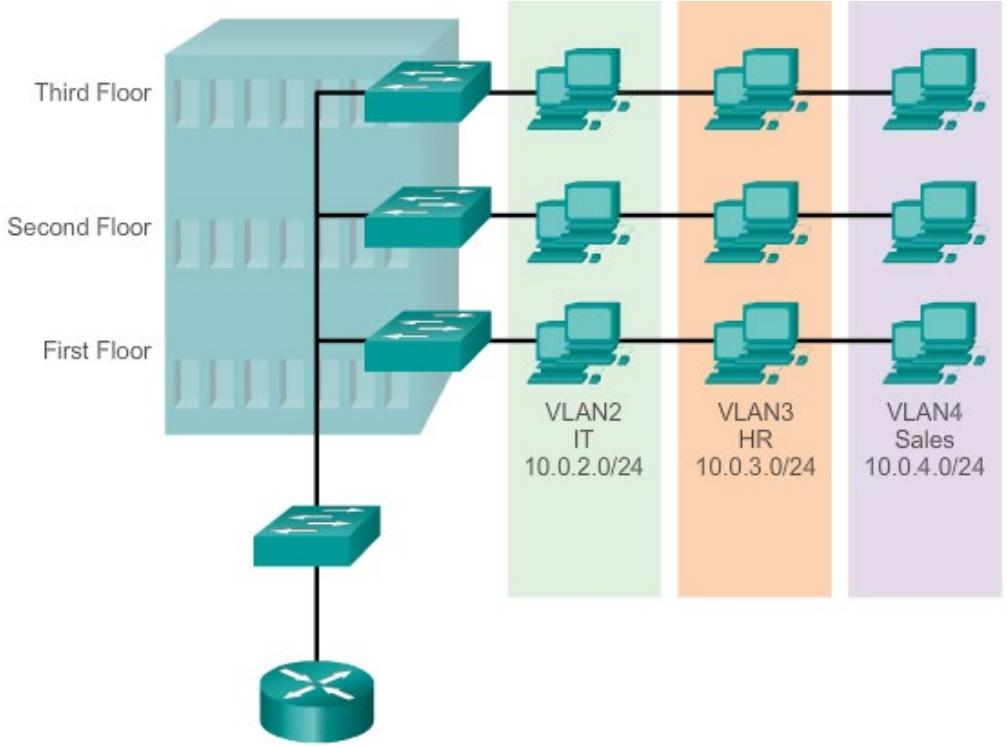


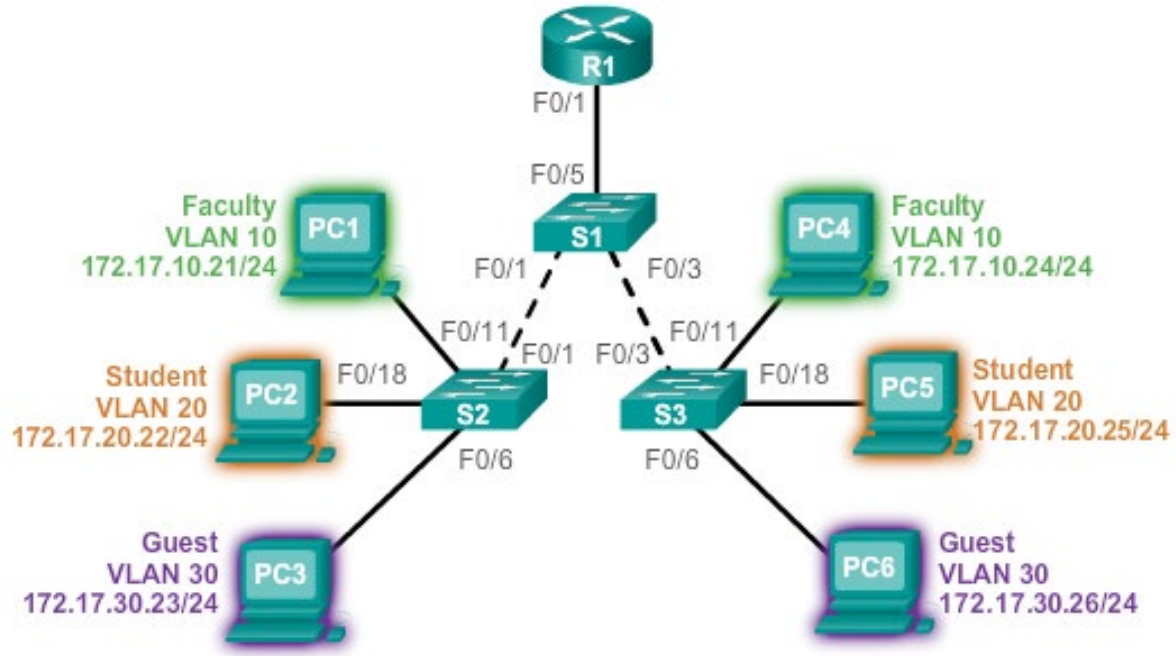
- **Default VLAN** (**VLAN 1 by default**)
- **Native VLAN (VLAN 1 by default)**
  - Used for untagged traffic (later)
- **User VLANs**
  - Each IP subnet is a separate VLAN
- **Management VLAN**
  - VLAN to connect to infrastructure devices such a switches
- **Voice VLAN**
  - VLAN used to connect IP phones
- **Guest VLAN**
  - For to connect guests and others who do not have access to internal resources, perhaps Internet access only
- **Garbage VLAN**
  - For unused ports not yet configured for a specific VLAN

User VLAN examples

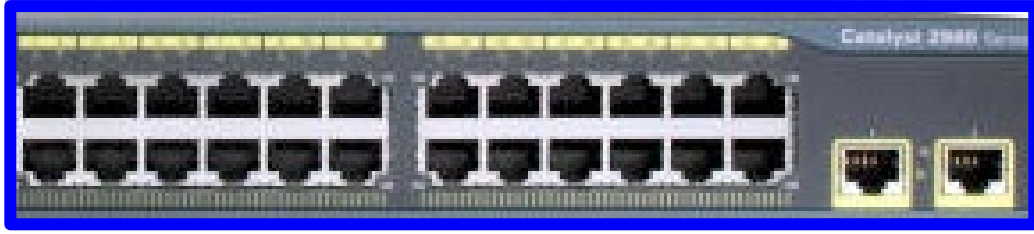
VLAN = Subnet

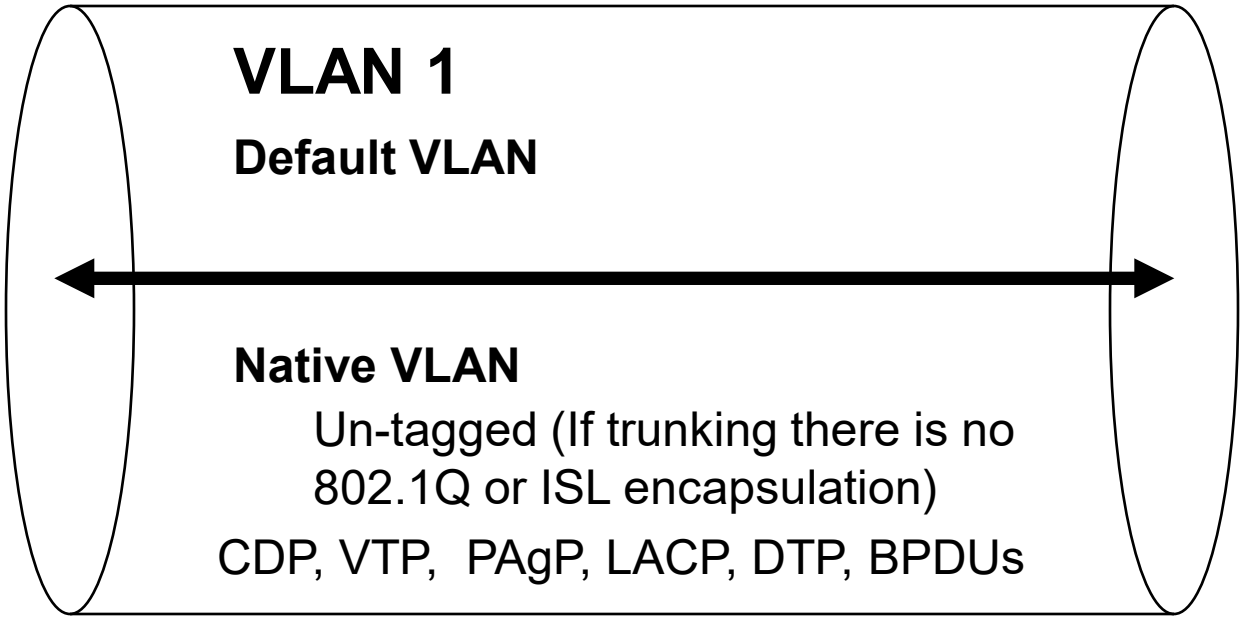
- **Business VLANs**
  - **IT VLAN**
  - **HR VLAN**
  - **Sales VLAN**
- **College**
  - **Student VLAN**
  - **Faculty VLAN**
  - **Guest VLAN**





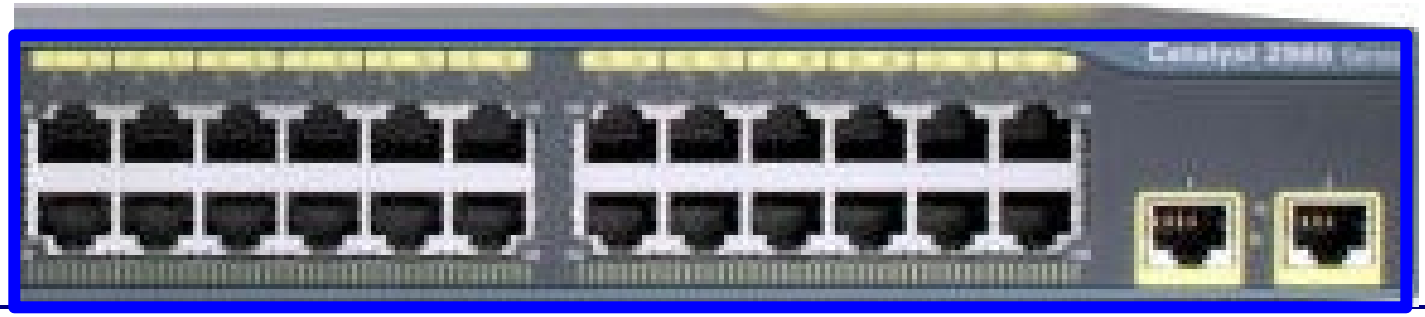
Default VLAN





- By default all traffic is carried across VLAN 1.
- By default all ports are on VLAN 1
- VLAN 1 is:
  - The **default VLAN** (all user traffic)
  - **Native VLAN**: No trunking encapsulation even if configured as a trunk coming).
  - All Layer 2 control traffic (e.g., DTP, VTP, STP BPDUs, PAgP, LACP, CDP, etc.), are associated with VLAN 1

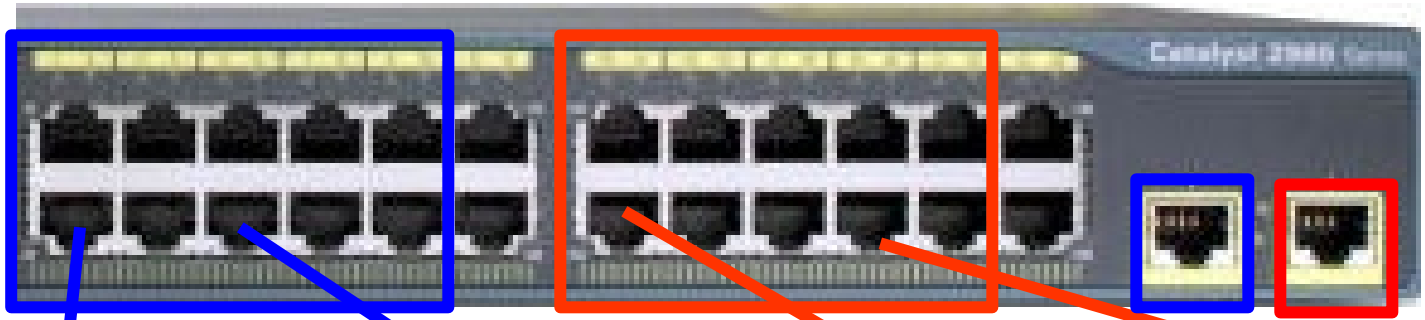
Default VLAN 1



```
S1# show vlan

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
```

- VLAN 1 **cannot be deleted**
- Security best practices:
  - Avoid using VLAN 1 for all VLANs other than control traffic which must be on VLAN1
- In other words, create additional VLANs

User or Data VLANs



MAC aa.aa — A — 192.168.10.10 255.255.255.0

MAC bb.bb — B — 192.168.10.11 255.255.255.0

HR Department

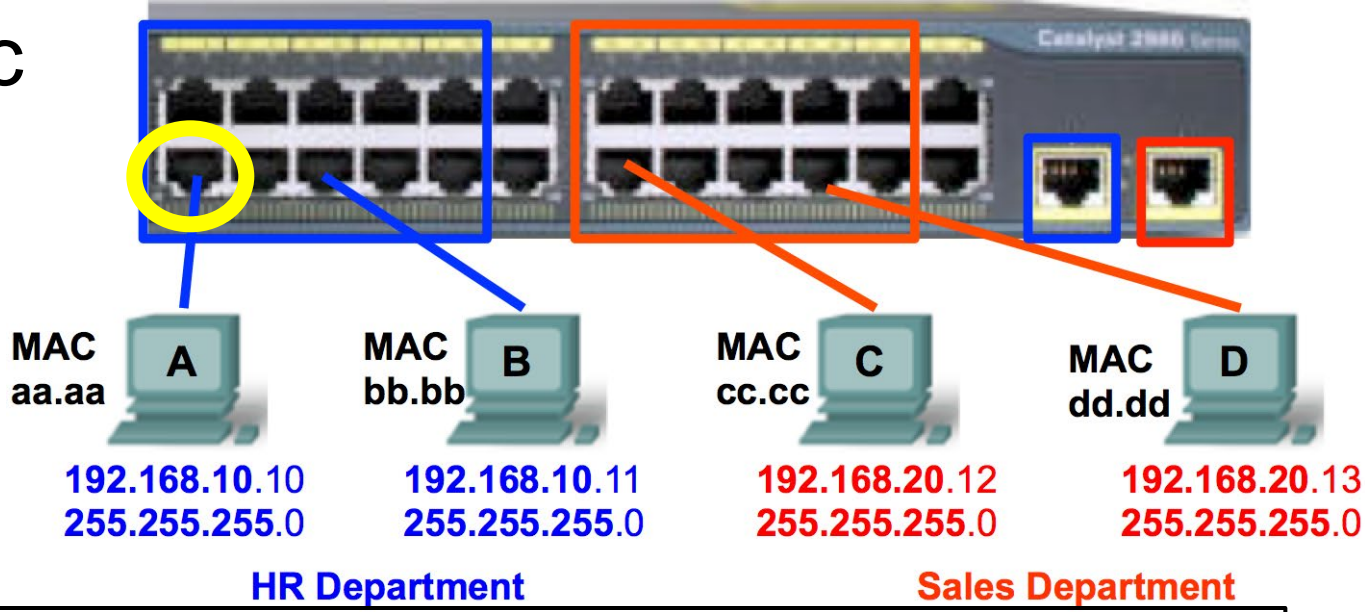
MAC cc.cc — C — 192.168.20.12 255.255.255.0

MAC dd.dd — D — 192.168.20.13 255.255.255.0

Sales Department

- These are VLANs used for different user VLANs/subnets
- For user data traffic
- What about the ports not in the Red or Blue VLAN?
- They are still in VLAN 1 (default VLAN)
- Change them to the Voice (VoIP) VLAN later.

