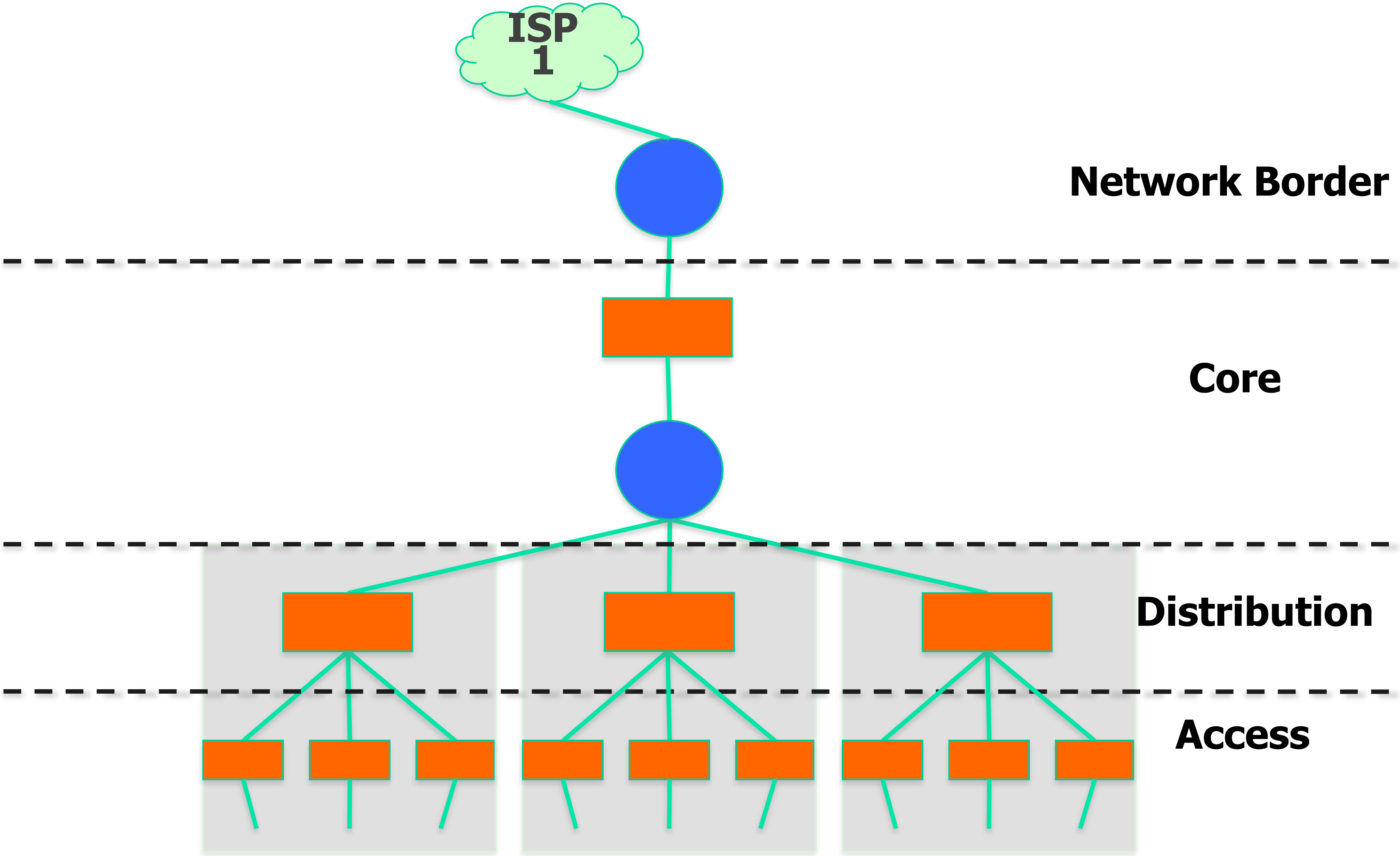
Layer-2 Network Design

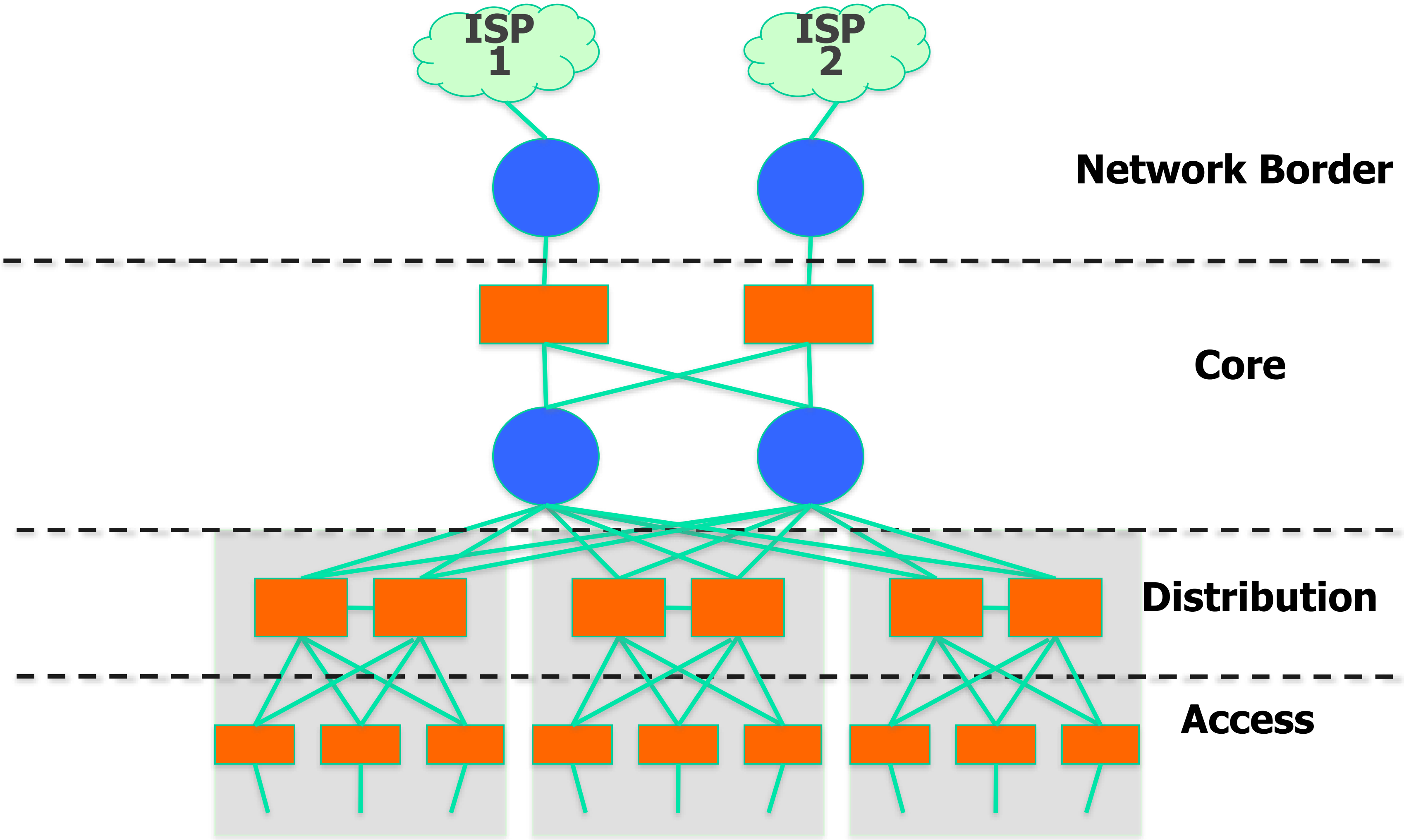
- A good network design is modular and hierarchical, with a clear separation of functions:
  - Core: Resilient, few changes, few features, high bandwidth, CPU power
  - Distribution: Aggregation, redundancy
  - Access: Port density, affordability, security features, many adds, moves and changes

https://nsrc.org/wrc/data/2010/15678359774b67528c8924a/lecture-02-wed-layer2-vlans.pdf

Layer-2 Network Design - Simple



Layer-2 Network Design - Redundant



https://nsrc.org/wrc/data/2010/15678359774b67528c8924a/lecture-02-wed-layer2-vlans.pdf

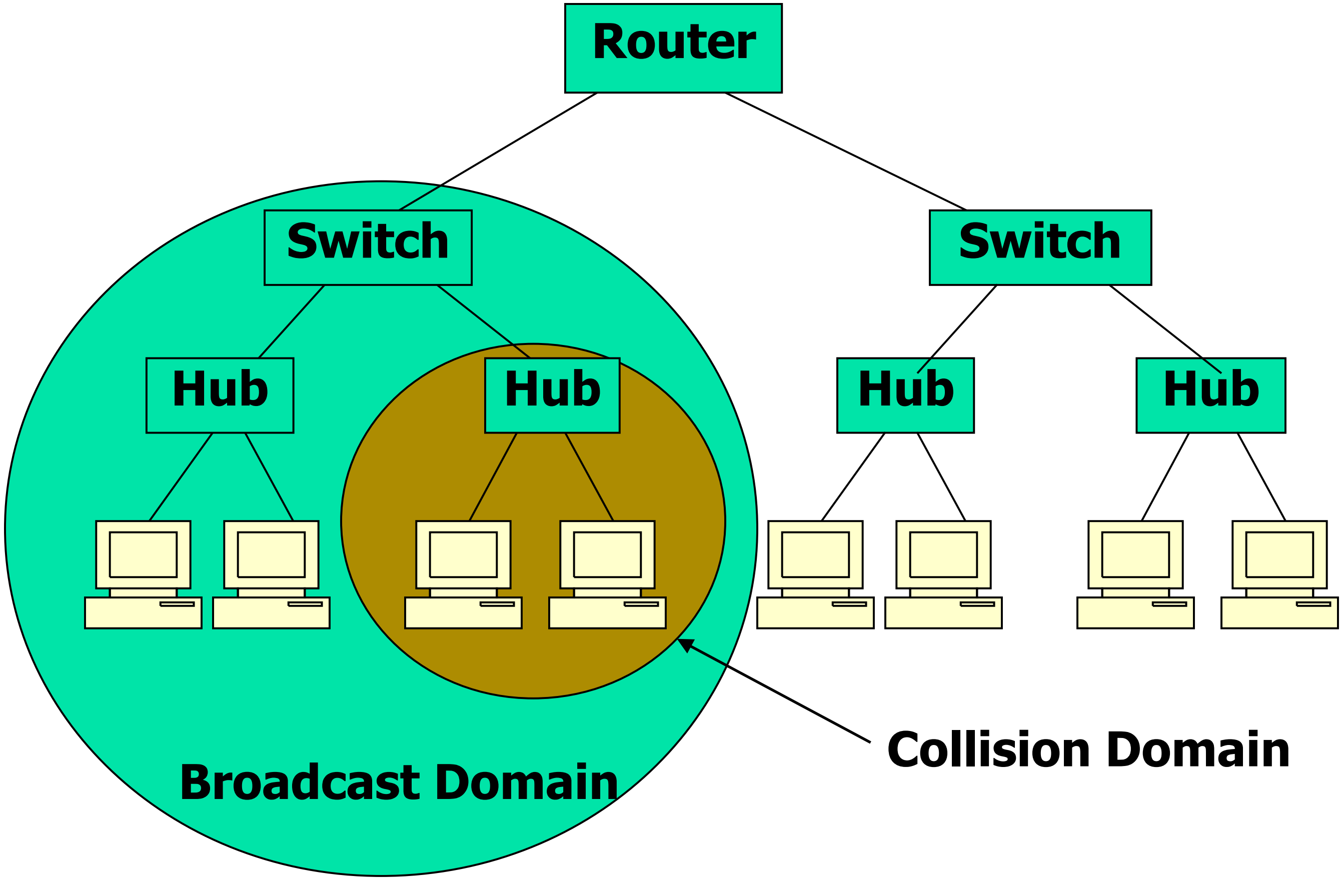
In-Building and Layer 2

- There is usually a correspondence between building separation and subnet separation
  - Switching inside a building
  - Routing between buildings
- This will depend on the size of the network
  - Very small networks can get by with doing switching between buildings
  - Very large networks might need to do routing inside buildings

Layer 2 Concepts

- Layer 2 protocols basically control access to a shared medium (copper, fiber, electro-magnetic waves)
- Ethernet is the de-facto wired-standard today
  - Reasons:
    - Simple
    - Cheap
    - Manufacturers keep making it faster
- Wireless (802.11a,b,g,n) is also Layer-2 technology.
      - 802.11ac (Wi-Fi 5)
        802.11ax (Wi-Fi 6)
        802.11ax (Wi-Fi 6E)
        802.11be (Wi-Fi 7) ?

