SCS 2205
Computer Networks I

Networking Devices & Network Design

Dr. Ajantha Atukorale /UCSC

Network Devices

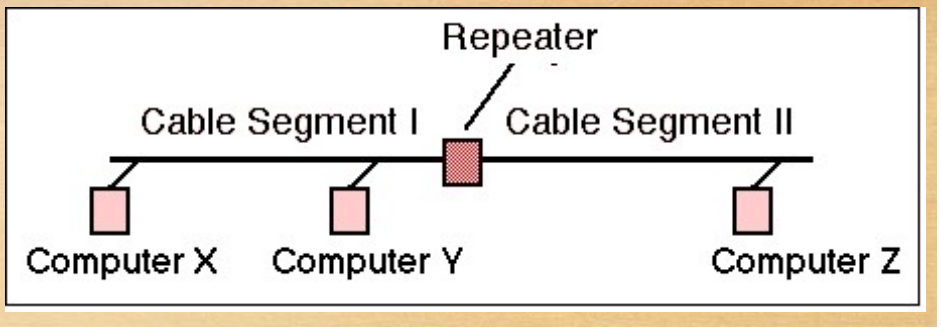
NICs, Repeaters, hubs, bridges, switches, routers

Devices and the layers at which they operate

Layer	Name of Layer	Device
3	Network	Routers, layer 3 switches
2	Data Link	Switches, bridges, NIC's
1	Physical	Hubs, Repeaters

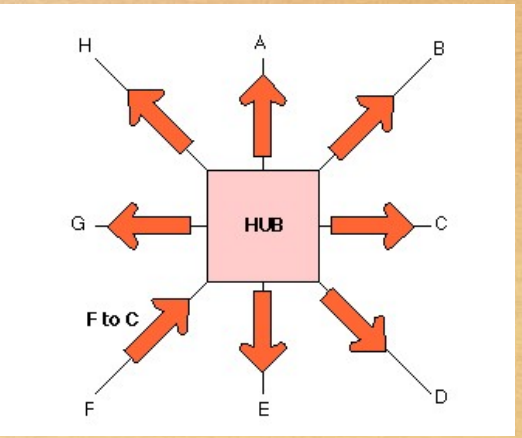
Repeaters

- Signal attenuation or signal loss – signal degrades over distance
- Repeaters **clean**, **amplify**, and **resend** signals that are weakened by long cable length.
- Built-in to hubs or switches
- Allow smaller LANs to grow into larger ones by moving transmissions from one network segment to another
- Represent a simple and relatively inexpensive means of enlarging a network
- Operates at the **physical layer**

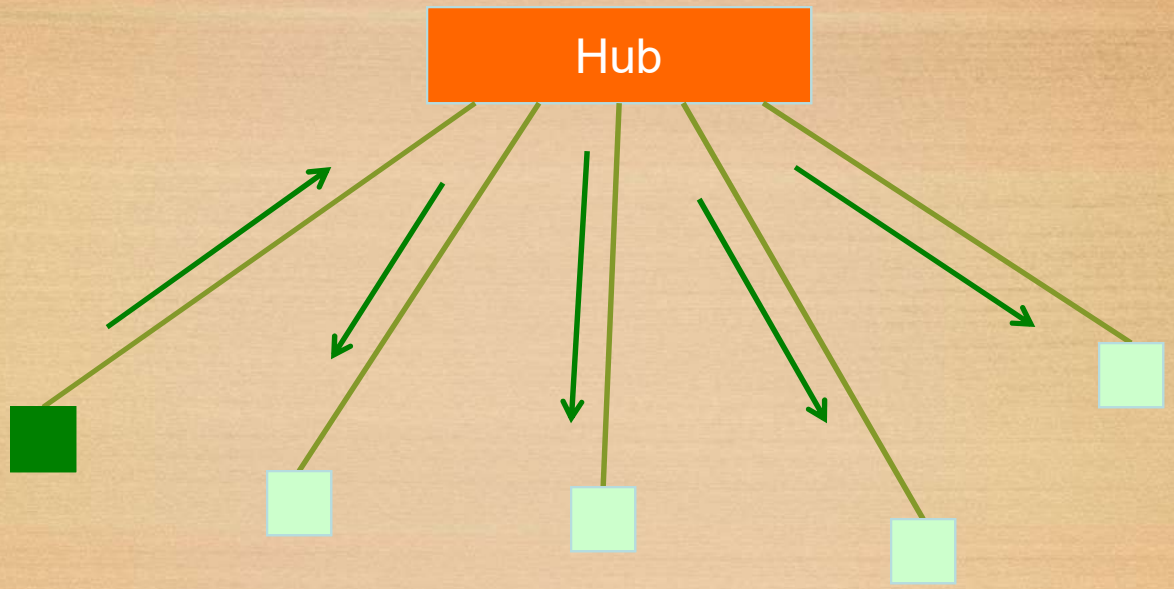


Hubs

- OSI **layer 1** hardware
- Hubs regenerate and retime network signals
- Hubs propagate signals through the network
- They are used as network concentration points
- **Uplink port** – crossover mode or straight through mode
- Receives a frame on one port and sends it out every other port, always
- They cannot **filter** network traffic
- They cannot determine **best path**
- They are really **multi-port** repeaters
- **Collision** domain is not reduced



Hub



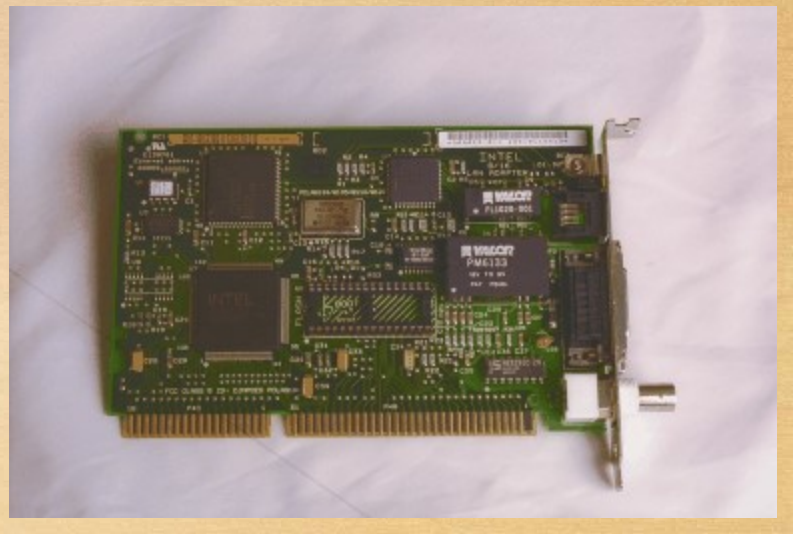
A frame sent by one node is always sent to **every other node**. Hubs are also called "repeaters" because they just "repeat" what they hear.

NIC's
(Network Interface Cards)

- Every network interface device has this **unique** physical address
- These addresses are **48 bits** long, and expressed as 12 hexadecimal digits
- First/left 6 hex digits represent the **vendor**, and the last/right 6 hex digits specify the **serial number** which vendor assigned

Vendor Unique ID	Serial Number

- E.g.
- MAC Address: 08 00 20 00 70 DF
- Vendor: Sun Microsystems (080020)

