Ethernet and switches

selected topics
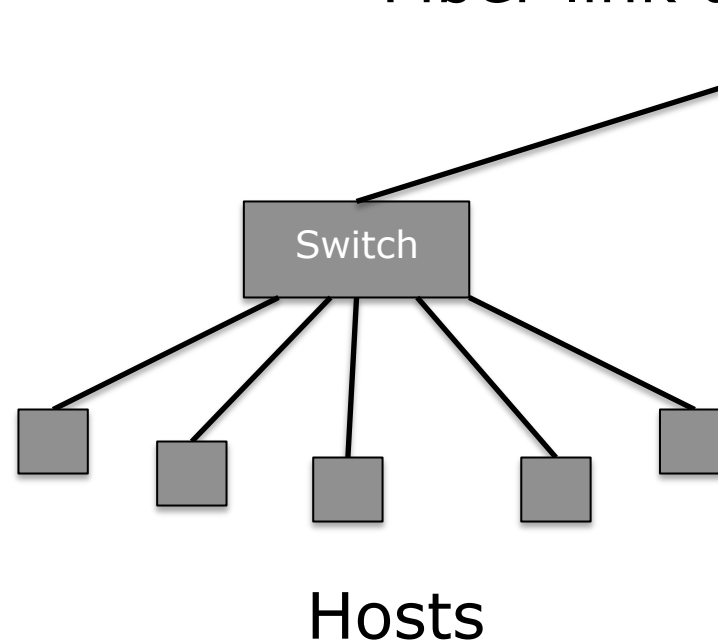
Agenda

- Scaling ethernet infrastructure
- VLANs

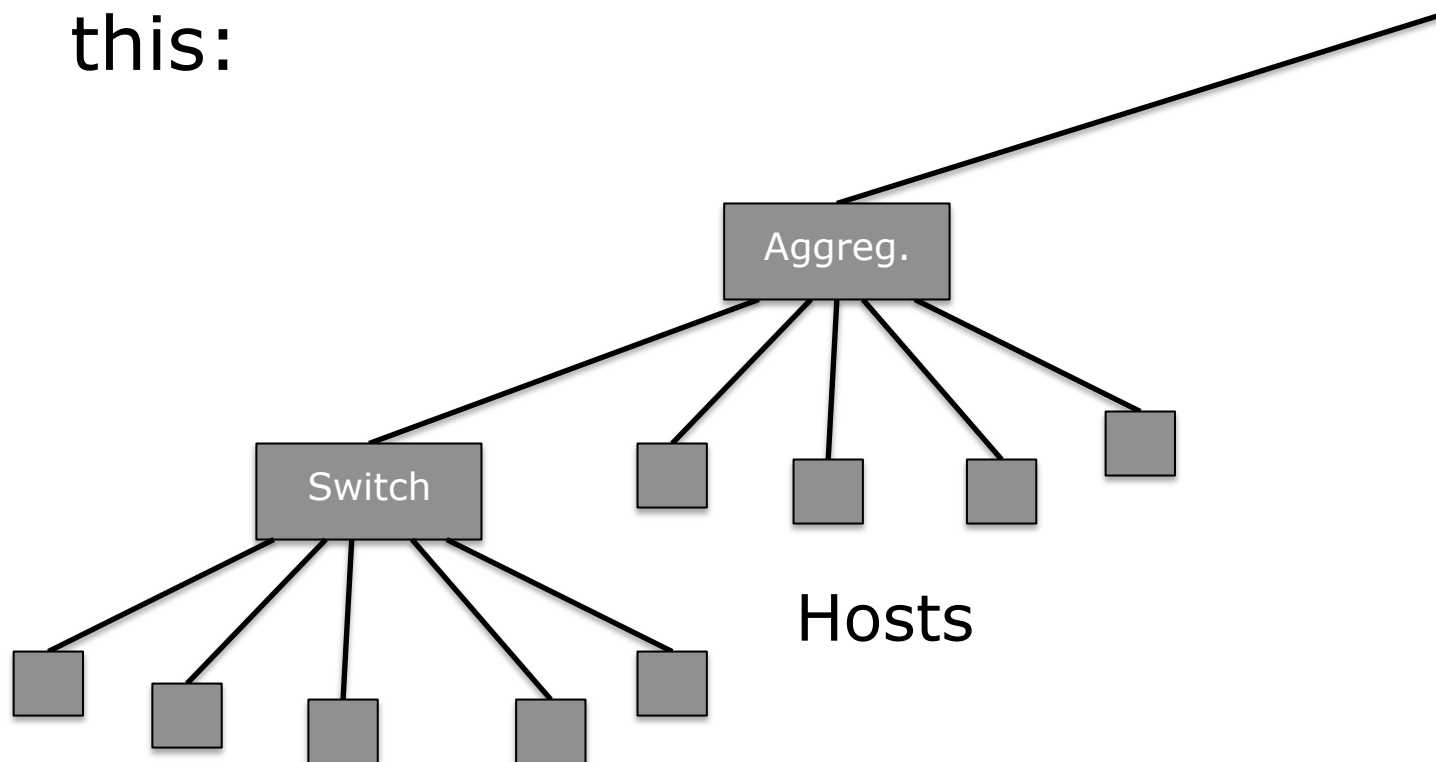# Build Incrementally

- Start small

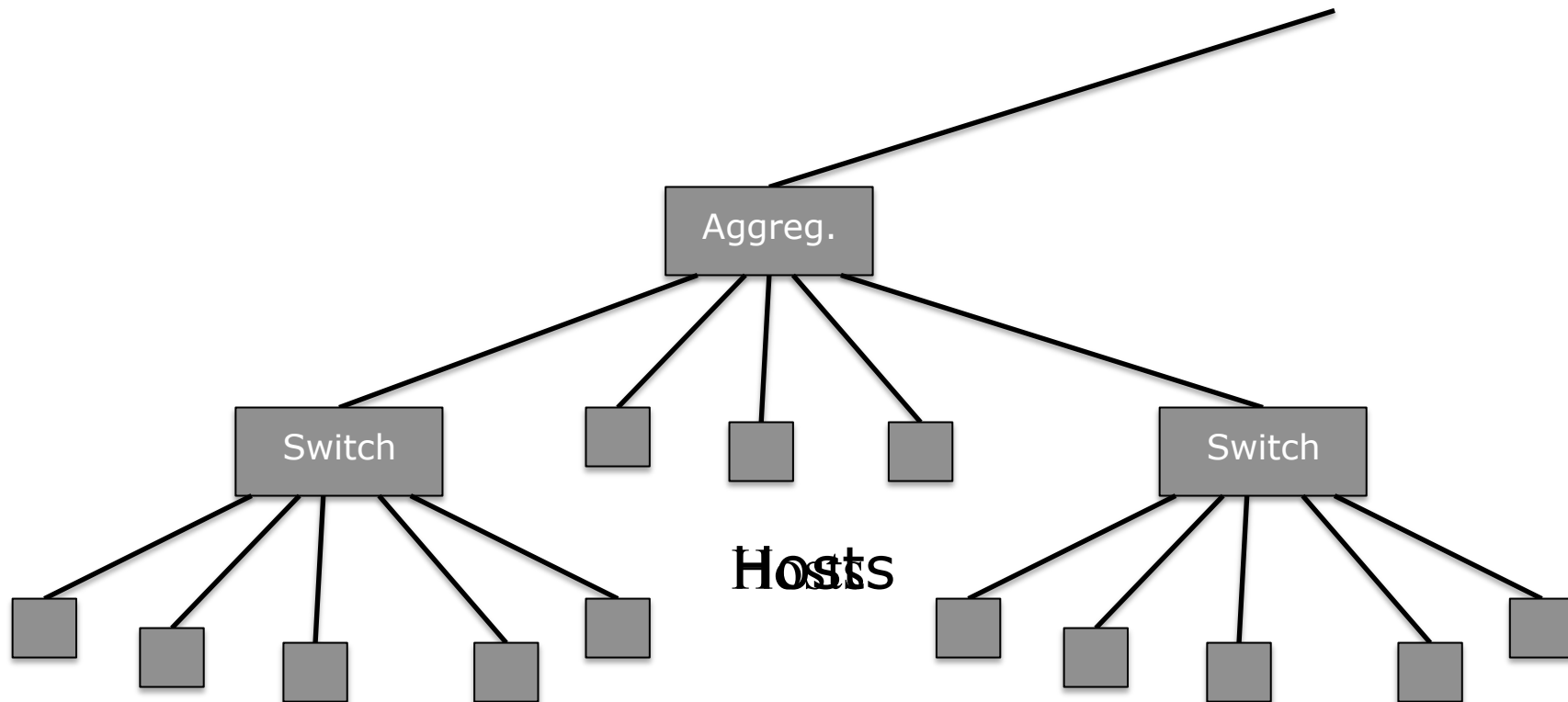Fiber link to distribution switch