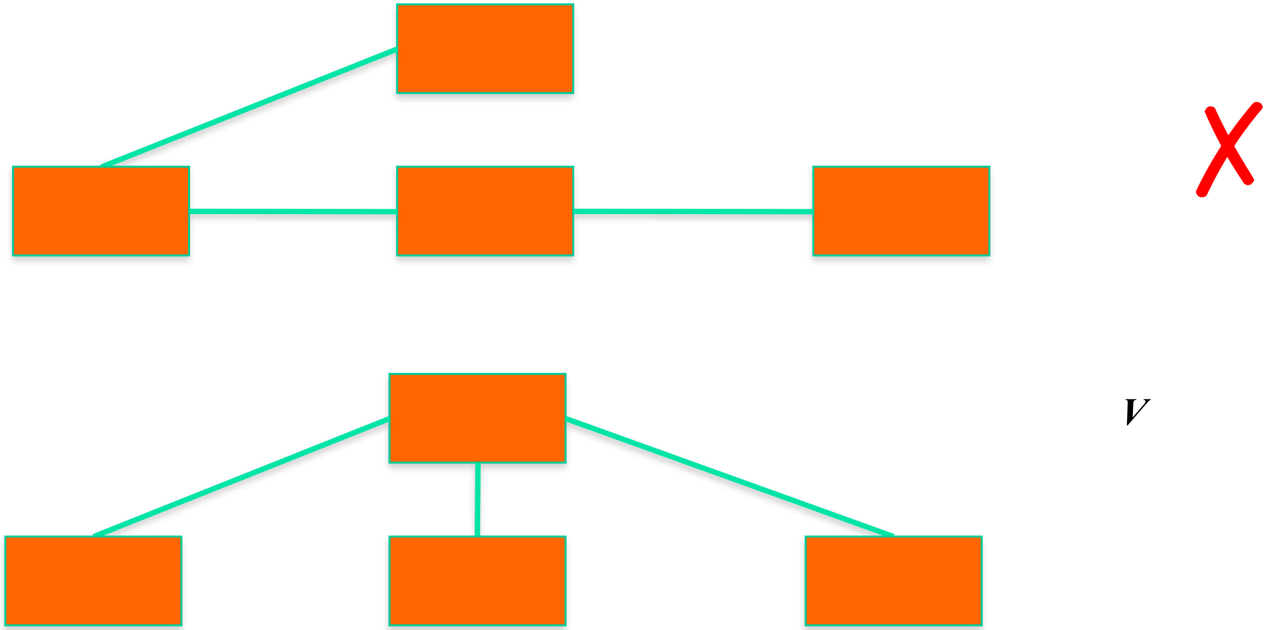
Traffic Domains



Layer 2 Network Design Guidelines

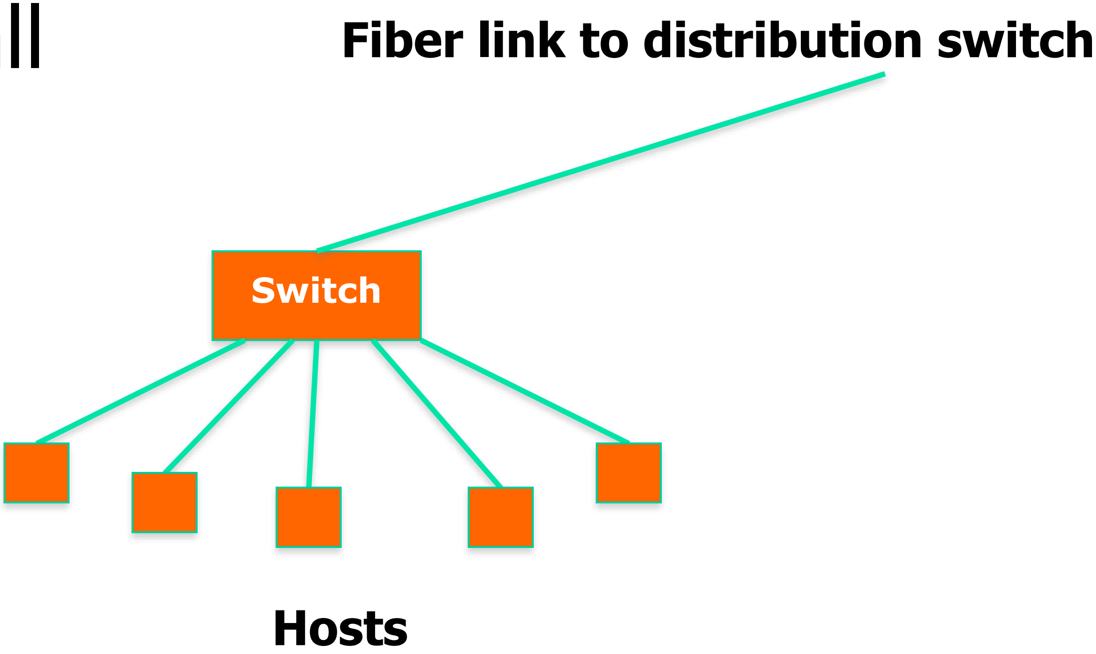
- Always connect hierarchically
  - If there are multiple switches in a building, use an aggregation switch
  - Locate the aggregation switch close to the building entry point (e.g. fiber panel)
  - Locate edge switches close to users (e.g. one per floor)
    - Max length for Cat 5 is 100 meters

Minimize Path Between Elements



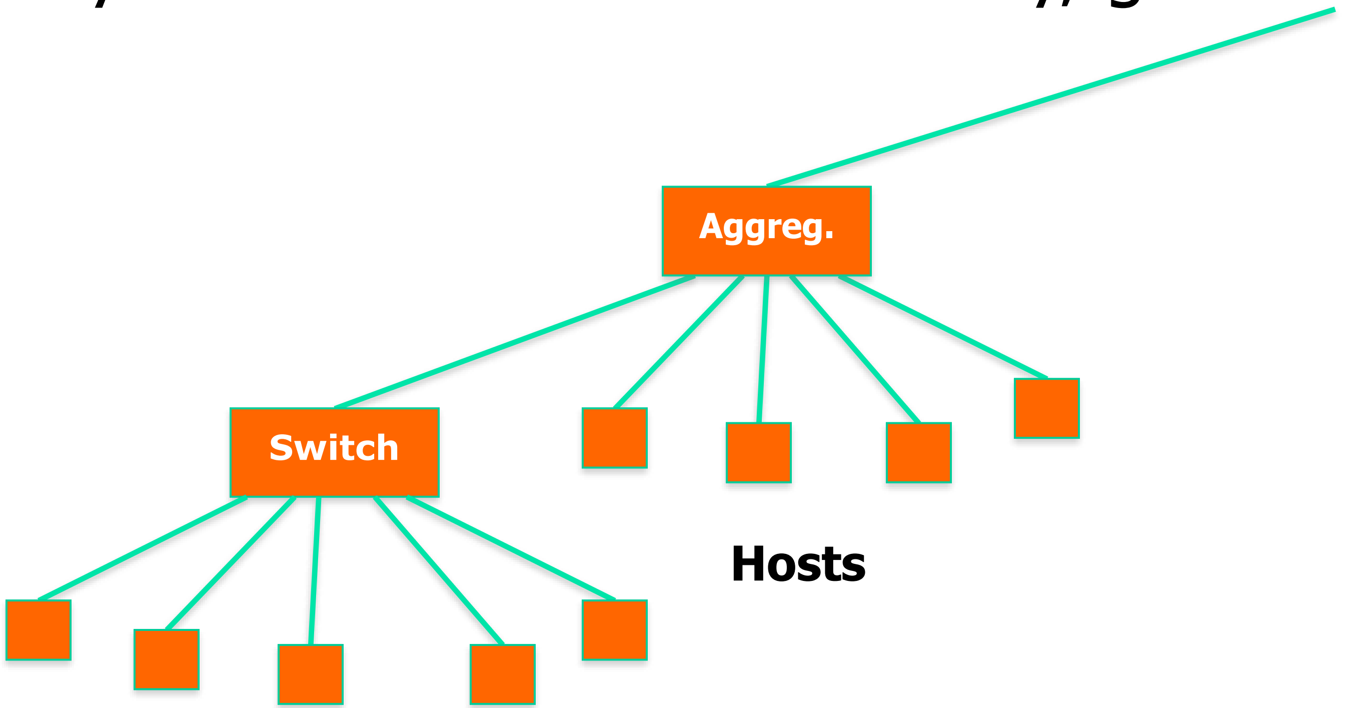
Build Incrementally

- Start small



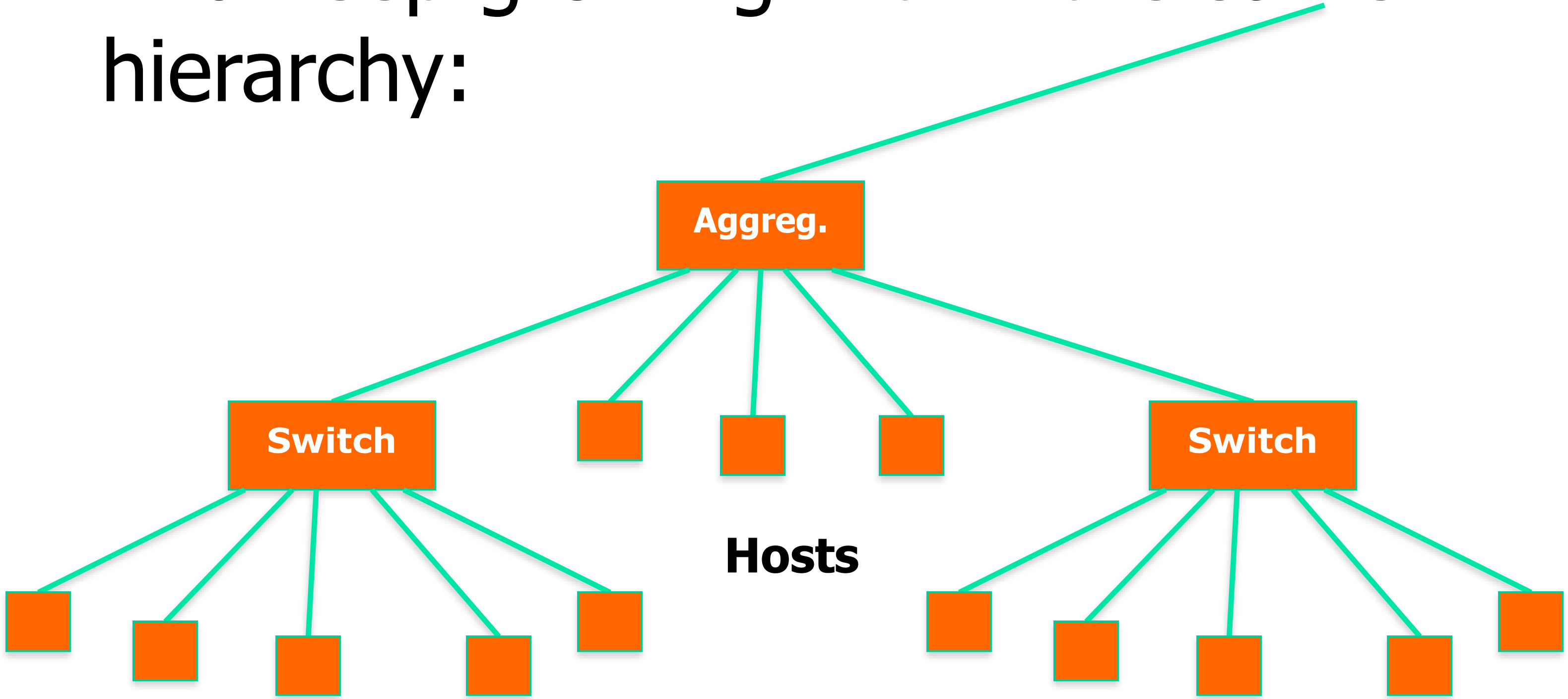
Build Incrementally

- As you have demand and money, grow like this:



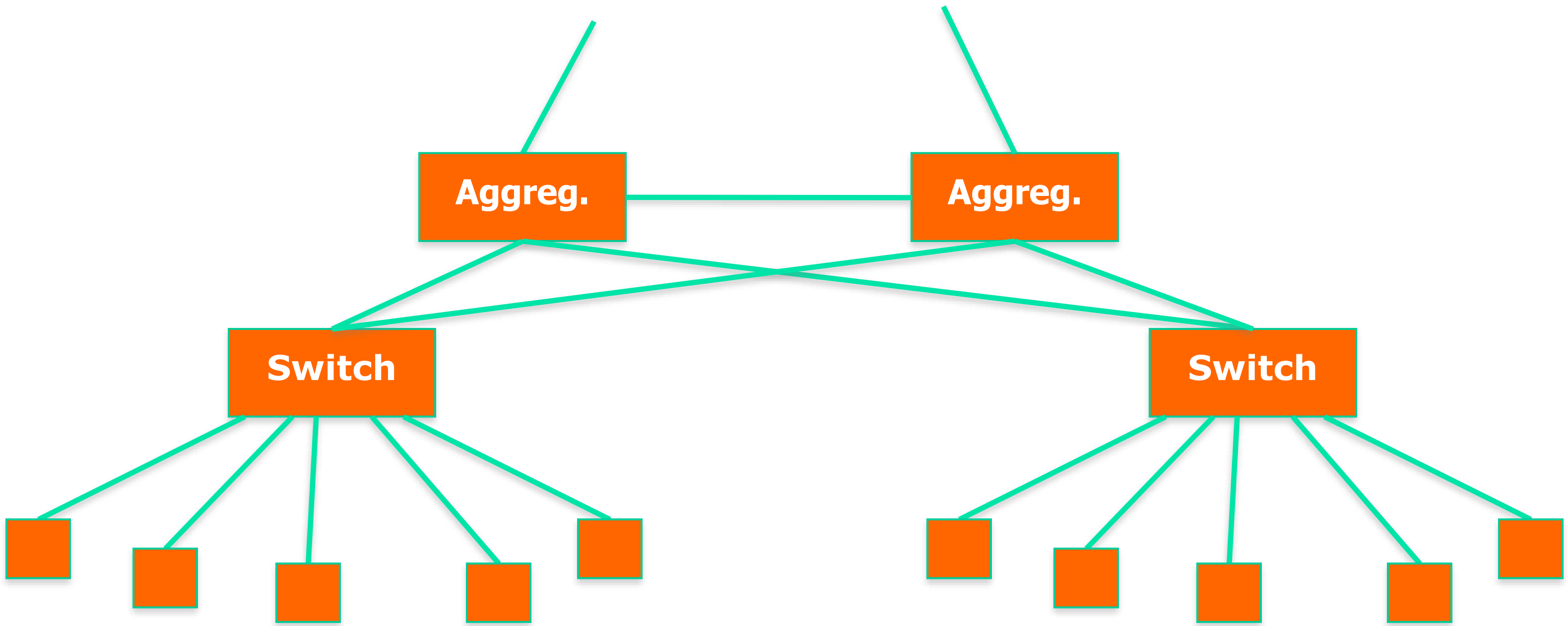
Build Incrementally

- And keep growing within the same hierarchy:



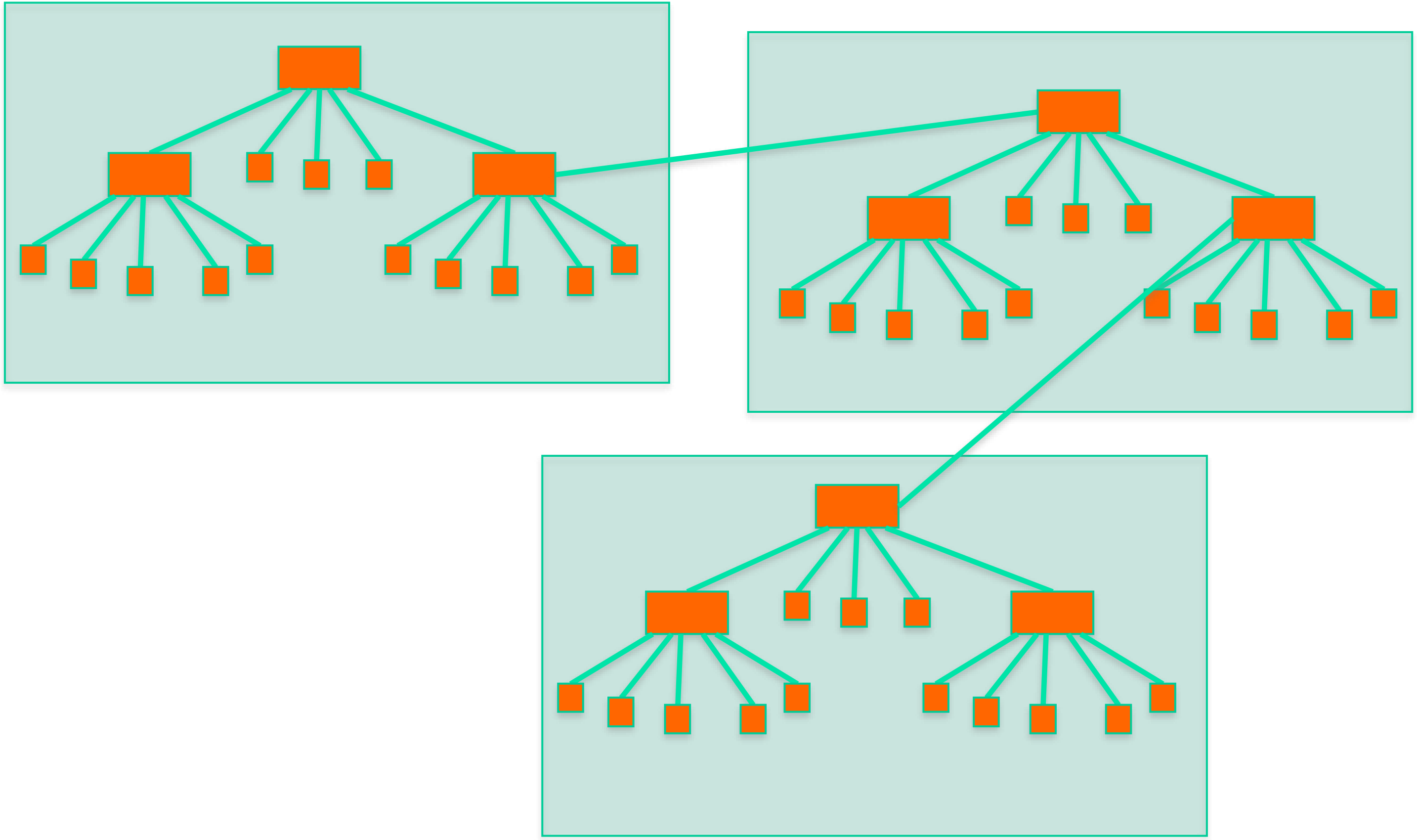
Build Incrementally

- At this point, you can also add a redundant aggregation switch:



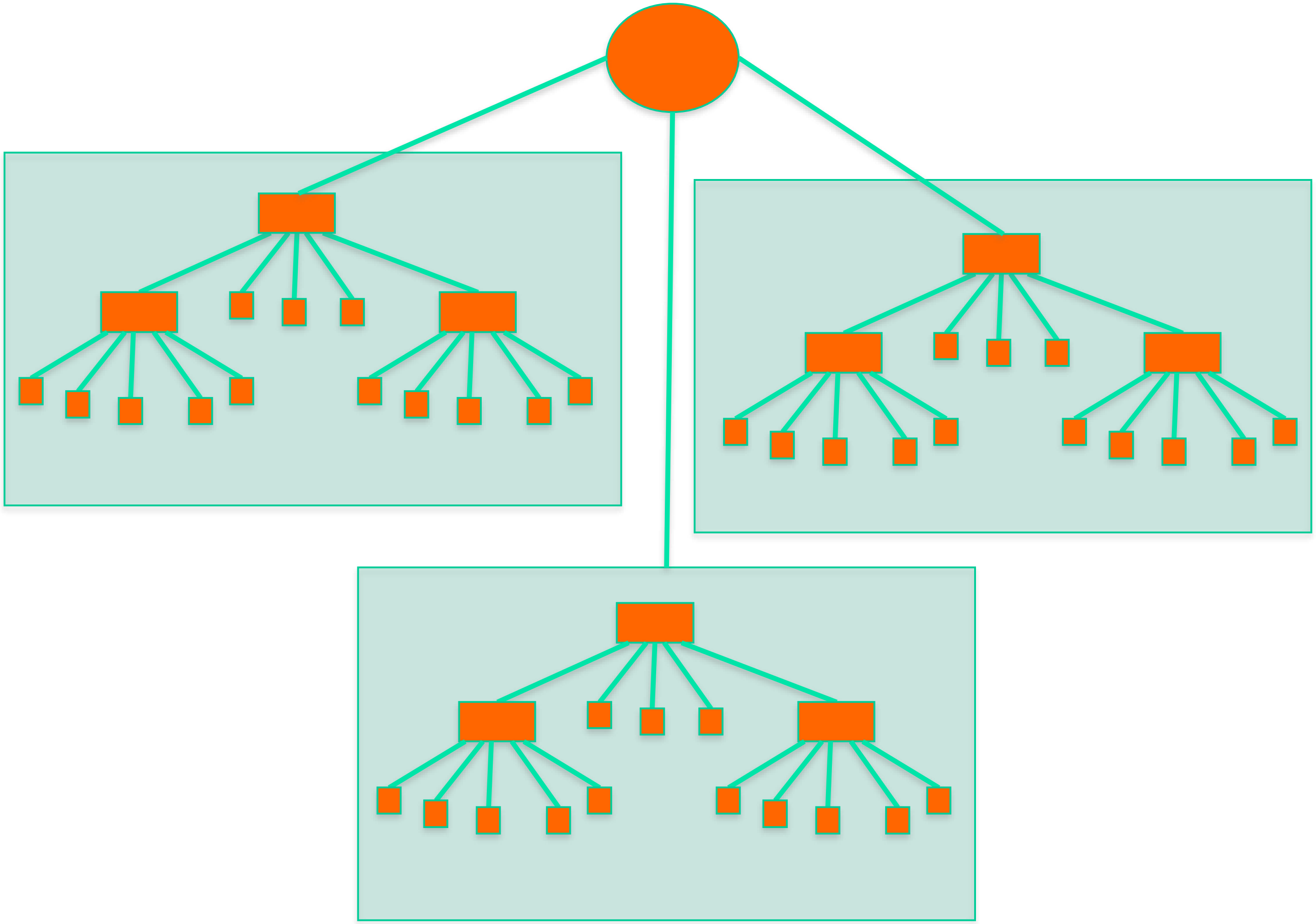
Do not daisy-chain

- Resist the temptation of doing this:



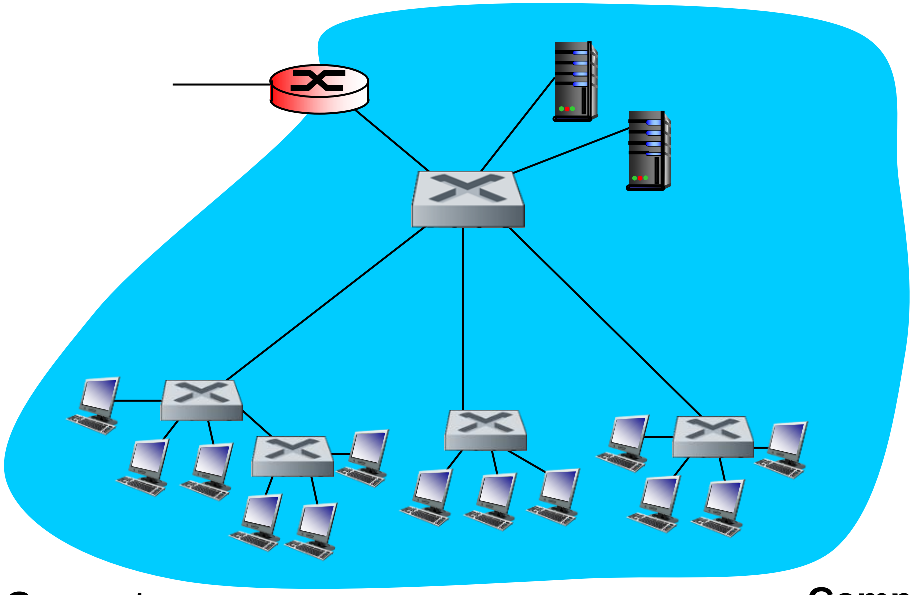
✗

Connect buildings hierarchically



V

VLANs: motivation

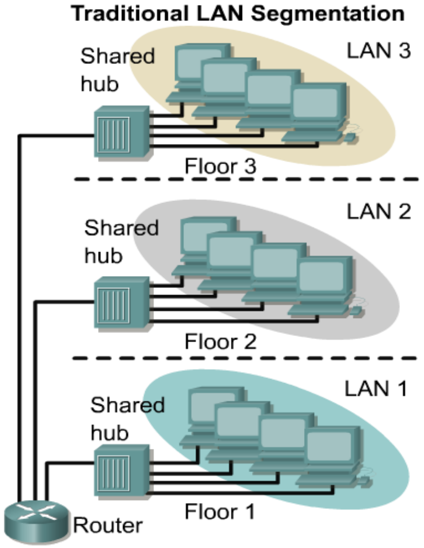


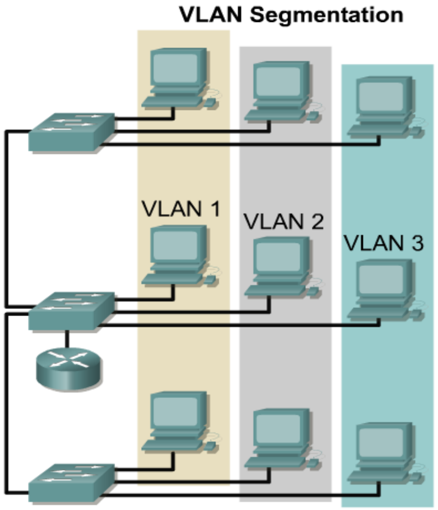
consider:

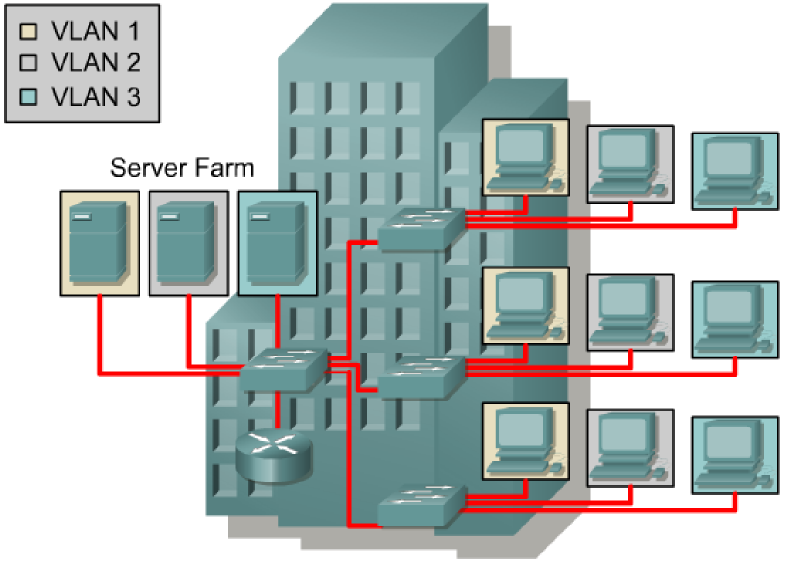
- CS user moves office to EE, but wants connect to CS switch?
- single broadcast domain:
  - all layer-2 broadcast traffic (ARP, DHCP, unknown location of destination MAC address) must cross entire LAN
  - security/privacy, efficiency issues

A good network design is modular and hierarchical, with a clear separation of functions:
***Core**: Resilient, few changes, few features, high bandwidth, CPU power*
***Distribution**: Aggregation, redundancy*
***Access**: Port density, affordability, security features, many adds, moves and changes*

VLAN







- **VLANs provide segmentation based on broadcast domains.**
- VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.
- VLANs function by logically segmenting the network into **different broadcast domains** so that packets are only switched between ports that are designated for the same VLAN.

What is VLAN

The IEEE 802.1D-2004 standard played a part in the evolution of Ethernet LANs to VLANs

- VLAN is a logical grouping of networking devices.
- When we create VLAN, we actually break large broadcast domain in smaller broadcast domains.
- Consider VLAN as a subnet.
- Same as two different subnets cannot communicate with each other without **router**, different **VLANs also requires router** to communicate.

Advantage of VLAN

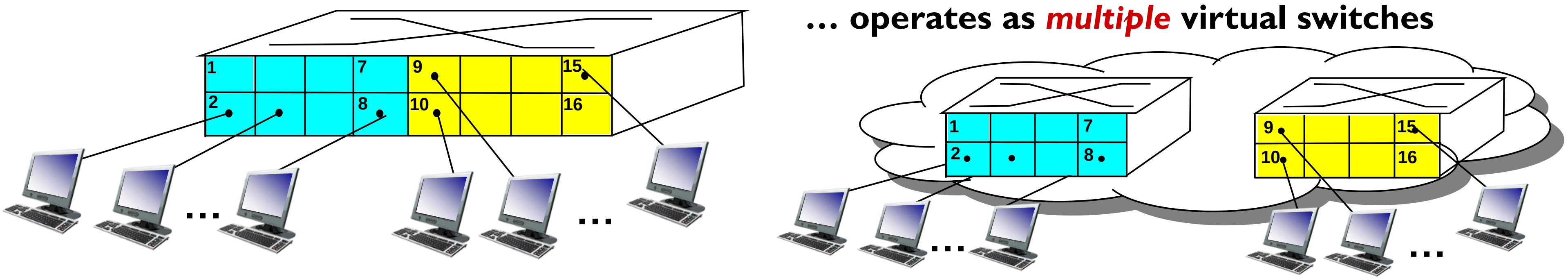
- Solve broadcast problem
- Reduce the size of broadcast domains
- Allow us to **add additional layer of security**
- Make device management easier
- Allow us to implement the logical **grouping of devices by function** instead of location

Disadvantages of VLAN :

- Managing larger networks can be pretty complex.
- When you need to add a new VLAN, you need to configure all the switches to accommodate it.
- VLAN's interoperability can be complex as well.

Virtual LANs (VLANs)

- Allow us to split switches into separate (virtual) switches
- Only members of a VLAN can see that VLAN’s traffic
- Inter-vlan traffic must go through a router



… operates as *multiple* virtual switches

Electrical Engineering (VLAN ports 1-8)

Computer Science (VLAN ports 9-16)

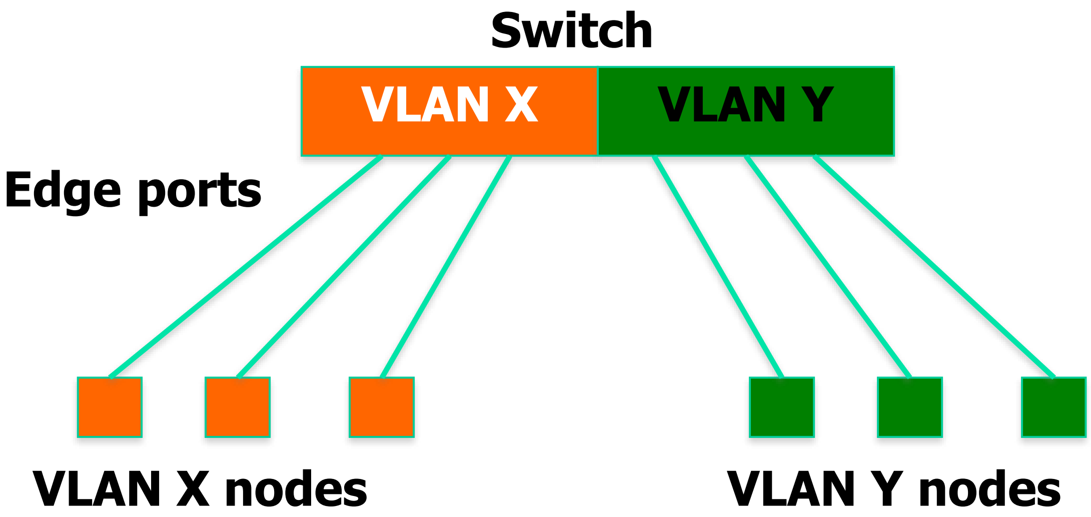
Electrical Engineering (VLAN ports 1-8)

Computer Science (VLAN ports 9-16)

Local VLANs

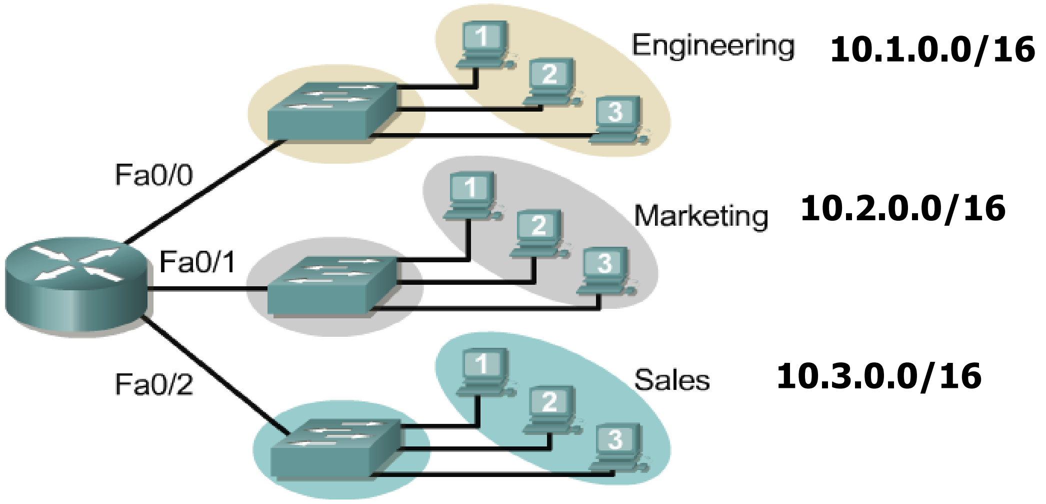
- 2 VLANs or more within a single switch
- VLANs address scalability, security, and network management.
- Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- ***Edge ports***, where end nodes are connected, are configured as members of a VLAN
- The switch behaves as several virtual switches, sending traffic only within VLAN members.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain.
- Traffic should only be routed between VLANs.

Local VLANs



Broadcast domains with VLANs and routers

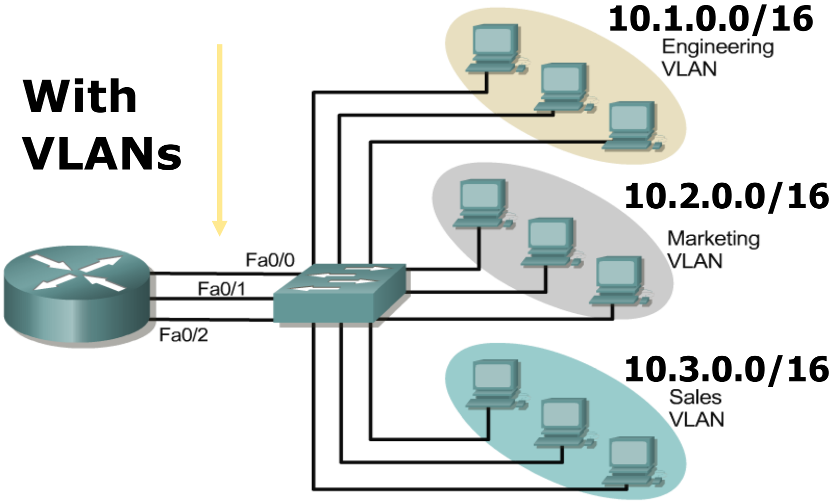
Without VLANs:



- **Without VLANs**, each group is on a different IP network and on a different switch.

