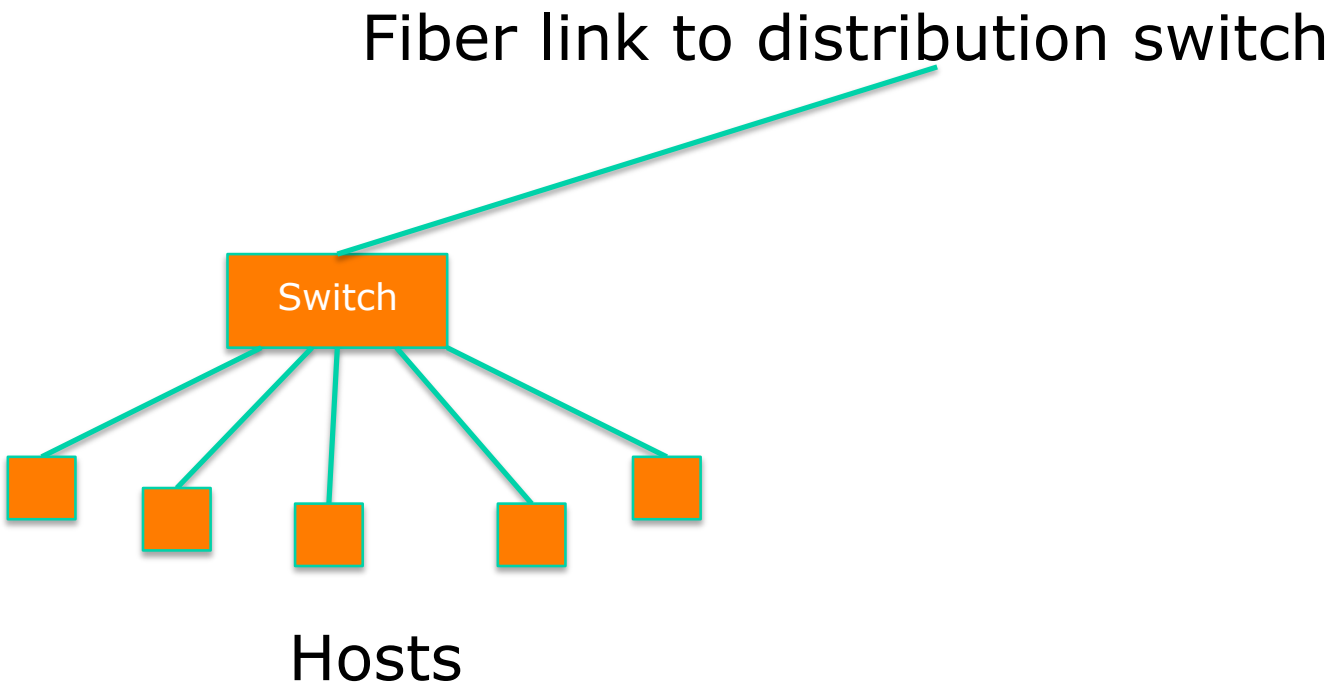
VLANs and 802.1q

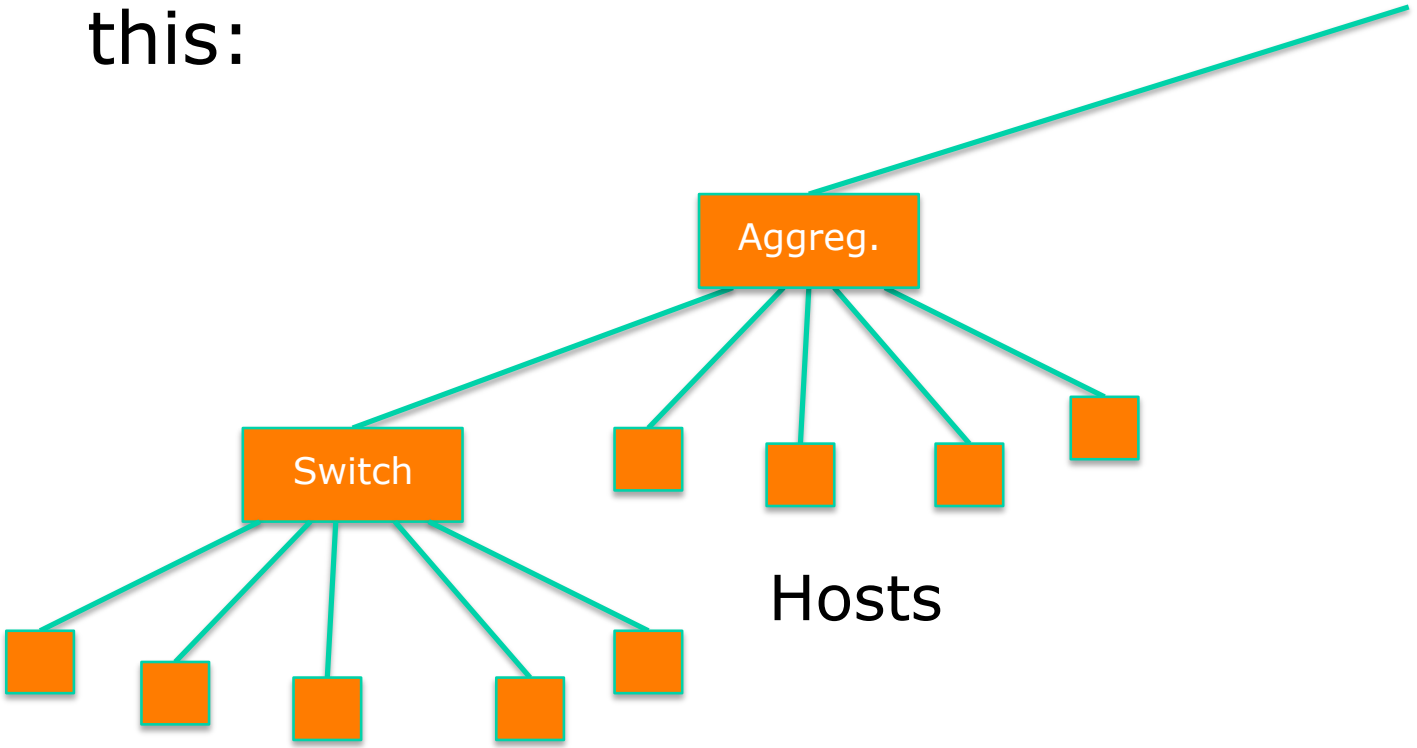
Build Incrementally

- Start small



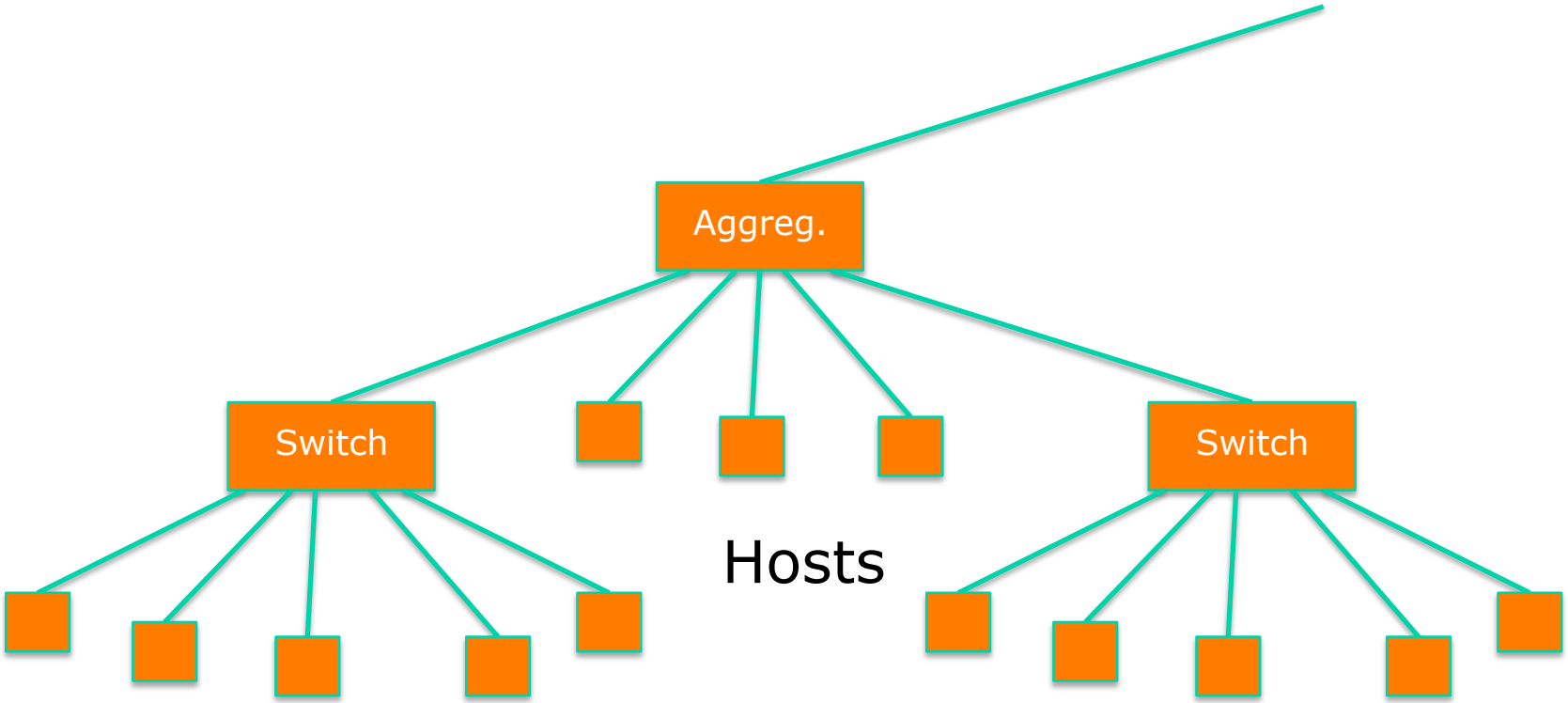