Switch

Hosts

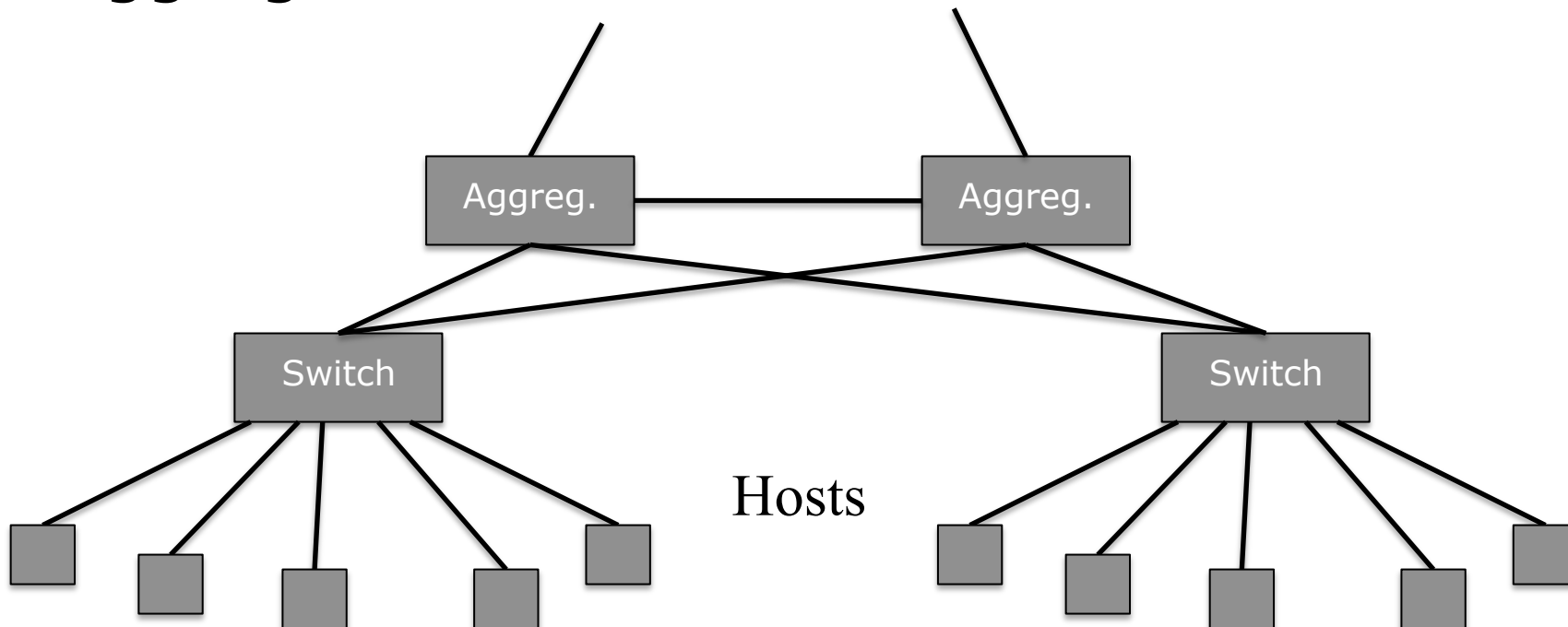# Build Incrementally

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

Build Incrementally

- And keep growing within the same hierarchy:

Aggreg.