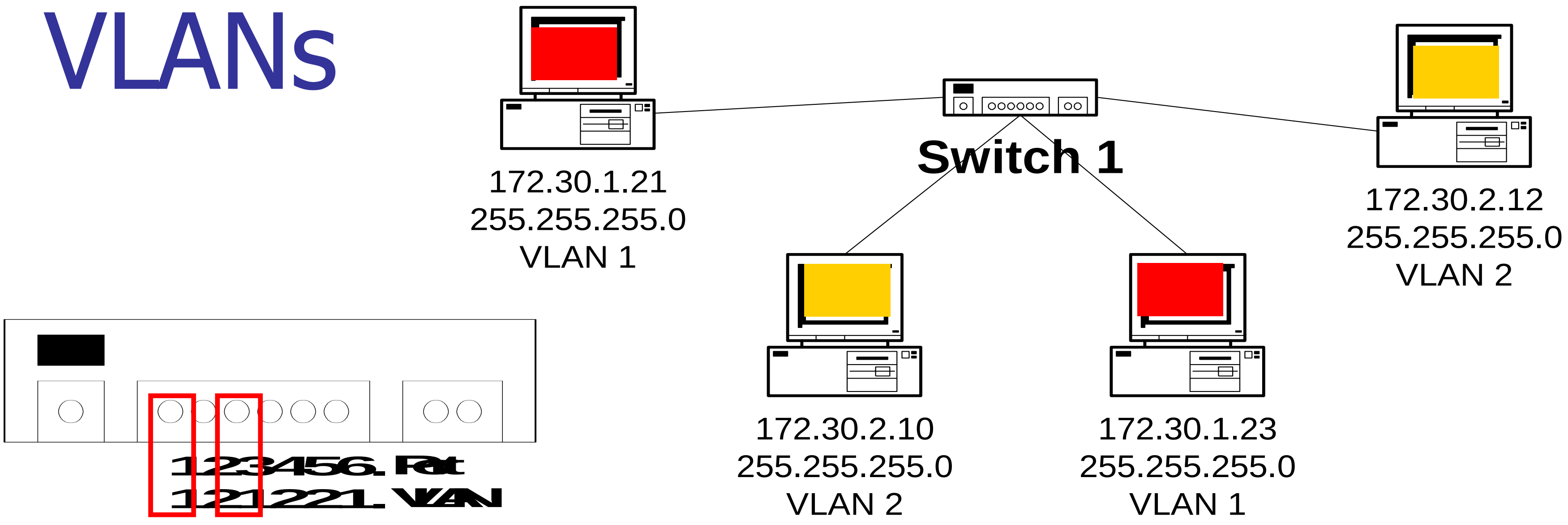
One link per VLAN or a single VLAN Trunk (later)

With VLANs



- **Using VLANs**. Switch is configured with the ports on the appropriate VLAN. Still, each group on a different IP network; however, they are all on the same switch.

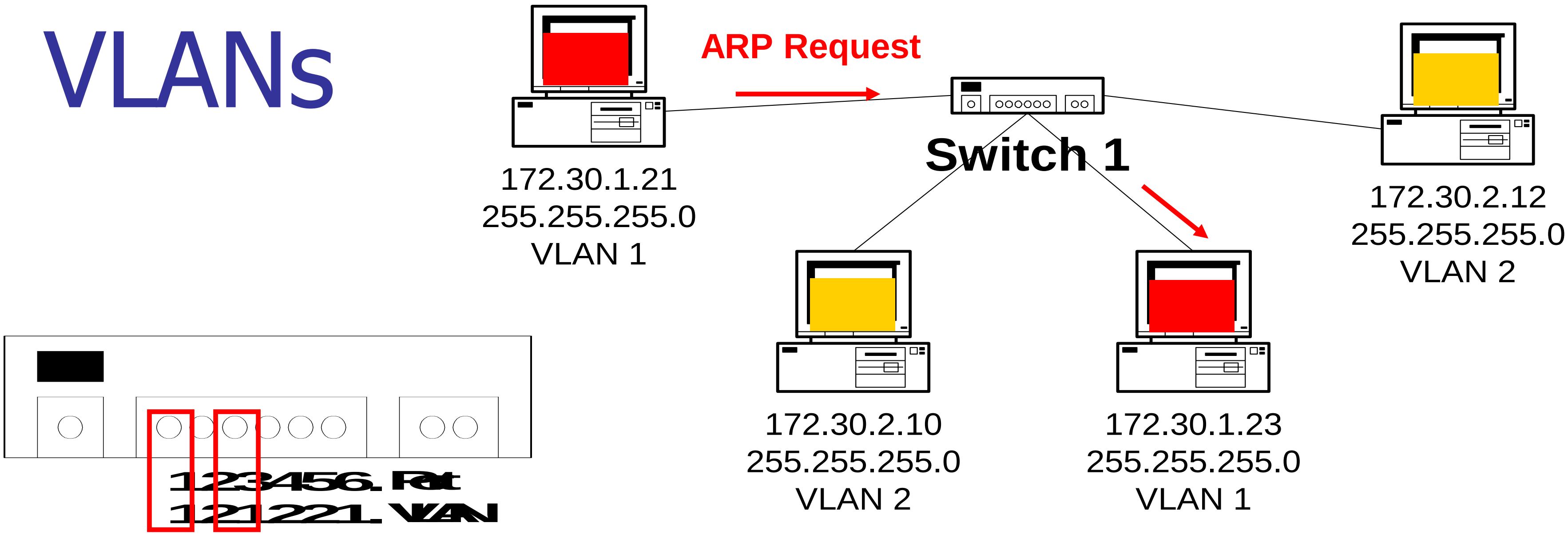
VLANs



Two VLANs = Two subnets

- Important notes on VLANs:
- VLANs are assigned to switch ports.
- There is no “VLAN” assignment done on the host (usually).
- In order for a host to be a part of that VLAN, it must be assigned an IP address that belongs to the proper subnet.
- *Remember:* ***VLAN = Subnet***

VLANs

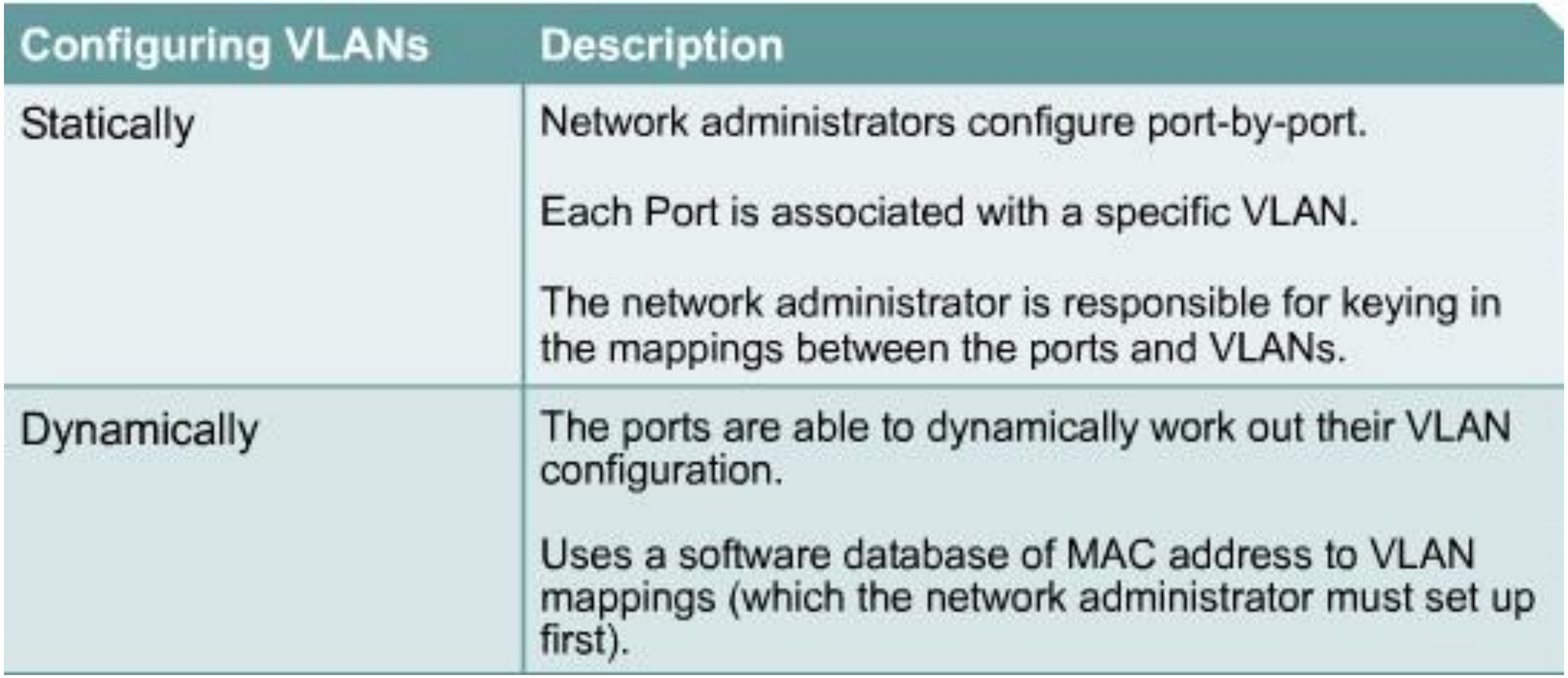


Two VLANs = Two subnets

- VLANs separate broadcast domains!
  e.g. without VLAN the ARP would be seen on all subnets.
- Assigning a host to the correct VLAN is a 2-step process:
  - Connect the host to the correct port on the switch.
  - Assign to the host the correct IP address depending on the VLAN membership

VLAN operation

- Network administrators are responsible for configuring VLANs both manually and statically.
- The key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically.



Configuring VLANs	Description
Statically	Network administrators configure port-by-port. Each Port is associated with a specific VLAN. The network administrator is responsible for keying in the mappings between the ports and VLANs.
Dynamically	The ports are able to dynamically work out their VLAN configuration. Uses a software database of MAC address to VLAN mappings (which the network administrator must set up first).

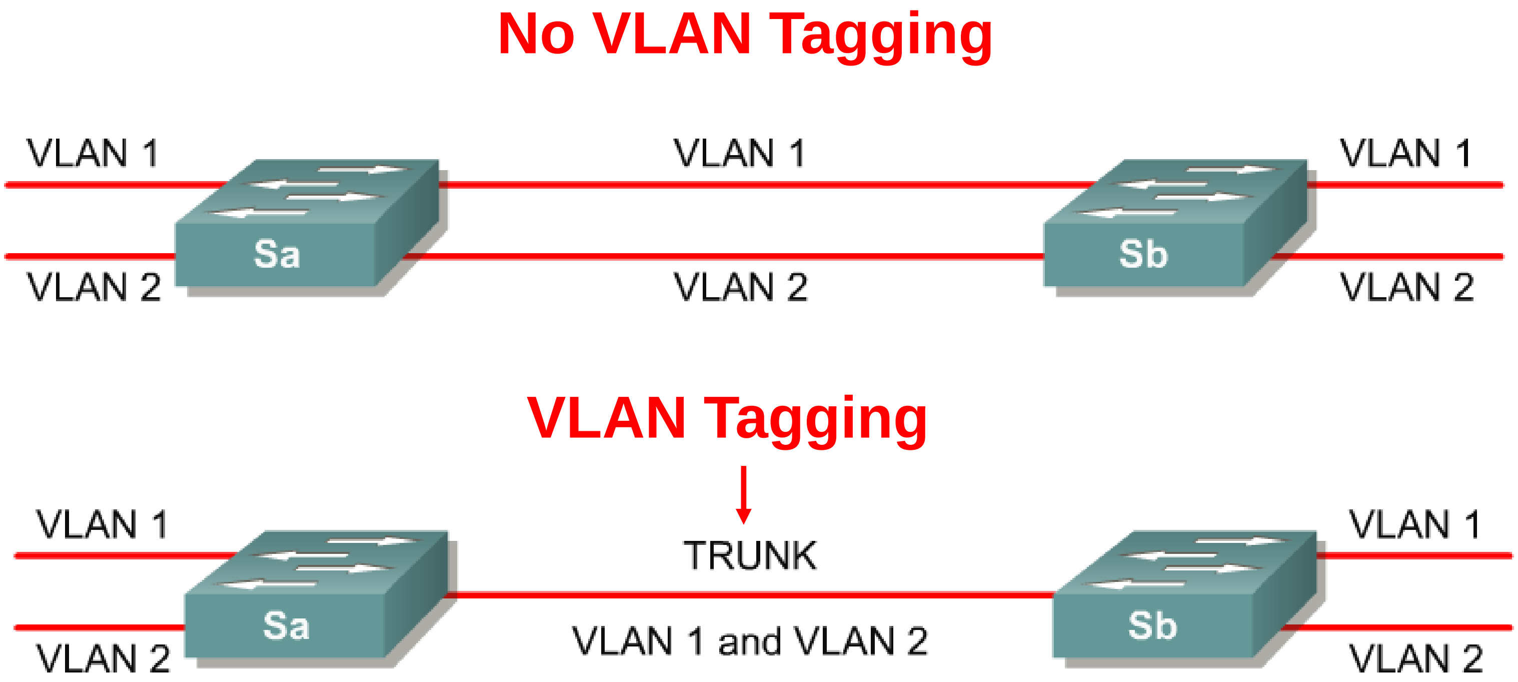
VLAN operation

- As a device enters the network, it automatically assumes the VLAN membership
  of the port to which it is attached.
- The default VLAN for every port in the switch is VLAN 1 and cannot be deleted.
- All other ports on the switch may be reassigned to alternate VLANs.