Build Incrementally

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



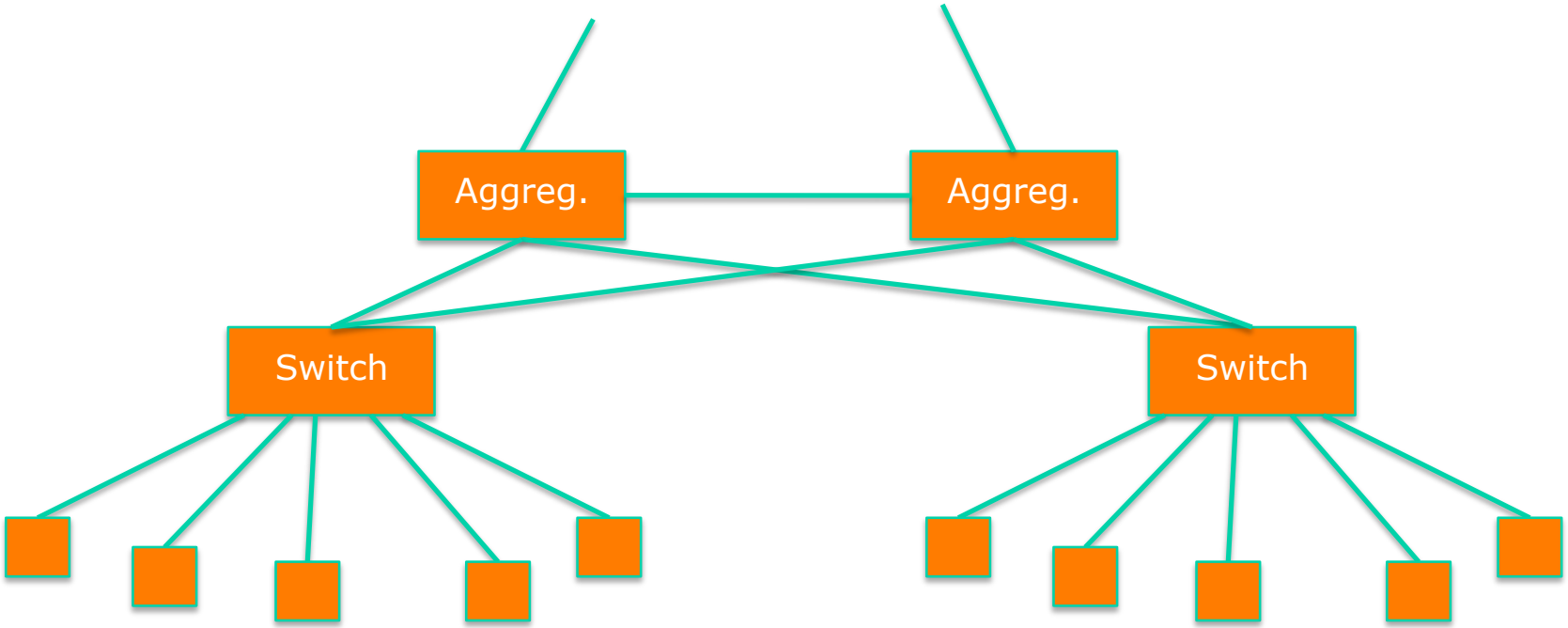
Build Incrementally

- And keep growing within the same hierarchy:



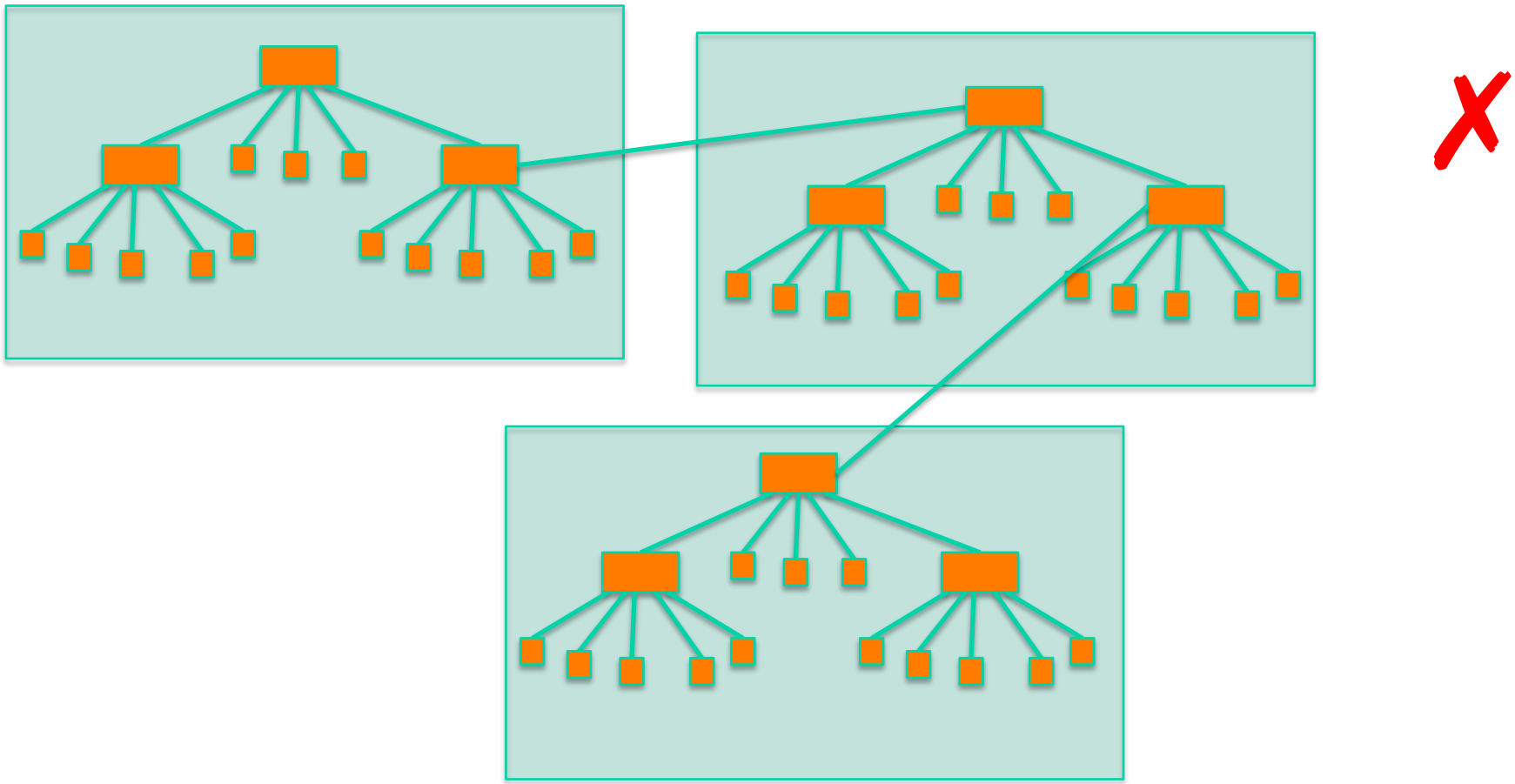
Build Incrementally

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