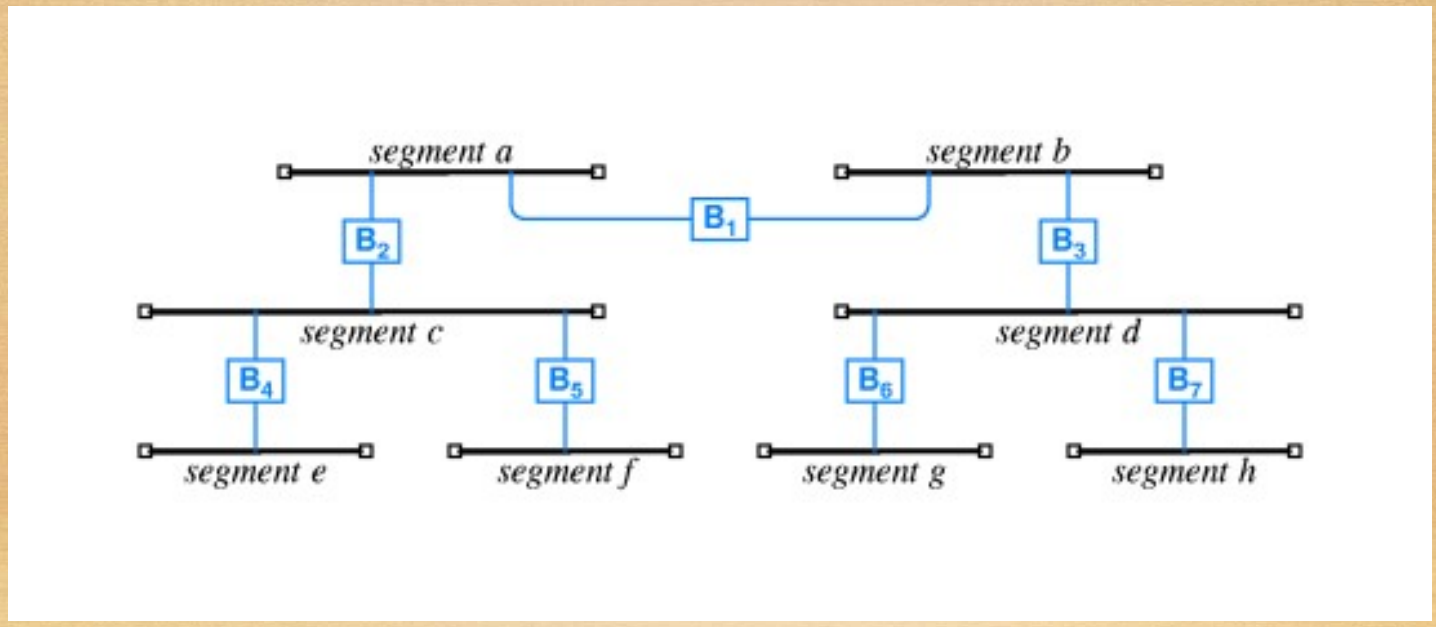


Bridges

- A **layer 2** device designed to create two or more LAN segments, each of which is a separate collision domain.
- The purpose is to **filter** traffic on a LAN, to keep local traffic local, yet allow connectivity to other segments of the network.
- Filter traffic by looking at the MAC address (**Frame filtering**)
- If the frame is addressed to a MAC address on the local side of the bridge, it is **not forwarded** to the other segment
- MAC addresses on the other segment are **forwarded**
- Bridges maintain a **MAC address table** for both segments they are connected to

Cycle of bridges

- Bridged network can span many segments
- Broadcasts are sent to **all** segments



Switched networks

- Shared Ethernet networks perform best when kept to 30-40 percent full capacity
- This is a result of CSMA/CD (Ethernet)
- A LAN switch is a high-speed multiport bridge which segments each port into its **own collision domain** and can access the full bandwidth

Switch

- ***Learns*** the location of each node by looking at the **source address** of each incoming frame, and builds a ***forwarding table***
- ***Forwards*** each incoming frame to the port where the destination node is
  - Reduces the collision domain
  - Makes more efficient use of the wire
  - Nodes don't waste time checking frames not destined to them

Store and Forward Switches

- Do error checking on **each frame** after the entire frame has arrived into the switch
- If the error checking algorithm determines there is no error, the switch looks in its MAC address table for the port to which to forward the destination device
- Highly **reliable** because doesn't forward bad frames
- **Slower** than other types of switches because it holds on to each frame until it is completely received to check for errors before forwarding

Cut Through Switch

- **Faster** than store and forward because doesn't perform error checking on frames
- Reads address information for each frame as the frames enter the switch
- After looking **up the port of the destination** device, frame is forwarded
- Forwards bad frames
  - **Performance penalty** because bad frames can't be used and replacement frames must be sent which creates additional traffic

Fragment free cut through switch

- **Combines** speed of cut through switch with error checking functionality
- Forwards all frames initially, but determines that if a particular port is receiving too many bad frames, it reconfigures the port to **store and forward mode**
- Preferred switching solution

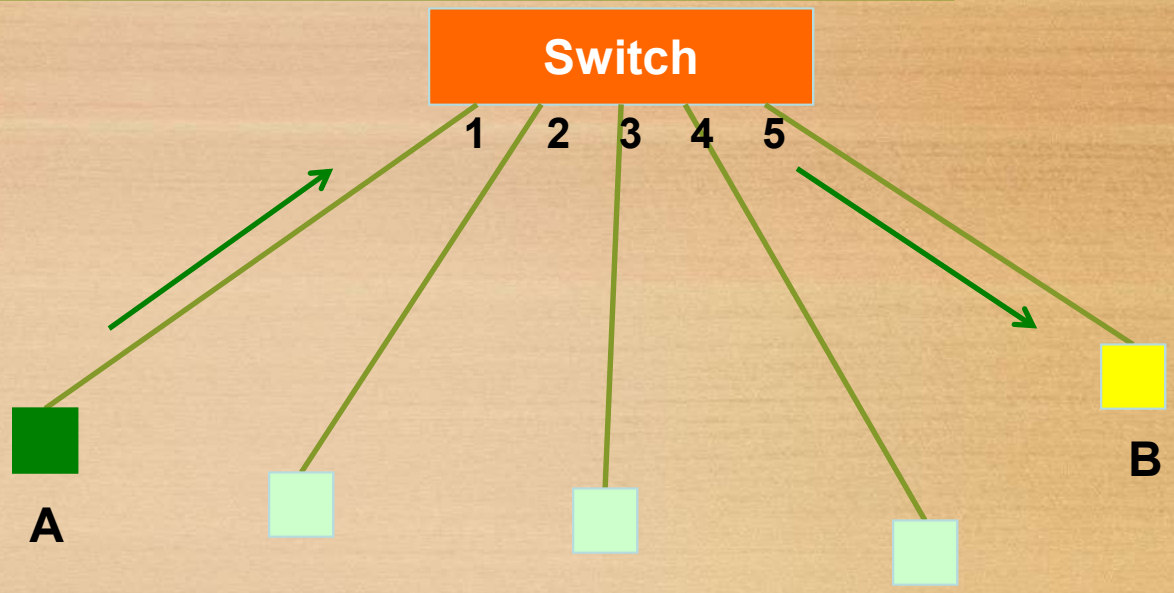
Unmanaged/Intelligent switches

- Unmanaged – provides LAN's with all the benefits of switching
- Good for small networks
- Intelligent switches tracks and reports LAN performance statistics
- Have a database ASIC (application specific integrated circuit) on board to collect and store data which you view through a software interface

Switch

Forwarding Table

Address	Port
AAAAAAAAAAAA	1
BBBBBBBBBBBB	5

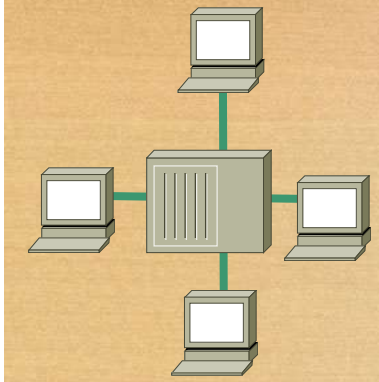
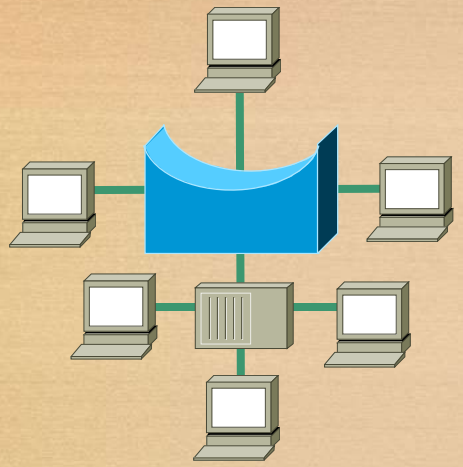
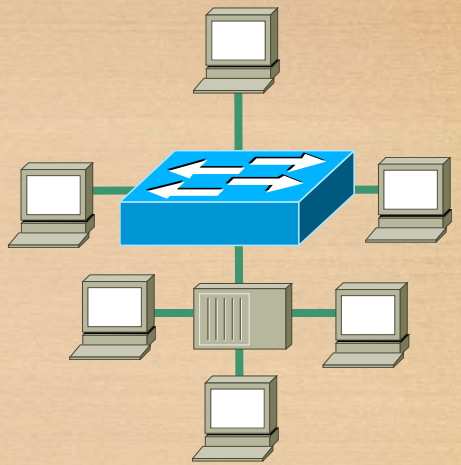
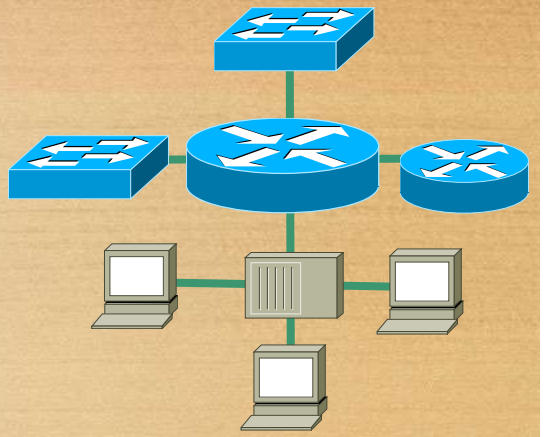


- A switch broadcasts some frames:
  - When the destination address is not found in the table
  - When the frame is destined to the **broadcast address** (FF:FF:FF:FF:FF:FF)
  - When the frame is destined to a **multicast** Ethernet address
- So, switches do not reduce the **broadcast domain**!