Switch

Switch

Hosts

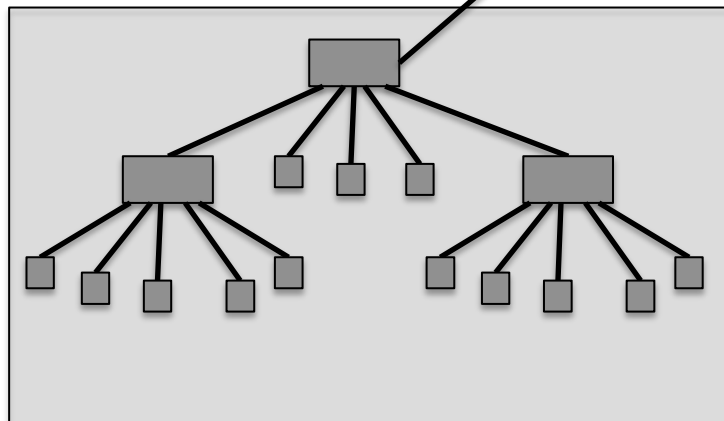# Build Incrementally

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

Aggreg.

Aggreg.

Switch

Switch

Hosts

Do not daisy-chain

- Resist the temptation of doing this:
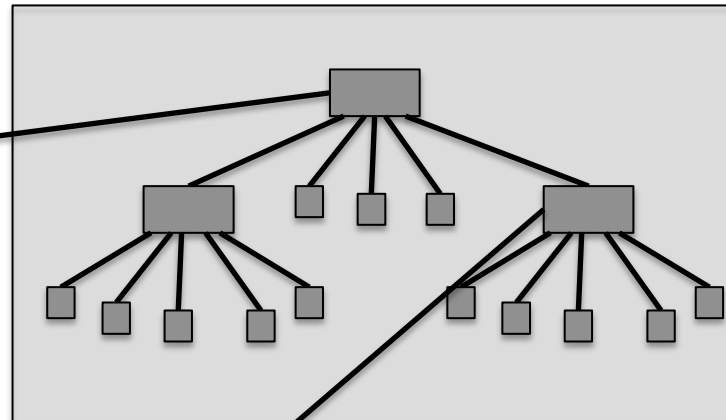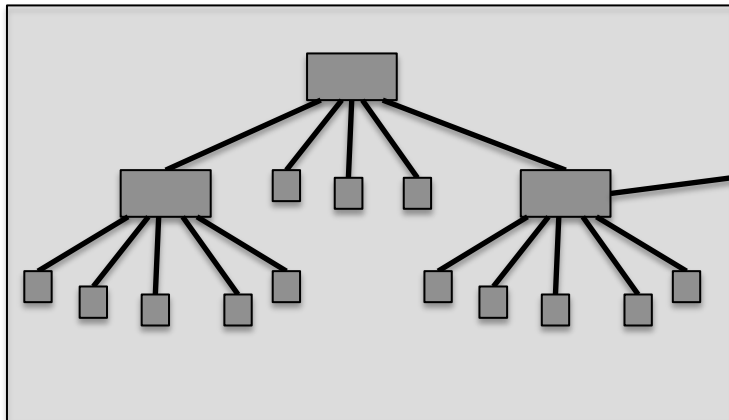
Connect buildings hierarchically
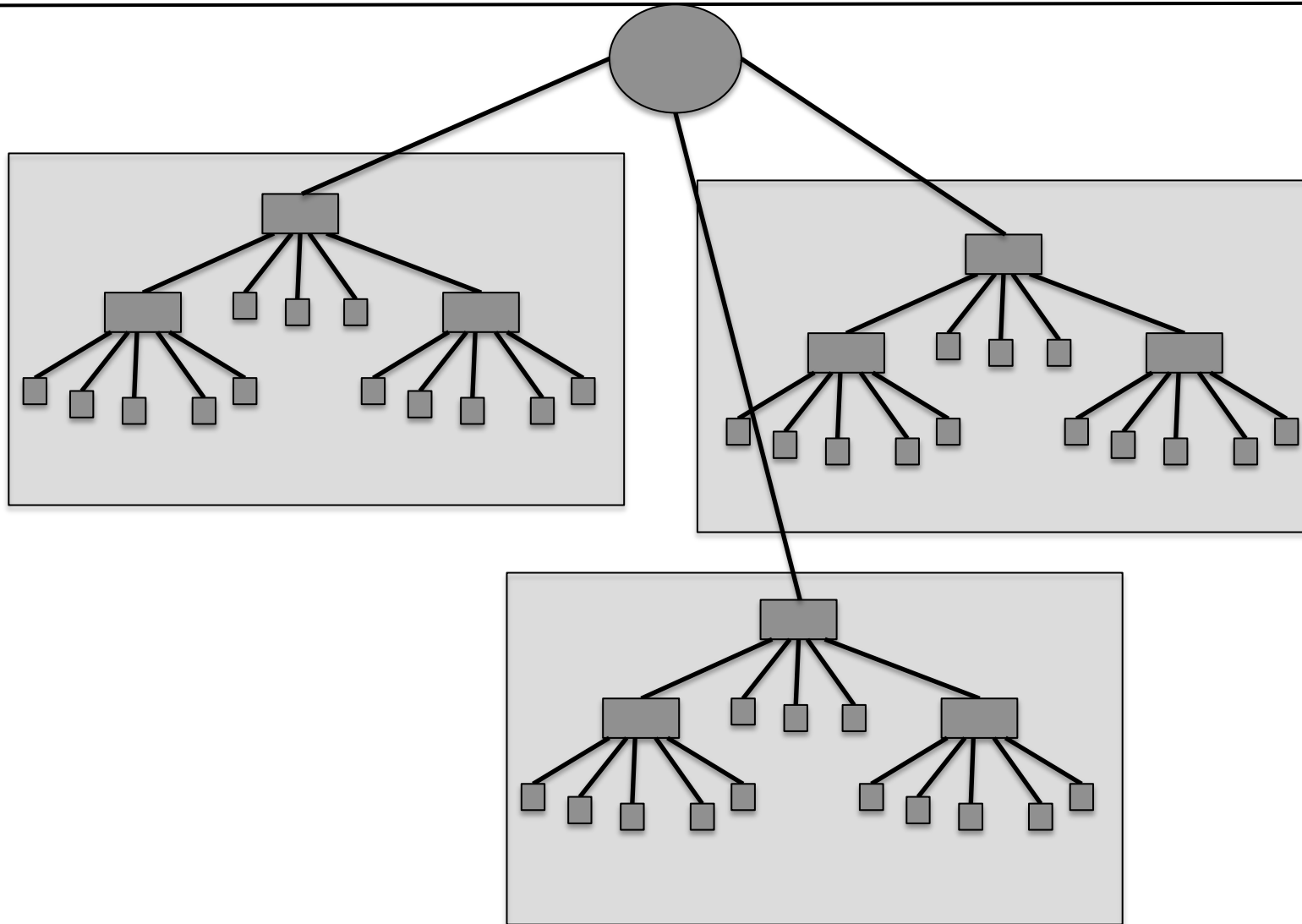
Agenda

