Lecture 8: Backbone Networks

Acknowledgement: Materials presented in this lecture are predominantly based on slides from:

- *Business Data Communications and Networking,* J. Fitzgerald, A. Dennis, 11th ed., 2013, John Wiley & Sons, Chapter 7
- *Computer Networking: A Top Down Approach,* J. Kurose, K. Ross, 7th ed., 2017, Addison-Wesley, Chapter 5

Backbone Networks Overview

- Components of Backbone Networks
  - Switches, Routers/Gateways
- Backbone network architectures
  - Backbone layers
  - Switched and routed backbone
- Virtual LANs (VLANs)
  - IEEE 802.1Q VLAN standard. Tagging.
  - How the VLAN works.

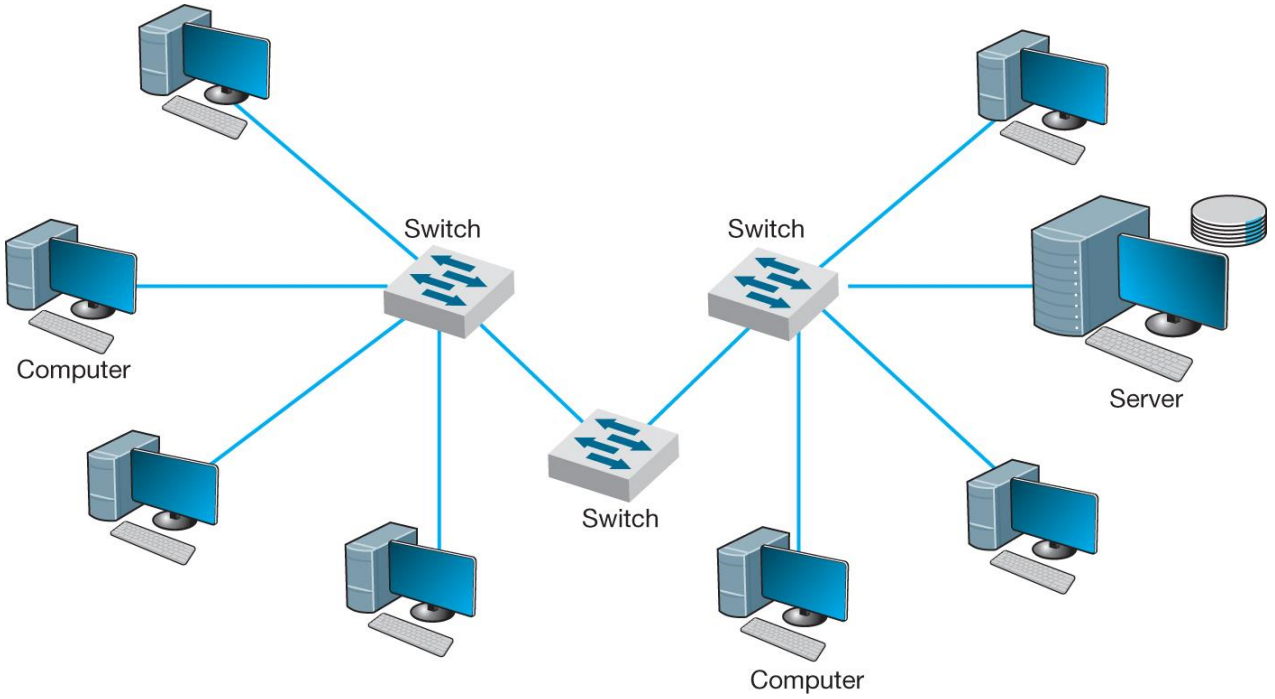
Backbone Networks

- Backbone networks link together variety of network components
- BNs can link LANs in building, between building, campuses/enterprises,
  - Making information transfer possible between departments
  - Use high speed circuits to connect LANs
  - Provide connections to other backbones, Metropolitan and Wide Area Networks (MANs, WANs) and the Internet
- Sometimes referred to as
  - An enterprise network
  - A campus-wide network

Backbone Network Components

- Network cable
  - Functions in the same way as in LANs
  - Optical fiber - more commonly chosen because it provides higher data rates
- Hardware devices
  - Computers or special purpose devices used for interconnecting networks:
    - Switches
    - Routers
    - Gateways

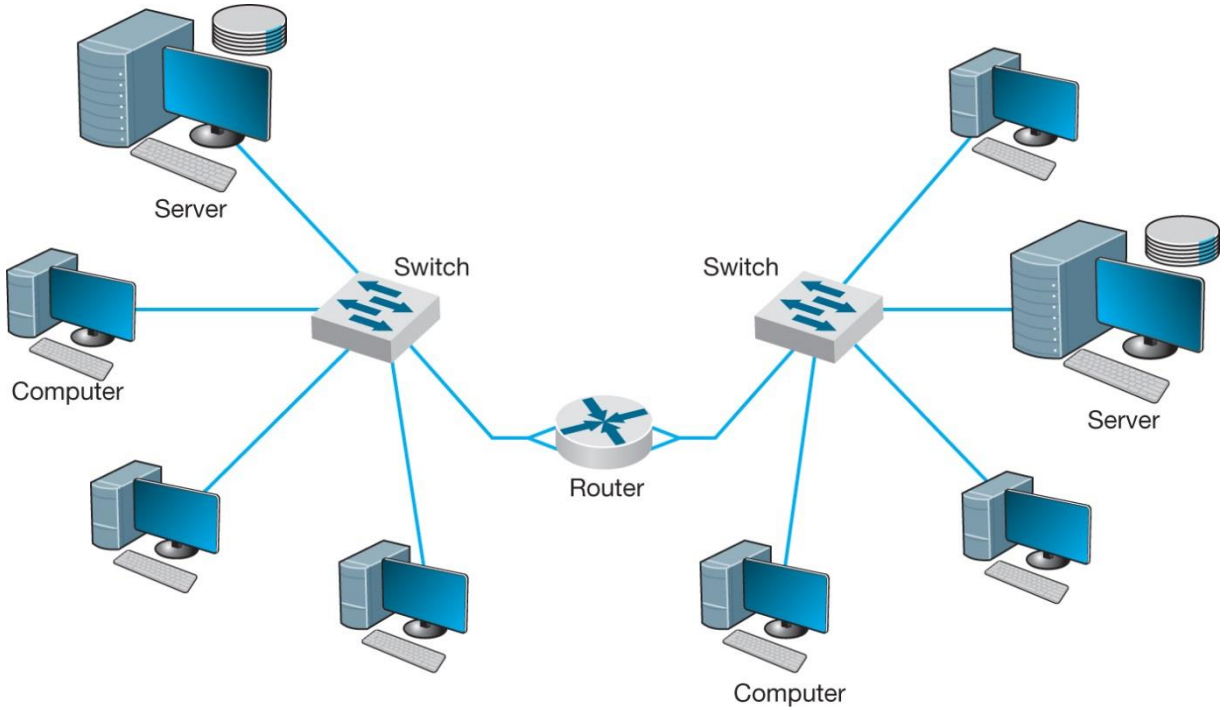
Switches



- Switches operate at the data link layer – layer-2 switches
- Backbone switches are the same as LAN switches

- They connect two or more network segments that use the same data link (e.g. Ethernet) and network protocol (e.g. IP)
- They may connect the same or different types of cable (e.g. fibre optics and UTP cables)
- Switches use the data link layer address to forward packets between network segments

Routers (1)