Creating Static User VLANs




```
S1# configure terminal
S1(config)# vlan 10
S1(config-vlan)# name HR
S1(config-vlan)# exit
S1(config)# interface fastethernet 0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# end
S1#
```

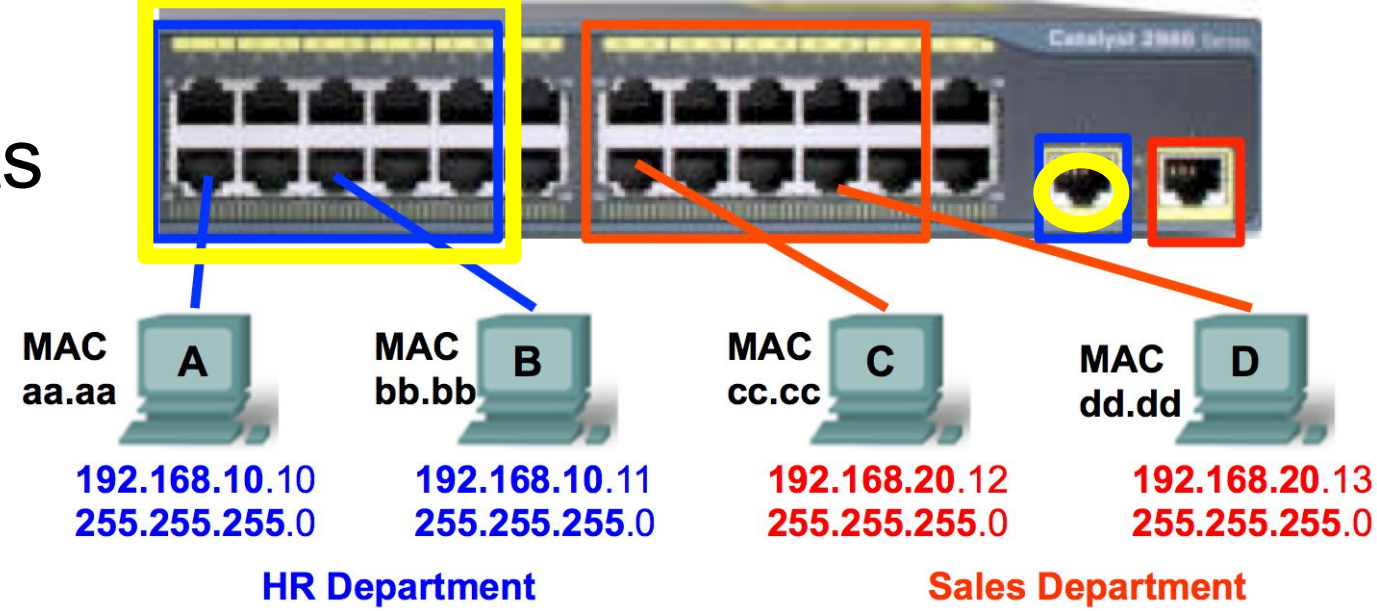
VLAN name is optional

Single host attached, not another switch (trunk)… later

VLAN 10 assigned to the port

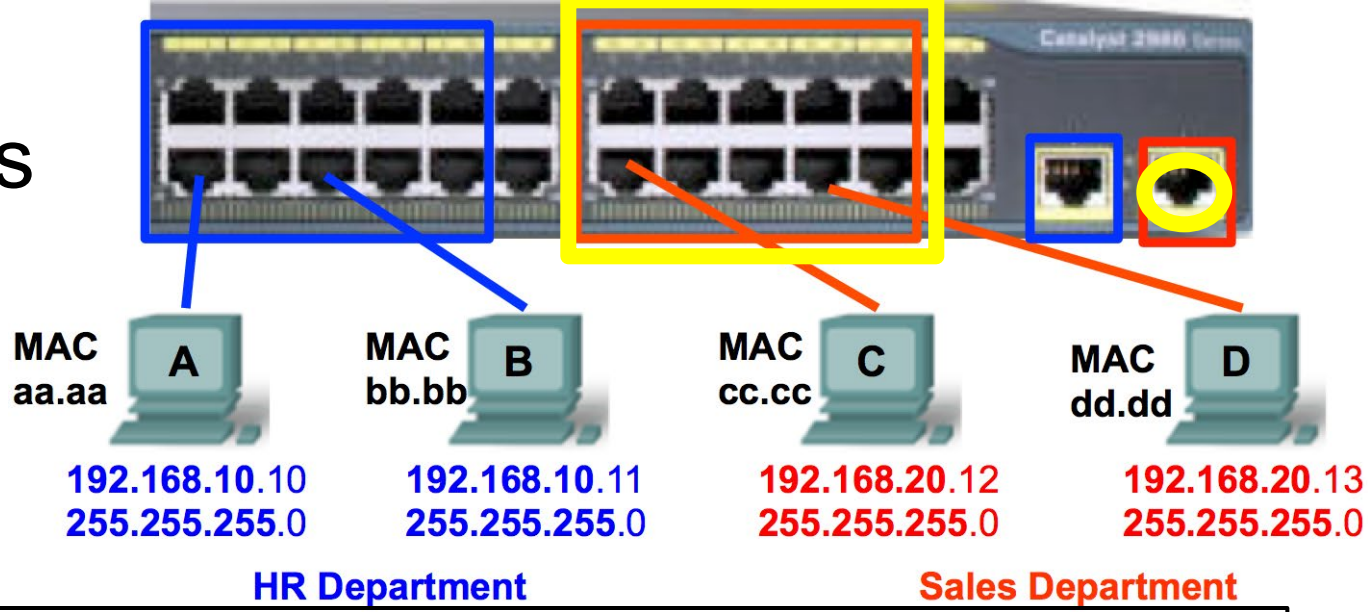
- Ports on a switch are manually assigned (CLI) to a VLAN.
  - If you assign an interface to a VLAN that does not exist, the new VLAN is created for you.
- Note: Dynamic VLANs can be configured using a special server called a VLAN Membership Policy Server (VMPS). Beyond the scope of this course.

Configuring a Range of Ports



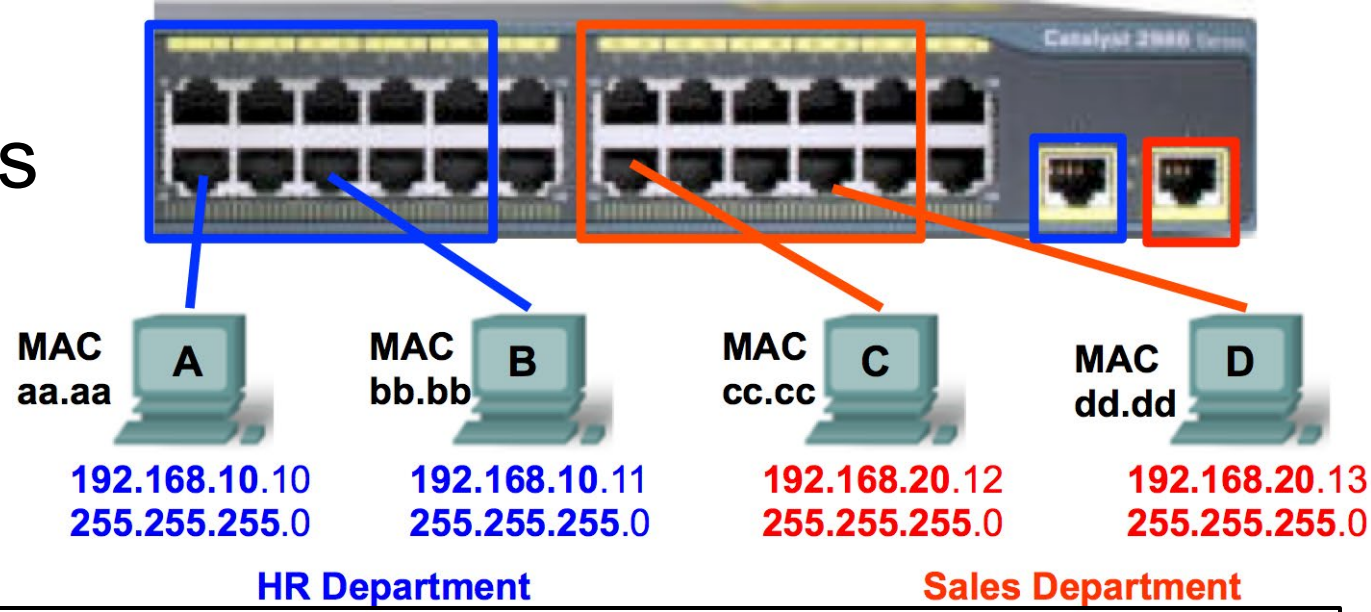

```
S1(config)# interface range fastethernet 0/1 - 10
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# exit
S1(config)# interface gigabitethernet 0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# end
S1#
```

Configuring a Range of Ports



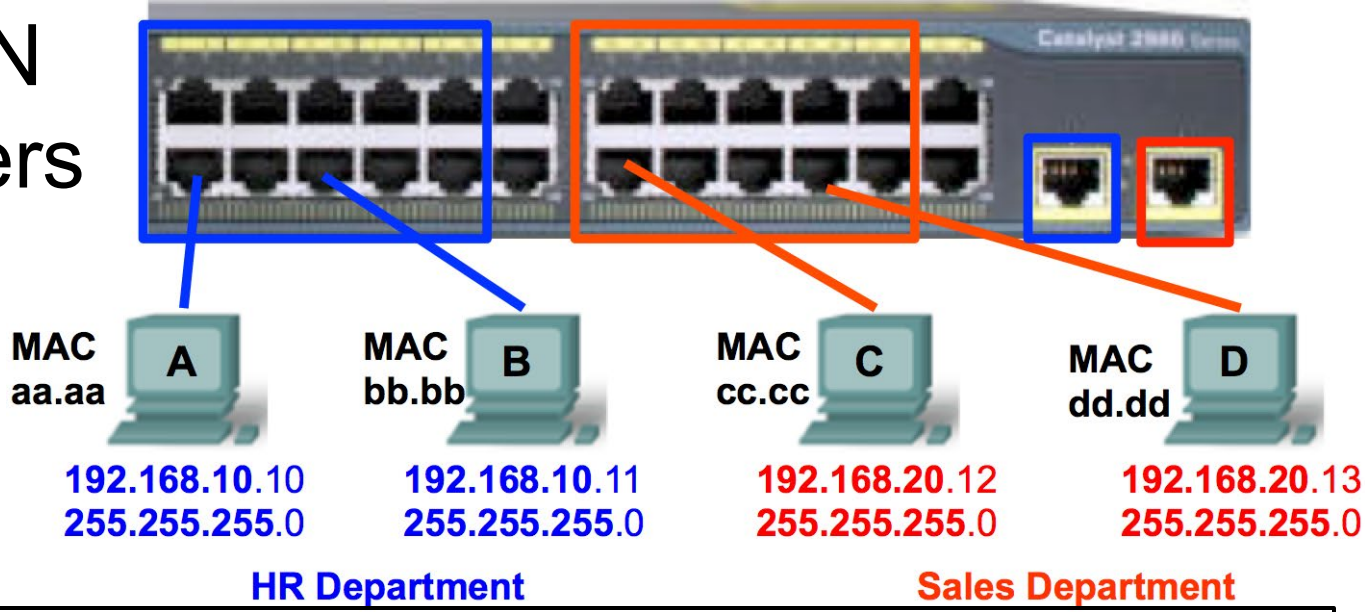

```
S1(config)# vlan 20
S1(config-vlan)# name SALES
S1(config-vlan)# exit
S1(config)# interface range fastethernet 0/13 - 22
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 20
S1(config-if-range)# exit
S1(config)# interface gigabitethernet 0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
```

Configuring a Range of Ports



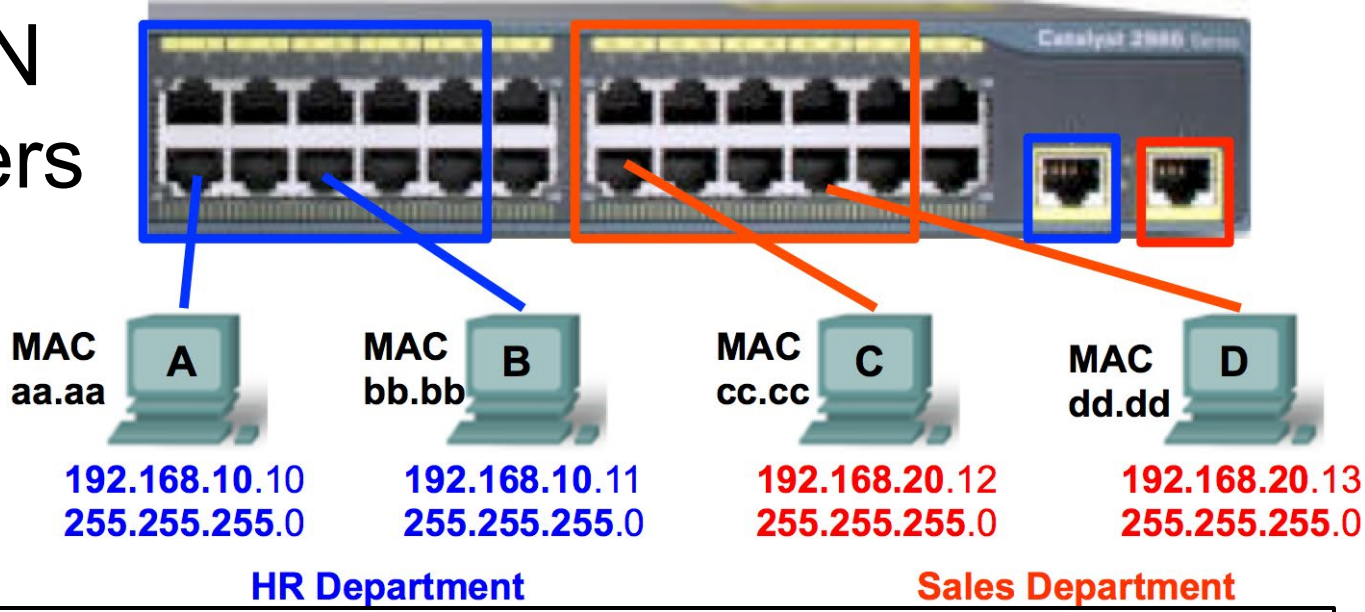

```
S1# show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/11, Fa0/12, Fa0/23, Fa0/24
10   HR                                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Gi0/1
20   SALES                             active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Gi0/2
```

Verifying VLAN Port Parameters




```
S1# show interface fa 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 10 (HR)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
<some output omitted>
S1#
```

Verifying VLAN Port Parameters




```
S1# show interface fa 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Verifying VLANs

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/11, Fa0/12, Fa0/23, Fa0/24
10   HR                                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Gi0/1
20   SALES                             active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
S1#
```

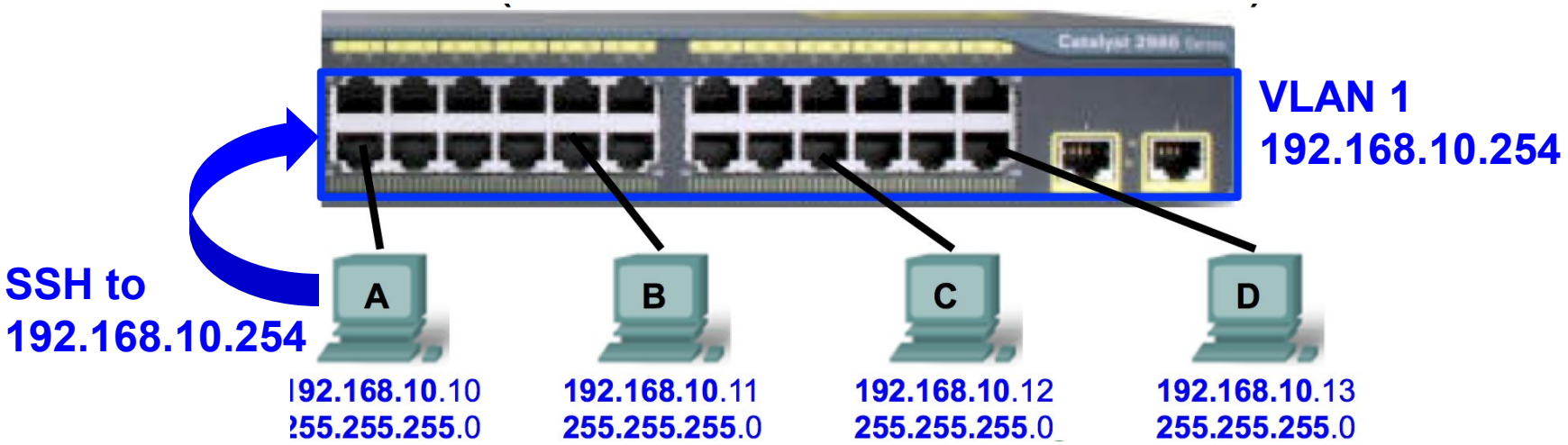
Verifying VLANs

```
S1# show vlan id 10

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
10   HR                                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Gi0/1

<output omitted>

S1# show vlan name SALES

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
20   SALES                             active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Gi0/2

<output omitted>

S1#
```