- Scaling ethernet infrastructure
- VLANs

Definition

LAN

- Broadcast domain

Local VLANs

Switch

VLAN X VLAN Y

VLAN X nodes   VLAN Y nodes
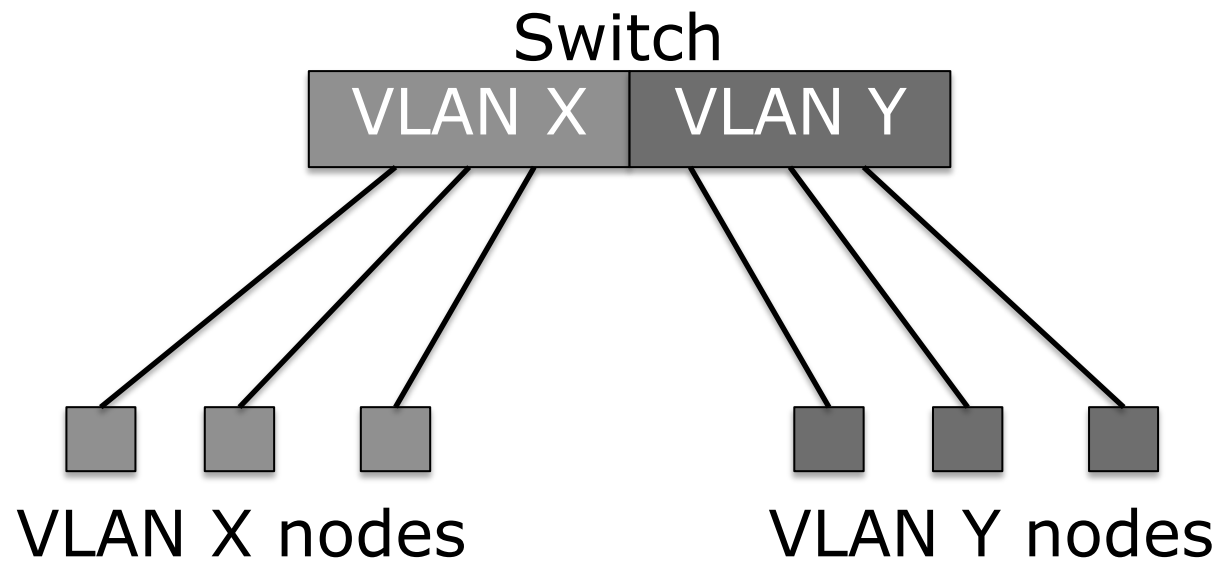
Virtual LANs (VLANs)