VLANs across switches

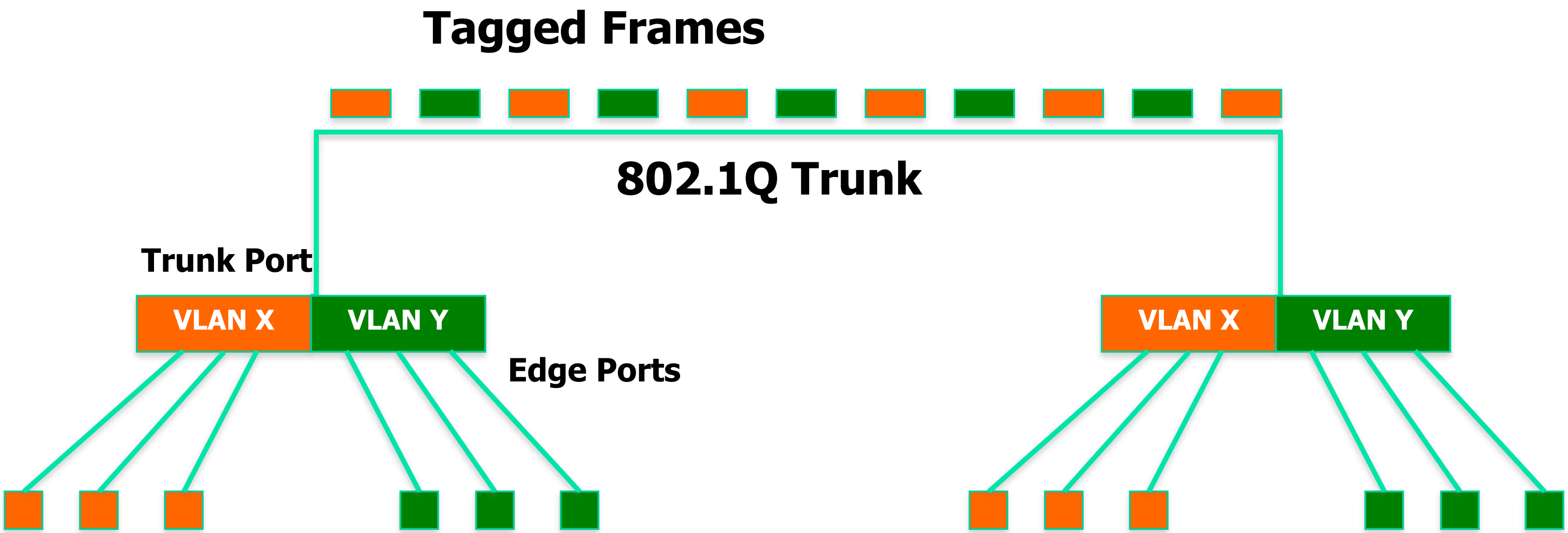
- Two switches can exchange traffic from one or more VLANs
- Inter-switch links are configured as ***trunks***, carrying frames from all or a subset of a switch’s VLANs
- Each frame carries a ***tag*** that identifies which VLAN it belongs to

VLANs across switches



- **VLAN tagging** is used when a single link needs to carry traffic for more than one VLAN.

VLANs across switches

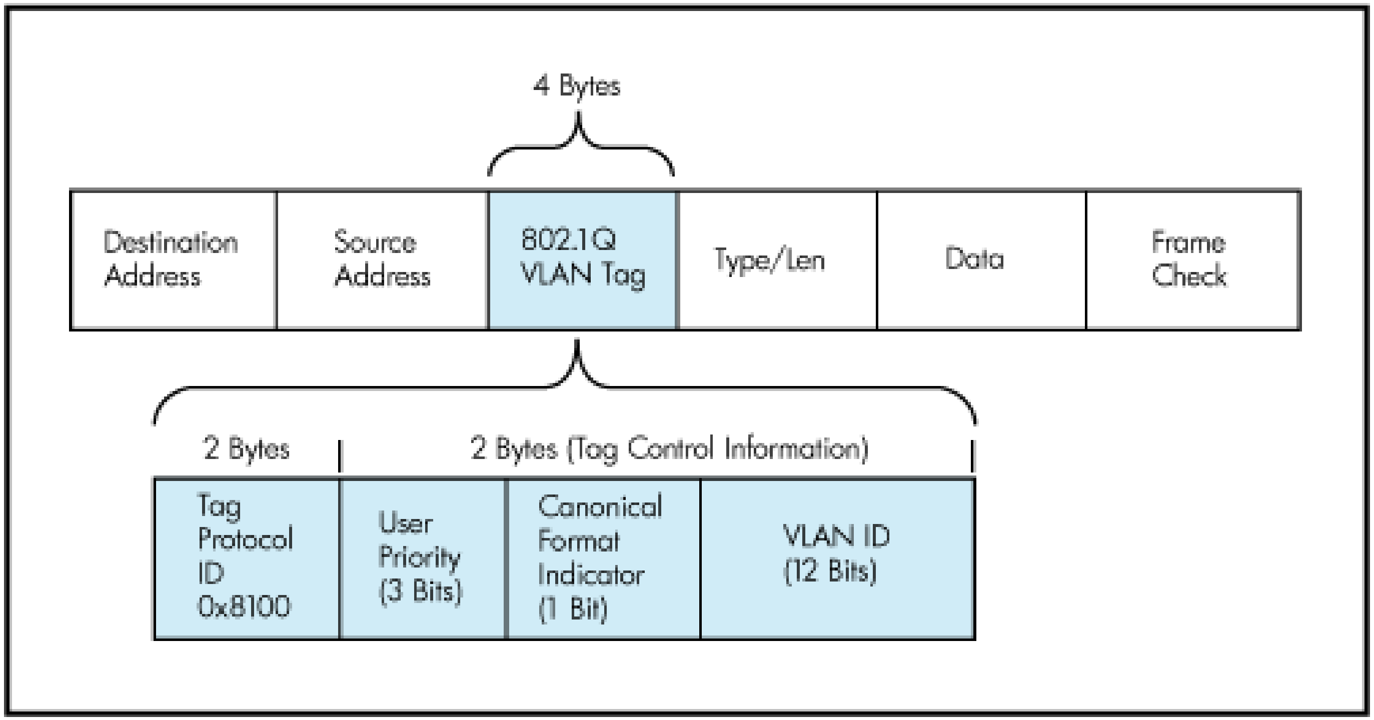


This is called "VLAN Trunking"

802.1Q

- The IEEE standard that defines how ethernet frames should be ***tagged*** when moving across switch trunks
- This means that switches from *different vendors* are able to exchange VLAN traffic.

802.1Q tagged frame



4 Bytes

Destination Address

Source Address

802.1Q VLAN Tag

Type/Len

Data

Frame Check

2 Bytes

2 Bytes (Tag Control Information)

Tag Protocol ID 0x8100

User Priority (3 Bits)

Canonical Format Indicator (1 Bit)

VLAN ID (12 Bits)

Tagged vs. Untagged

- Edge ports are not tagged, they are just “members” of a VLAN
- You only need **to tag frames in switch-to-switch links** (trunks), when transporting multiple VLANs
- **A trunk** can transport both tagged and untagged VLANs
    - As long as the two switches agree on how to handle those

VLANS increase complexity

- You can no longer “just replace” a switch
    - Now you have VLAN configuration to maintain
- You have to make sure that all the switch-to-switch trunks are carrying all the necessary VLANs
    - Need to keep in mind when adding/removing VLANs

Good reasons to use VLANs

- You want to segment your network into multiple subnets, but can’t buy enough switches
  - Hide sensitive infrastructure like IP phones, building controls, etc.
- Separate control traffic from user traffic
  - Restrict who can access your switch management address

Bad reasons to use VLANs

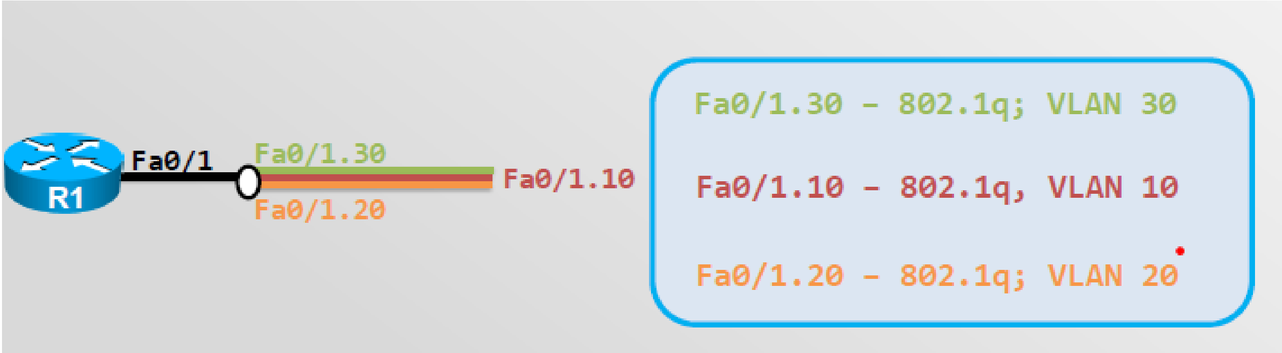
- Because they will completely secure your hosts (or so you think)
- Because they allow you to extend the same IP network over multiple separate buildings

Do not build too many VLAN

- Extending a VLAN to multiple buildings across trunk ports
- Bad idea because:
  - Broadcast traffic is carried across all trunks from one end of the network to another
  - Broadcast storm can spread across the extent of the VLAN
  - Maintenance and troubleshooting nightmare

Router-on-a-Stick Inter-VLAN Routing

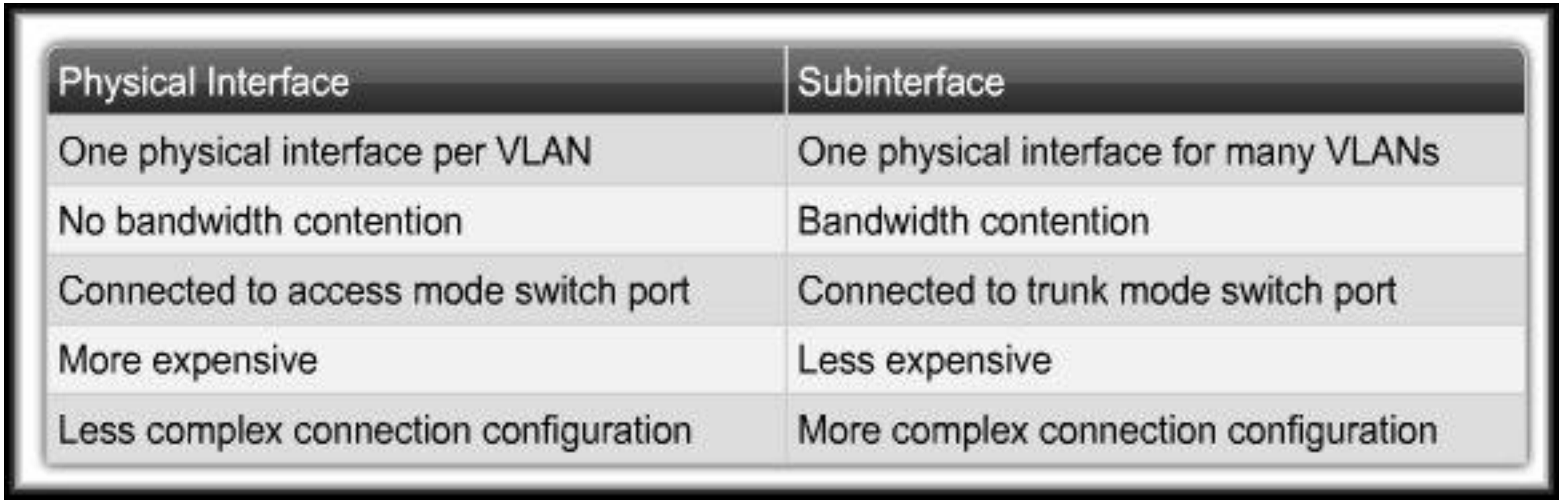
- The ‘router-on-a-stick’ inter-VLAN routing method overcomes the limitation of the legacy inter-VLAN routing method.
- It only requires one physical Ethernet interface to route traffic between multiple VLANs on a network.
- A router Ethernet interface is configured as an 802.1Q trunk and connected to a trunk port on a Layer 2 switch.
- Specifically, the router interface is configured **using subinterfaces to identify routable VLANs.**
- The configured subinterfaces are software-based virtual interfaces. Each is associated with a single physical Ethernet interface. Subinterfaces are configured in software on a router.