Verifying VLANs

```
S1(config)# vlan 444
S1(config-vlan)# end
S1# show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/11, Fa0/12, Fa0/23, Fa0/24
10   HR                                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Gi0/1
20   SALES                             active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Gi0/2
444  VLAN0444                          active
<output omitted>
S1# conf t
S1(config)# no vlan 444
S1(config)# end
S1# show vlan id 444
VLAN id 444 not found in current VLAN database
S1#
```

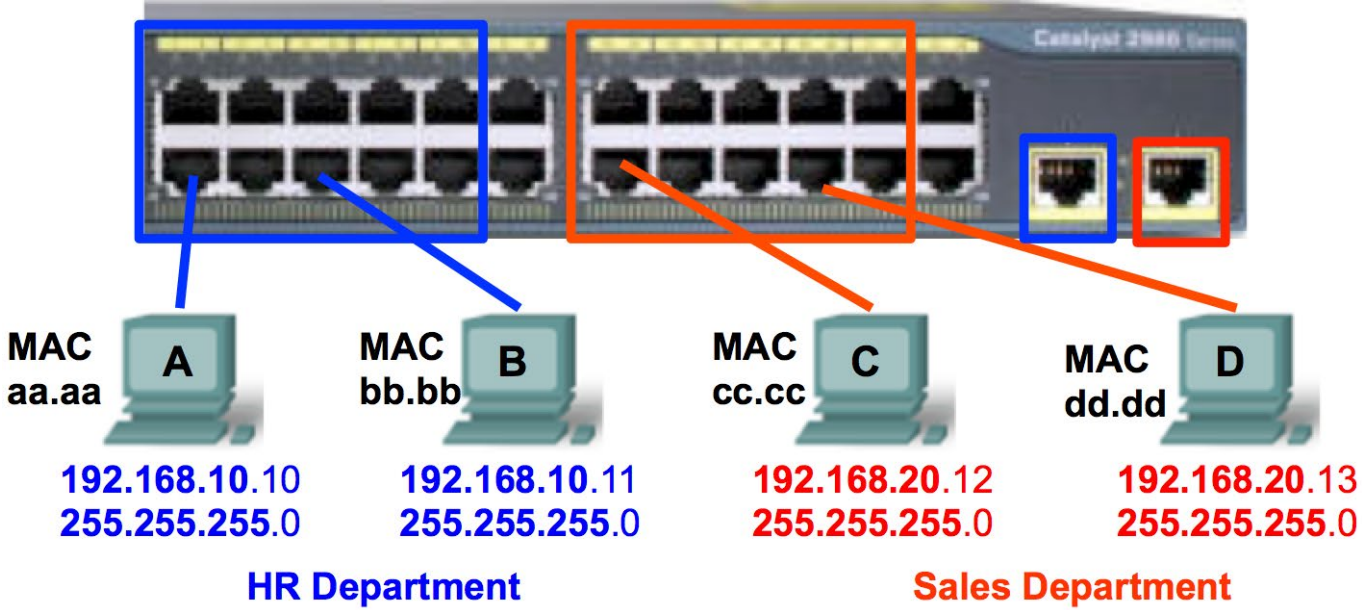
Management VLAN 1




```
S1(config)# inter vlan 1
S1(config-if)# description Management VLAN
S1(config-if)# ip address 192.168.10.254 255.255.255.0
S1(config-if)# no shutdown
```

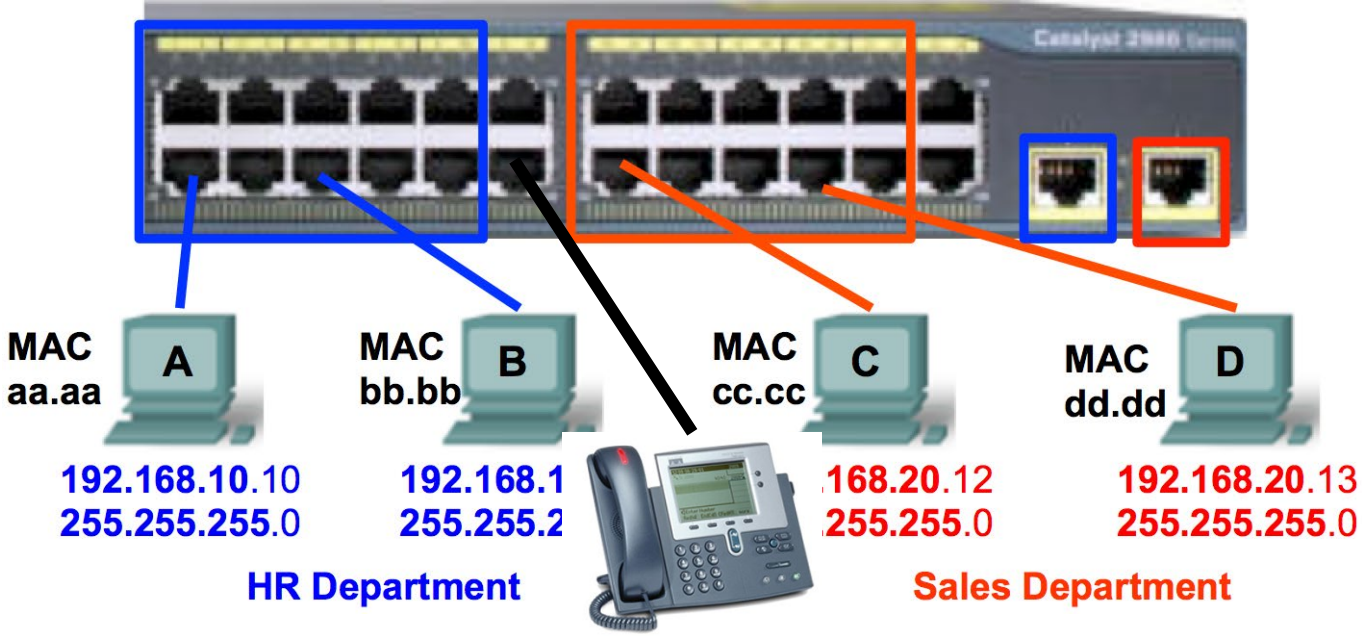
- A switch can be managed via HTTP, Telnet, SSH, or SNMP.
  - A management VLAN is used to manage the infrastructure devices including switches, routers, AP, etc.
- Security best practice is to change the management VLAN to a VLAN **other than VLAN 1.**
- We will discuss this later, because we will need to route to the management VLAN.

Native VLAN



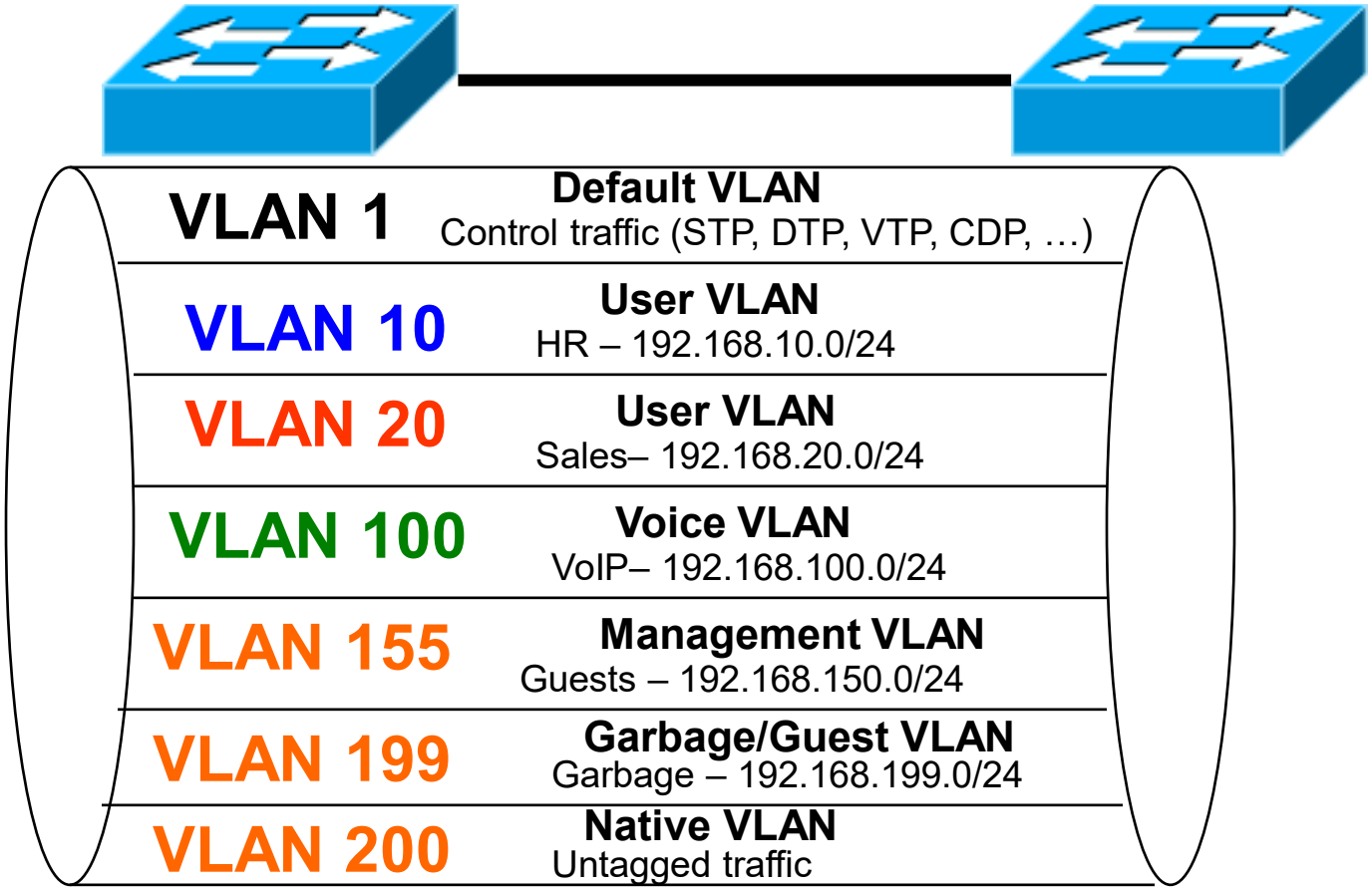
- A native VLAN is assigned to an IEEE 802.1Q trunk port (later).
  - Incoming traffic can be tagged (VLAN) or untagged traffic.
  - Native VLANs are set out in the IEEE 802.1Q specification to maintain backward compatibility with untagged traffic.
- Security best practice is to change the native VLAN to a VLAN other than VLAN 1.
- We will come back to this **later**…

Voice VLAN

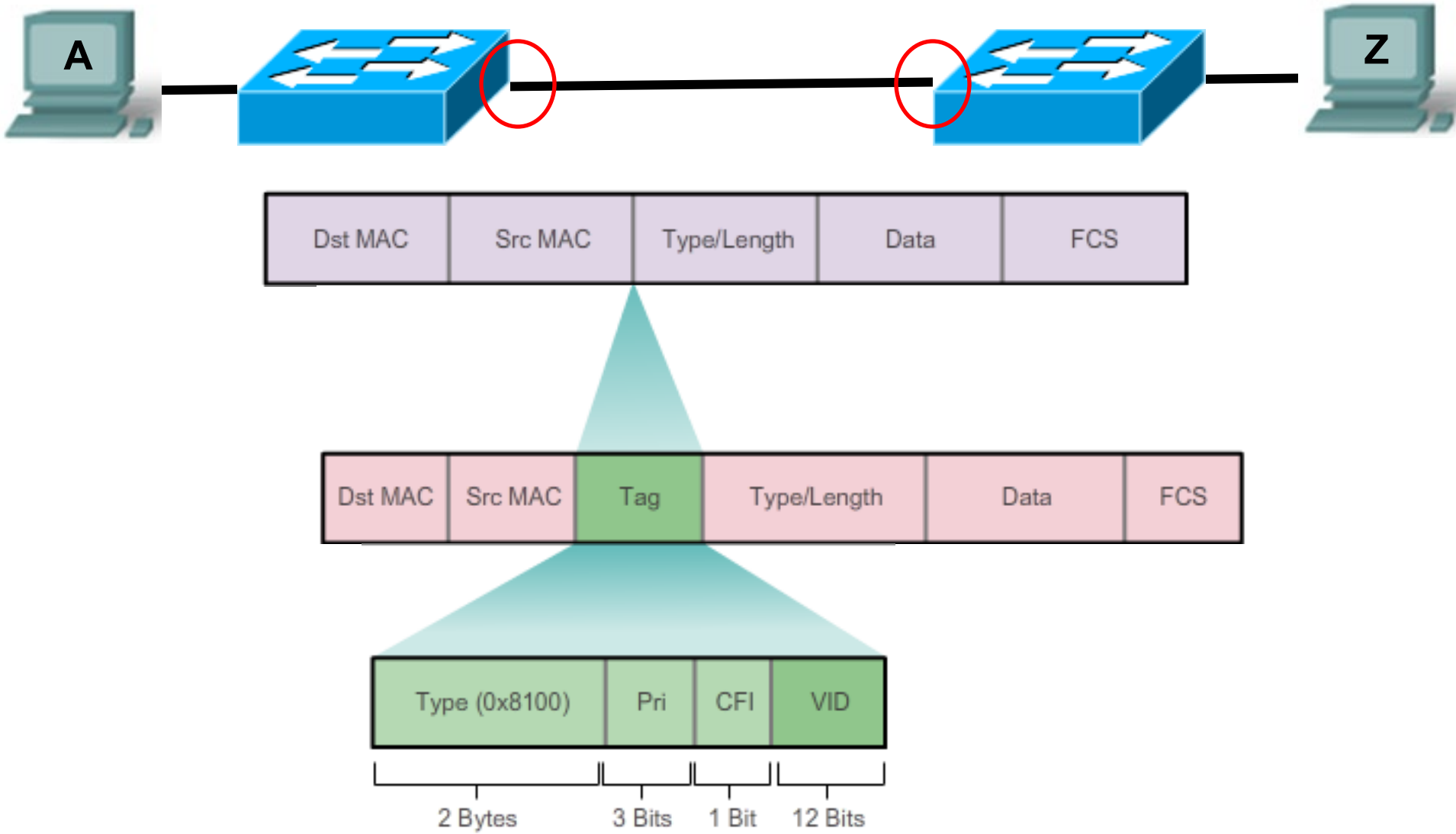


- VoIP traffic requires:
  - Assured bandwidth to ensure voice quality.
  - Transmission priority over other types of network traffic.
  - Ability to be routed around congested areas on the network.
  - Delay of less than 150 milliseconds (ms) across the network.
- Security best practice is that voice traffic must be placed in a separate VLAN.

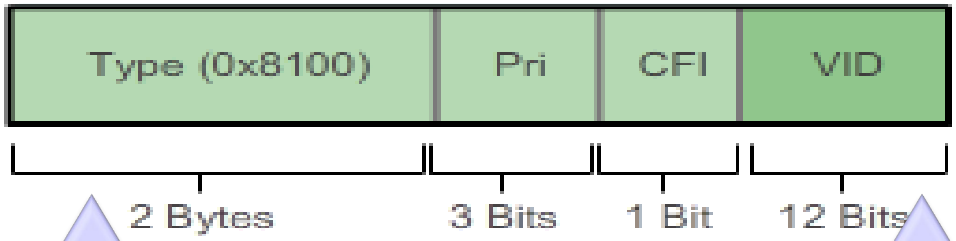
VLAN Trunks



- A point-to-point link that carries more than one VLAN.
- Extend VLANs across multiple switches
- Cisco supports 802.1Q standard
  - Some older switches support legacy Cisco ISL



- The TAG is **added** by the switch before it goes over a trunk link.
- The TAG is **removed** by the switch at the other end of the trunk link.