- 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

Some Hosts Need Privacy/Separation
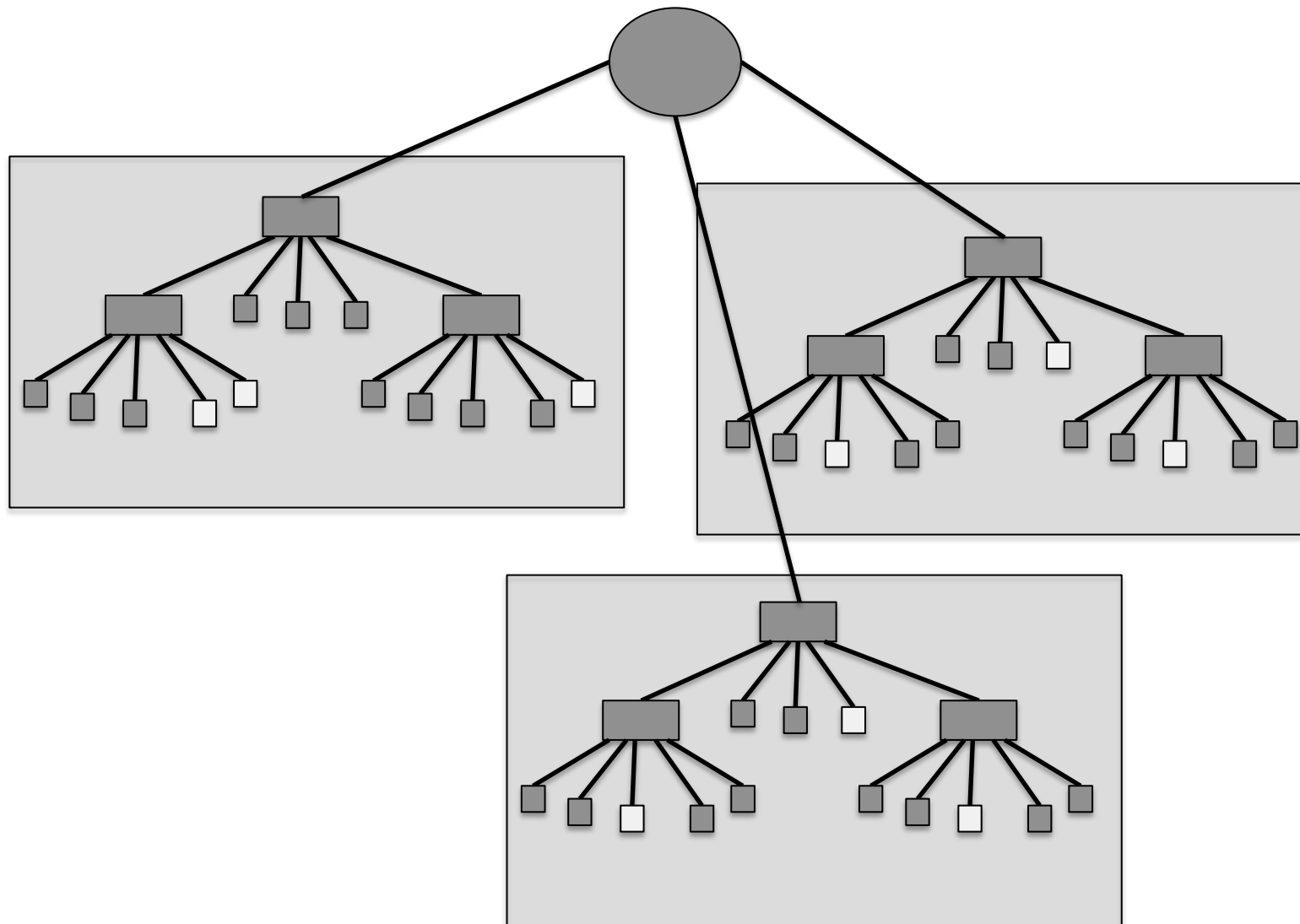
VLAN introduction
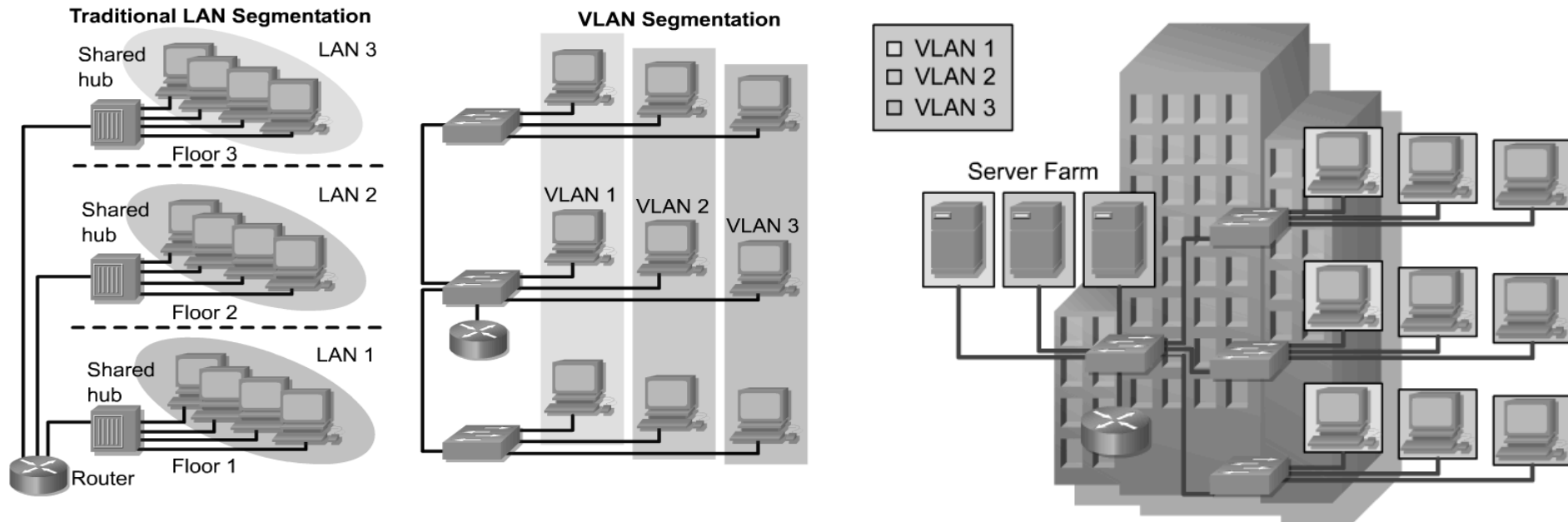
- **VLANs provide segmentation based on broadcast domains.**

- 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.

Broadcast domains with VLANs and routers

Without VLANs:

Fa0/0

Fa0/1

Fa0/2

Engineering 10.1.0.0/16

Marketing 10.2.0.0/16

Sales 10.3.0.0/16
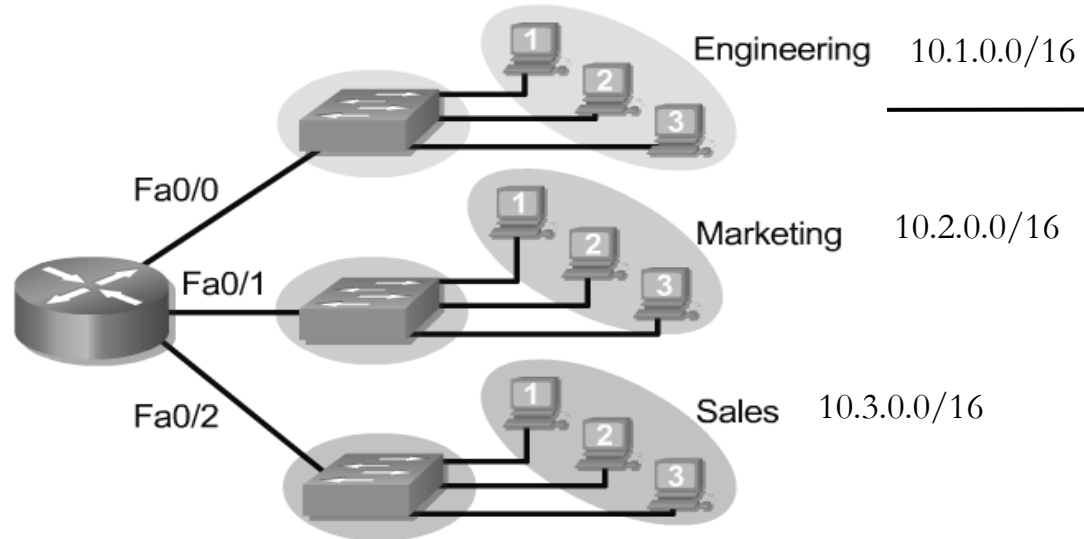
- Without VLANs, each group is on a different IP network and on a different switch.