- Operate at the network layer: layer-3 devices

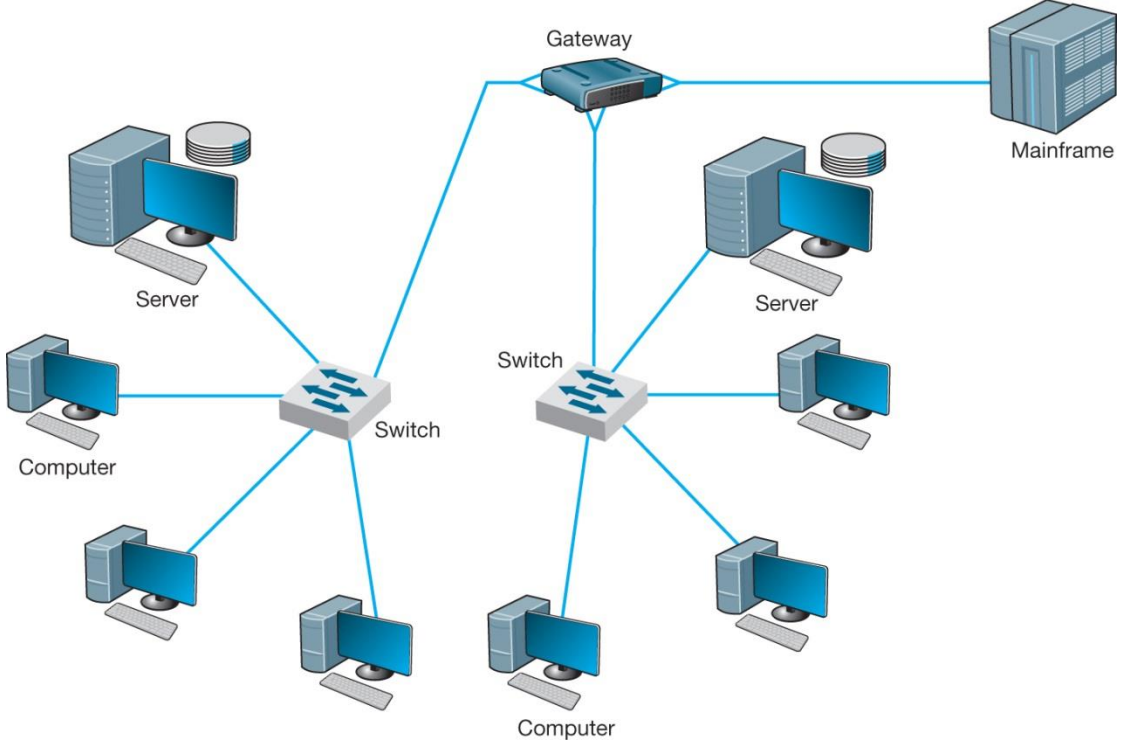
- A router examines the destination address of the network layer
- Strips off the data link layer packet
- Chooses the “best” route for a packet (via routing tables)
- Adds the new data link layer packet
- Forwards only those messages that need to go to other networks

Routers (2)

- Compared to Switches, Routers:
  - Perform more processing
  - Process only messages specifically addressed to it
  - Recognize that the message is specifically addressed to it before the message is passed to the network layer for processing
  - Builds the new data link layer packet for transmitted packets
- Routers create new data link layer frame but do not change the network layer packet (addresses).

Gateways

- A LAN router with DHCP
- Operate at network layer and use network layer addresses in processing



- Traditionally gateways were used to connect two or more networks that use the same or different data link and network protocols
- Some work at the application layer
- Process only those messages addressed to them
- Traditionally, gateways could translate one network layer protocol into another, translate data link layer protocols, and open sessions between application programs, thus overcoming both hardware and software incompatibilities.

Backbone Network (BN) Architectures

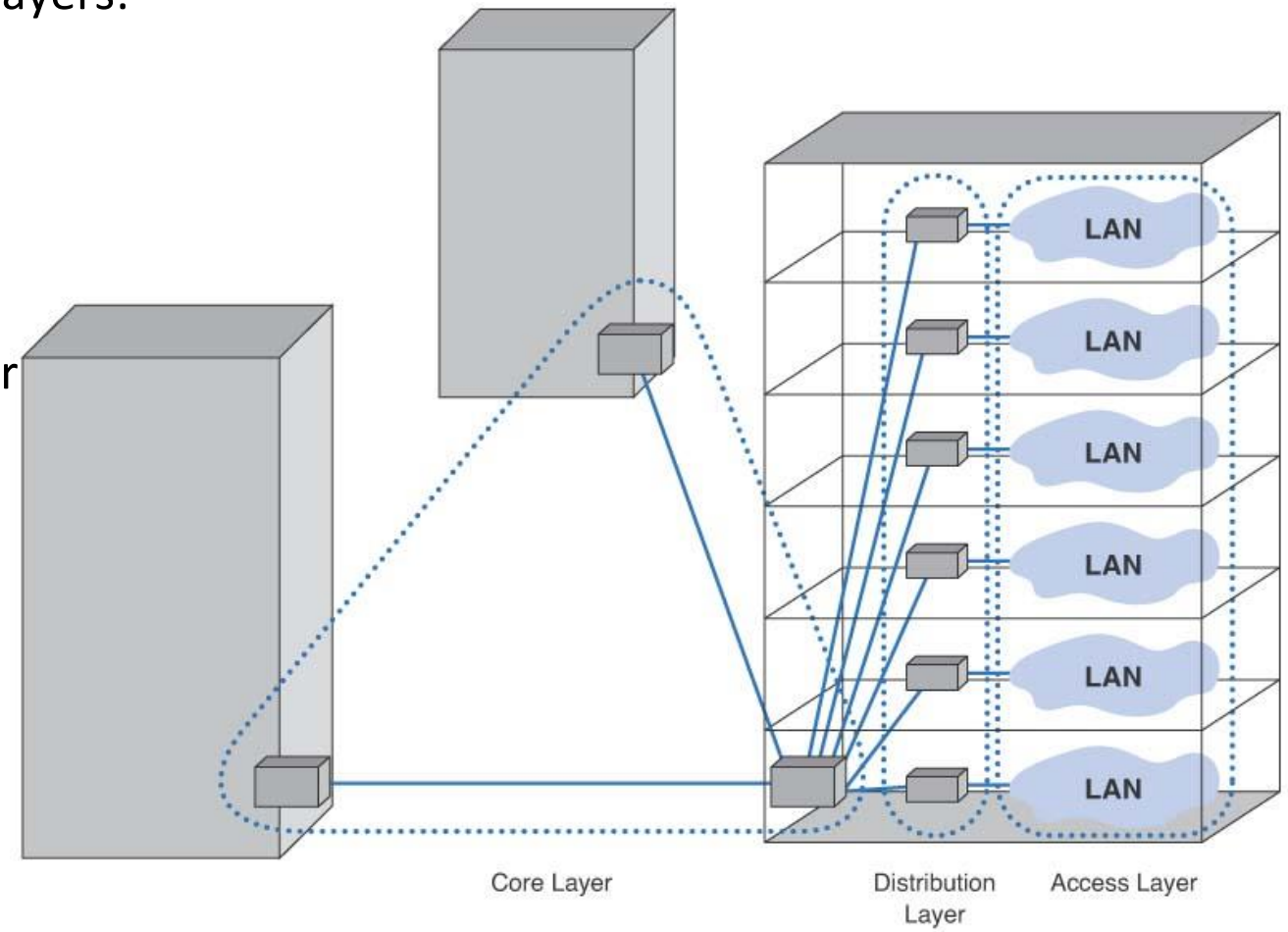
- The BN architecture describes:
  - the way in which the backbone interconnects the networks attached to it
  - how the packets from one network move through the backbone to other networks.
- Three fundamental architectures that can be combined in different ways:
  - routed backbones
  - switched backbones
  - virtual LANs (VLANs)
- These architectures are mixed and matched to build sets of BNs.

Backbone Network Design Layers

Network designers use the concepts of **technology layers**.
Three design/technology layers:

1. *Access layer:* used in LANs attached to BB (e.g. 100Base-T,)
2. *Distribution layer:* connects LANs together (e.g. switches and TCP/IP gateways)
3. *Core layer:* connects different backbone networks together in enterprise network

   (the WAN layer might be needed in big organizations)