Tag protocol ID (TPID)

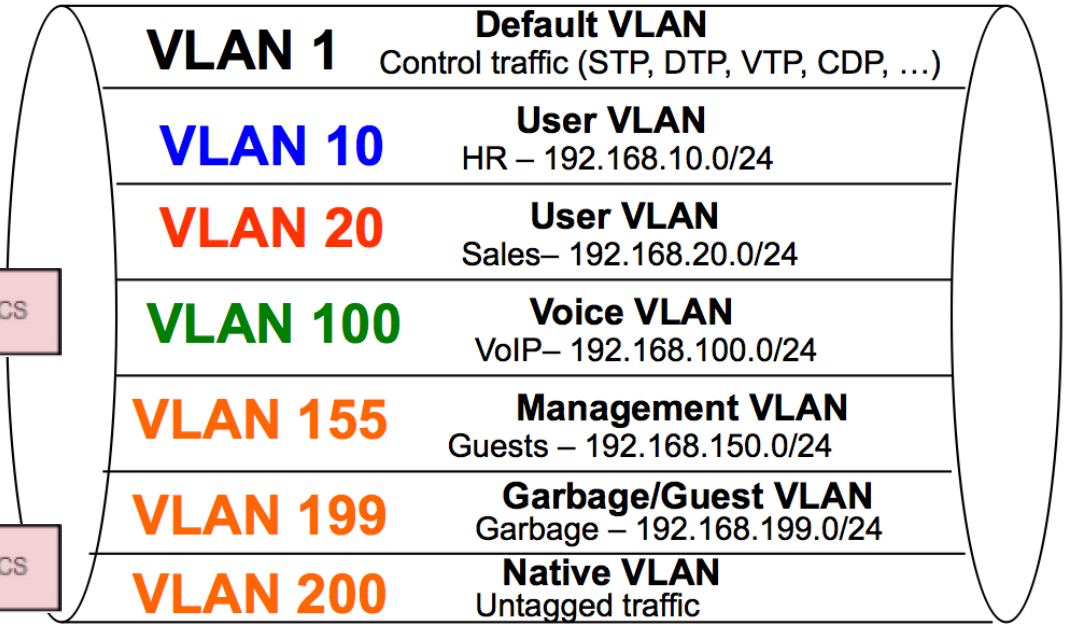
Ethernet is 0x8100.

Priority
Used for QoS (802.1p standard) specifies how to expedite transmission of Layer 2 frames

VLAN ID (VID)
VLAN identification number that supports up to 4096 VLAN IDs

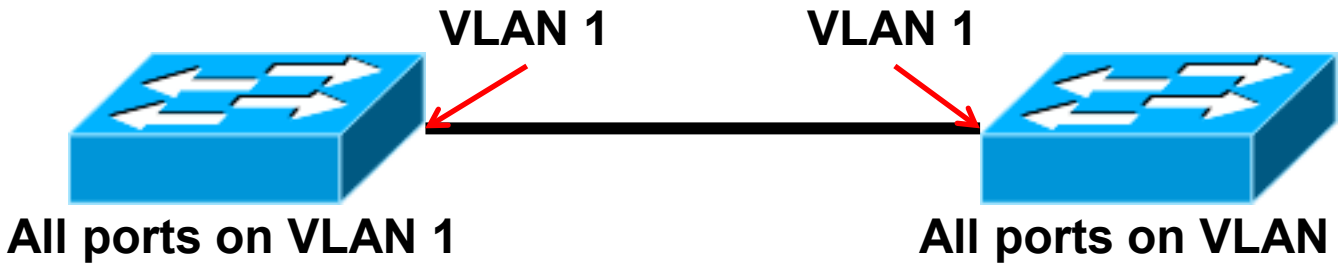
Canonical Format Identifier (CFI)
Enables Token Ring frames to be carried across Ethernet links

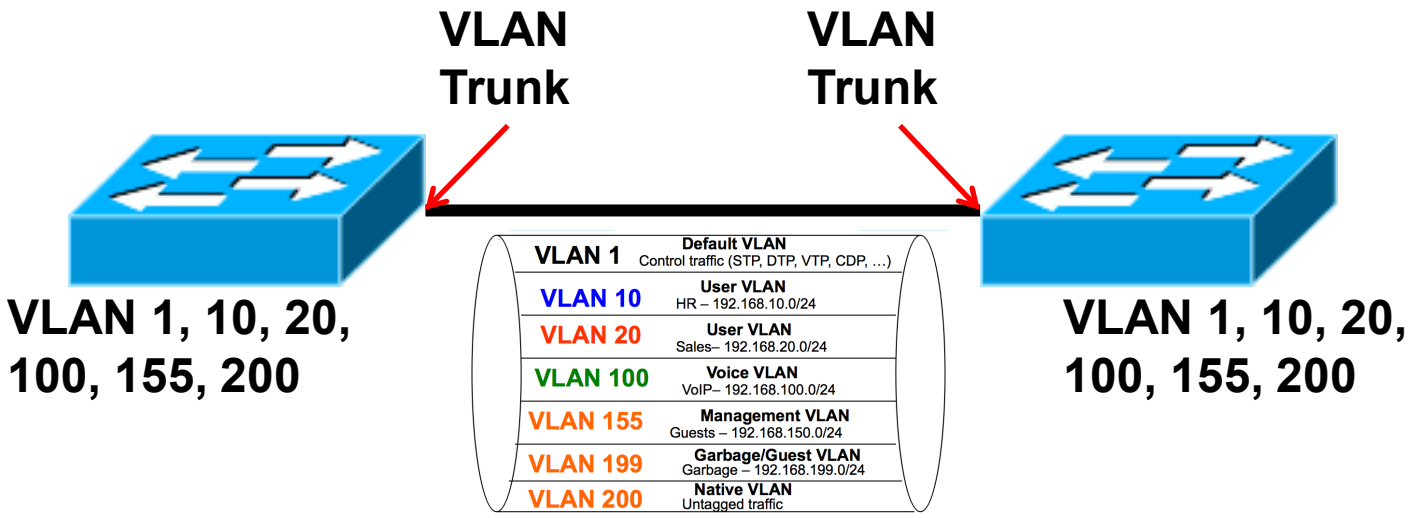
Native VLAN



- Native VLAN
  - For devices that do not support tagging.
  - All trunks must have a native VLAN
  - ***Native VLAN must be the same on both ends (both switches).***
  - Can be modified to be a VLAN other than VLAN 1.
  - Should **not** be used for user VLAN or Management VLAN.
  - Control traffic (CDP, VTP, PAgP, DTP) still transmitted over VLAN 1.
    - If Native VLAN is other than VLAN 1 then control traffic on VLAN 1 is sent tagged.
  - It is fine to leave VLAN 1 as the Native VLAN but should only carry control traffic and not user or management traffic.

Inter-switching links: Default and Trunking



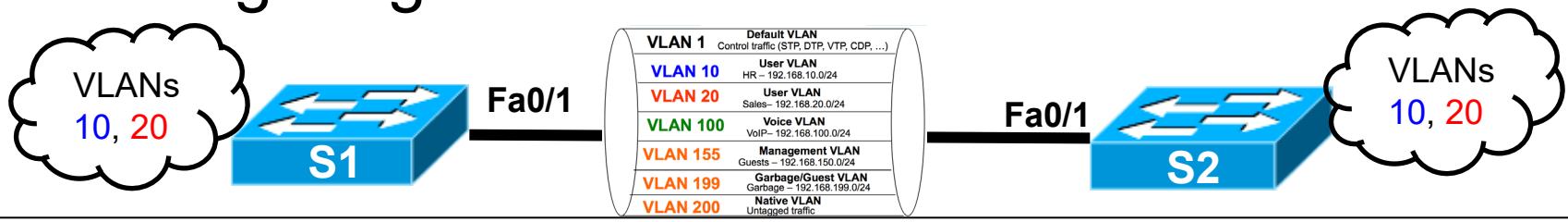


Configuring VLAN Trunks


```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/11, Fa0/12, Fa0/23, Fa0/24
10   HR                                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Gi0/1
20   SALES                             active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
```

```
S2# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
10   VLAN0010                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
20   VLAN0020                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20
```

Configuring VLAN Trunks

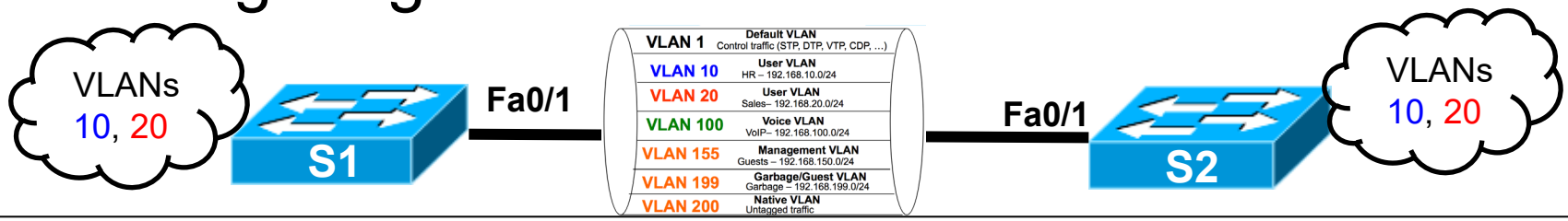



```
S1(config)# inter fa 0/1
S1(config-if)# no switchport access vlan 10
S1(config-if)# switchport trunk encapsulation dot1q
! Only needed on switches that also support ISL

S1(config-if)# switchport mode trunk
S1(config-if)#
```

```
S2(config)# inter fa 0/1
S2(config-if)# no switchport access vlan 10
S2(config-if)# switchport mode trunk
S2(config-if)#
```

- Minimum configuration.

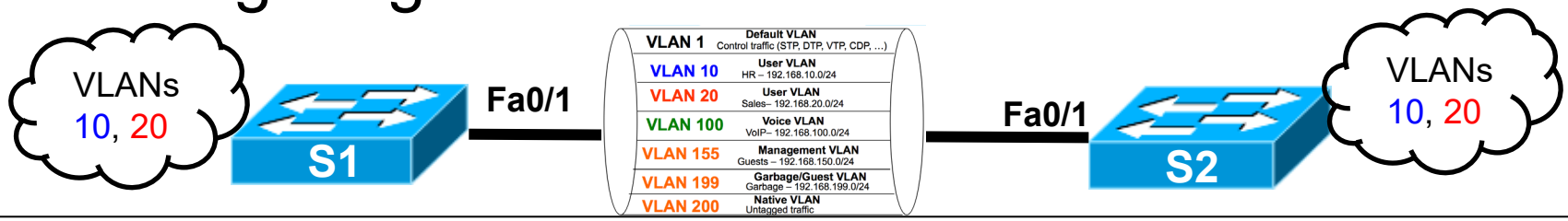
Configuring VLAN Trunks




```
S1# show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/11, Fa0/12, Fa0/23, Fa0/24
10   HR                                active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Gi0/1
20   SALES                             active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Gi0/2
```

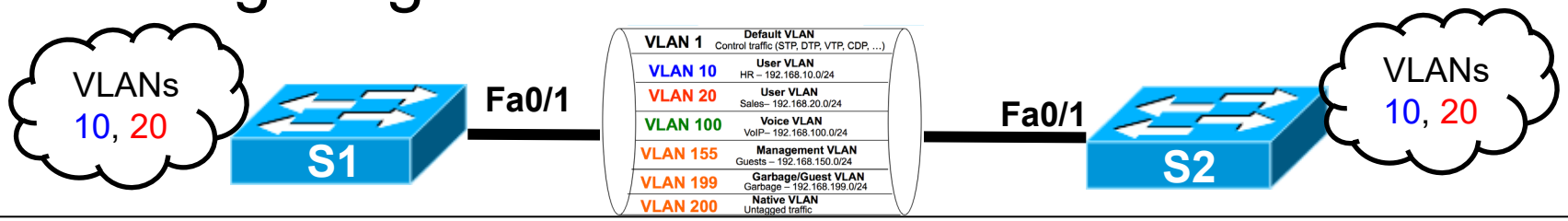
- No trunking information.
- Fa 0/1 no longer included in VLAN 10

Configuring VLAN Trunks




```
S1# show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       none
S1#
```

Configuring the Native VLAN

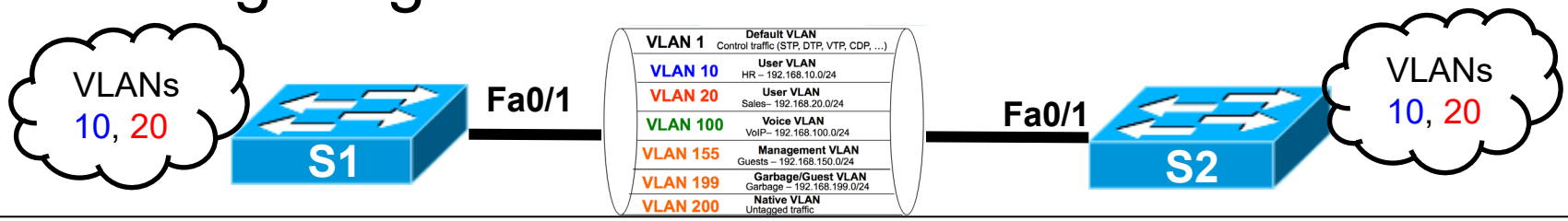



```
S1(config)# inter fa 0/1
S1(config-if)# switchport trunk native vlan 200
*Mar  1 01:59:34.927: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered
   on FastEthernet0/1 (200), with S2 FastEthernet0/1 (1)
S1(config-if)#
```

```
*Mar  1 02:00:39.267: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered
   on FastEthernet0/1 (1), with S1 FastEthernet0/1 (200).
S2(config)# inter fa 0/1
S2(config-if)# switchport trunk native vlan 200
S2(config-if)#
```

- VLAN 200 (Native VLAN) does not need to be created on either switch but…
- It must match on both ends of the trunk!
- Control data (CDP, STP, etc.) is still sent across VLAN 1 but is now tagged.

Configuring the Native VLAN

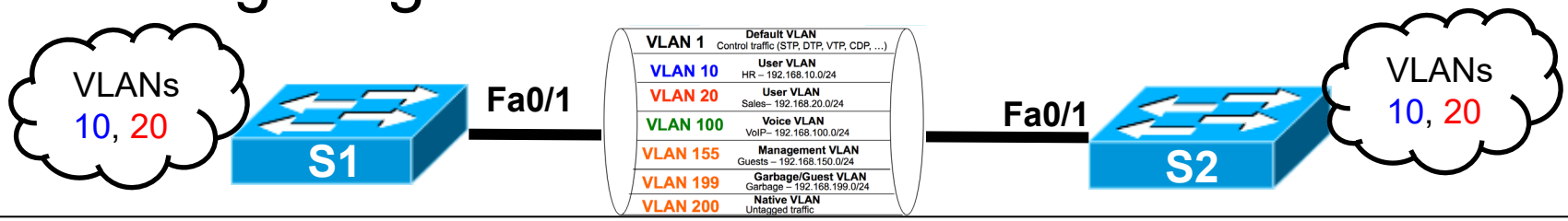



```
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      200

Port        Vlans allowed on trunk
Fa0/1       1-4094
```

```
S2# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      200

Port        Vlans allowed on trunk
Fa0/1       1-4094
```

- Happy native VLANs now!
- How about limiting which VLANs are allowed on the trunk?

Configuring Allowed VLANs

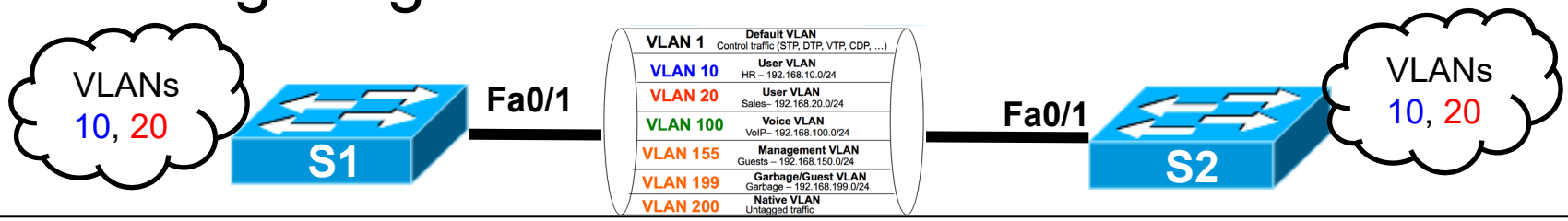



```
S1(config)# inter fa 0/1
S1(config-if)# switchport trunk allowed vlan 10,20,200
```

```
S2(config)# inter fa 0/1
S2(config-if)# switchport trunk allowed vlan 10,20,200
```

- No space between VLANs.
- If the native VLAN (200) is not on the list, it is not a problem.
- The trunk will not allow any data traffic for the native VLAN.