- 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

Fa0/0
Fa0/1
Fa0/2

10.1.0.0/16
Engineering VLAN

10.2.0.0/16
Marketing VLAN

10.3.0.0/16
Sales VLAN

16

VLANs

172.30.1.21
255.255.255.0
VLAN 1

Switch 1

172.30.2.12
255.255.255.0
VLAN 2

1	2	3	4	5	6	.	Port
1	2	1	2	2	1	.	VLAN

172.30.2.10
255.255.255.0
VLAN 2

172.30.1.23
255.255.255.0
VLAN 1
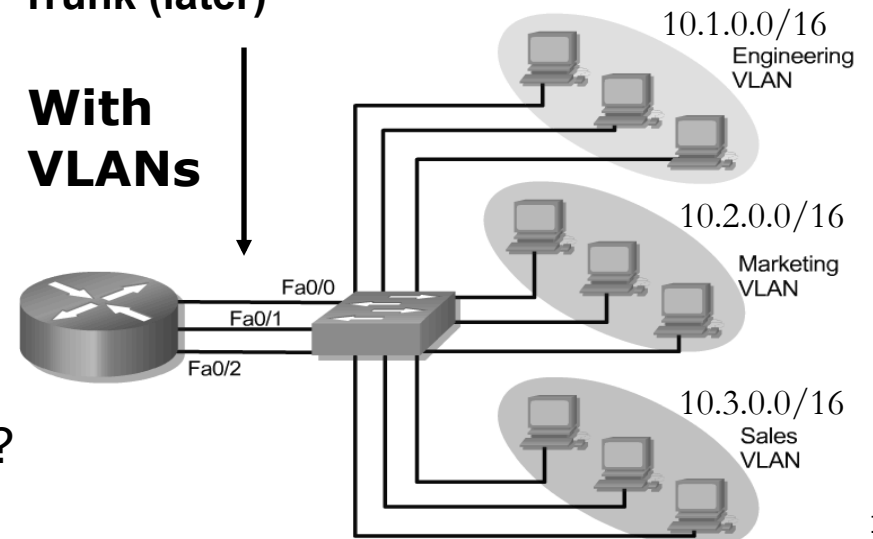
Two **VLANs** = Two **subnets**
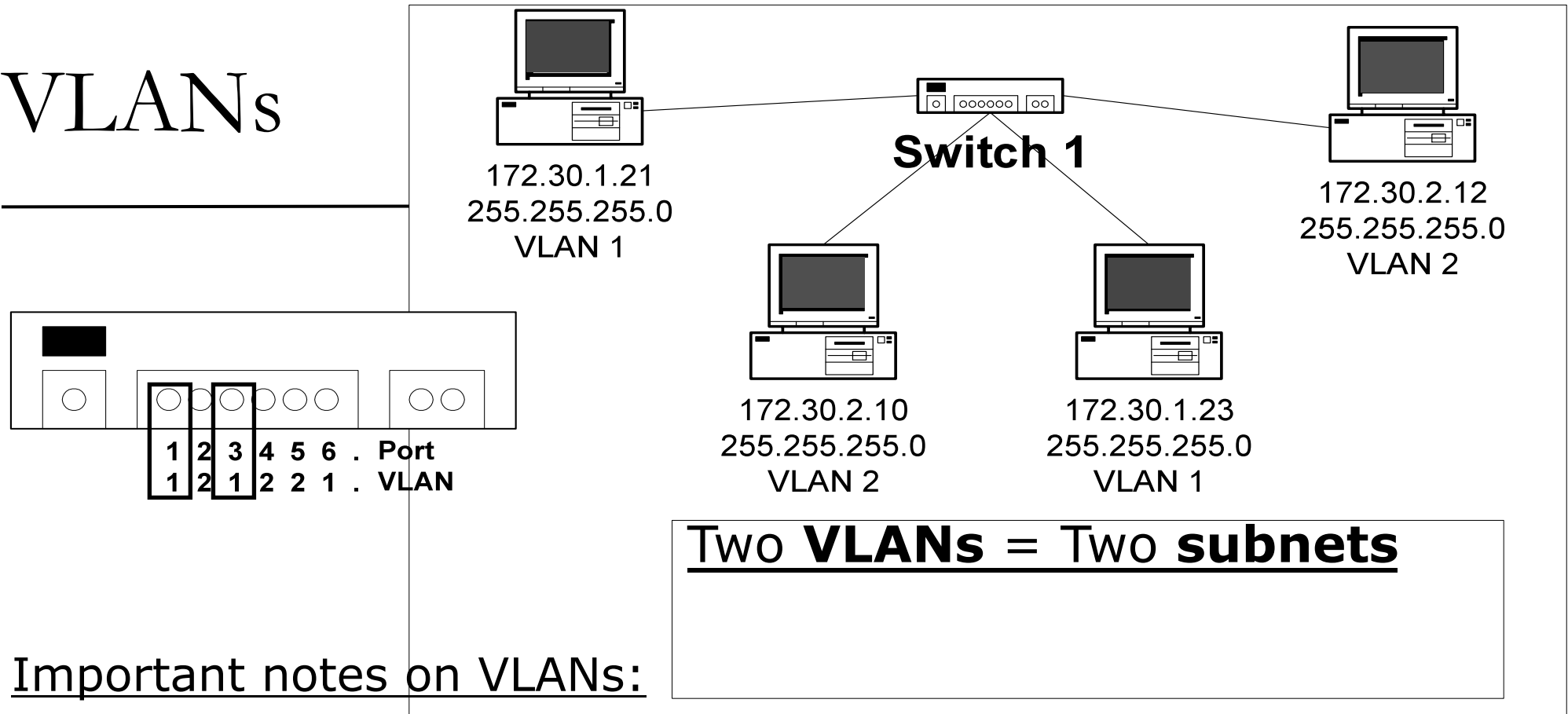
Important notes on VLANs:

- 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

ARP Request

172.30.1.21
255.255.255.0
VLAN 1

Switch 1

172.30.2.12
255.255.255.0
VLAN 2

172.30.2.10
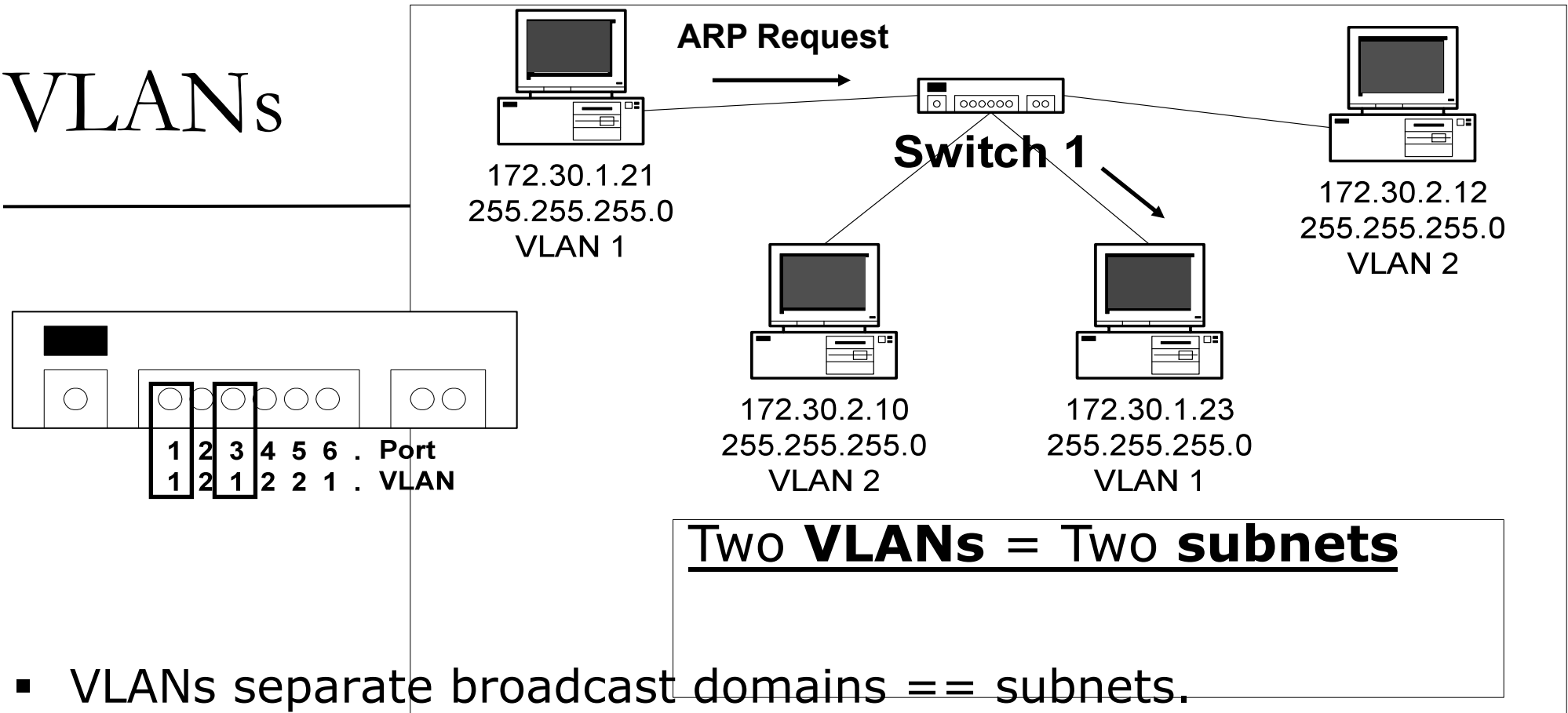255.255.255.0
VLAN 2

172.30.1.23
255.255.255.0
VLAN 1

| 1 | 2 | 3 | 4 | 5 | 6 | . | Port |
| 1 | 2 | 1 | 2 | 2 | 1 | . | VLAN |

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
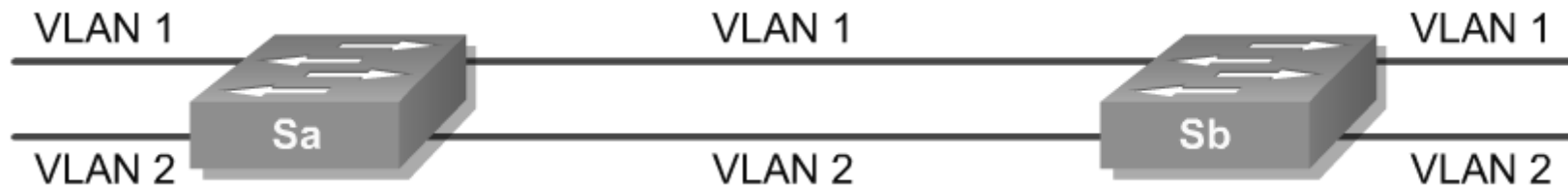
VLAN operation

- 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

No VLAN Tagging

VLAN 1	VLAN 1	VLAN 1
Sa	Sb	
VLAN 2	VLAN 2	VLAN 2

VLAN Tagging

↓

TRUNK

VLAN 1 and VLAN 2

VLAN 1 ... Sa ... VLAN 2 ... Sb ... VLAN 1 ... VLAN 2
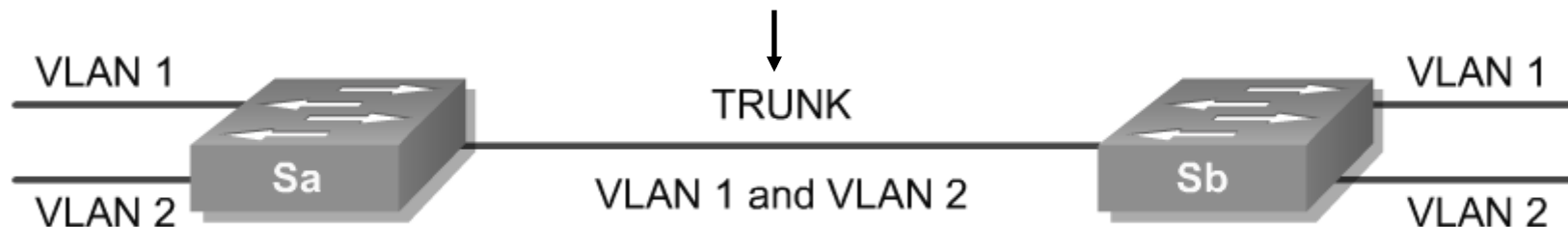
- VLAN tagging is used when a single link needs to carry traffic for more than one VLAN.