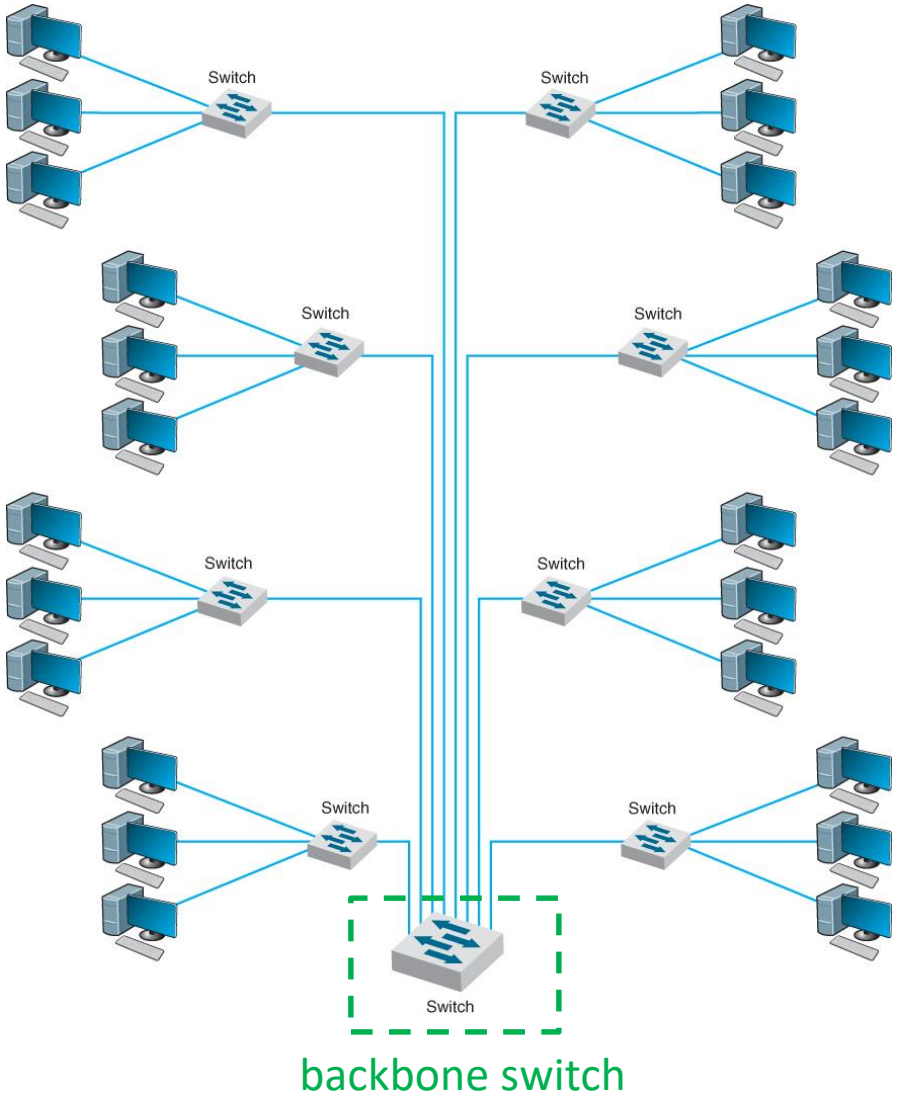


Fundamental Backbone Architectures

- ***Switched Backbones*:** most common type of backbone, used in distribution layer, used in new buildings, sometimes in core layer. Typically a rack/cabinet based.
- ***Routed Backbones*:** move packets along backbone on the basis of the network layer address. Sometimes called sub-netted backbone
- ***Virtual LANs*:** networks in which computers are assigned into LAN segments by software rather than by hardware; can be single switch or multi-switch VLANs. Very popular technology.

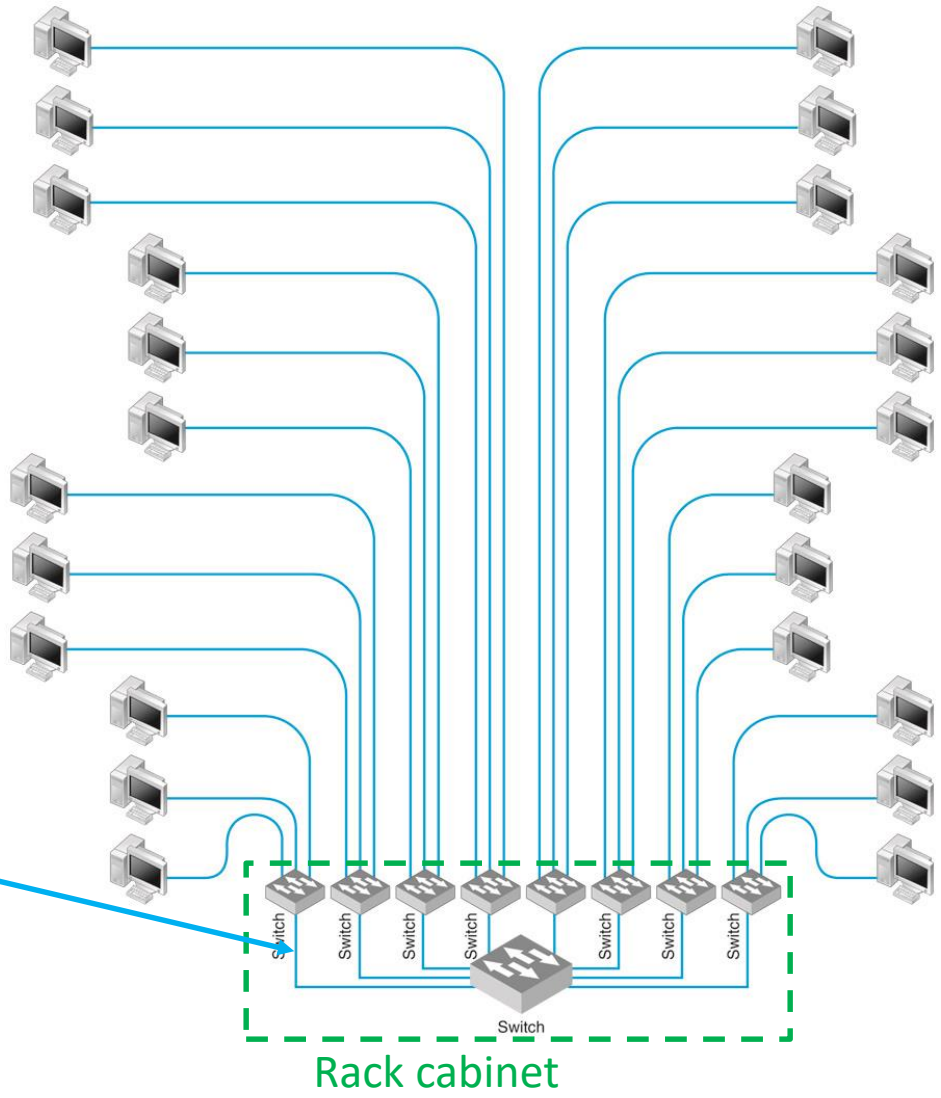
Switched Backbone

- Switches forming LANs (access layer) are connected to the backbone switch (distribution layer)
- Advantages:
  - High performance due to simultaneous access of switched operations
  - A simpler more easily managed network – less devices
  - What about the ARP broadcasting?