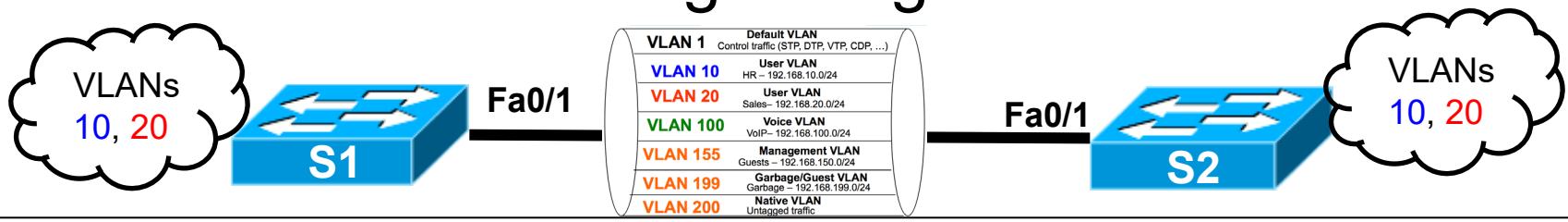
Configuring Allowed VLANs




```
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      200

Port        Vlans allowed on trunk
Fa0/1       10,20,200
```

```
S2# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      200

Port        Vlans allowed on trunk
Fa0/1       10,20,200
```

What's in the running-config?

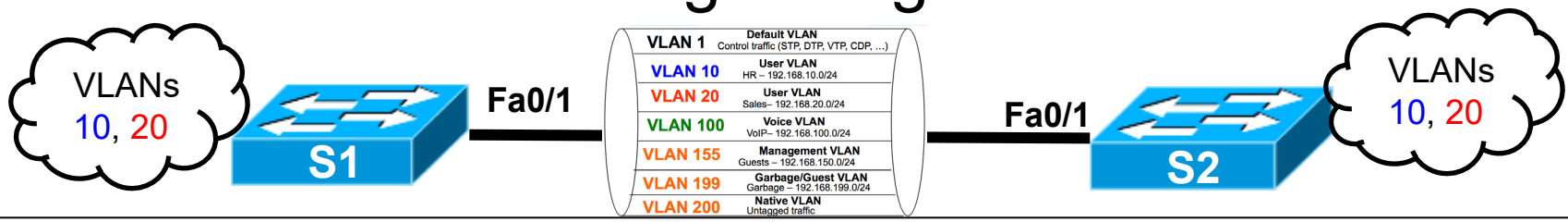



```
interface FastEthernet0/1
 switchport trunk native vlan 200
 switchport trunk allowed vlan 10,20,200
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access

<continued>
```

Trunk link

VLAN 10 access port

What's in the running-config?

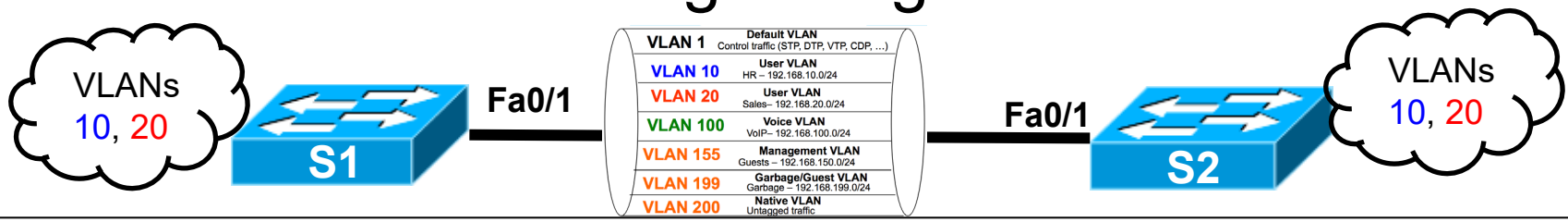



```
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 20
 switchport mode access
```

No configuring…. Default VLAN 1
(Should be in garbage, temporary VLAN if port is not in use)

VLAN 20 access port

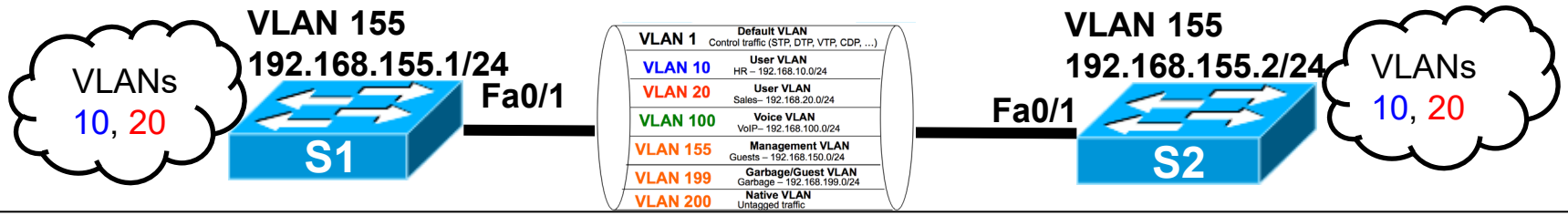
What's in the running-config?




```
!
interface Vlan1
 no ip address
 shutdown
!
```

SVI (Switch Virtual Interface)
Management VLAN
No current IP Address
Still in VLAN 1

Configuring Management VLAN

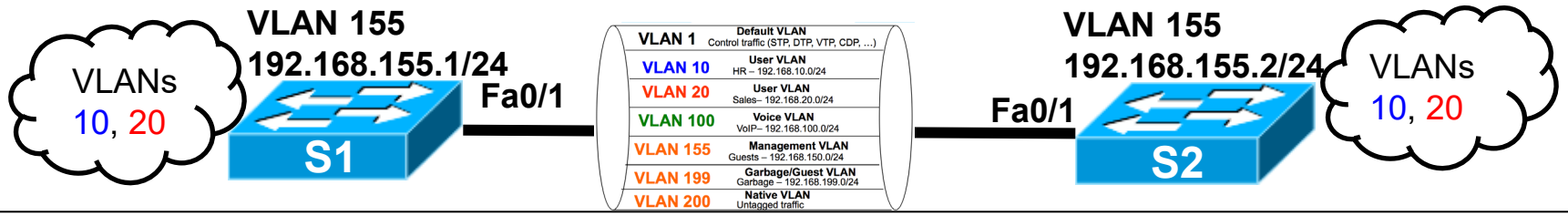



```
S1(config)# interface vlan 155
S1(config-if)# ip address 192.168.155.1 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# vlan 155
S1(config-vlan)# name MANAGEMENT
S1(config-vlan)#
```

```
S2(config)# interface vlan 155
S2(config-if)# ip add 192.168.155.2 255.255.255.0
S2(config-if)# no shutdown
S2(config-if)# exit
S2(config)# vlan 155
S2(config-vlan)# name MANAGMENT
S2(config-vlan)# end
S2# ping 192.168.155.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.158.155.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

???

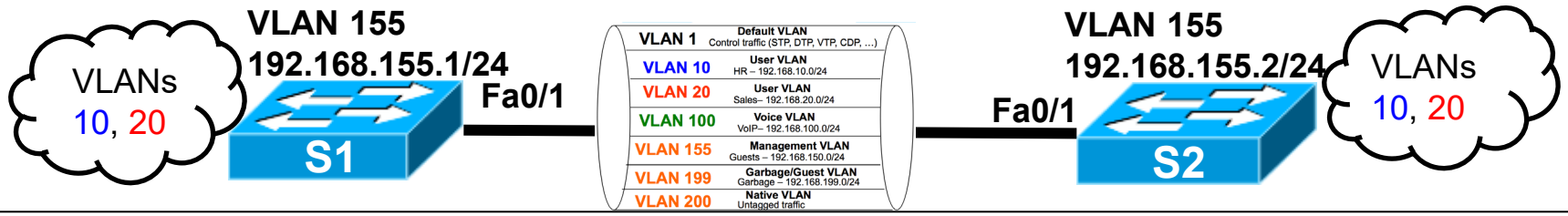
Configuring Management VLAN




```
S1(config)# inter fa 0/1
S1(config-if)# switchport trunk allowed vlan 10,20,200,155
```

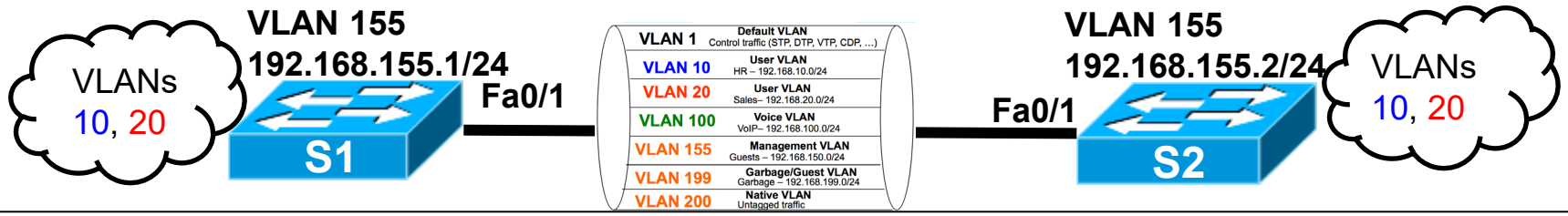
```
S1(config)# inter fa 0/1
S1(config-if)# switchport trunk allowed vlan 10,20,200,155
S1(config-if)# end
S2# ping 192.168.155.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.155.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
S2#
```

Verifying VLANs Once More



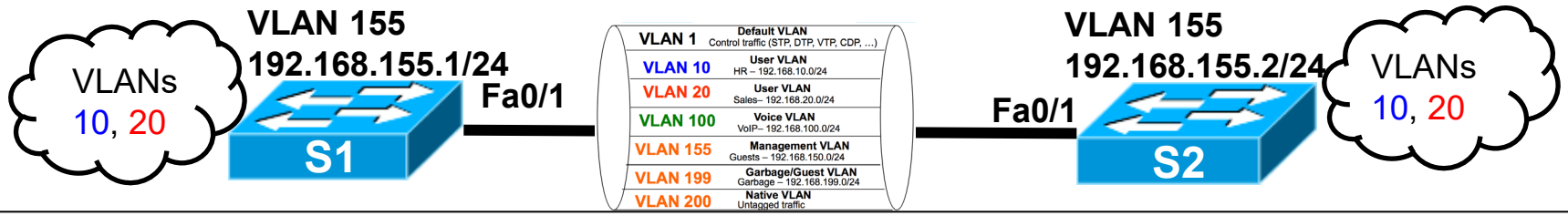

```
S1# show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/11, Fa0/12, Fa0/23, Fa0/24
10   HR                                active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Gi0/1
20   SALES                             active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Gi0/2
155  MANAGEMENT                        active
```

Verifying VLANs Once More




```
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      200

Port        Vlans allowed on trunk
Fa0/1       10,20,155,200

S1# show interface vlan 155
Vlan155 is up, line protocol is up
  Hardware is EtherSVI, address is 189c.5dff.fac1 (bia 189c.5dff.fac1)
  Internet address is 192.168.155.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported

<output omitted>
```

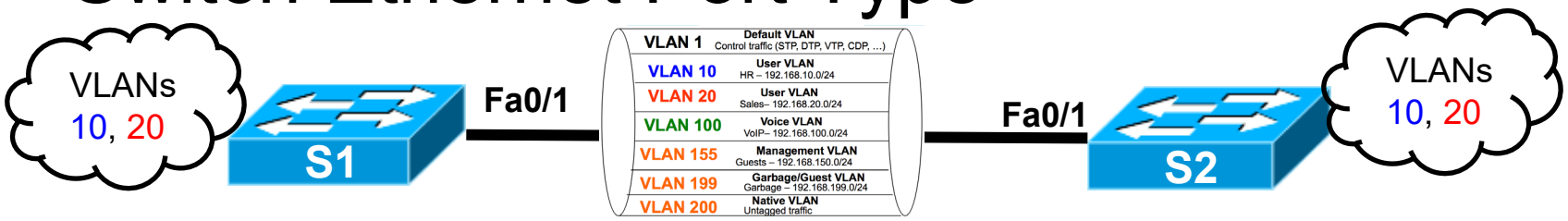
Verifying VLANs Once More