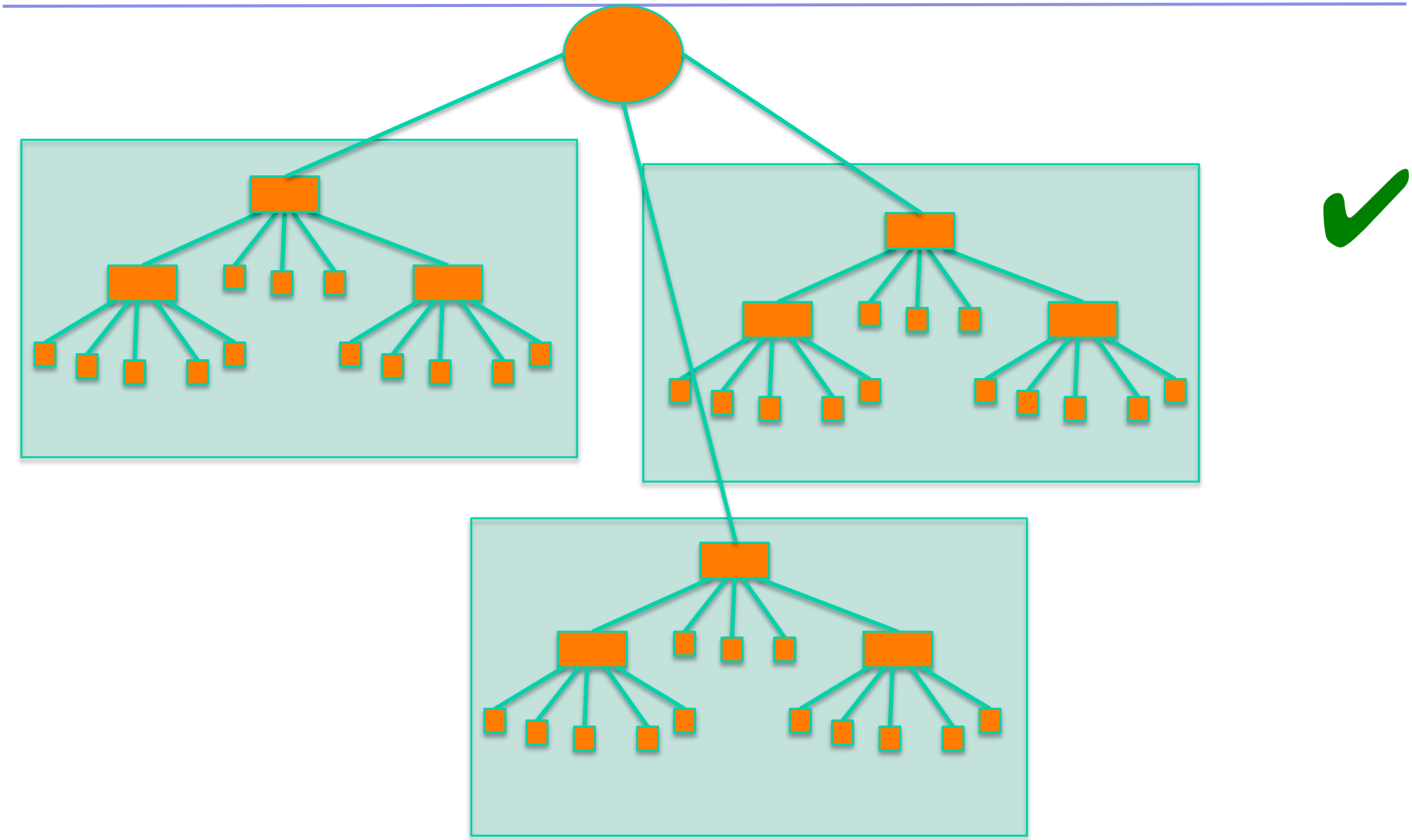


Do not daisy-chain

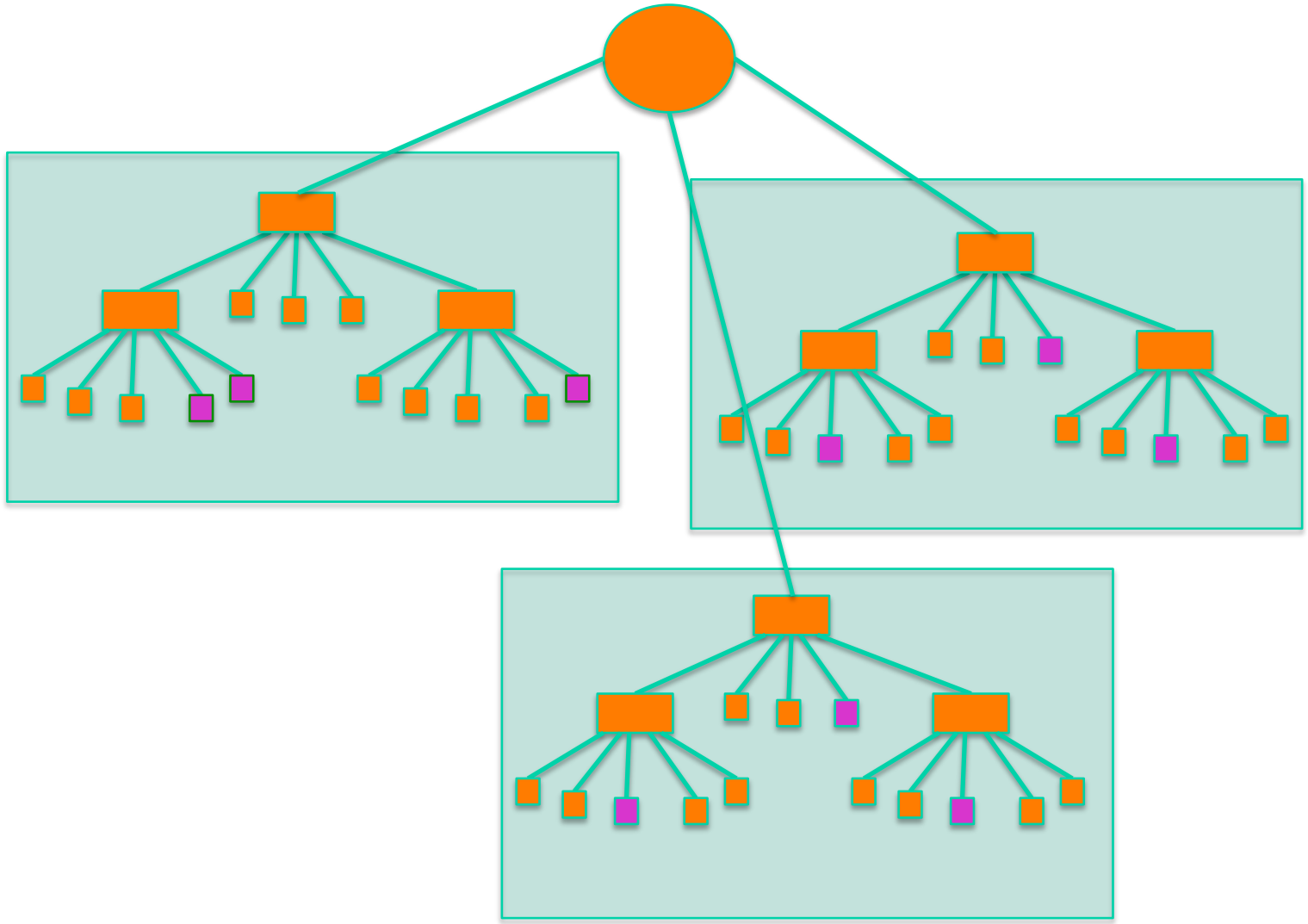
- Resist the temptation of doing this:



Connect buildings hierarchically



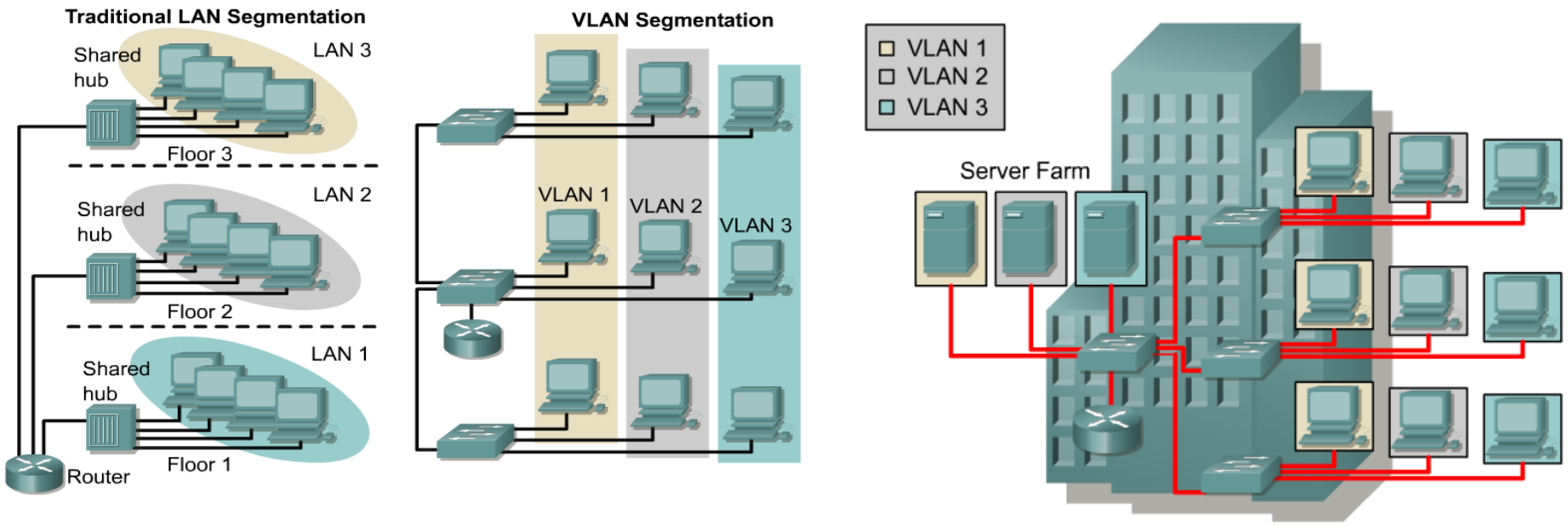
Some Hosts Need Privacy/Separation



Virtual LANs (VLANs)

- Allows us to split switches into separate (virtual) switches
- Only members of a VLAN can see that VLAN's traffic
- Inter-VLAN traffic must be routed (i.e. go through a router) because they are separate subnets

VLAN introduction

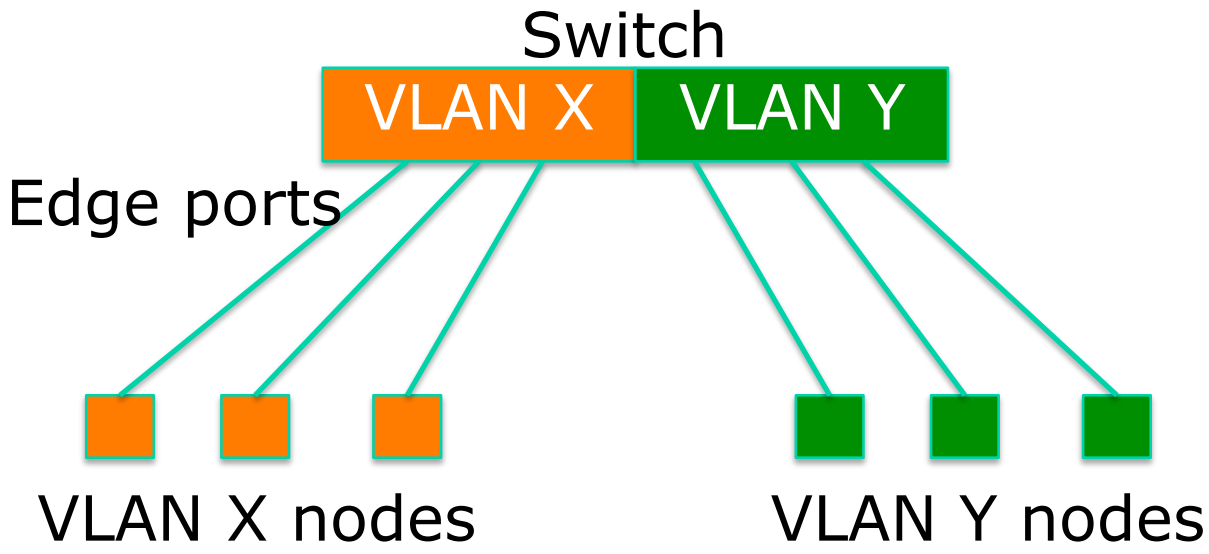


- **VLANs provide segmentation based on broadcast domains.**
- VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.