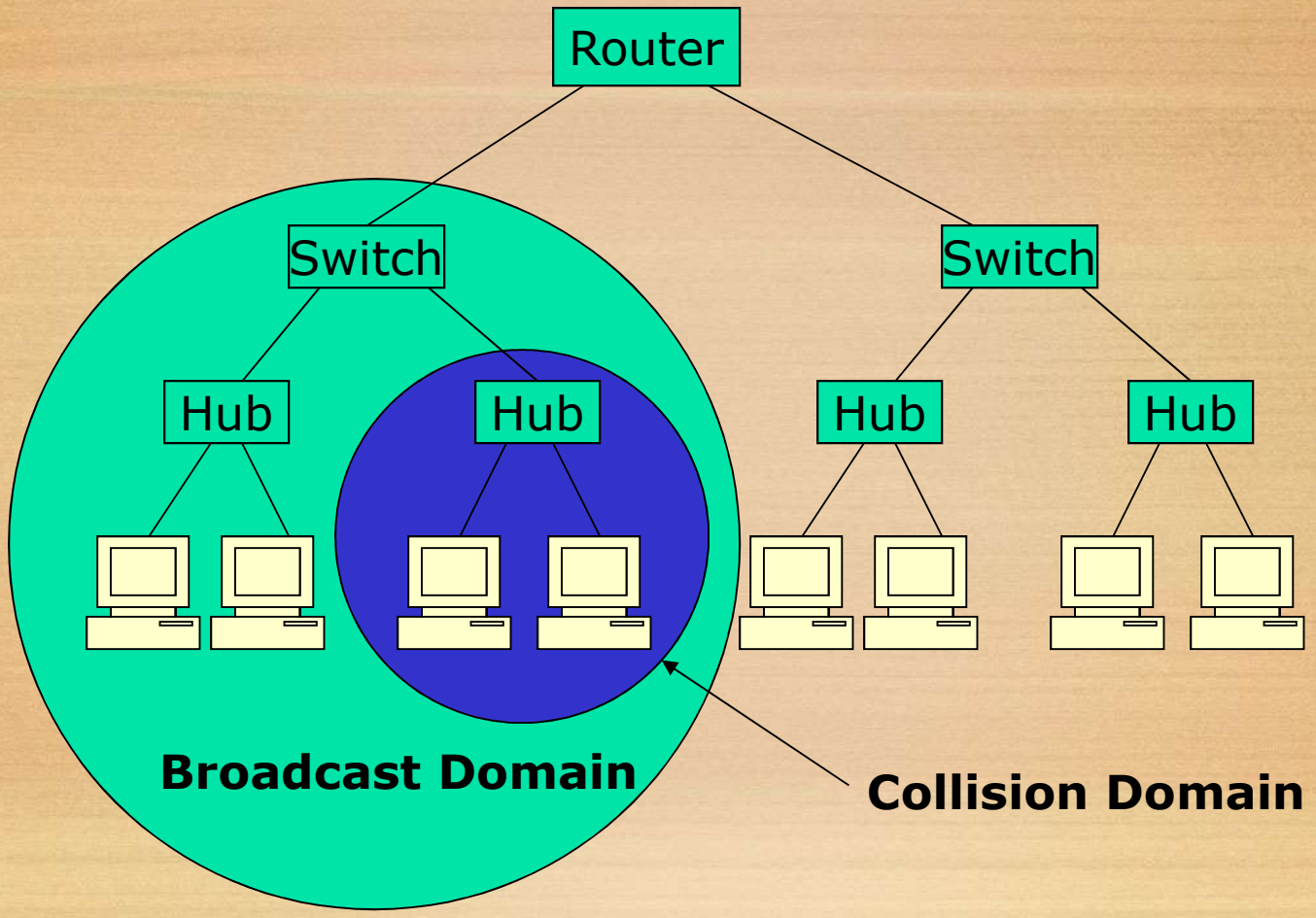
Switch vs. Router

- Routers more or less do with **IP packets** what switches do with **Ethernet frames**
  - A router looks at the IP packet destination and checks its ***routing table*** to decide where to forward the packet
- Some differences:
  - IP packets travel inside Ethernet frames
  - IP networks can be logically segmented into *subnets*
  - Switches do not usually know about IP, they only deal with Ethernet frames
- Routers do not forward Ethernet broadcasts. So:
  - **Switches reduce the collision domain**
  - **Routers reduce the broadcast domain**
- This becomes really important when trying to **design** hierarchical, scalable networks that can grow sustainably

Network Device Domains

Hub	Bridge	Switch	Router
			
Collision Domains:			
1	4	4	4
Broadcast Domains:			
1	1	1	4

Traffic Domains



Traffic Domains

- Try to eliminate collision domains
  - Get rid of hubs!
- Try to keep your broadcast domain limited to no more than 250 simultaneously connected hosts
  - Segment your network using routers

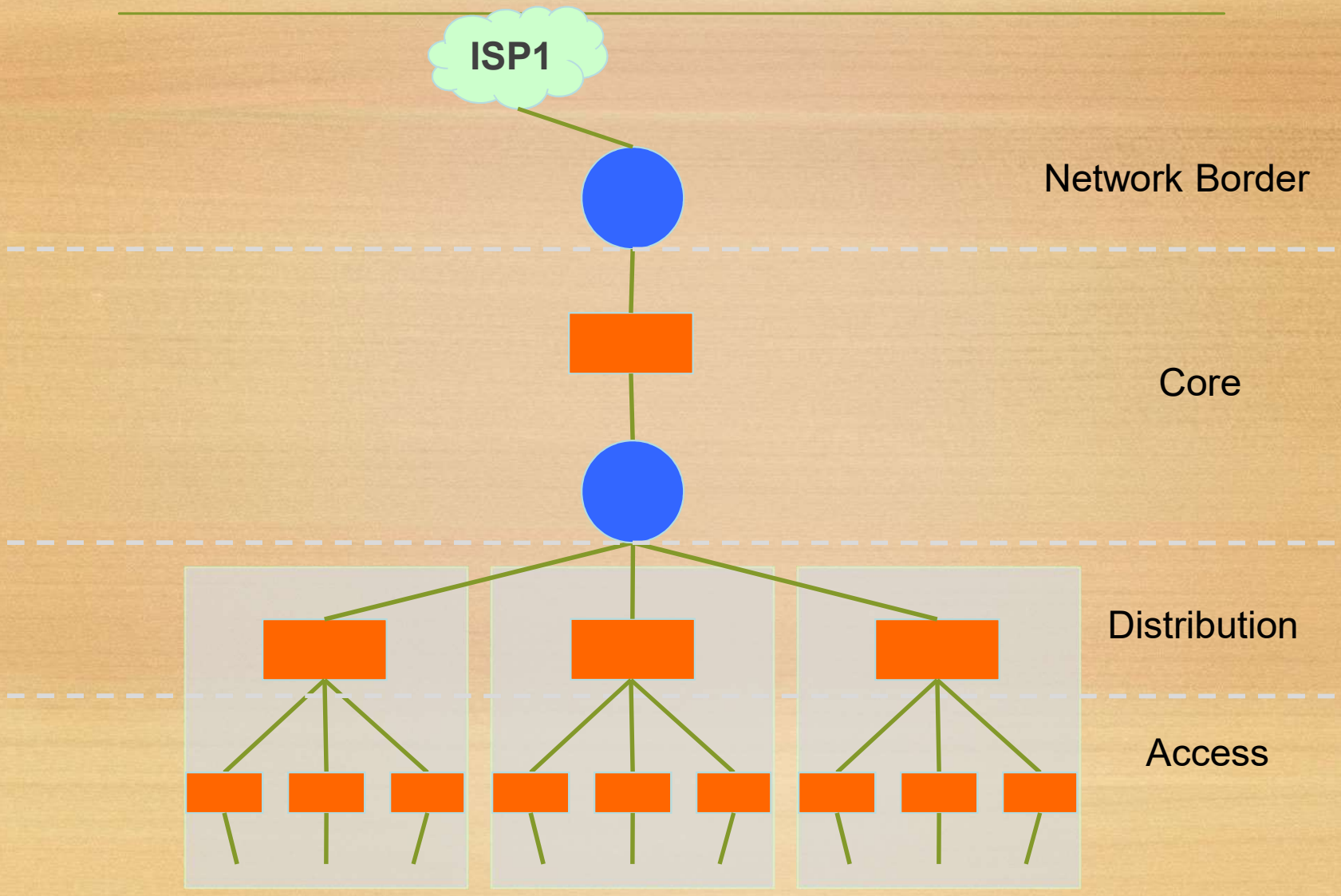
Layer 3 switch

- By definition a **switch filters** or forwards frames based on MAC addresses. This makes a switch a layer 2 device.
- Now we have **layer 3 switches** which have **routing** capability. If a data frame can't be switched it is routed.
- Each port is a separate LAN port, but the forwarding engine actually calculates and stores routes based on IP addresses, not MAC addresses
- Usually support **only IP**