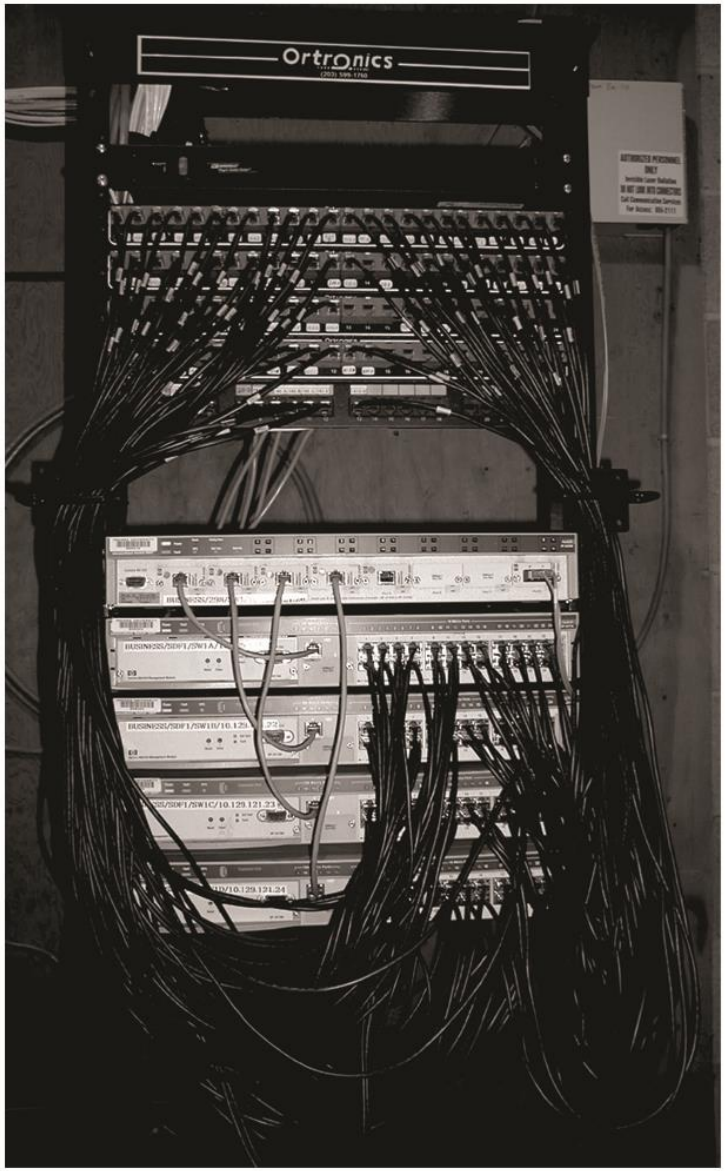


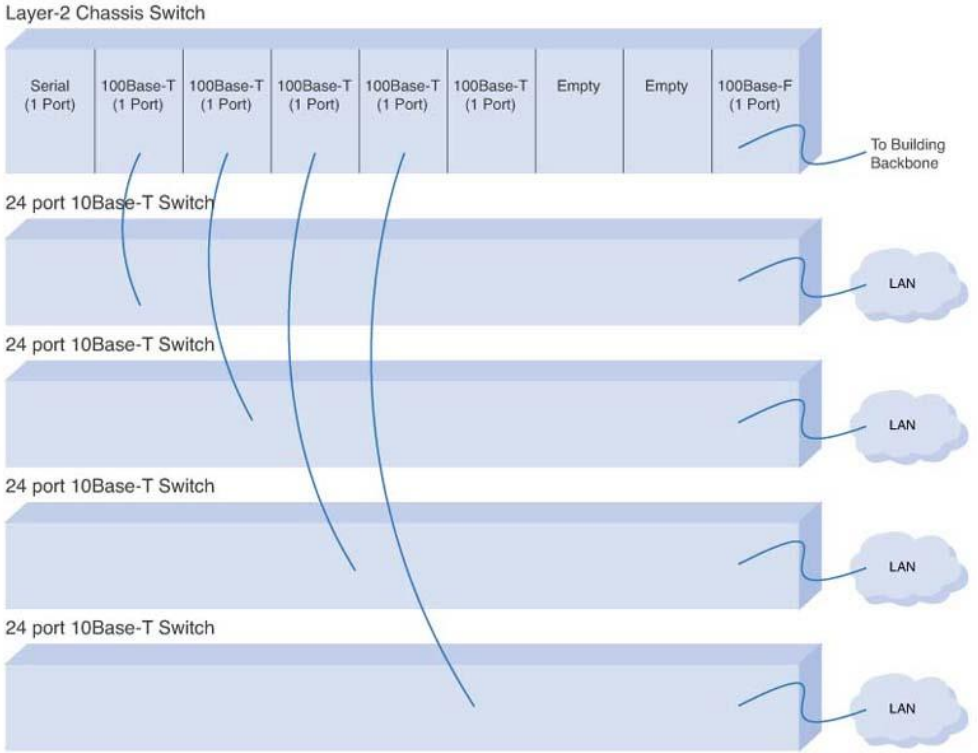
Rack-Mounted Switched Backbones

- Places all network switch equipment physically in one "rack" room/cabinet
  - Easy maintenance and upgrade
  - Requires more cable, but usually small part of overall cost
- Main/Central Distribution Facility (MDF, CDF)
  - Another name for the rack room
  - Place where many cables come together
  - Patch cables used to connect devices on the rack
- Easier to move computers among LANs



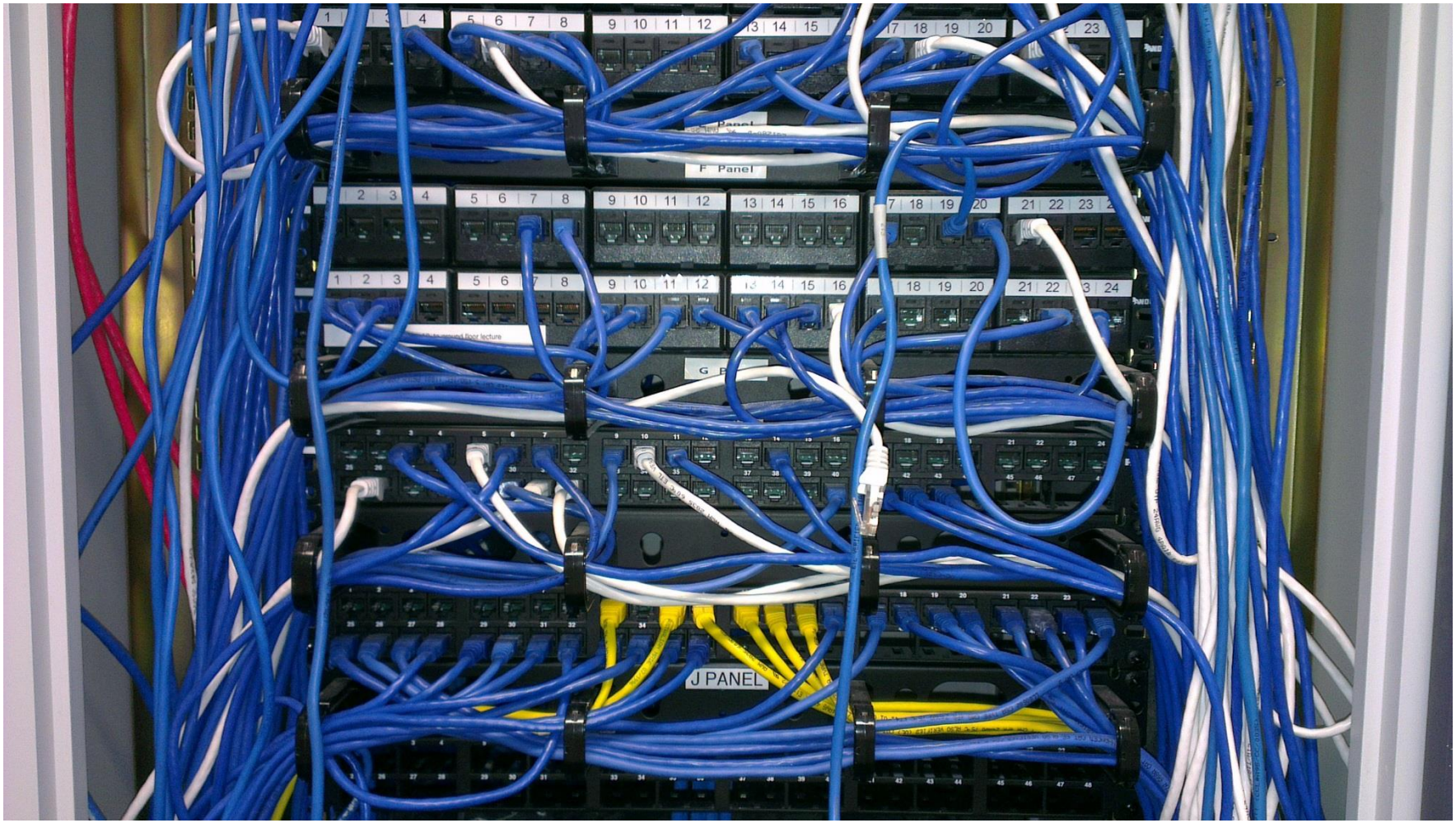
Main Distribution Facility (MDF) – Rack mounted equipment