```
S1# show interface fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 200 (Inactive)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<output omitted>
Trunking VLANs Enabled: 10,20,155,200
```

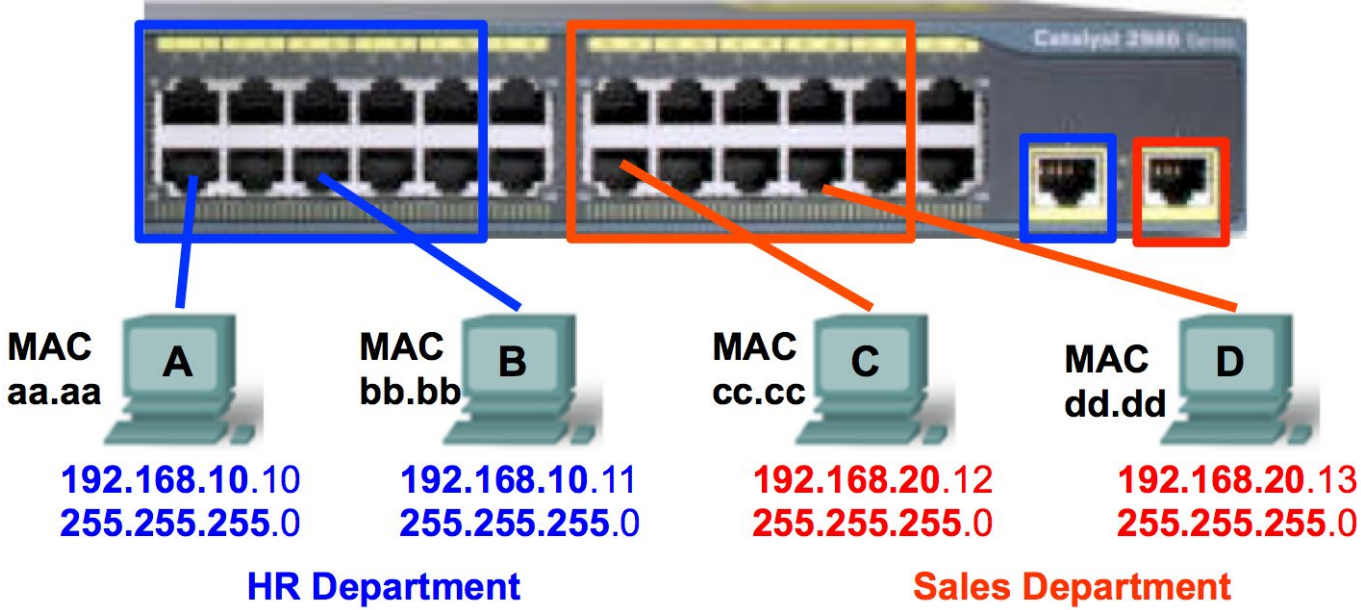
Dynamic Trunk Protocol

Switch Ethernet Port Type



- Switch Ethernet ports can be set to:
  - **Mode access:** Non-trunking port used to connect to end-devices.
  - **Mode trunk:** Trunking port to carry VLAN information to another switch.

Access Port

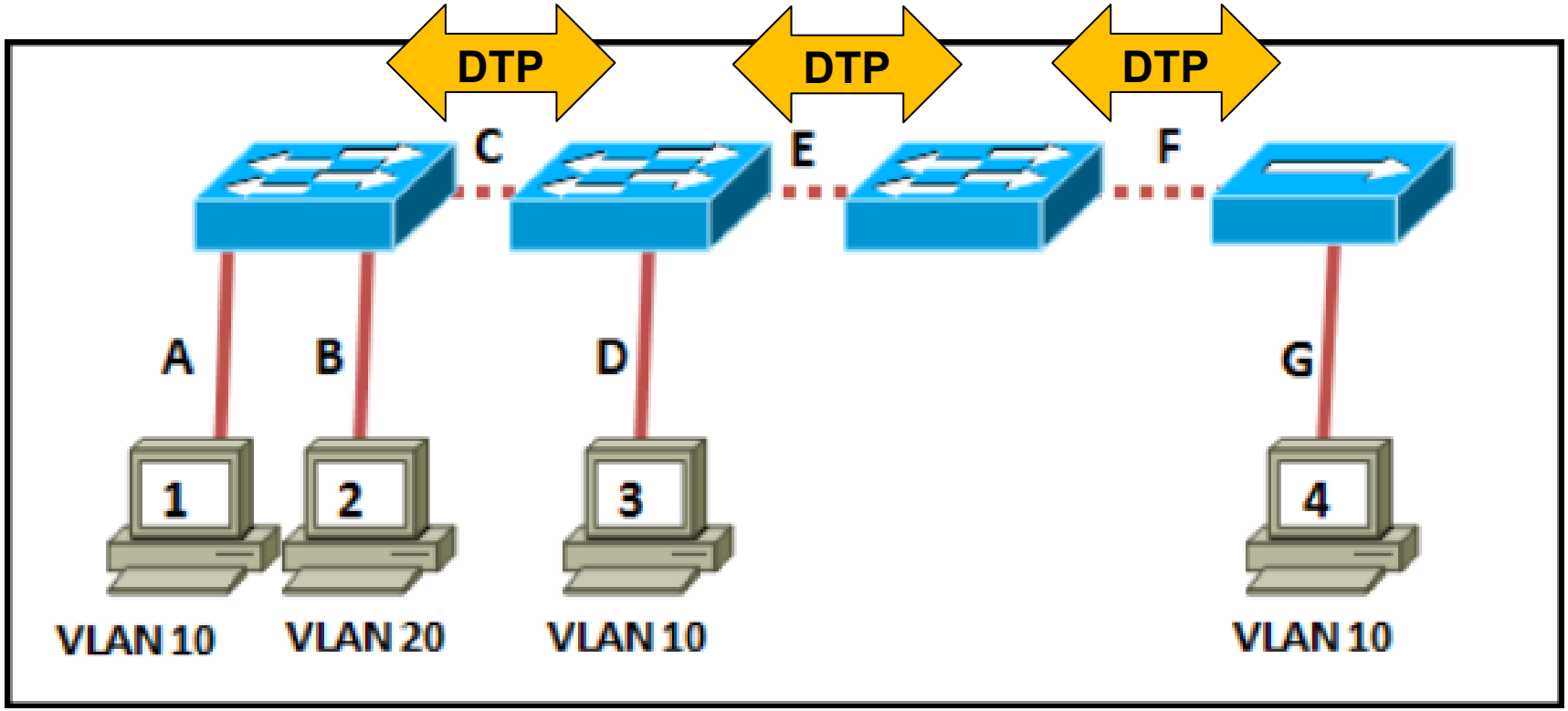


S1(config-if) # **`switchport mode access`**

- Forces the link into access port.
- **It will never become a trunk!**

- Use to connect a host, server, printer, …

Dynamic Trunking Protocol - DTP



- DTP is a Cisco proprietary protocol that negotiates trunking parameters between switches.
  - Operates on a point-to-point basis only, between network devices.
  - Designed to make interconnecting switches with VLANs easier.
- DTP is only available on Cisco switches and not supported by other vendors.

Four DTP Trunking Modes

```
S1(config-if)# switchport mode ?
  access    Set trunking mode to ACCESS unconditionally
  dynamic   Set trunking mode to dynamically negotiate access or trunk mode
  trunk     Set trunking mode to TRUNK unconditionally
S1(config-if)# switchport mode dynamic ?
  auto      Set trunking mode dynamic negotiation parameter to AUTO
  desirable Set trunking mode dynamic negotiation parameter to DESIRABLE
S1(config-if)# switchport mode dynamic
```

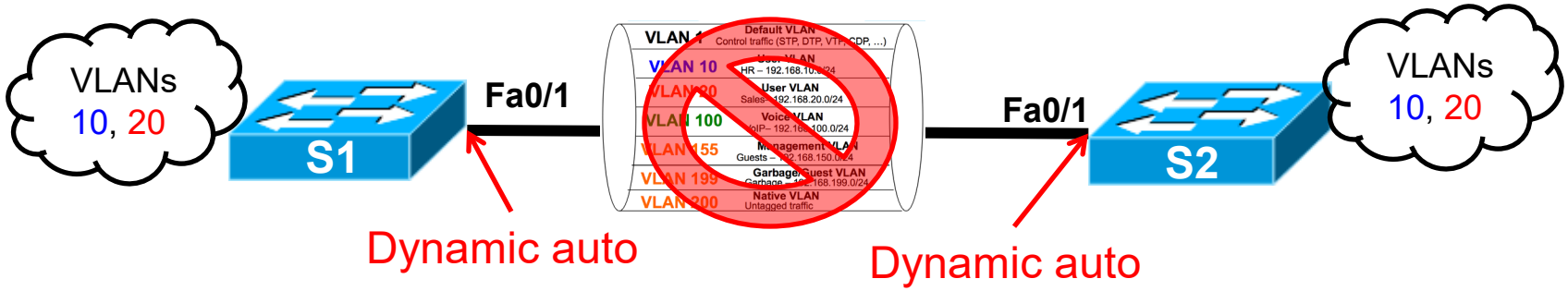
- **On (default): Default mode.** It's locked into TRUNK mode.
  - **`switchport mode trunk`**
- **Dynamic Desirable:** (default mode on Catalyst 2950 / 3550)
  - **`switchport mode dynamic desirable`**
- **Dynamic Auto:**
  - **`switchport mode dynamic auto`**
- **Disabled:** Nonegotiate. Turns off DTP.
  - **`switchport nonegotiate`**

Non-trunking by default

```
S2# show interfaces fastethernet 0/21 switchport
Name: Fa0/21
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

How the port was configured.

How the is operating.



- Ports on the 2960 and 3560 are set to **dynamic auto** by default.
  - Does not trunk if both sides default to **dynamic auto**
- This results in the interface being in access mode (non-trunking)

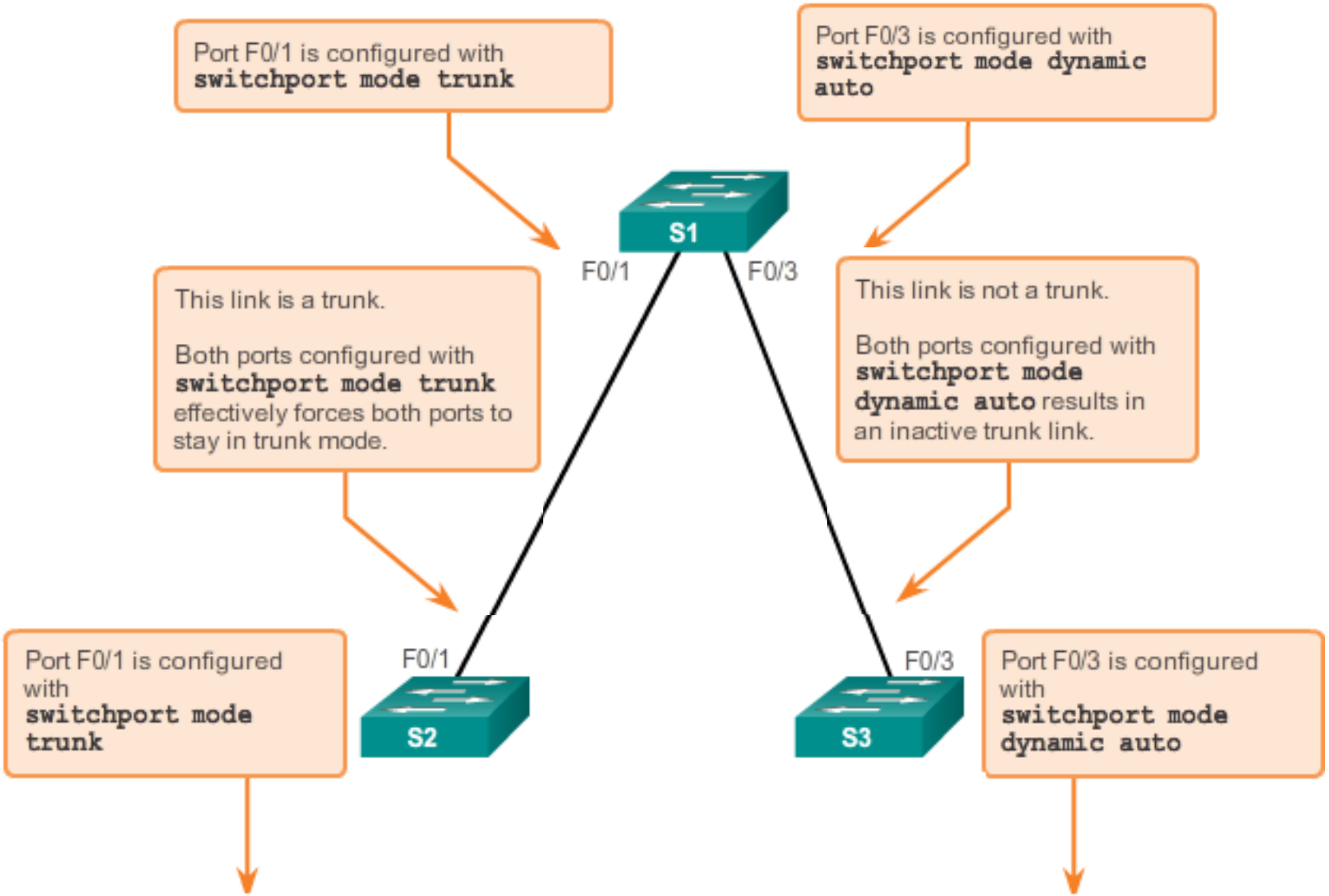
```
S1(config-if)# switchport mode ?
```

Dynamic Trunking Protocol (DTP)

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

- **Access** - Puts the interface into **permanent non-trunking mode** and **negotiates to convert the link into a non-trunk link.** The interface becomes a non-trunk interface even if the neighboring interface does not agree to the change.
- **Trunk** - Puts the interface into **permanent trunking mode** and **negotiates to convert the link into a trunk** link. The interface becomes a trunk interface even if the neighboring interface does not agree to the change.
- **Nonegotiate** - Puts the interface into **permanent trunking mode but prevents the interface from generating DTP frames**. You must configure the neighboring interface manually as a trunk interface to establish a trunk link. Use this mode when connecting to a device that does not support DTP.
- **Dynamic desirable** - Makes the interface **actively attempt to convert the link to a trunk link**. The interface becomes a **trunk** interface **if** the neighboring interface is set to **trunk, desirable, or auto mode**.
- **Dynamic auto** - Makes the interface **willing to convert the link to a trunk link**. The interface becomes a trunk interface **if** the neighboring interface is set to **trunk or desirable mode**. This is the **default mode for all Ethernet interfaces in Cisco IOS.**

Trunk Modes Must be Compatible



DTP Mode: On (default)

- S1(config-if) # **`switchport mode trunk`**
  - Forces the link into permanent trunking (even if the neighbor doesn't agree)
  - **Enables DTP** and exchanges DTP frames.

- Will trunk if remote is configured with:
  - **On** `switchport mode trunk`
  - **Desirable** `switchport mode dynamic desirable`
  - **Dynamic Auto** `switchport mode dynamic auto`

- Will not trunk if remote is configured with:
  - **Non-negotiate** `switchport nonegotiate`
  - **Access** `switchport mode access`

DTP Dynamic Desirable

- S1(config-if) # **`switchport mode dynamic desirable`**
  - Causes the port to proactively attempt to become a trunk.
  - **Enables DTP** and exchanges DTP frames.

- Will trunk if remote is configured with:
  - **On** `switchport mode trunk`
  - **Desirable** `switchport mode dynamic desirable`
  - **Dynamic Auto** `switchport mode dynamic auto`

- Will not trunk if remote is configured with:
  - **Non-negotiate** `switchport nonegotiate`
  - **Access** `switchport mode access`

DTP Dynamic Auto

- S1(config-if) # **`switchport mode dynamic auto`**
  - Causes the port to passively be willing to convert to trunking.
  - **Enables DTP** and exchanges DTP frames.

- Will trunk if remote is configured with:
  - **On** **`switchport mode trunk`**
  - **Desirable** **`switchport mode dynamic desirable`**

- Will not trunk if remote is configured with:
  - **Dynamic Auto** **`switchport mode dynamic auto`**
  - **Non-negotiate** `switchport nonegotiate`
  - **Access** `switchport mode access`

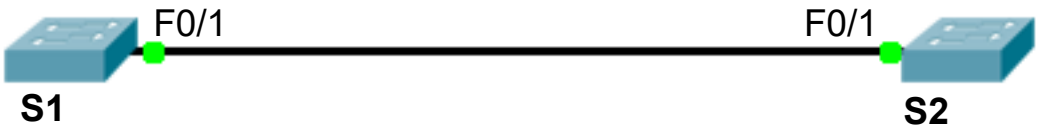
DTP Disabled

- S1(config-if) # `switchport nonegotiate`
  - Forces the port to permanently trunk.
  - **Disables DTP** and does not exchange any DTP frames.

- Use to trunk with a different vendor's switch.

#1 - “Trunk ” or “No Trunk”

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
```

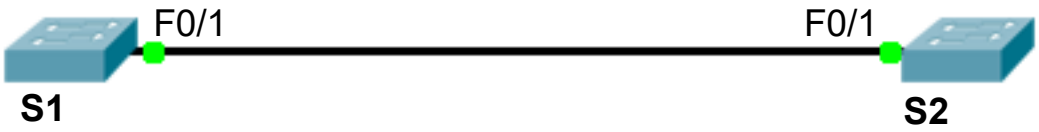



```
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
```

- Will the ports trunk automatically?

#2 - “Trunk ” or “No Trunk”

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
```

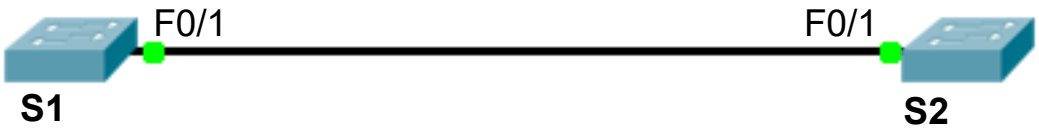



```
S2(config)# interface fa0/1
S2(config-if)# switchport mode dynamic desirable
```

- Will the ports trunk automatically?

#3 - “Trunk ” or “No Trunk”

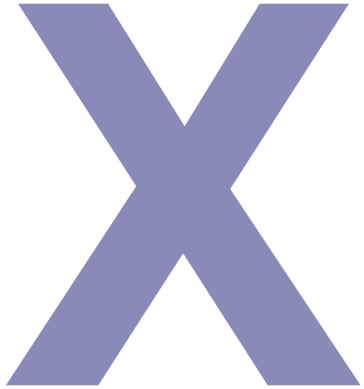
```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
```



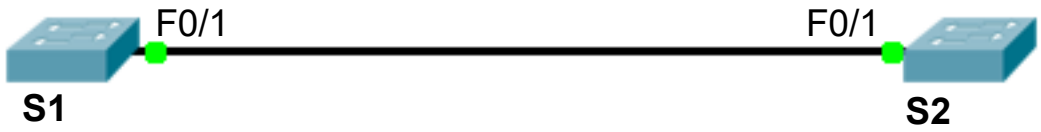

```
S2(config)# interface fa0/1
S2(config-if)# switchport mode dynamic auto
```

- Will the ports trunk automatically?

#4 - “Trunk ” or “No Trunk”



```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
```

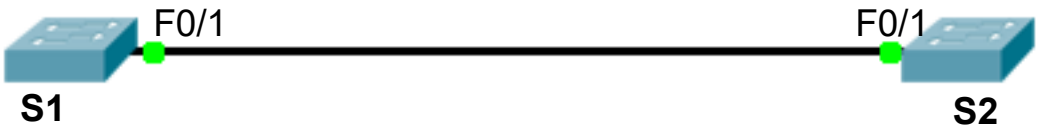



```
S2(config)# interface fa0/1
S2(config-if)# switchport nonegotiate
```

- Will the ports trunk automatically?