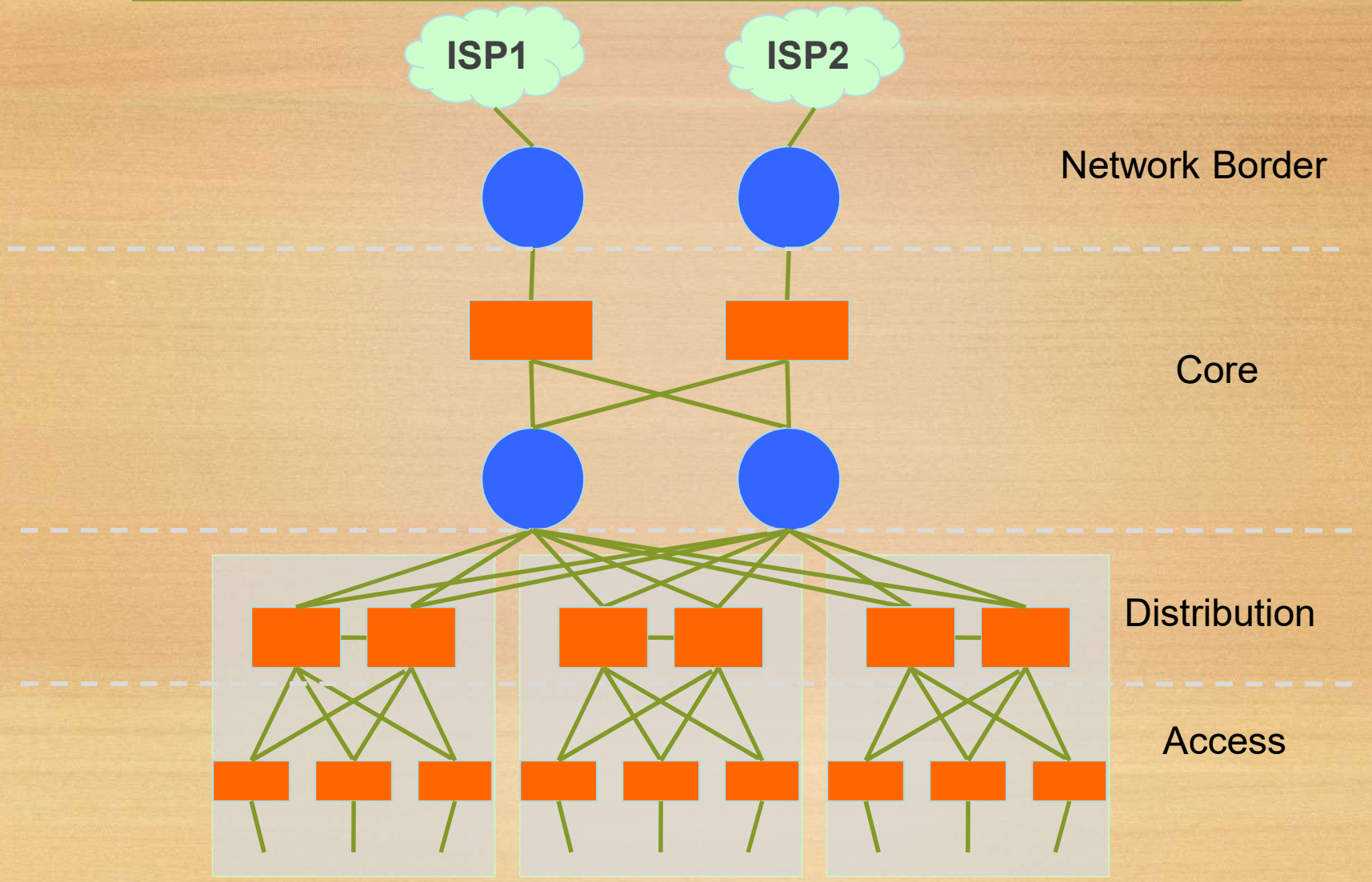
Campus Network Design - Review

- 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

Campus Network Design - Simple



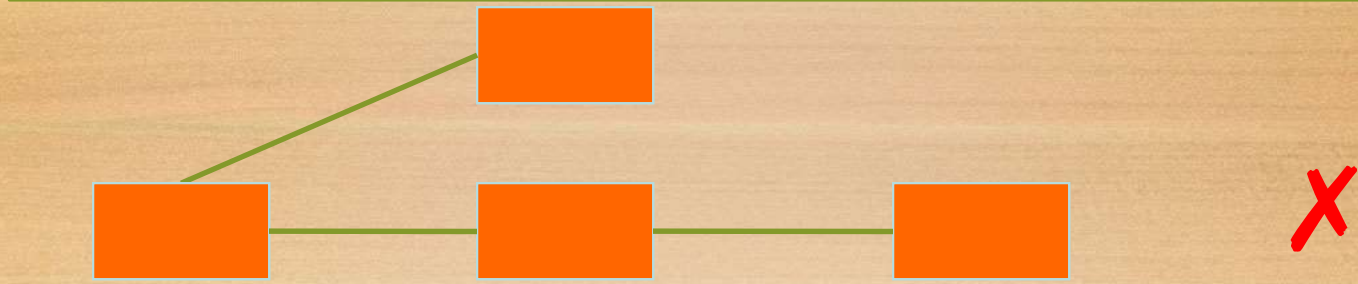
Campus Network Design - Redundant



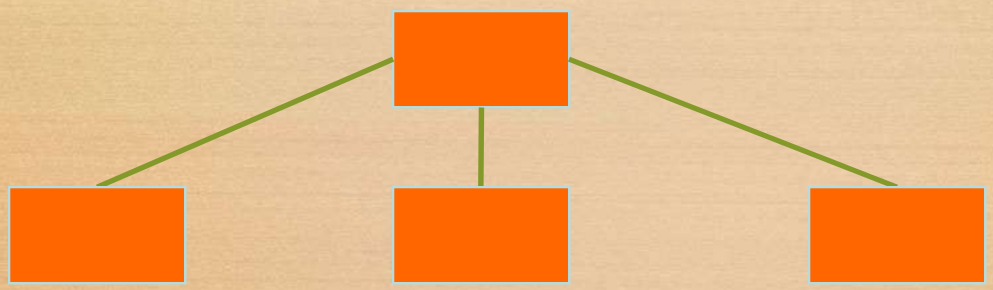
Layer 2 Network Design Guidelines

- 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