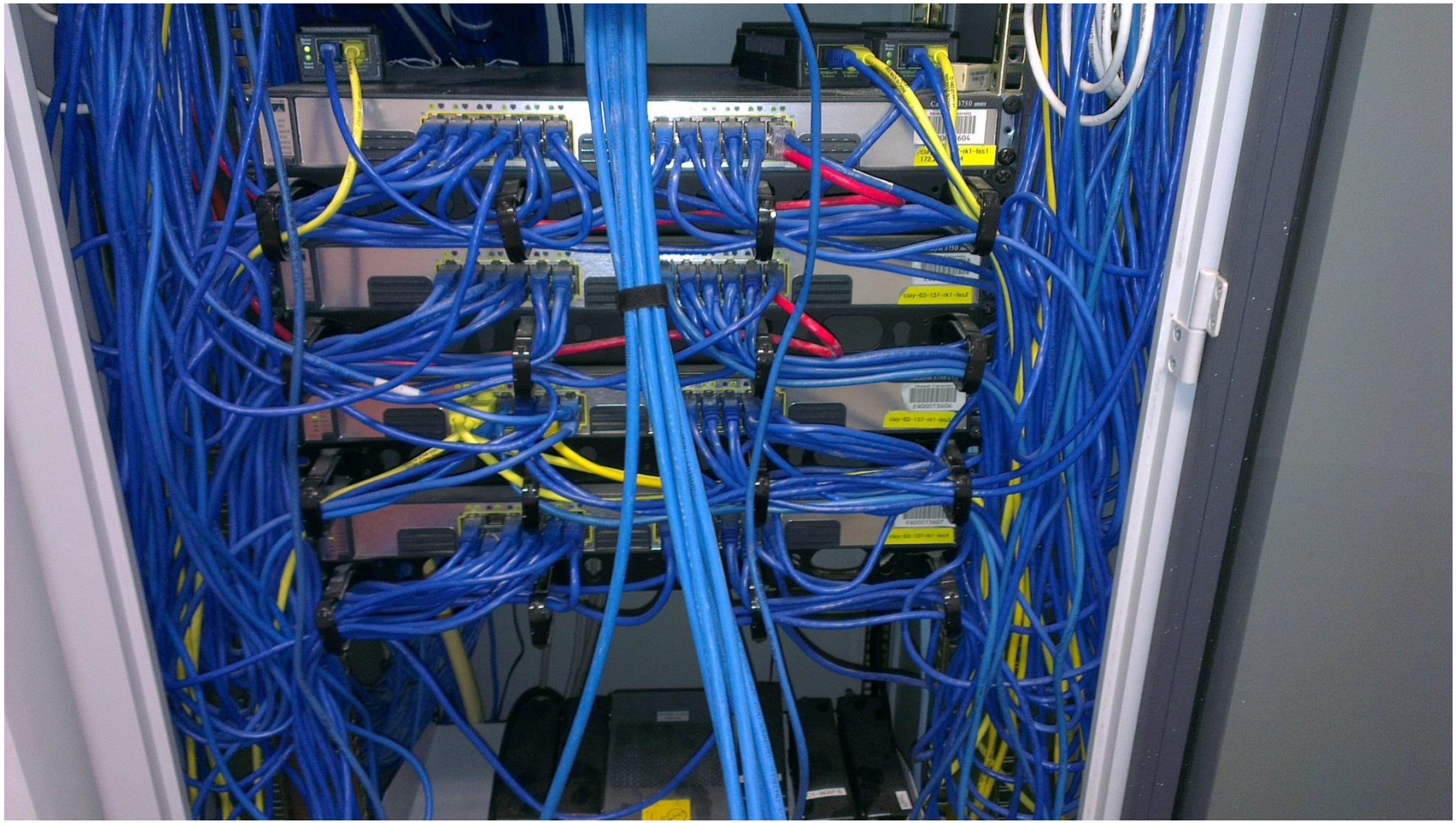


- Top: patch panel. The cables from each room are wired into the rear of the patch panel
- Four bottom panels: 24 port 100Base-T switches (the LAN switches -- the access layer)
- Centre: the Layer-2 chassis backbone switch (the distribution layer). There are four 100Base-T ports and one 1000Base-F switch that connects all the LANs over the fiber-optic cable to the building switch/router