Local VLANs

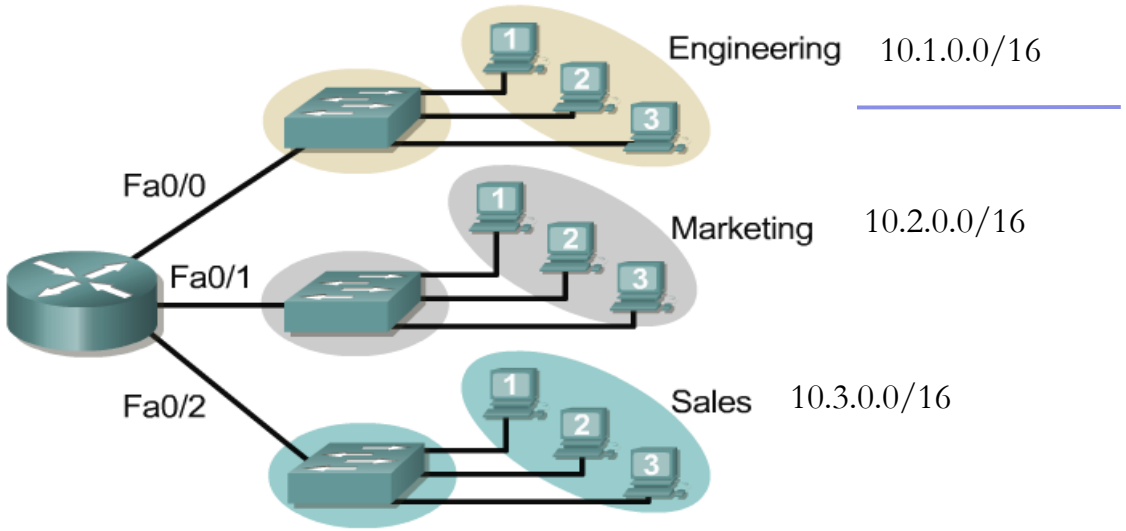
- 2 VLANs or more within a single switch
- VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- ***Edge ports***, where end nodes are connected, are configured as members of a VLAN
- The switch behaves 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 domain.
- Traffic should only be routed between VLANs.

Local VLANs



Broadcast domains with VLANs and routers

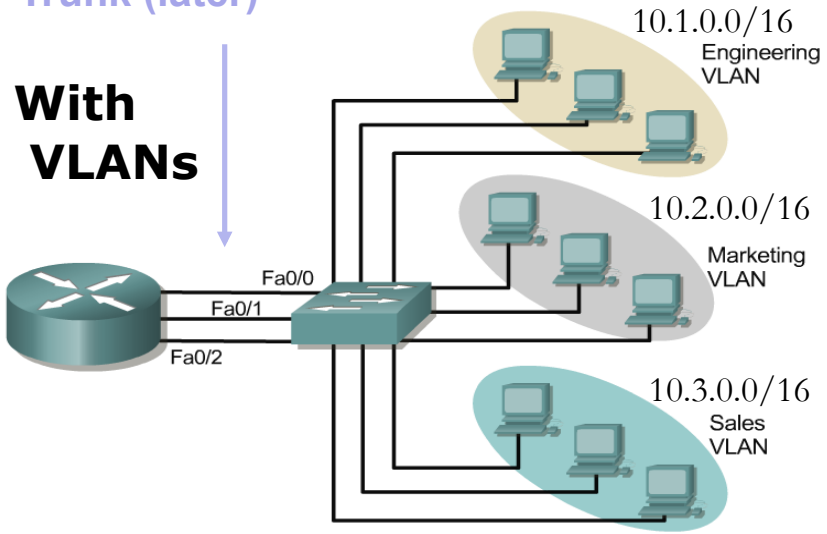
Without VLANs:



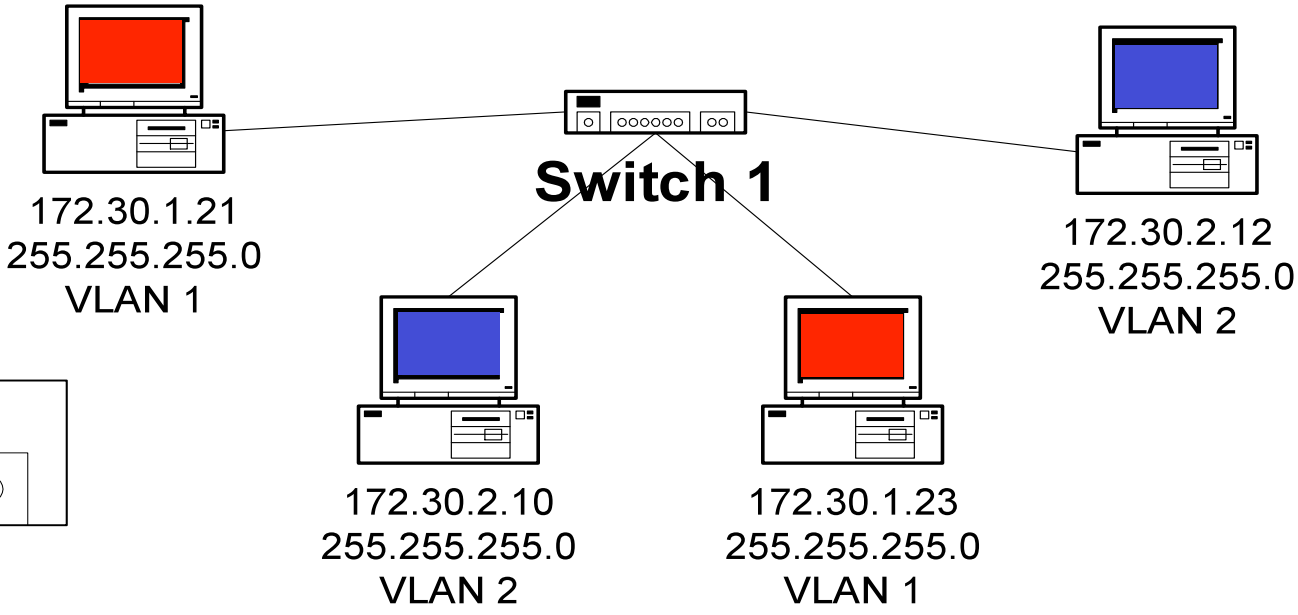
- Without VLANs, each group is on a different IP network and on a different switch.
- Using VLANs. Switch is configured with the ports on the appropriate VLAN. Still, each group on a different IP network; however, they are all on the same switch.
- What are the broadcast domains in each?