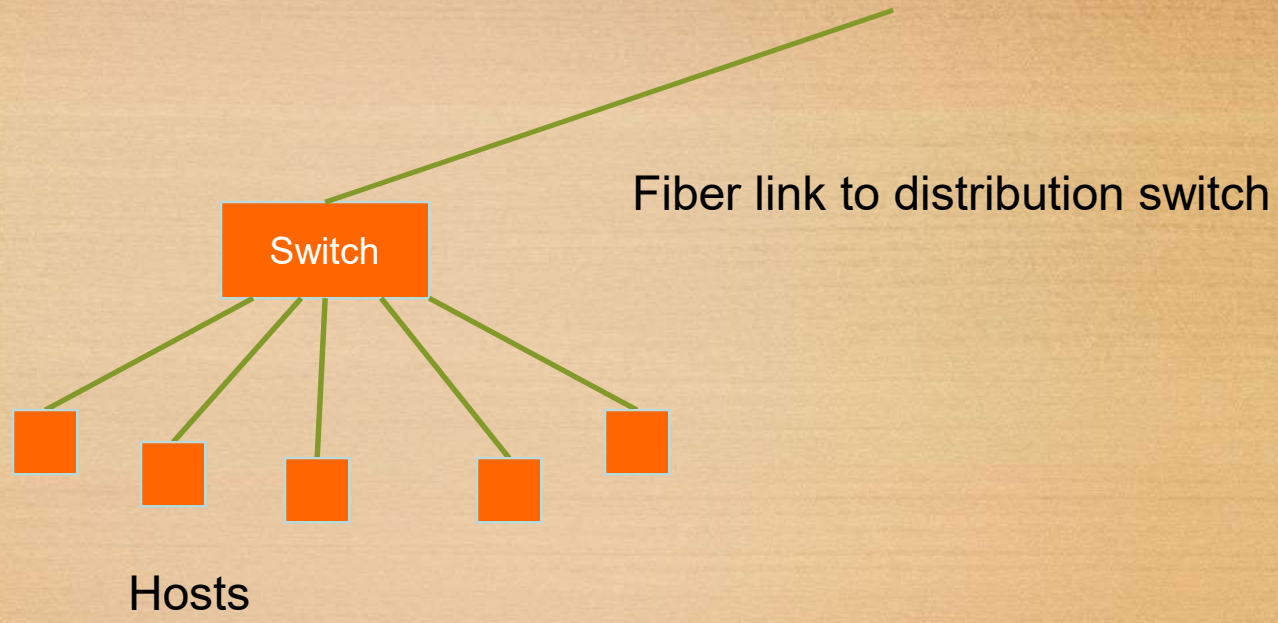
✗



✓

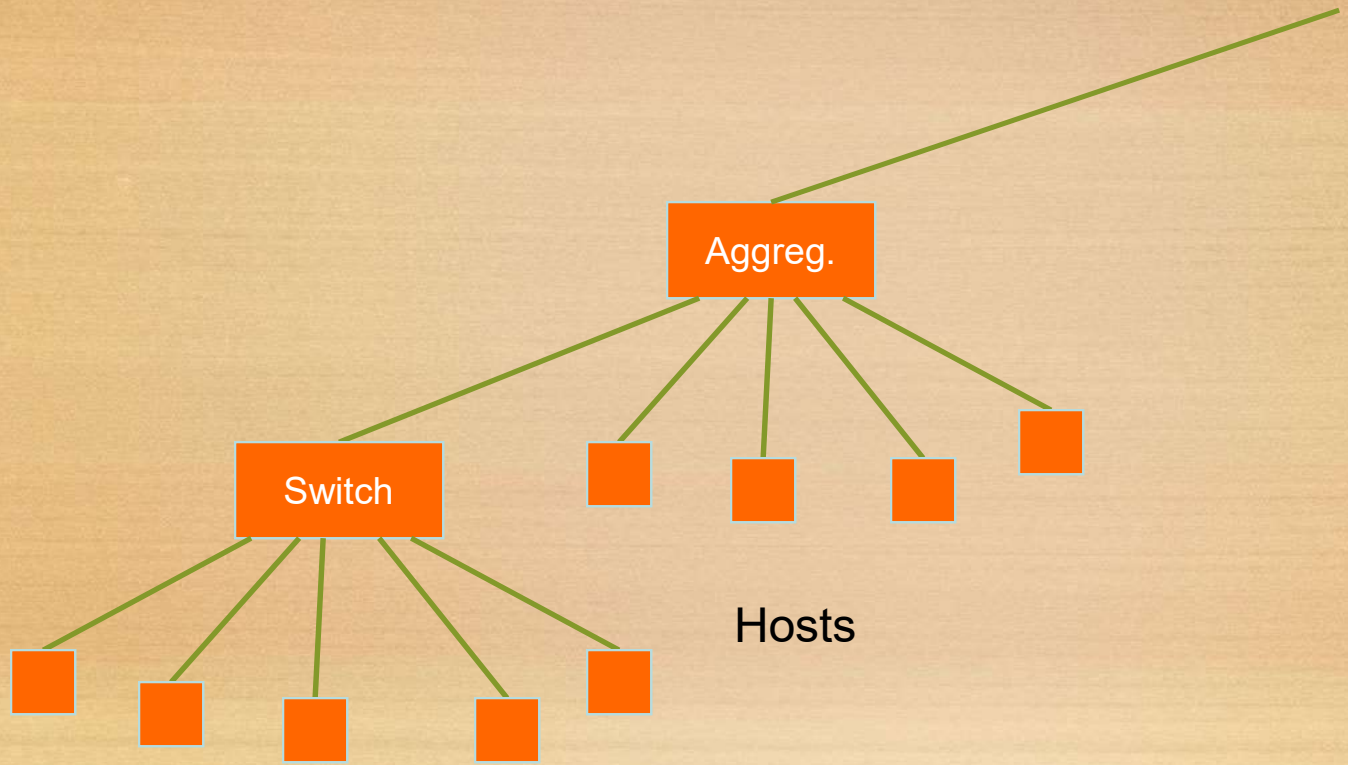
Build Incrementally

- Start small



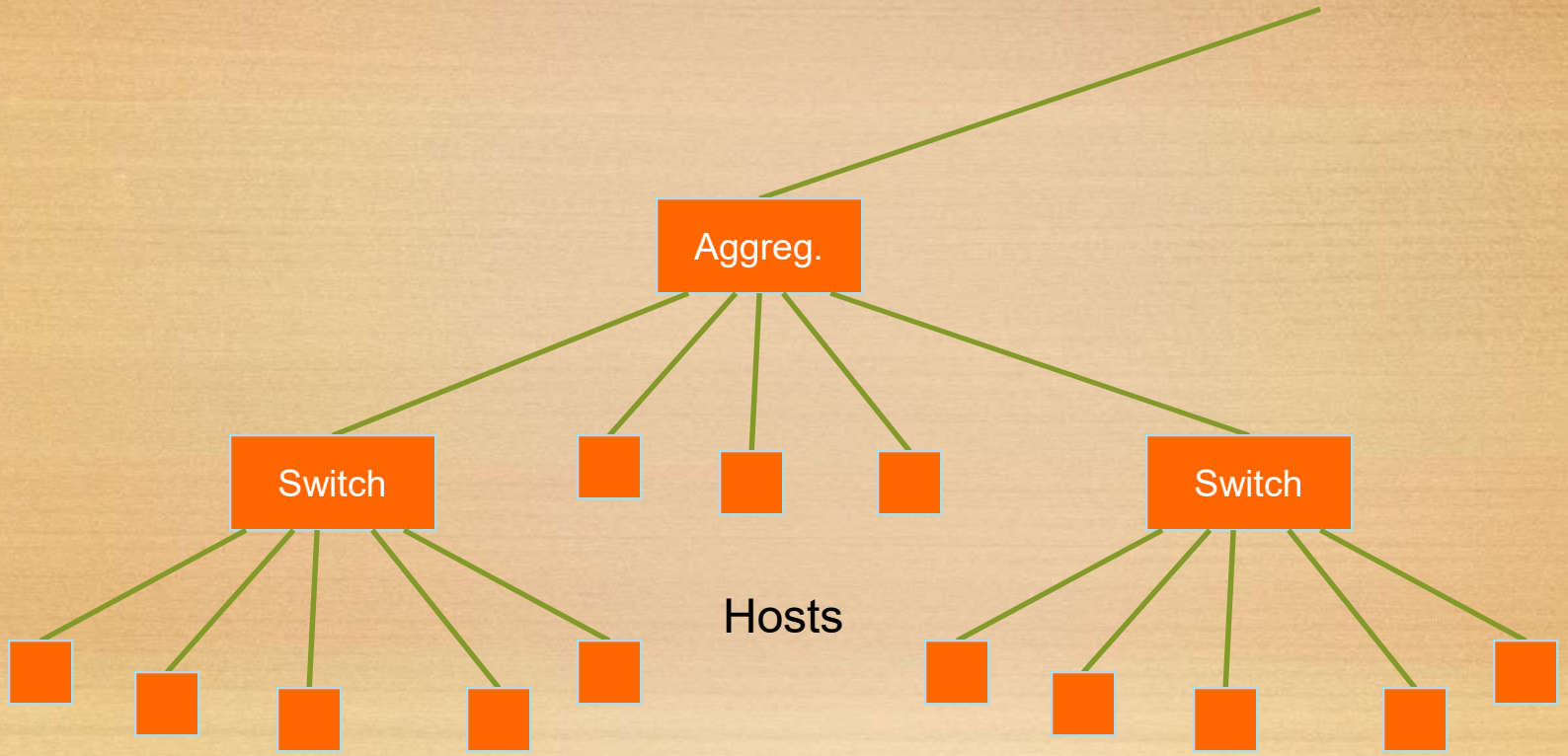
Build Incrementally

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



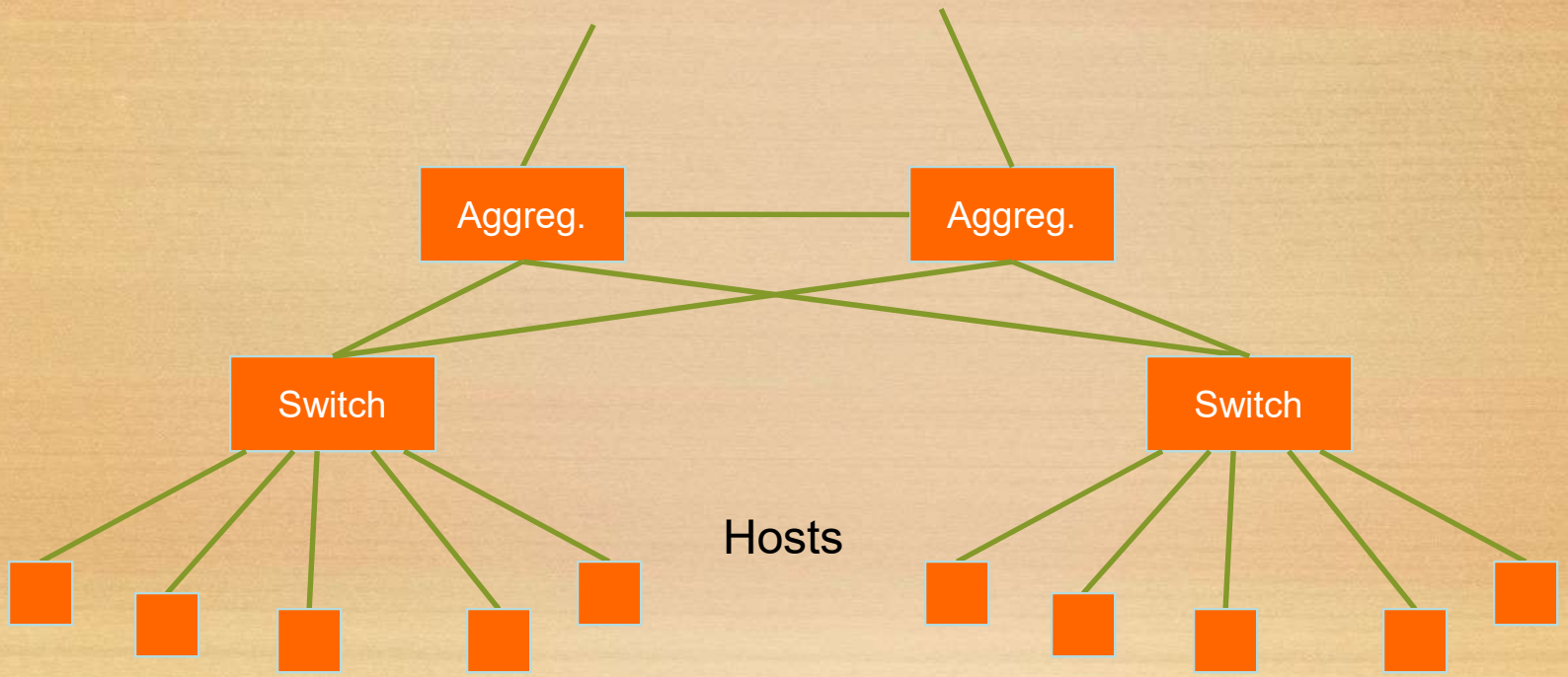
Build Incrementally

- And keep growing within the same hierarchy:



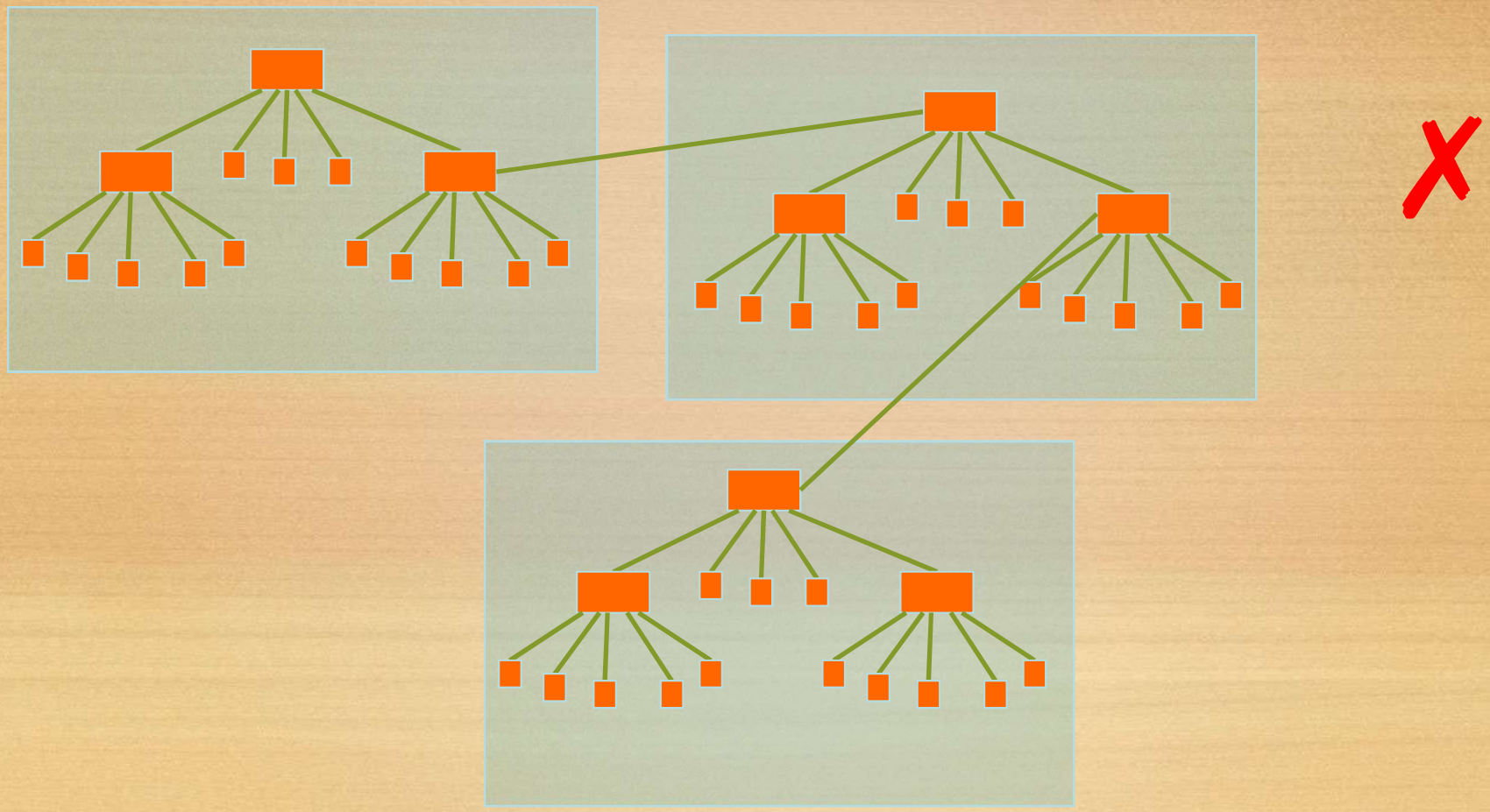
Build Incrementally

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

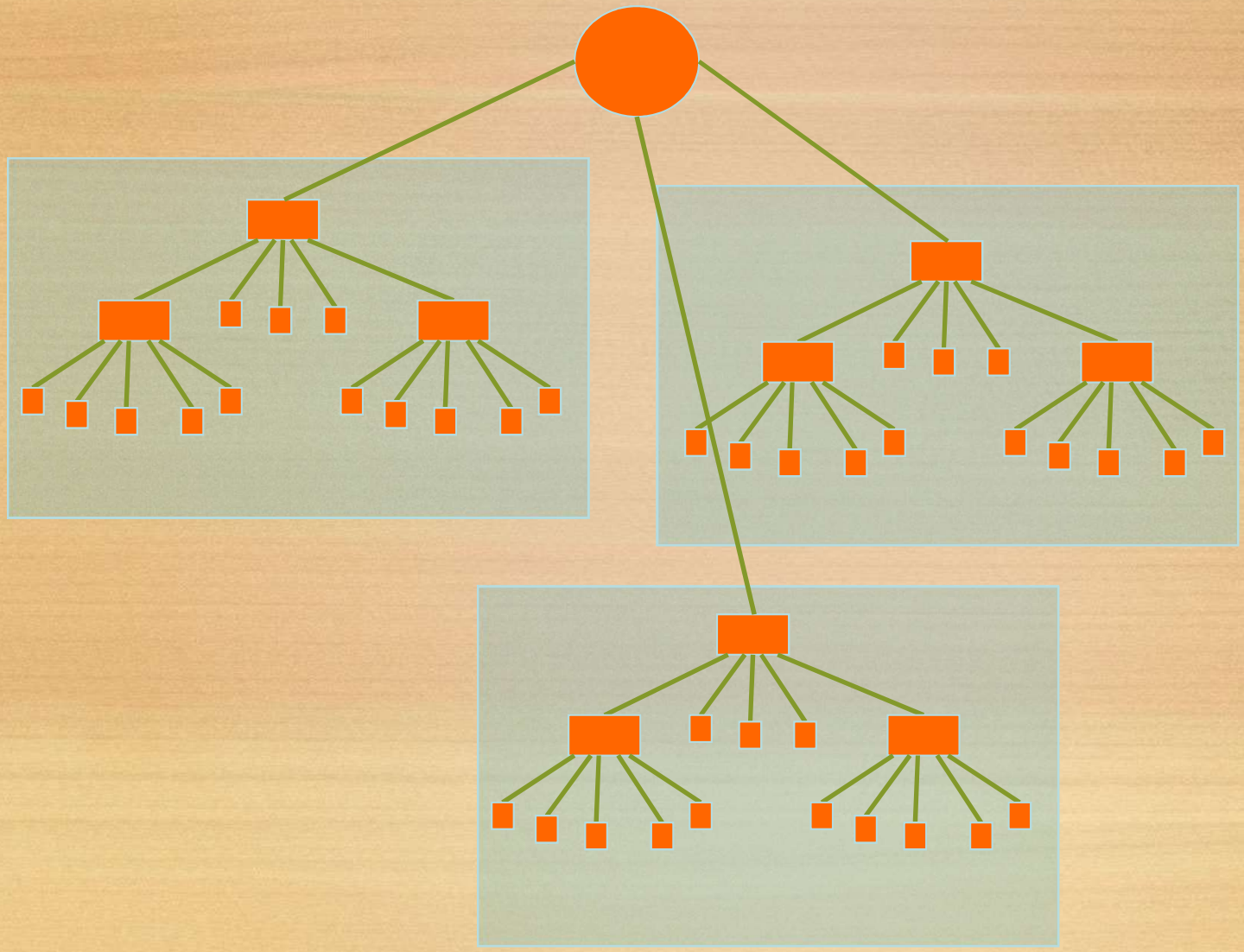


Do not daisy-chain

- Resist the temptation of doing this:



Connect buildings hierarchically



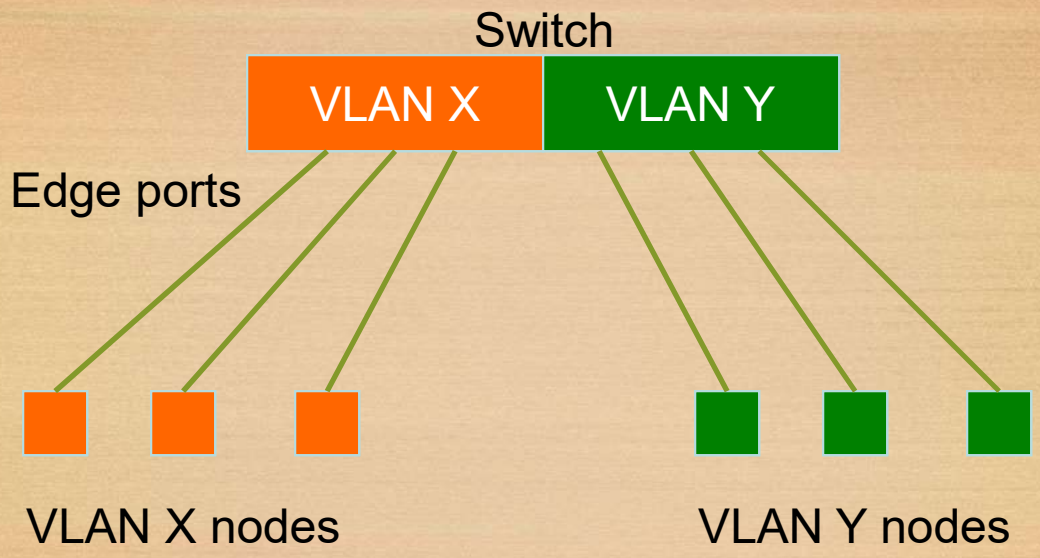
Virtual LANs (VLANs)

- 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**

Local VLANs

- Two VLANs or more within a single switch
- ***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

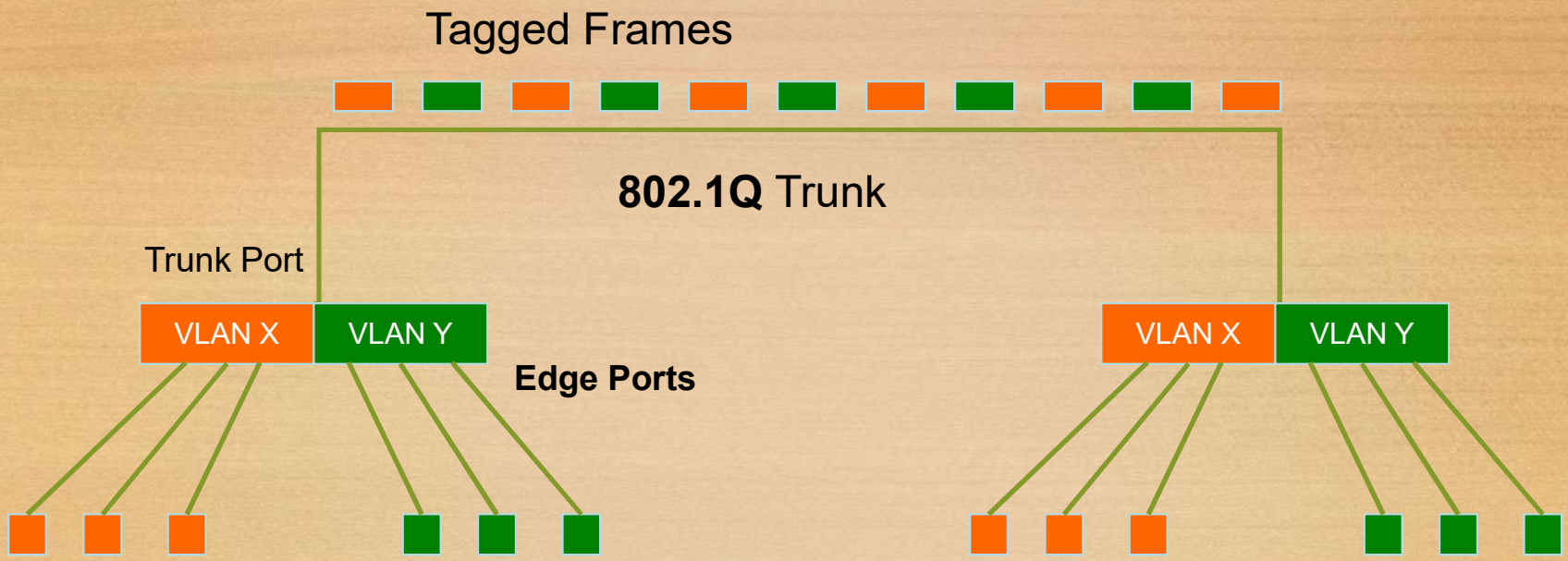