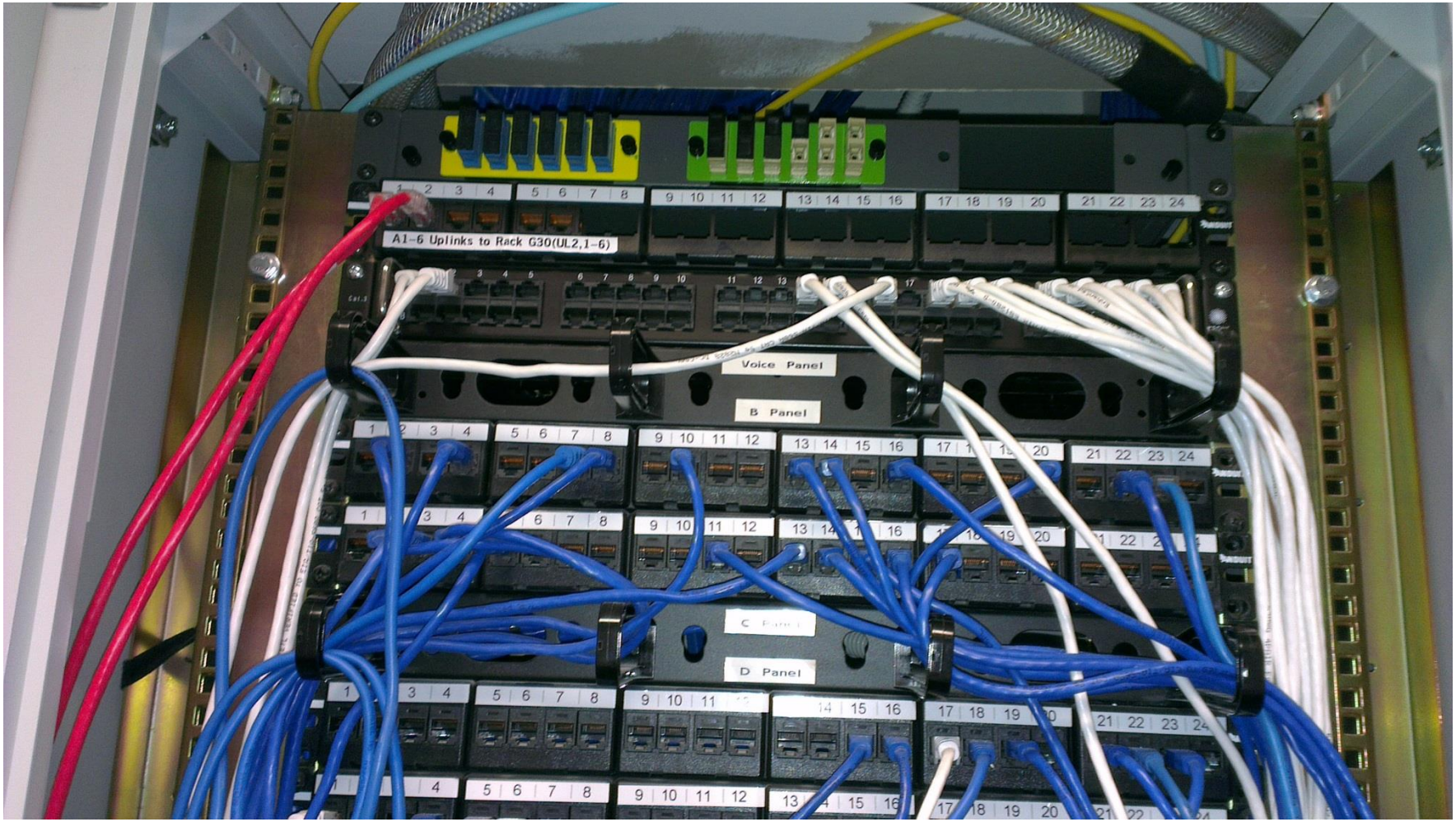
Another patch panel



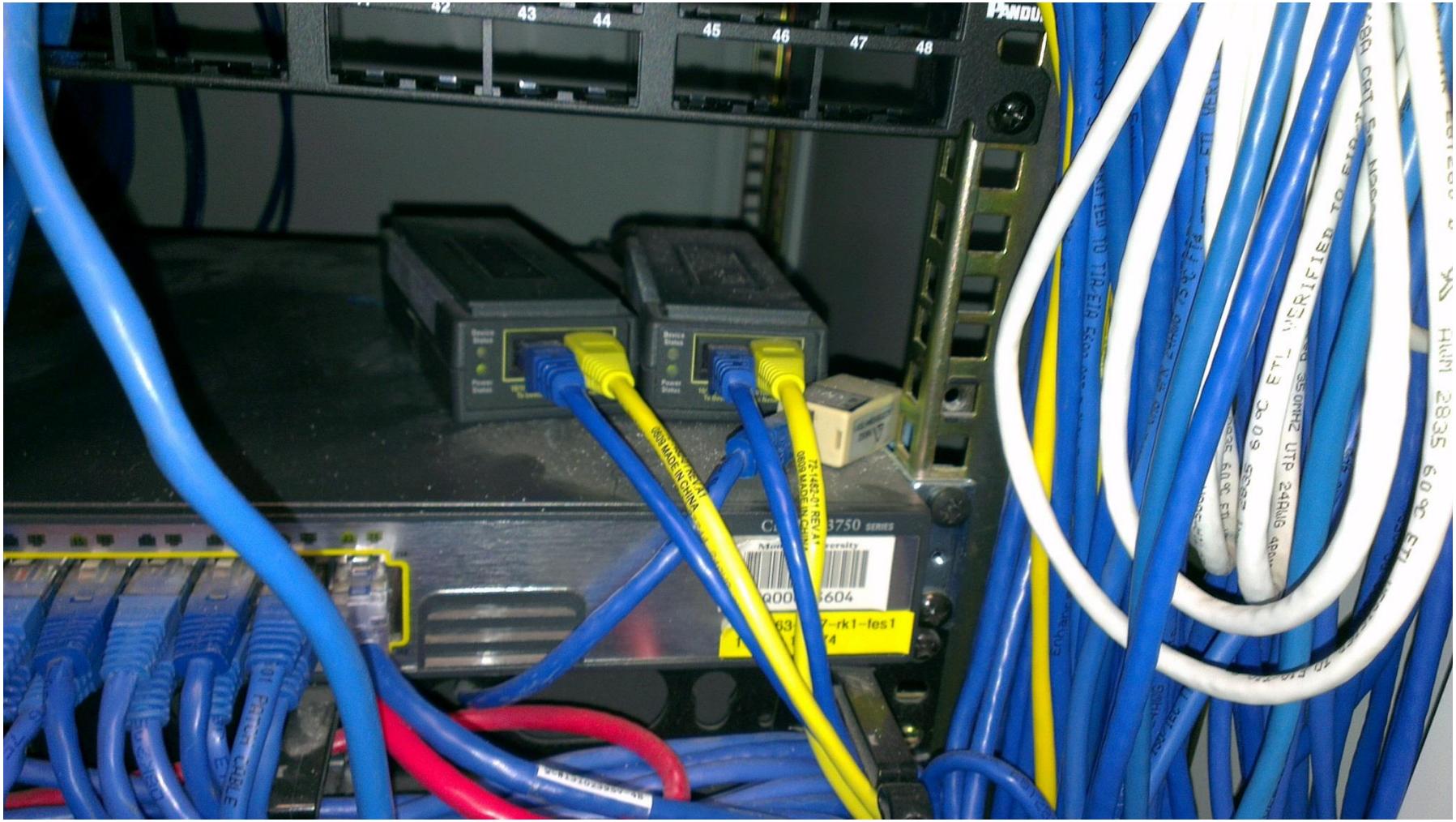
Cisco switches



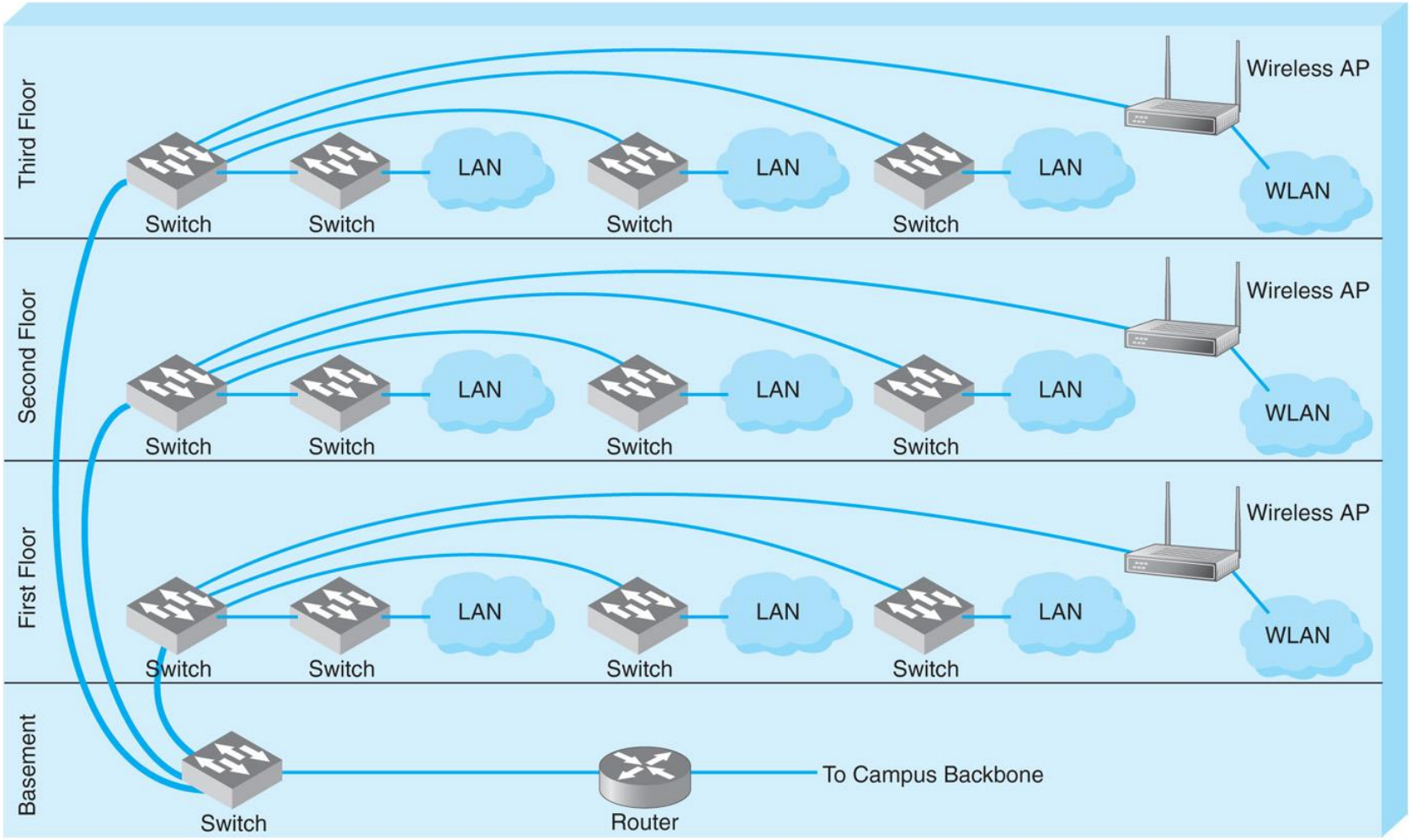
Uplink fibre optics connections



What that might be?

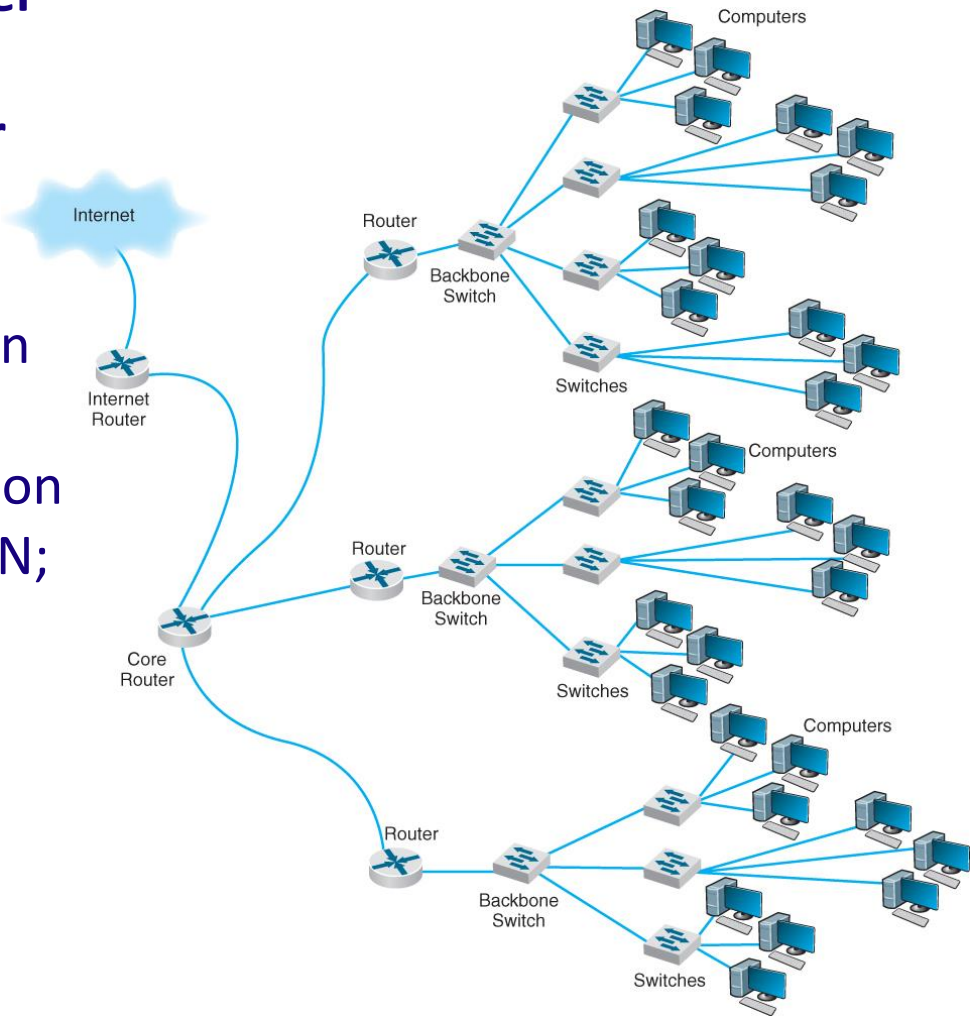


Example: Switched backbones at Indiana University



Routed Backbone

- Move packets using **network layer addresses**
- Commonly used at the **core layer**
  - Connecting LANs in different buildings in the campus
  - Can be used at the distribution layer as well
- Main advantage: LAN segmentation
  - Each message stays in one LAN; unless addressed outside the LAN
  - Easier to manage, LANs are separate entities, segments
- Main disadvantages
  - Tend to impose time delays
  - Require more management than switches