VLANs across switches

Tagged Frames

802.1Q Trunk

Trunk Port

VLAN X VLAN Y

Edge Ports

VLAN X VLAN Y
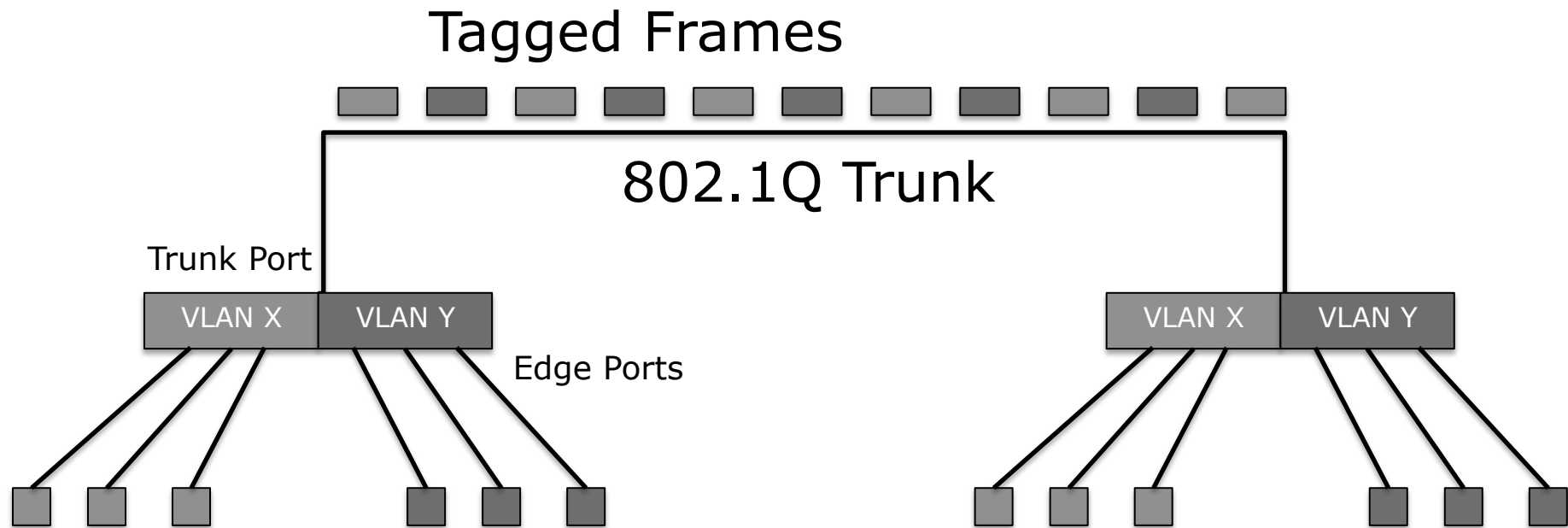
This is called "VLAN Trunking"

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

Normal Ethernet frame

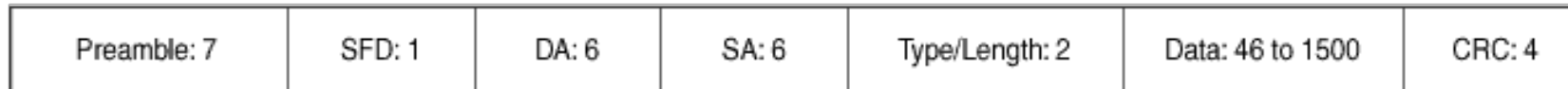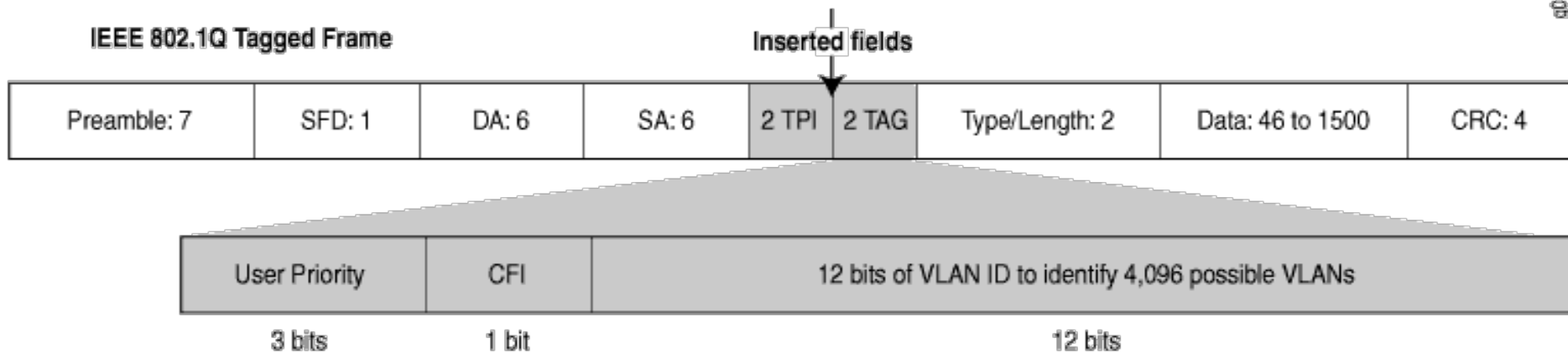| Preamble: 7	SFD: 1	DA: 6	SA: 6	Type/Length: 2	Data: 46 to 1500	CRC: 4

IEEE 802.1Q Tagged Frame   Inserted fields

Preamble: 7	SFD: 1	DA: 6	SA: 6	2 TPI	2 TAG	Type/Length: 2	Data: 46 to 1500	CRC: 4

User Priority	CFI	12 bits of VLAN ID to identify 4,096 possible VLANs
3 bits	1 bit	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
  - 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
  - <u>Maintenance and troubleshooting nightmare</u>