Local VLANs



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



This is called “VLAN Trunking”

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 VLAN data

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

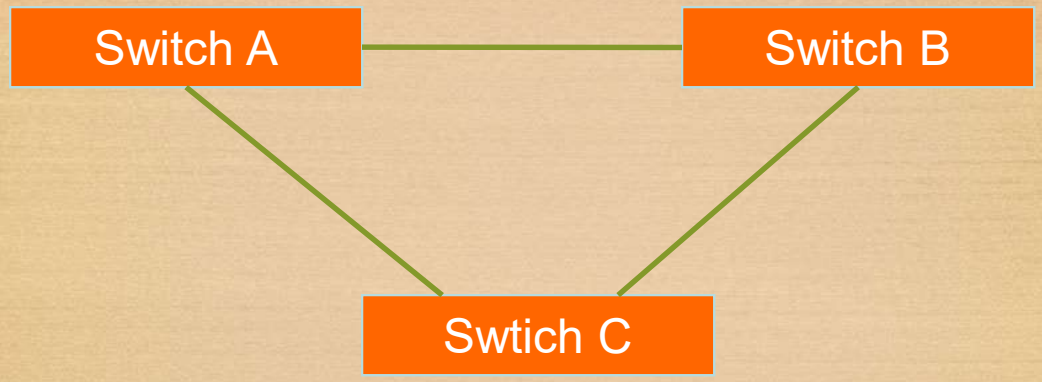
- You want to segment your network into multiple subnets, but can't buy enough switches
  - Hide sensitive infrastructure like IP phones, building controls, etc.
- Separate control traffic from user traffic
  - Restrict who can access your switch management address