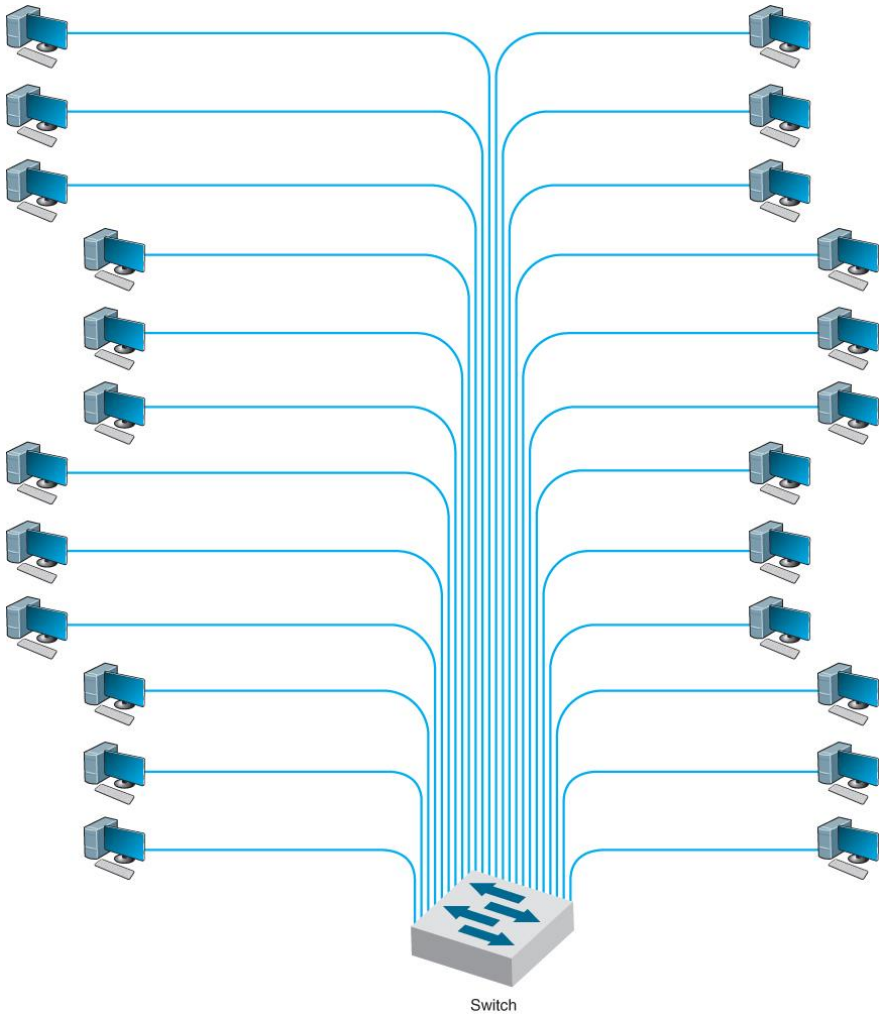


Virtual LANs (VLANs)

- A newest type of LAN-BN architecture
  - Made possible by high-speed intelligent switches
  - Computers assigned to LAN segments by software
- Often faster and provide more flexible network management
  - Much easier to assign computers to different segments
- More complex and typically used for larger networks
- Basic VLAN designs:
  - Single switch VLANs
  - Multi-switch VLANs

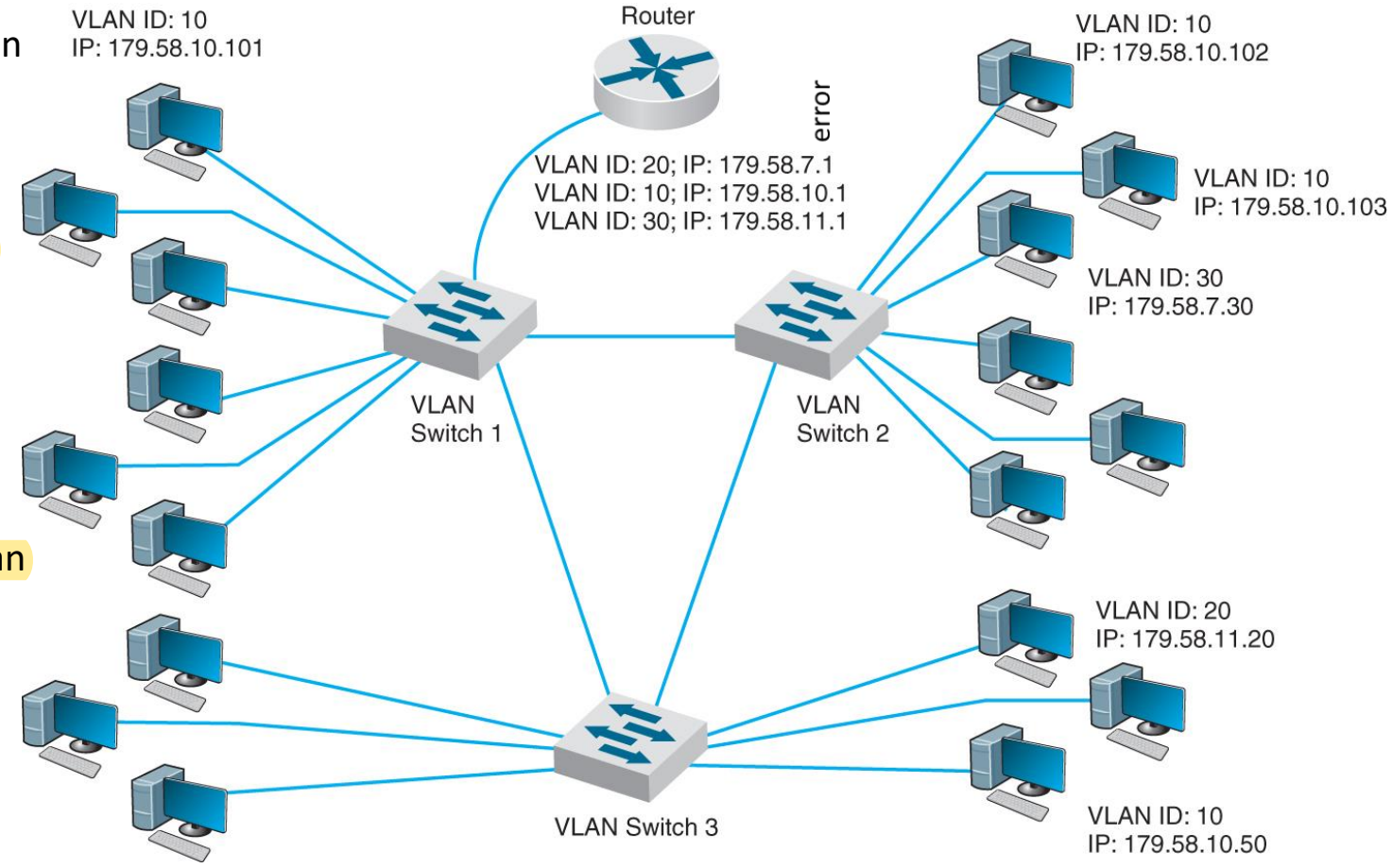
VLAN-based Backbone: a single switch VLAN

- Dozens or even hundreds computers are connected to a single VLAN switch
- The computers on the VLAN are assigned by software into different segments
- The VLAN segments function in the same way as physical LAN segments or subnets.
- Because VLAN switches can create multiple subnets, they act like routers or layer-3 switches, except the subnets are inside the switch, not between the switches
- VLAN switches that emulate shared circuits (hubs) are simpler than the ones with the full switch circuit capacity.