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

With VLANs



VLANs

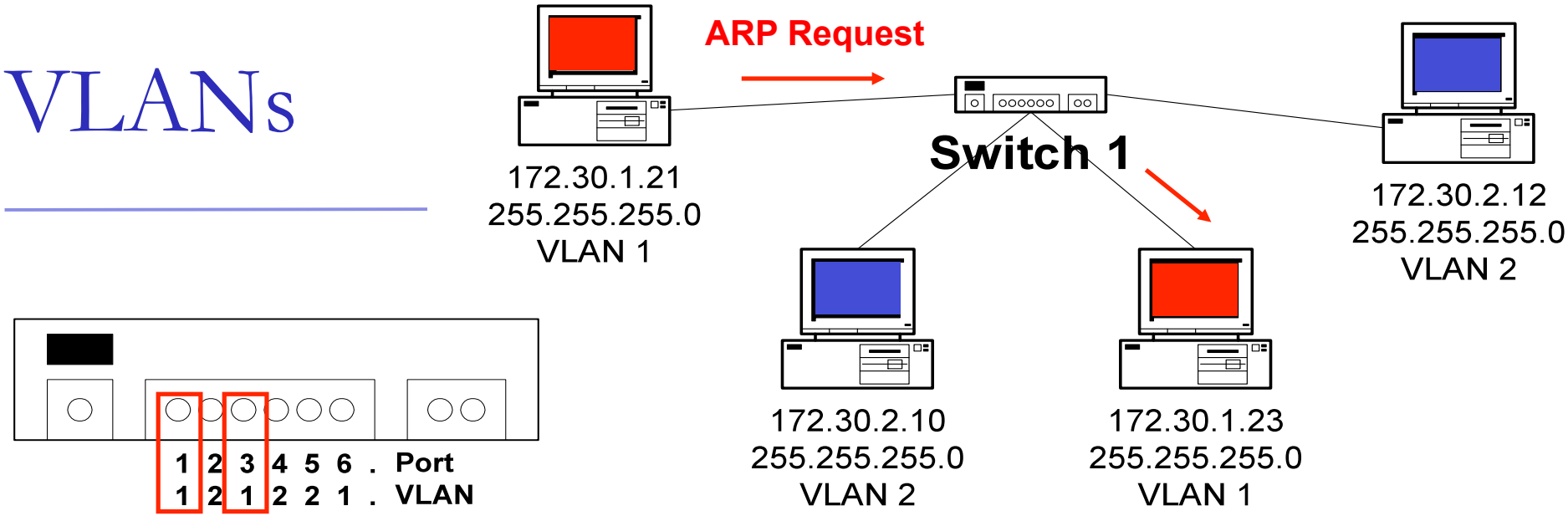


Two **VLANs** = Two **subnets**

Important notes on VLANs:

- VLANs are assigned to switch ports. There is no "VLAN" assignment done on the host.
- 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 == subnets.
  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

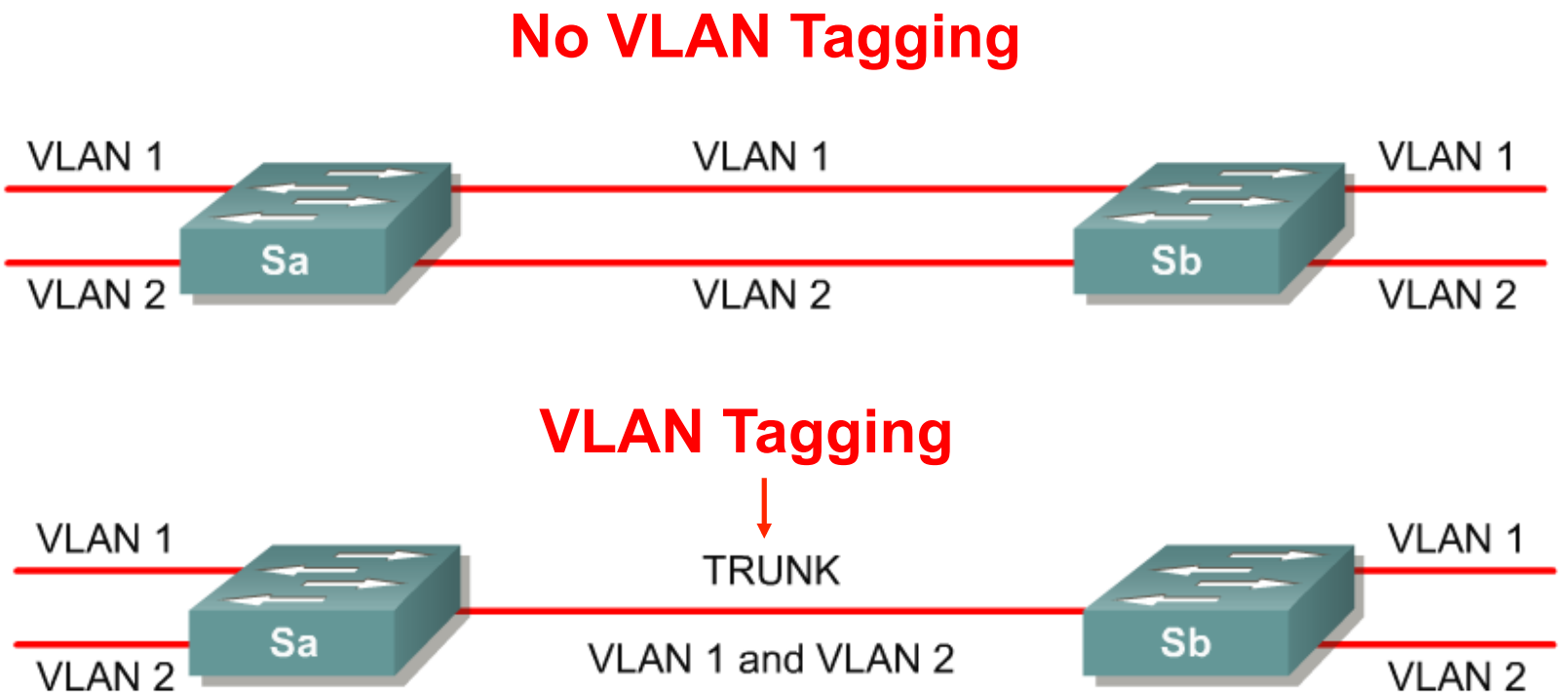
- As a device enters the network, it assumes the VLAN membership of the port to which it is attached.
- The default VLAN for every port in the switch is VLAN 1 and cannot be deleted.

  (This statement does not give the whole story. More in the lab later for interested groups…)
- All other ports on the switch may be reassigned to arbitrary VLANs.