R1
Fa0/1
Fa0/1.30
Fa0/1.10
Fa0/1.20
Fa0/1.30 – 802.1q; VLAN 30
Fa0/1.10 – 802.1q, VLAN 10
Fa0/1.20 – 802.1q; VLAN 20

Router-on-a-Stick Inter-VLAN Routing

- Each subinterface is independently configured with an IP address and VLAN assignment.
- Subinterfaces are configured for different subnets that correspond to their VLAN assignment. This facilitates logical routing.
- When VLAN-tagged traffic enters the router interface, it is forwarded to the VLAN subinterface.
- After a routing decision is made based on the destination IP network address, the router determines the exit interface for the traffic.
- If the exit interface is configured as an 802.1q subinterface, the data frames are VLAN-tagged with the new VLAN and sent back out the physical interface.

Physical interface / Subinterface

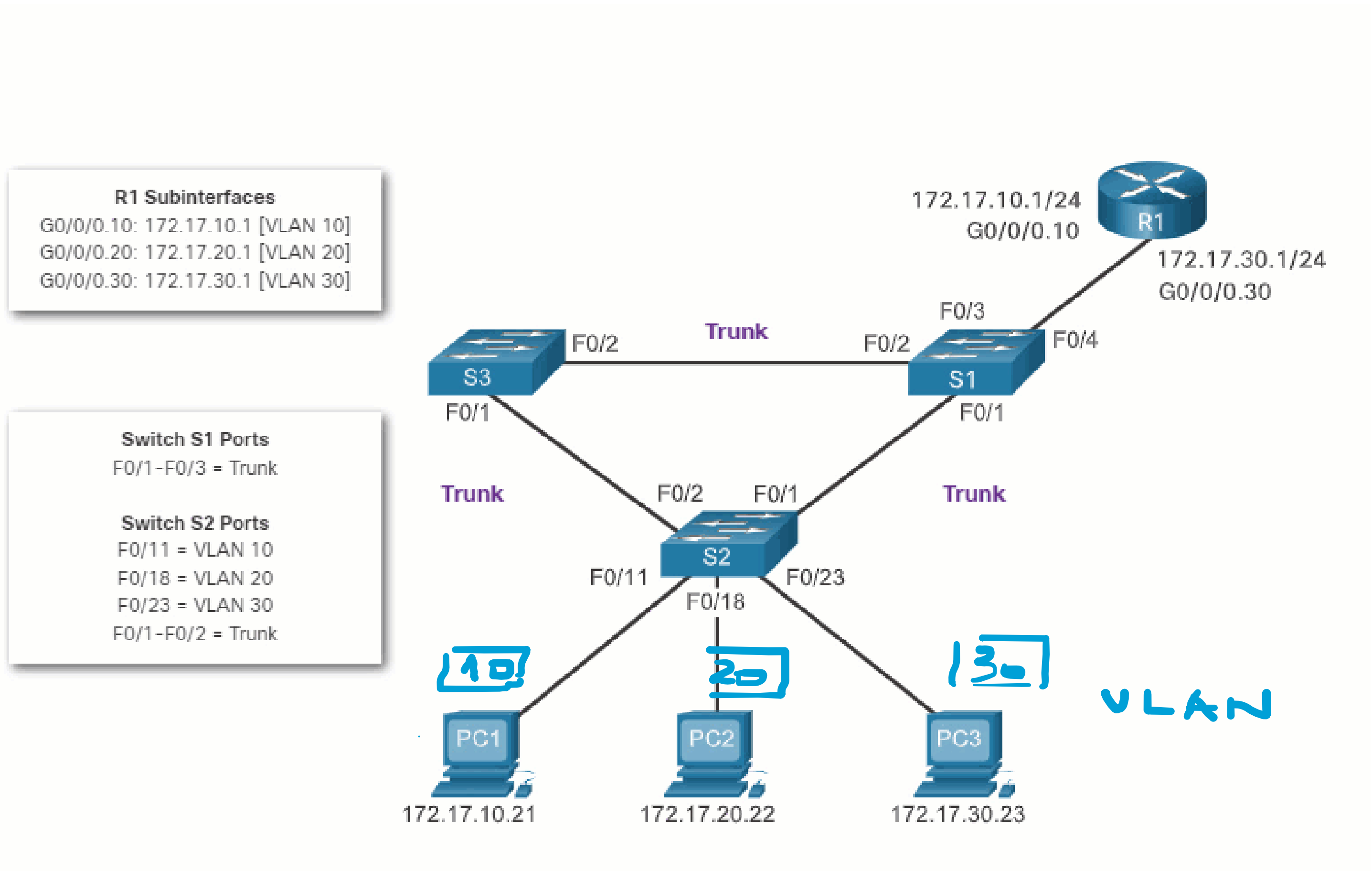


Physical Interface	Subinterface
One physical interface per VLAN	One physical interface for many VLANs
No bandwidth contention	Bandwidth contention
Connected to access mode switch port	Connected to trunk mode switch port
More expensive	Less expensive
Less complex connection configuration	More complex connection configuration

how a router-on-a-stick performs its routing function

view an animation of

https://itexamanswers.net/ccna-2-v7-0-curriculum-module-4-inter-vlan-routing.html



R1 Subinterfaces

G0/0/0.10: 172.17.10.1 [VLAN 10]
G0/0/0.20: 172.17.20.1 [VLAN 20]
G0/0/0.30: 172.17.30.1 [VLAN 30]

Switch S1 Ports

F0/1-F0/3 = Trunk

Switch S2 Ports

F0/11 = VLAN 10
F0/18 = VLAN 20
F0/23 = VLAN 30
F0/1-F0/2 = Trunk

- *As seen in the animation,* ***PC1 on VLAN 10 is communicating with PC3 on VLAN 30.***
- *When R1 accepts the tagged unicast traffic on VLAN 10, it routes that traffic to VLAN 30,*
- *using its configured subinterfaces.*
- *Switch S2 removes the VLAN tag of the unicast frame and forwards the frame out to PC3 on port F0/23.*
- *Note: The router-on-a-stick method of inter-VLAN routing does not scale beyond 50 VLANs.*

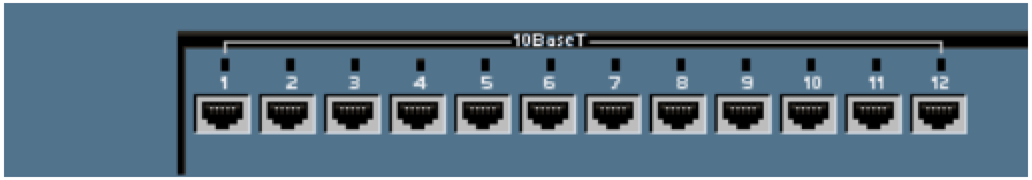
VLAN ranges

- ***VLAN 0, 4095***:*These are reserved VLAN which cannot be seen or used.*
- ***VLAN 1***: *It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can’t be deleted or edit but can be used.*
- ***VLAN 2-1001***: *This is a normal VLAN range. We can create, edit and delete these VLAN.*
- ***VLAN 1002-1005***: *These are CISCO defaults for FDDI and token rings. These VLAN can’t be deleted.*
- ***VLAN 1006-4094***: *This is the extended range of VLAN.*

Difference between LAN and VLAN

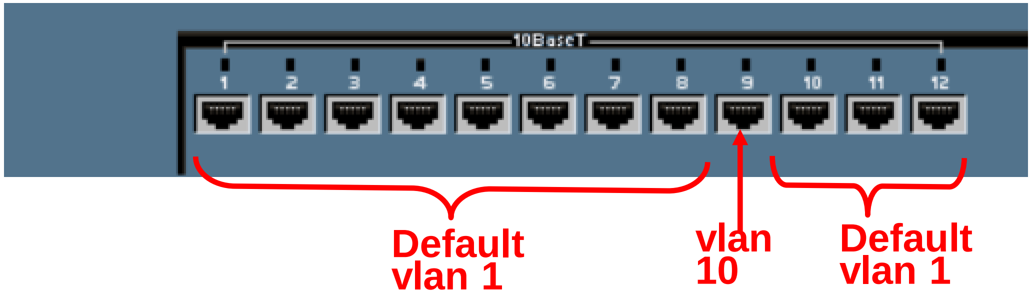
S. NO	LAN	VLAN
1.	LAN stands for Local Area Network.	VLAN stands for Virtual Local Area Network.
2.	The cost of Local Area Network is high.	The cost of Virtual Local Area Network is less.
3.	The latency of Local Area Network is high.	The latency of Virtual Local Area Network is low.
4.	The devices which are used in LAN are: Hubs, Routers and switch.	The devices which are used in VLAN are: Bridges and switch.
5.	In local area network, the Packet is advertised to each device.	In virtual local area network, packet is sent to specific broadcast domain.
6.	Local area network is less efficient than virtual local area network.	Virtual local area network is greater efficient than local area network.