#5 - “Trunk ” or “No Trunk”

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode dynamic desirable
```

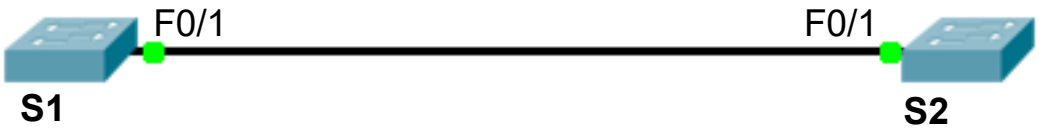



```
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
```

- Will the ports trunk automatically?

#6 - “Trunk ” or “No Trunk”

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode dynamic desirable
```

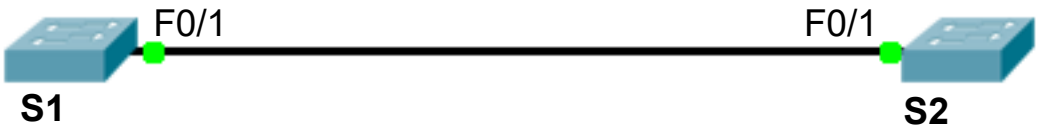



```
S2(config)# interface fa0/1
S2(config-if)# switchport mode dynamic desirable
```

- Will the ports trunk automatically?

#7 - “Trunk ” or “No Trunk”

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode dynamic desirable
```

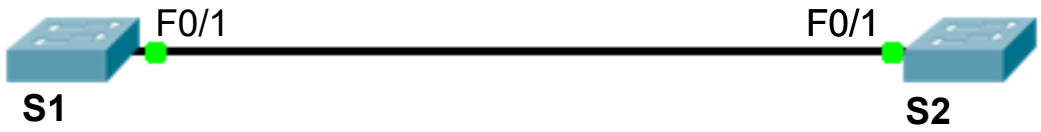



```
S2(config)# interface fa0/1
S2(config-if)# switchport mode dynamic auto
```

- Will the ports trunk automatically?

#8 - “Trunk ” or “No Trunk”

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode dynamic desirable
```

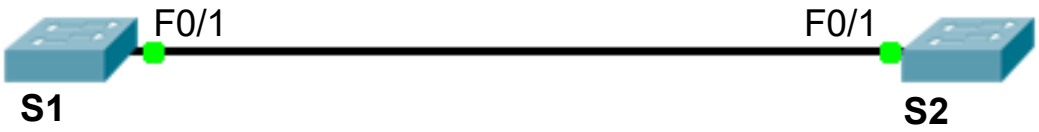



```
S2(config)# interface fa0/1
S2(config-if)# switchport nonegotiate
```

- Will the ports trunk automatically?

#9 - “Trunk ” or “No Trunk”

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode dynamic auto
```

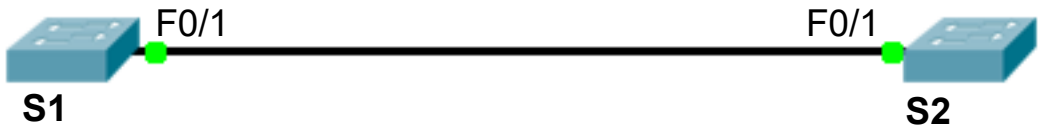



```
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
```

- Will the ports trunk automatically?

#10 - “Trunk ” or “No Trunk”

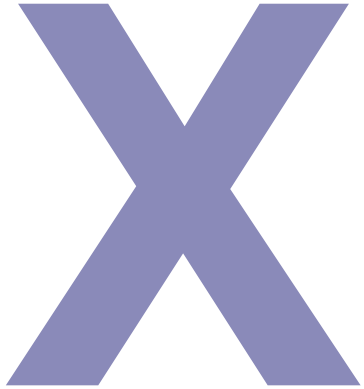
```
S1(config)# interface fa0/1
S1(config-if)# switchport mode dynamic auto
```



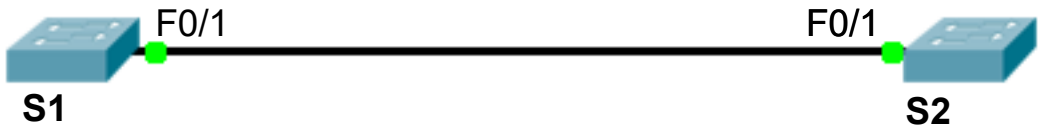

```
S2(config)# interface fa0/1
S2(config-if)# switchport mode dynamic desirable
```

- Will the ports trunk automatically?

#11 - “Trunk ” or “No Trunk”



```
S1(config)# interface fa0/1
S1(config-if)# switchport mode dynamic auto
```

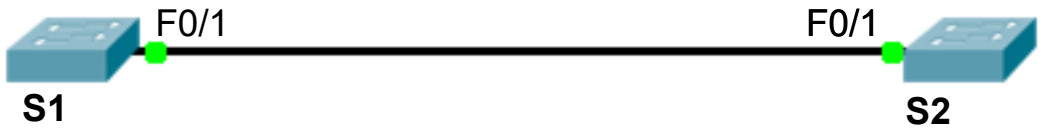



```
S2(config)# interface fa0/1
S2(config-if)# switchport mode dynamic auto
```

- Will the ports trunk automatically?

#12 - “Trunk ” or “No Trunk”

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode dynamic auto
```

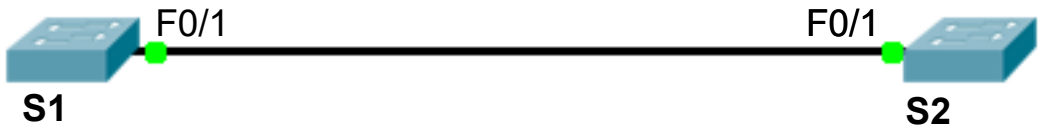



```
S2(config)# interface fa0/1
S2(config-if)# switchport nonegotiate
```

- Will the ports trunk automatically?

#13 - “Trunk ” or “No Trunk”

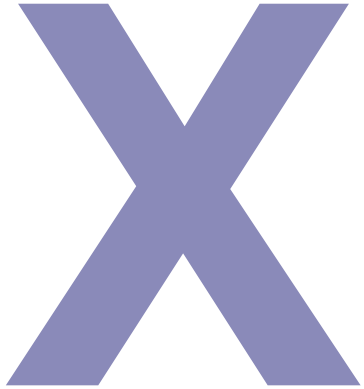
```
S1(config)# interface fa0/1
S1(config-if)# switchport nonegotiate
```



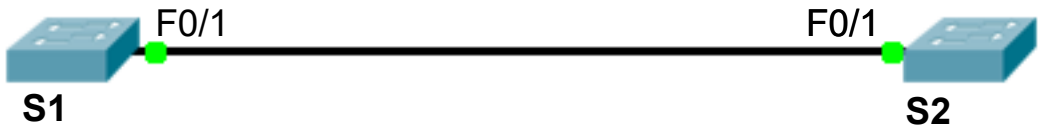

```
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
```

- Will the ports trunk automatically?

#14 - “Trunk ” or “No Trunk”



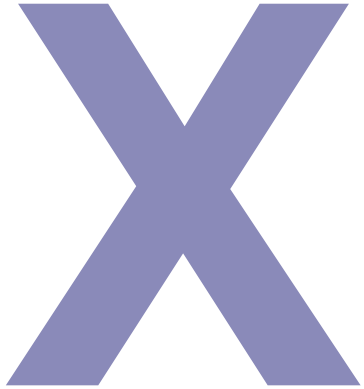
```
S1(config)# interface fa0/1
S1(config-if)# switchport nonegotiate
```



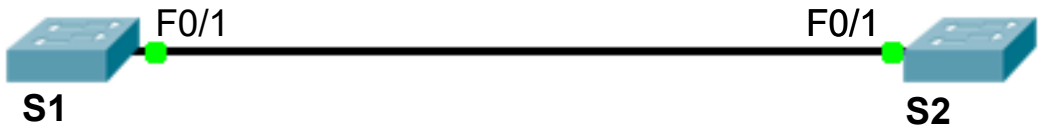

```
S2(config)# interface fa0/1
S2(config-if)# switchport mode dynamic desirable
```

- Will the ports trunk automatically?

#15 - “Trunk ” or “No Trunk”



```
S1(config)# interface fa0/1
S1(config-if)# switchport nonegotiate
```

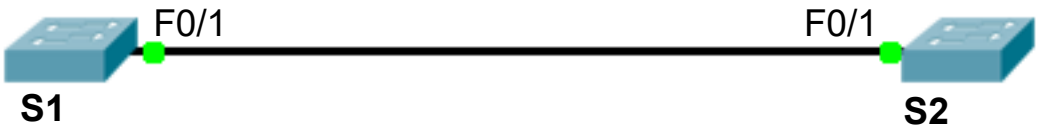



```
S2(config)# interface fa0/1
S2(config-if)# switchport mode dynamic auto
```

- Will the ports trunk automatically?

#16 - “Trunk ” or “No Trunk”

```
S1(config)# interface fa0/1
S1(config-if)# switchport nonegotiate
```




```
S2(config)# interface fa0/1
S2(config-if)# switchport nonegotiate
```

- Will the ports trunk automatically?

Verifying DTP Trunk Links

```
S1# show dtp interface f0/1
DTP information for FastEthernet0/1:
  TOS/TAS/TNS:                                TRUNK/ON/TRUNK
  TOT/TAT/TNT:                                802.1Q/802.1Q/802.1Q
  Neighbor address 1:                         0CD996D23F81
  Neighbor address 2:                         000000000000
  Hello timer expiration (sec/state):         12/RUNNING
  Access timer expiration (sec/state):        never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state):   never/STOPPED
  FSM state:                                  S6:TRUNK
  # times multi & trunk                       0
  Enabled:                                    yes
  In STP:                                     no

<output omitted>
```

TO CLEAR A SWITCH

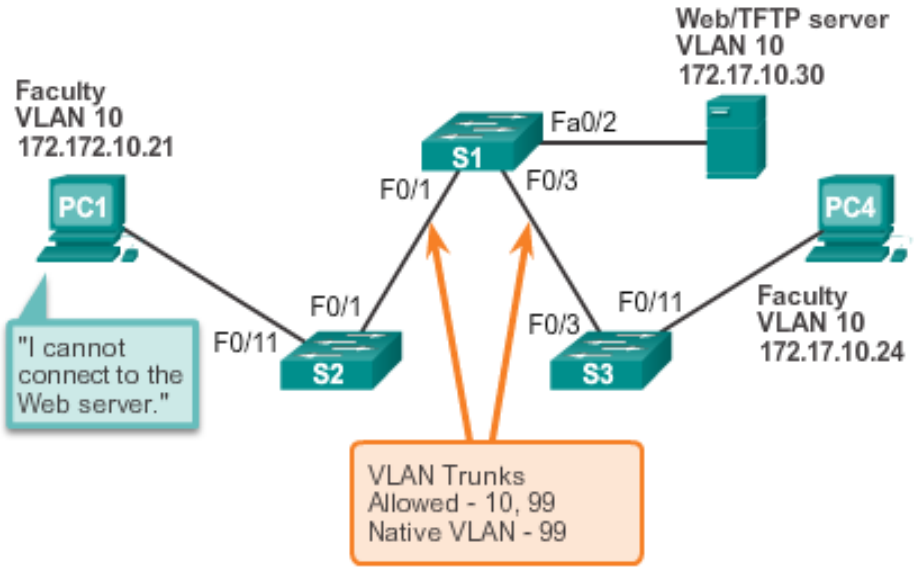
- ALWAYS DO THE FOLLOWING TO CLEAR A SWITCH!!