VLANs across switches

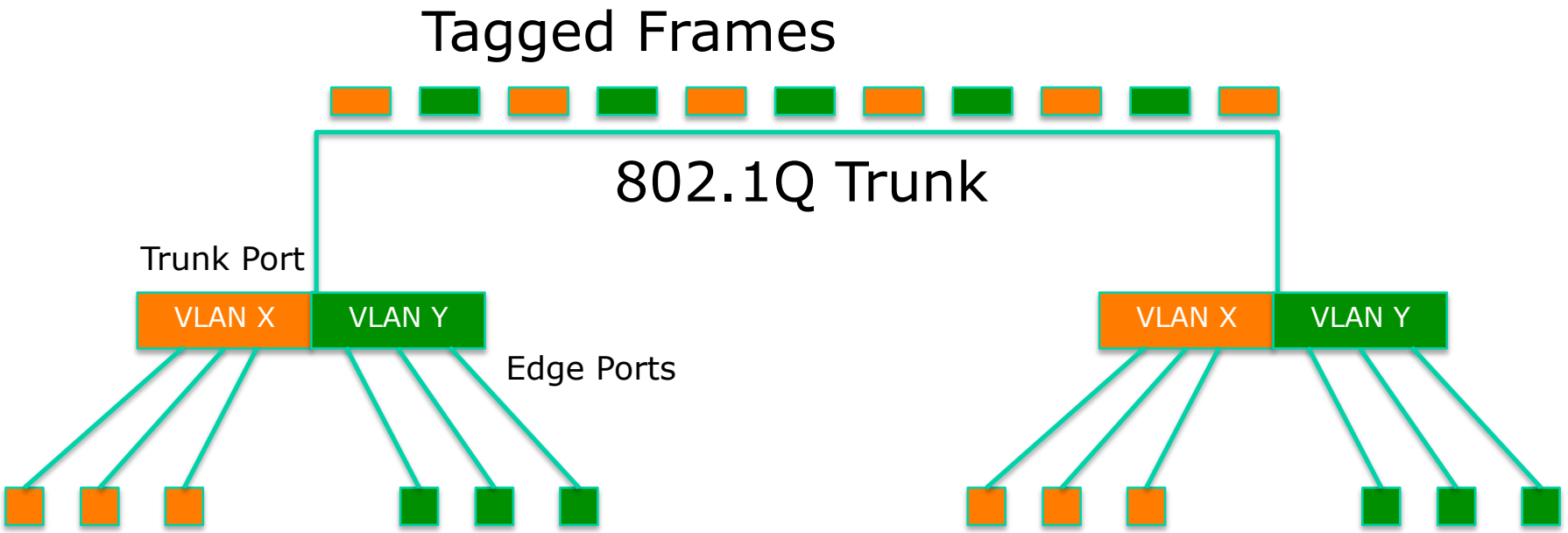
- Two switches can exchange traffic from one or more VLANs
- Inter-switch links are configured as ***trunks***, carrying frames from all or a subset of a switch's VLANs
- Each frame carries a ***tag*** that identifies which VLAN it belongs to

VLANs across switches



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

VLANs across switches

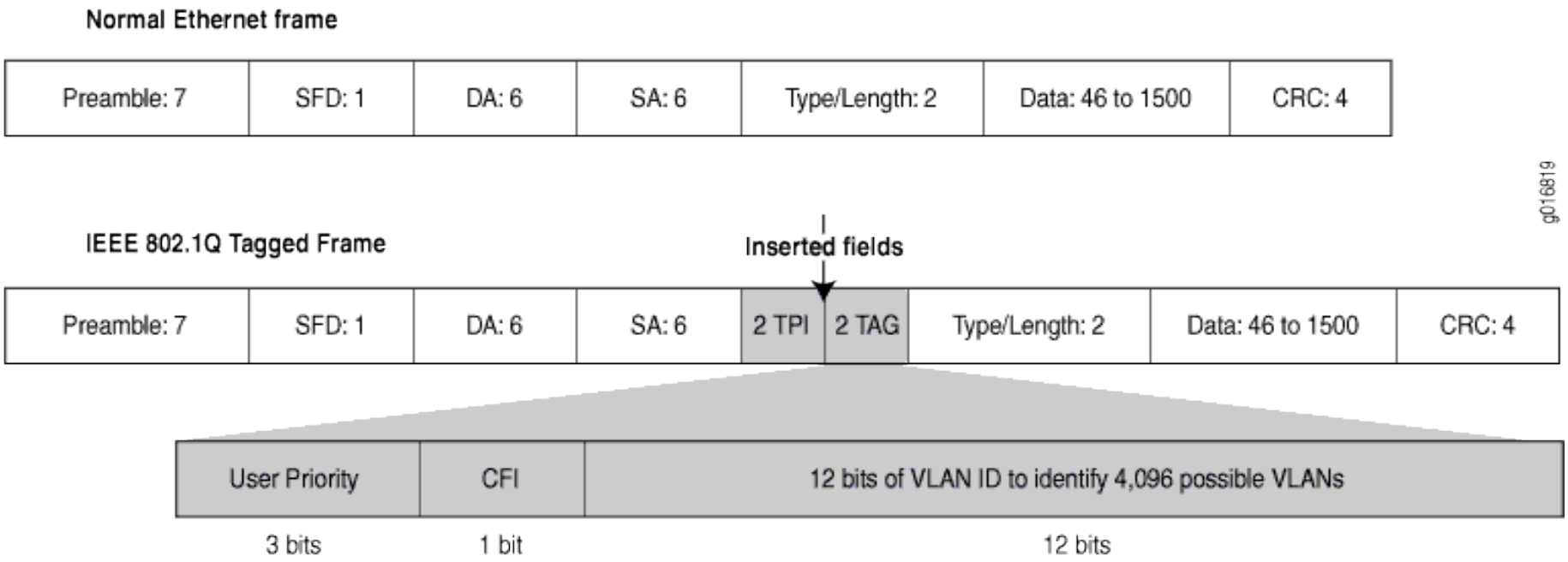


This is called “VLAN Trunking”

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



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
  - Field technicians need more skills
- 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 you can, and you feel cool ☺
- 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 "VLAN spaghetti"

- 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