Configuring static VLANs



- VLAN 1 is one of the factory-default VLANs.
- Configure VLANs:
  - Switch#conf t
  - Switch(config)#interface vlan 10
  - Switch(config-if)#ip address x.x.x.x m.m.m.m

Creating VLANs



- Create the VLAN:

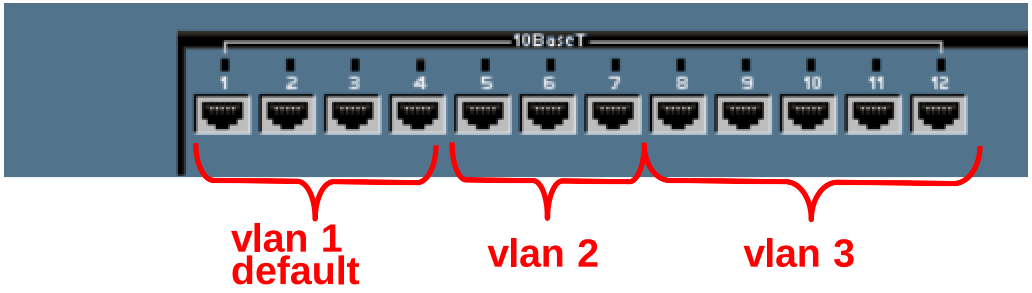
```
Switch#vlan database
Switch(vlan)#vlan vlan_number
Switch(vlan)#exit
```

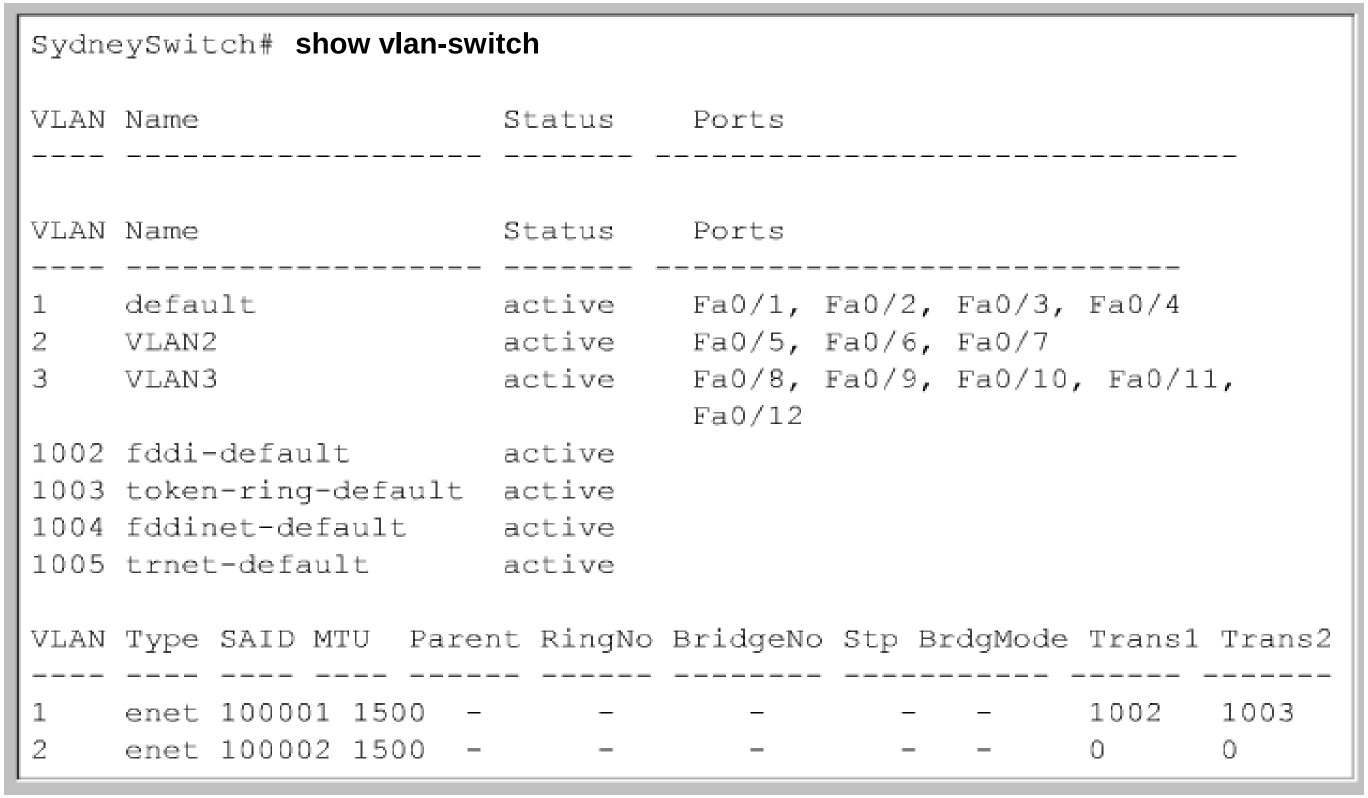
- Assign ports to the VLAN (in configuration mode):

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan 10
```

  - **access** – Denotes this port as an access port and not a trunk

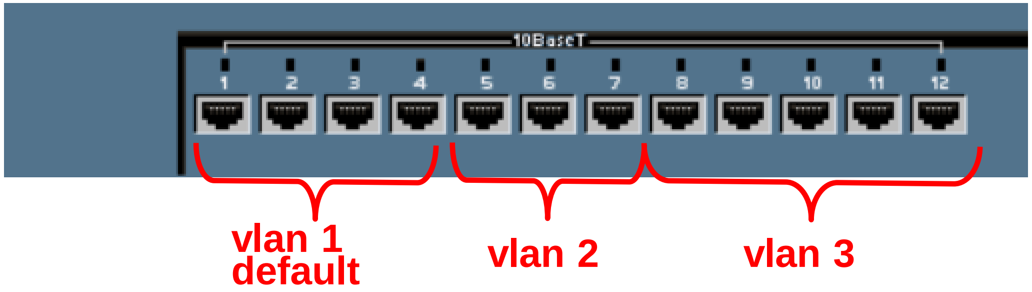
Verifying VLANs – show vlan-switch

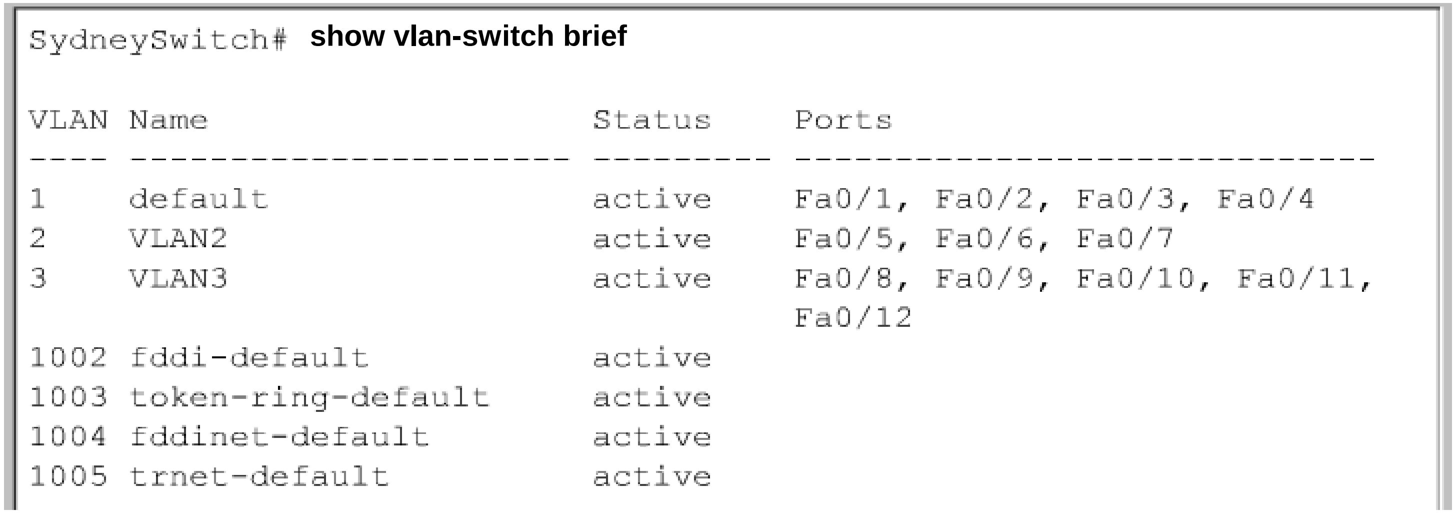




```
SydneySwitch# show vlan-switch

VLAN Name                Status    Ports
---- ------------------- ------- --------------------------------


VLAN Name                Status    Ports
---- ------------------- ------- -----------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2               active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3               active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                   Fa0/12
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active

VLAN Type SAID MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ---- ---- ---- ------ ------ -------- ----------- ------ -------
1    enet 100001 1500  -      -       -       -   -     1002  1003
2    enet 100002 1500  -      -       -       -   -     0     0
```

show vlan-switch brief





```
SydneySwitch# show vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                            active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                            active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                                Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

vlan database commands

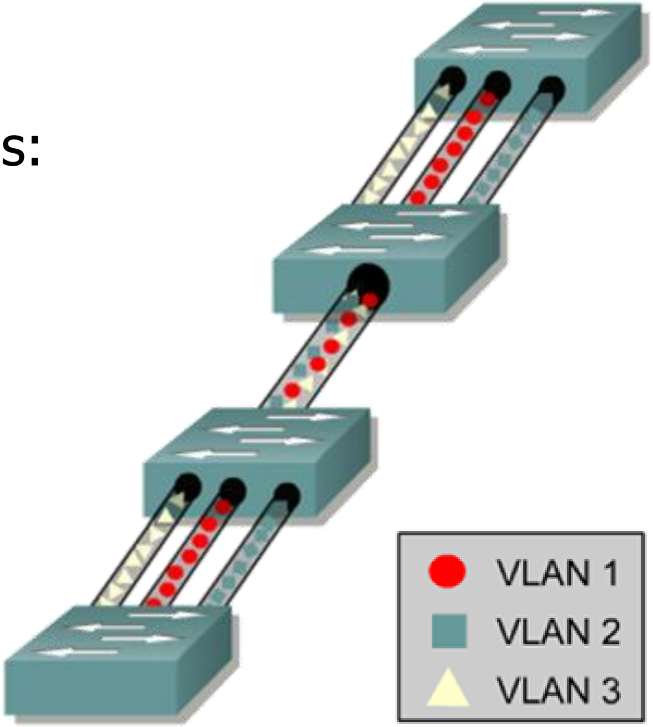
- Optional Command to add, delete, or modify VLANs.
- VLAN names, numbers, and **VTP** (VLAN Trunking Protocol) information can be entered which "may" affect other switches besides this one. (
- This does not assign any VLANs to an interface.

```
Switch#vlan database
Switch(vlan)#?
VLAN database editing buffer manipulation commands:
  abort   Exit mode without applying the changes
  apply   Apply current changes and bump revision number
  exit    Apply changes, bump revision number, and exit mode
  no      Negate a command or set its defaults
  reset   Abandon current changes and reread current database
  show    Show database information
  vlan    Add, delete, or modify values associated with a single VLAN
  vtp     Perform VTP administrative functions.
```

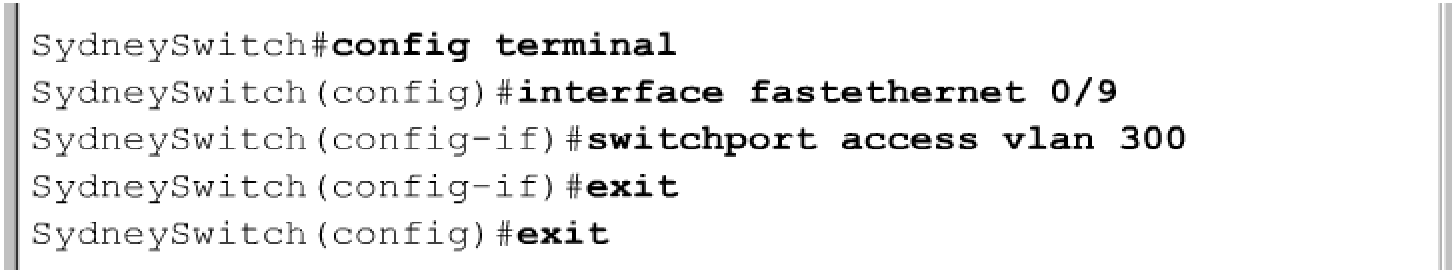
VLAN trunking

- To configure 802.1q trunking switch/router, first determine which ports on the switches will be used to connect the two switches together.
- Then in the Global configuration mode enter the following commands on both switches:

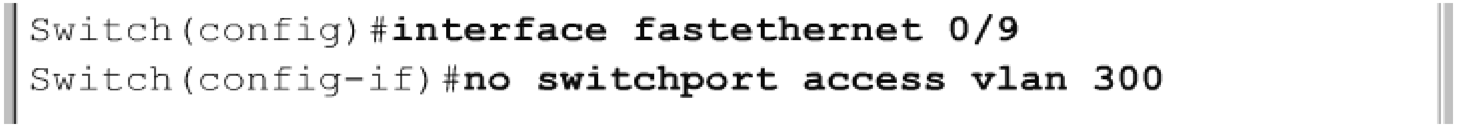
```
Switch_A(config)#interface fastethernet
             interface ifnumber
Switch_A(config-if)#switchport trunk
             encapsulation dot1q
```



Deleting a Port VLAN Membership



```
SydneySwitch#config terminal
SydneySwitch(config)#interface fastethernet 0/9
SydneySwitch(config-if)#switchport access vlan 300
SydneySwitch(config-if)#exit
SydneySwitch(config)#exit
```



```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#no switchport access vlan 300
```

```
Switch(config-if)#no switchport access vlan vlan_number
```

Deleting a VLAN

- Switch#**vlan database**
- Switch(vlan)#**no vlan** *vlan_number*
- Switch(vlan)#**exit**