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

S1# erase startup-config
Erasing the nvram filesystem will remove all configuration files!
  Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
S1# reload
Proceed with reload? [confirm]
```

Troubleshooting VLANs

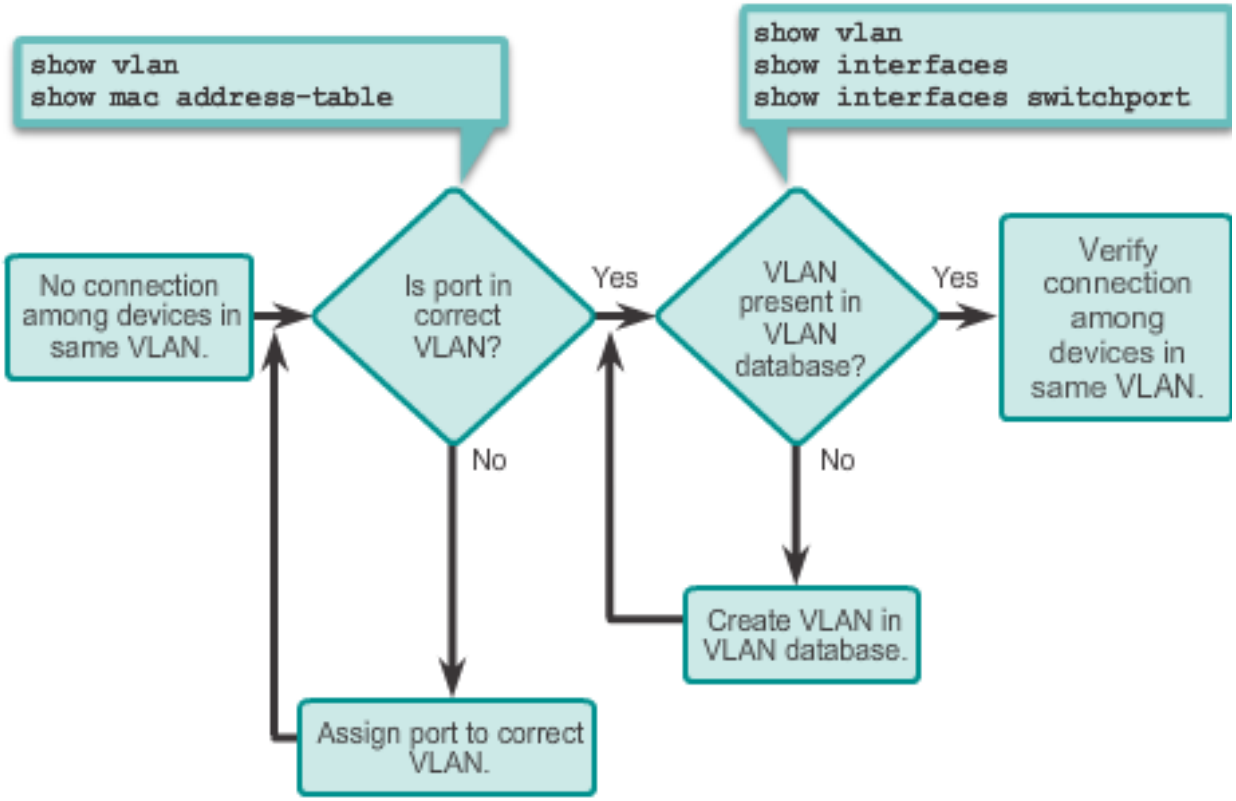
IP Addressing Issues with VLAN

- It is a common practice to ***associate a VLAN with an IP network.***
- Because ***different IP networks only communicate through a router***, all devices within a VLAN must be part of the same IP network to communicate.
- The figure displays that PC1 cannot communicate to the server because it has a wrong IP address configured.

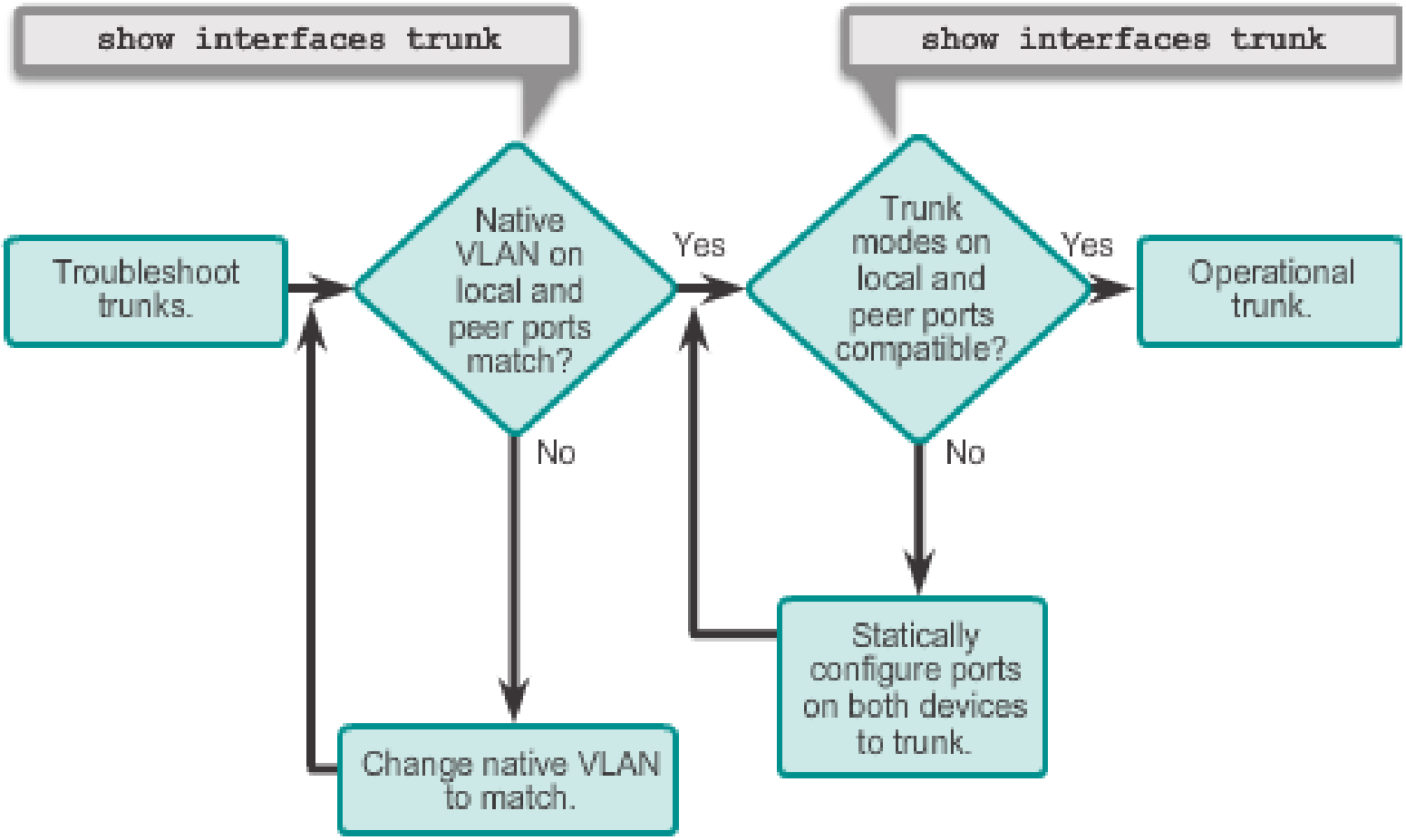


Missing VLANs

- If all the IP addresses mismatches have been solved, but the device still cannot connect, ***check if the VLAN exists in the switch***.



Introduction to Troubleshooting Trunks



Common Problems with Trunks

- Trunking issues are usually associated with incorrect configurations.
- The most common type of trunk configuration errors are:
  1. ***Native VLAN mismatches***
  2. ***Trunk mode mismatches***
  3. ***Allowed VLANs on trunks***
- If a trunk problem is detected, the best practice guidelines recommend to troubleshoot in the order shown above.

Trunk Mode Mismatches

- If a port on a trunk link is configured with a trunk mode that is incompatible with the neighboring trunk port, a trunk link fails to form between the two switches.
- Use the **show interfaces trunk** command to check the status of the trunk ports on the switches.
- To fix the problem, configure the interfaces with proper trunk modes.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

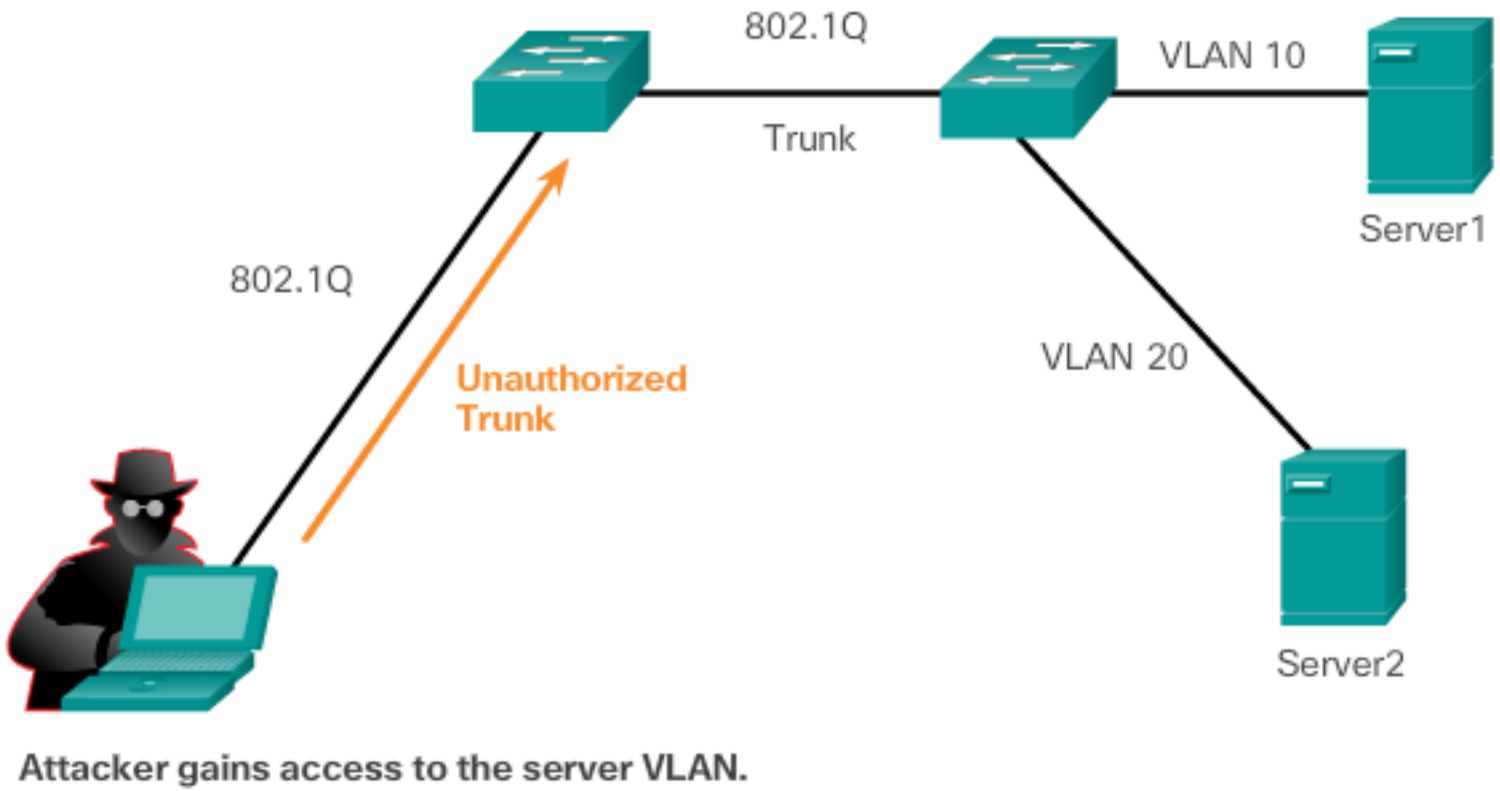
Incorrect VLAN List

- VLANs must be allowed in the trunk before their frames can be transmitted across the link.
- Use the **switchport trunk allowed vlan** command to specify which VLANs are allowed in a trunk link.
- Use the **show interfaces trunk** command to ensure the correct VLANs are permitted in a trunk.

Troubleshooting VLAN Security

Attacks on VLANs

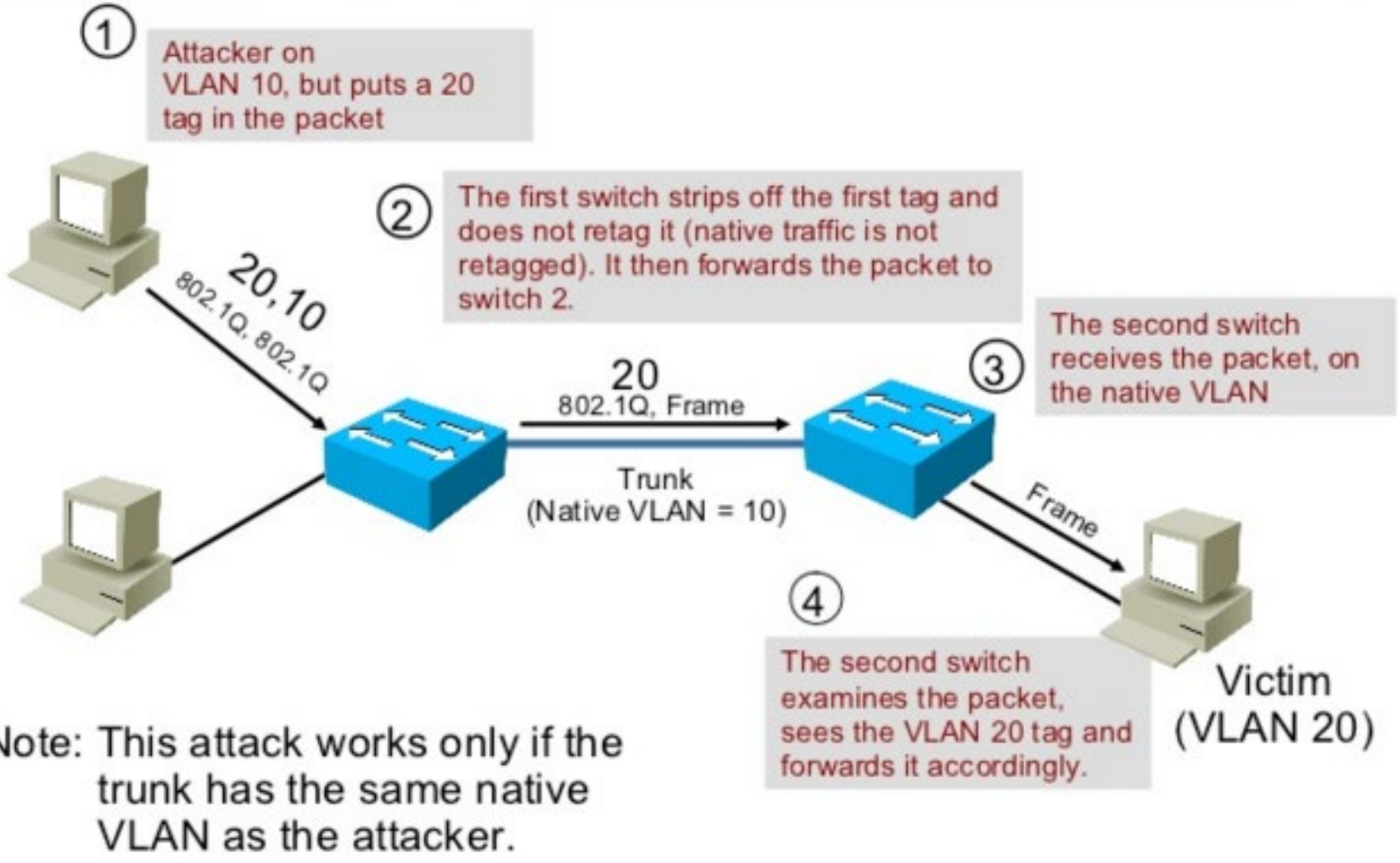
Switch Spoofing Attack



Attacker gains access to the server VLAN.

- To prevent a basic switch spoofing attack, turn off trunking on all ports, except the ones that specifically require trunking.

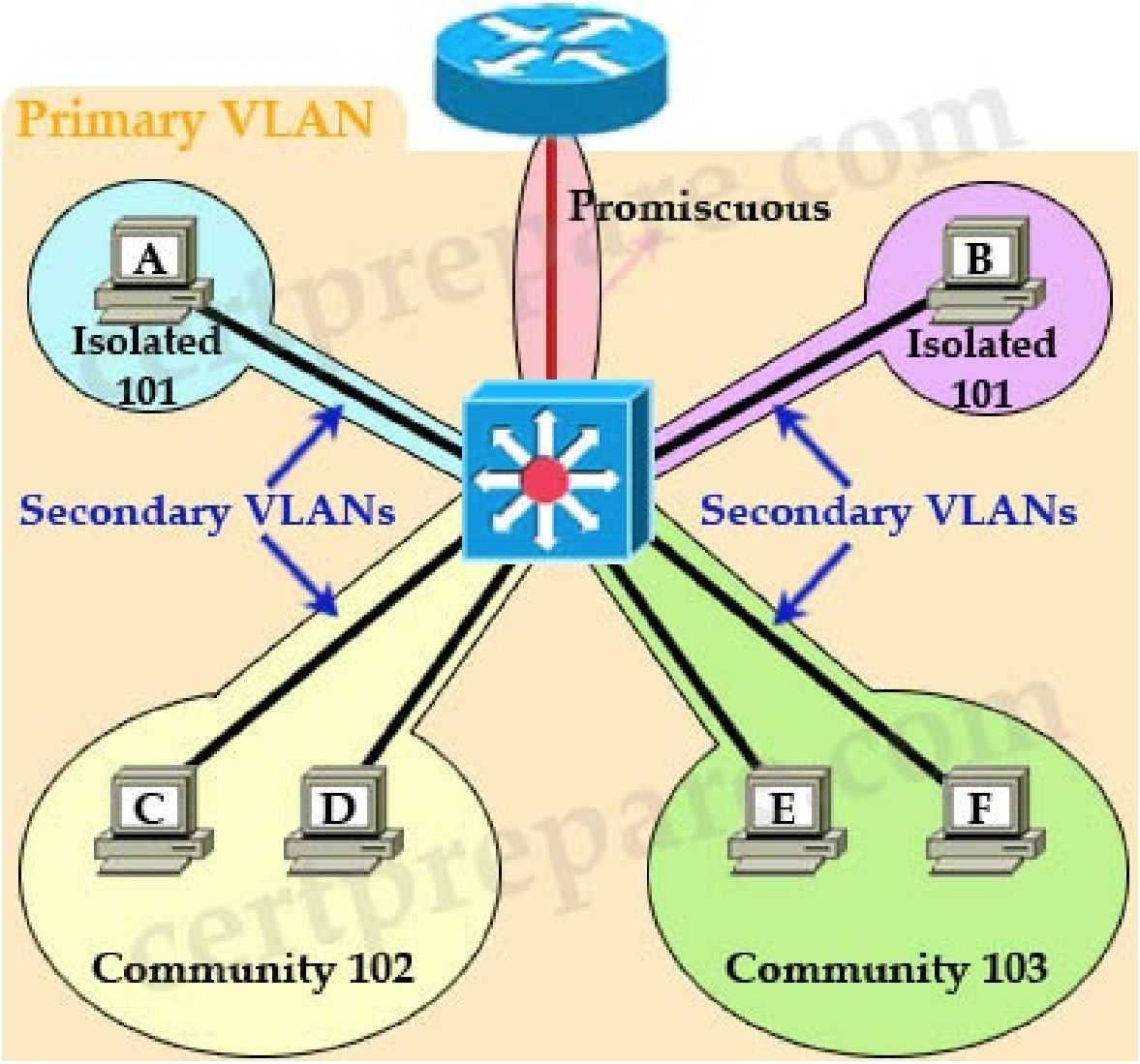
Double-Tagging Attack



- 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.

Attacks on VLANs

PVLAN Edge



- The Private VLAN (PVLAN) Edge feature, also known as protected ports, ensures that there is no exchange of unicast, broadcast, or multicast traffic between protected ports on the switch.

Chapter 3: Summary

This chapter:

- Introduced VLANs and their types
- Described the connection between VLANs and broadcast domains
- Discussed IEEE 802.1Q frame tagging and how it enables differentiation between Ethernet frames associated with distinct VLANs as they traverse common trunk links.
- Examined the configuration, verification, and troubleshooting of VLANs and trunks using the Cisco IOS CLI and explored basic security and design considerations.