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

Switching Loop

- When there is more than one path between two switches

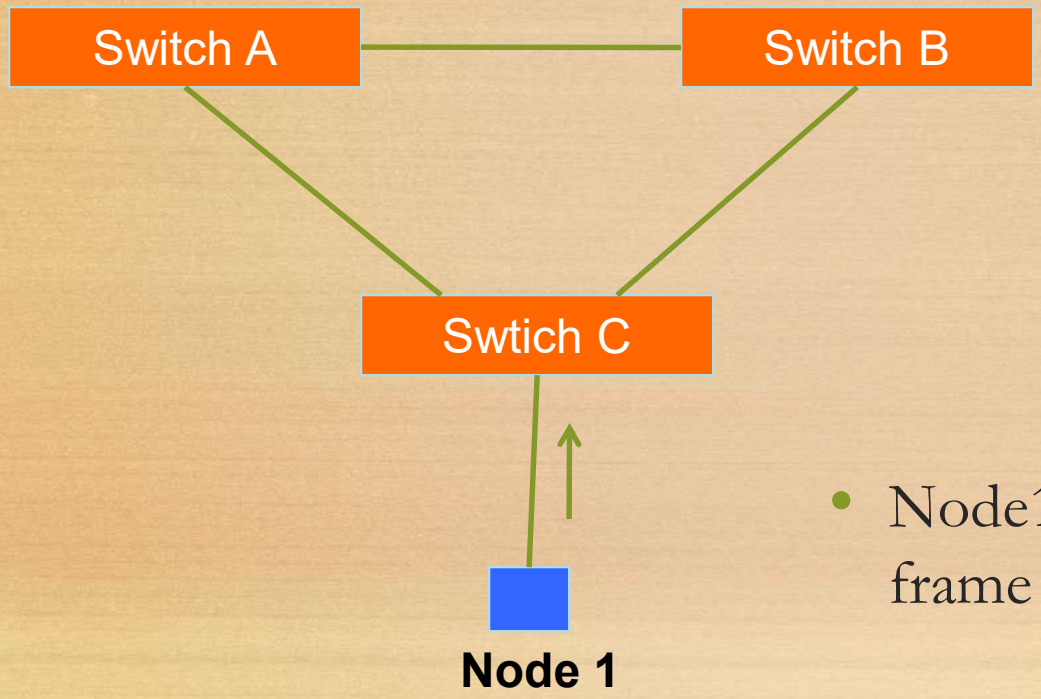


- What are the potential problems?

Switching Loop

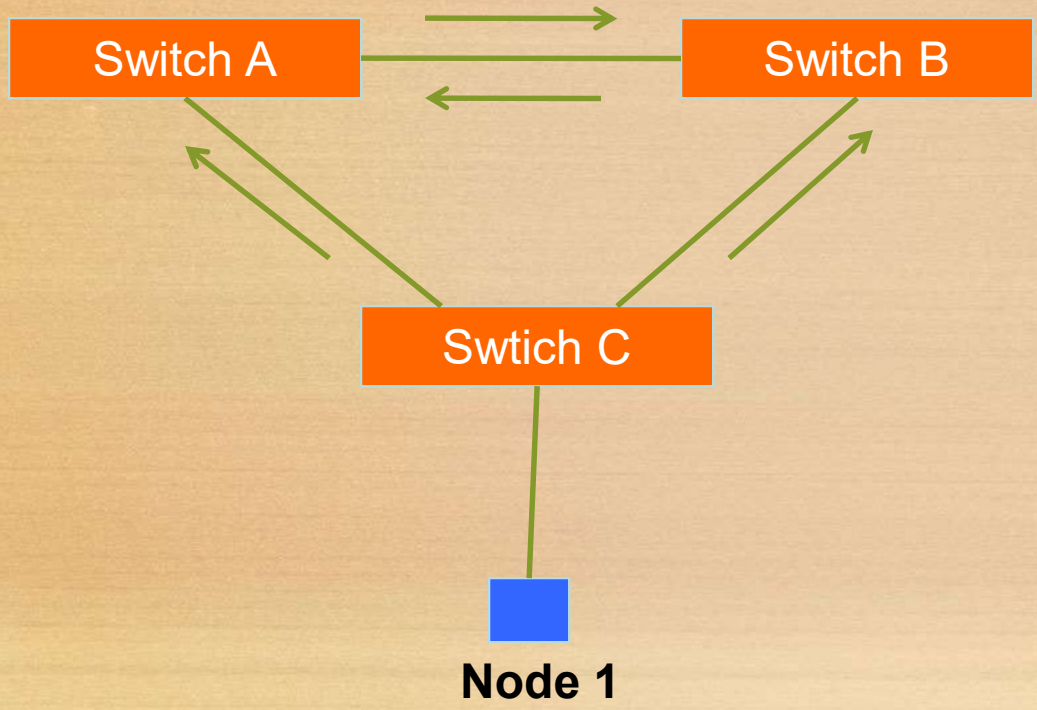
- If there is more than one path between two switches:
  - Forwarding tables become **unstable**
    - **Source MAC addresses** are repeatedly seen coming from different ports
  - Switches will **broadcast** each other's broadcasts
    - All **available bandwidth** is utilized
    - Switch processors cannot handle the **load**

Switching Loop



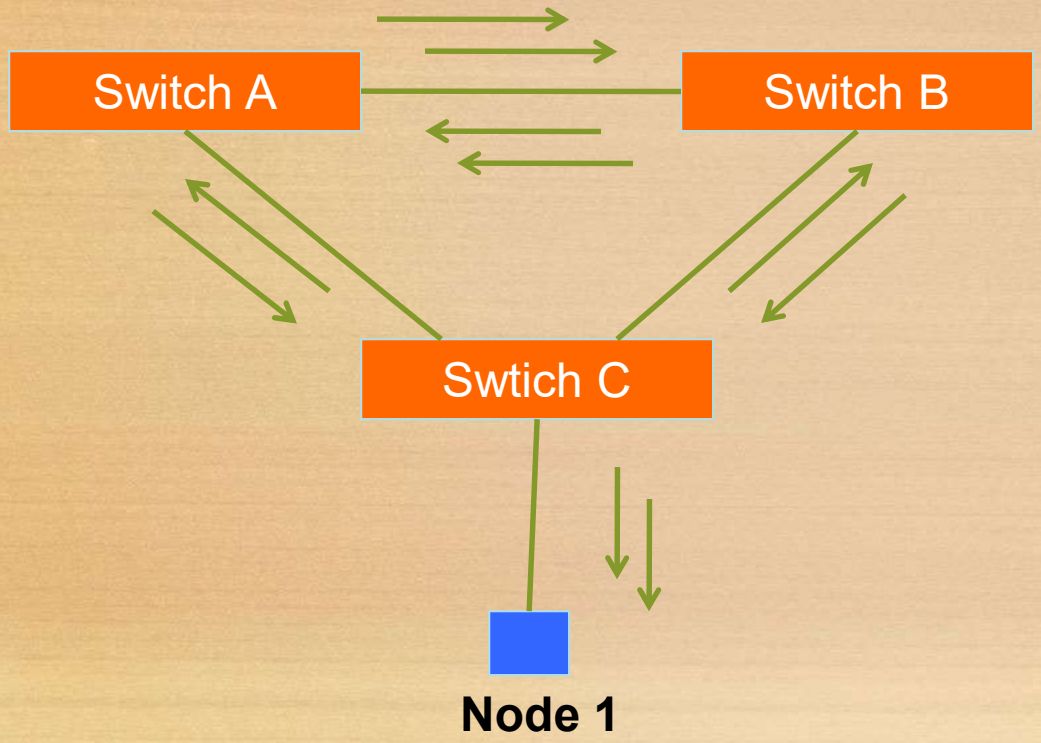
- Node1 sends a broadcast frame (e.g. an ARP request)

Switching Loop



- Switches A, B and C broadcast node 1's frame out every port

Switching Loop

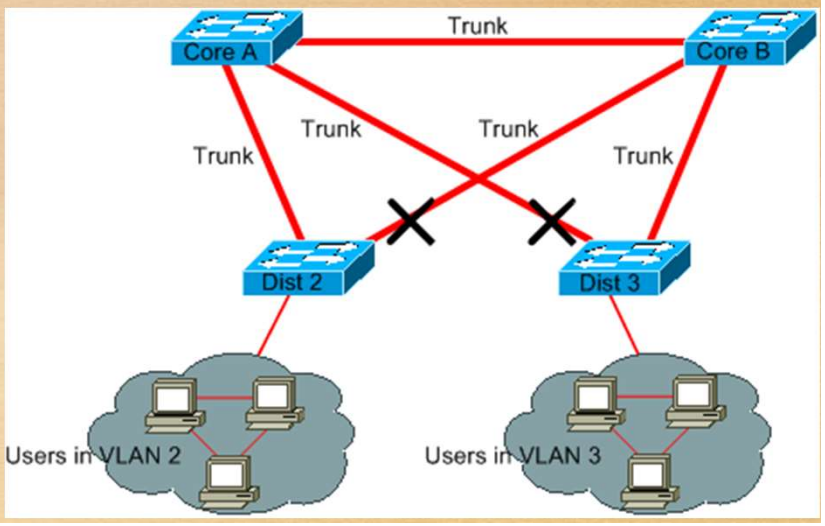


- But they receive each other's broadcasts, which they need to forward again out every port!
- The broadcasts are amplified, creating a **broadcast storm !!**

Good Switching Loops

- But you can take **advantage** of loops!
  - Redundant paths improve resilience when:
    - A switch fails
    - Wiring breaks
- How to achieve redundancy without creating dangerous traffic loops?

  ➔ **Spanning Tree Algorithm**



End of Lecture

Any Questions?