Multi-switch VLAN-Based Backbone

- Multi-switch VLAN can span different buildings
- Each computer is assigned into a VLAN that has a VLAN ID (VID)
- Each **VID** is matched to a traditional **IP subnet**
- Each computer gets an IP address from the switch: Similar to DHCP operation.
- Computers are assigned into the VLAN based on physical port they are plugged into

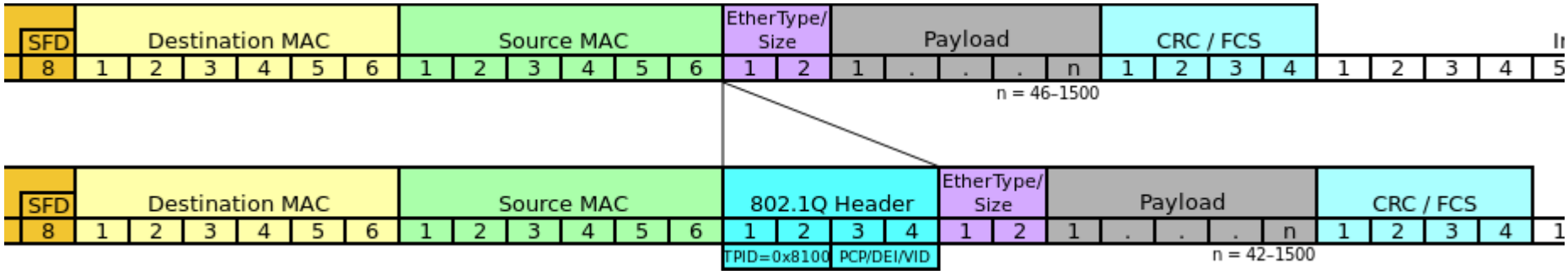


- In the example there are three VLANs with VIDs 10, 20 and 30
- VIDs are matched with the subnets:

  10 - 179.58.10.x, 20 - 179.58.11.x, 30 - 179.58.7.x,

802.1Q - VLAN Standard (1)

- VLAN switches use Ethernet 802.1Q **tagging standard** to move frames from one switch to another.
- When a VLAN switch receives an Ethernet frame that needs to go to a computer on another VLAN switch, it changes the Ethernet frame by inserting the 802.1Q header:



- Tag Protocol Identifier (TPID): a 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame.
- Recall from Lecture 3:

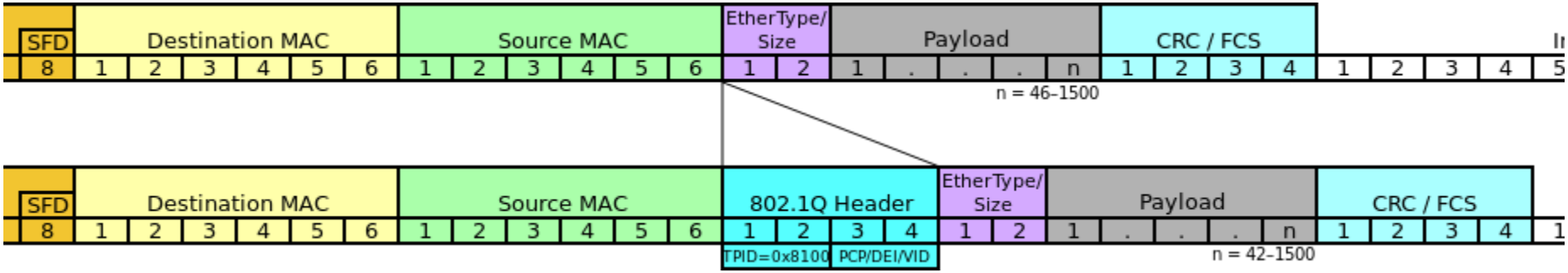
Length/type field

- **Length/type**, a 2-byte field, takes one of two meanings, depending on its numeric value.
- Length interpretation: If the value of this field is less than or equal to 1500 decimal (0x05DC hexadecimal), then the Length/Type field indicates the number of MAC client data octets contained in the subsequent MAC Client Data field of the basic frame .
- Type interpretation: If the value of this field is greater than or equal to 1536 decimal (0x0600 hexadecimal), then the Length/Type field indicates the Ethertype of the MAC client protocol.

  Examples of most common Ethertypes:

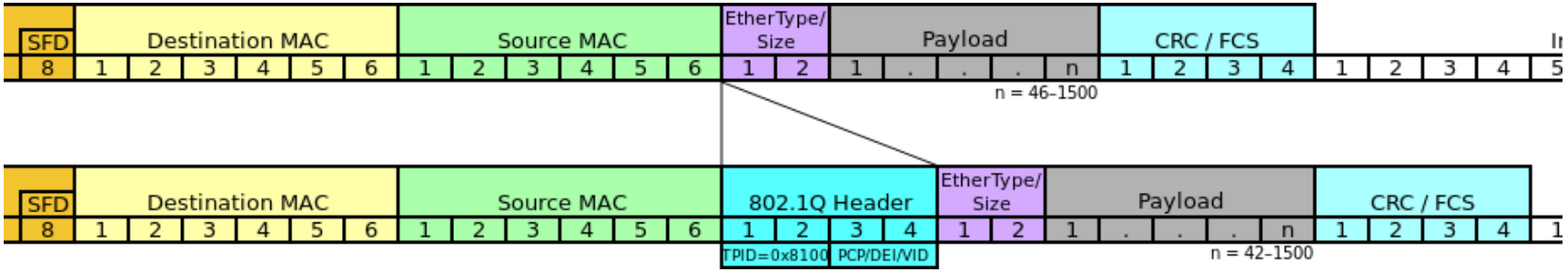
  - 0x0800 the frame contains IPv4 packet.
  - 0x0806 indicates an ARP frame
  - 0x8100 indicates the VLAN 802.1Q frame

802.1Q Header



- Tag Protocol Identifier (TPID): a 16-bit field set to a value of 0x8100
- PCP – Priority Code Point (3 bits) – to prioritize different classes of traffic
- DEI – Drop eligible indicator (1-bit). May be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion.
- VLAN Identifier (VID): a 12-bit field specifying the VLAN to which the frame belongs.

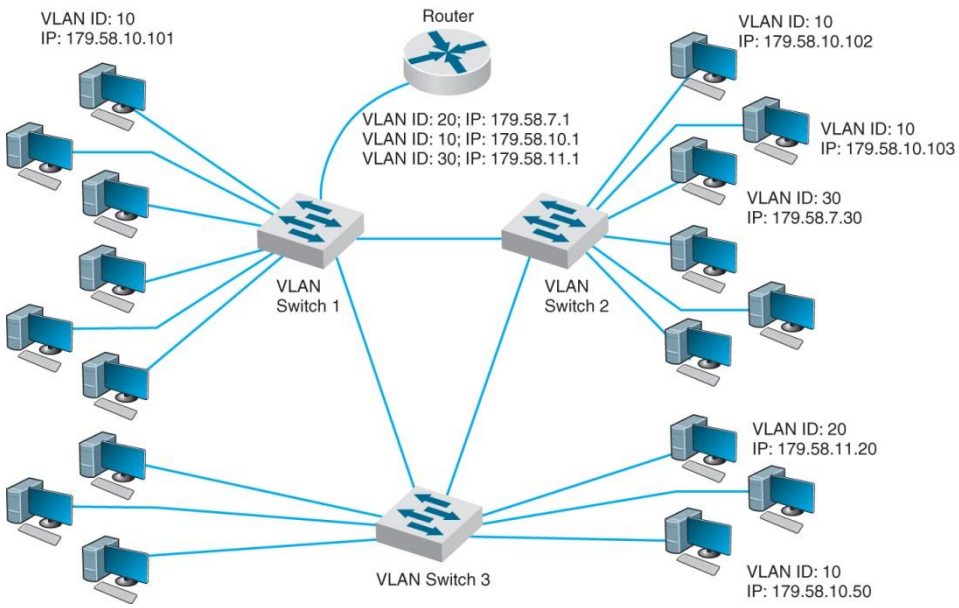
802.1Q in action



- Note that 802.1Q does not encapsulate the original frame.
- Instead, it inserts a 32-bit field between the source MAC address and the Ether Type/Length fields of the original frame.
- When a switch is configured, the network administrator defines which VLANs span which switches and also defines VLAN trunks-circuits that connect two VLAN switches and enables traffic to flow from one switch to another.
- As a switch builds its forwarding table, it receives information from other switches and inserts the Ethernet addresses of computers attached to them into its forwarding table along with the correct trunk to use to send frames to them.

Multi-switch VLAN

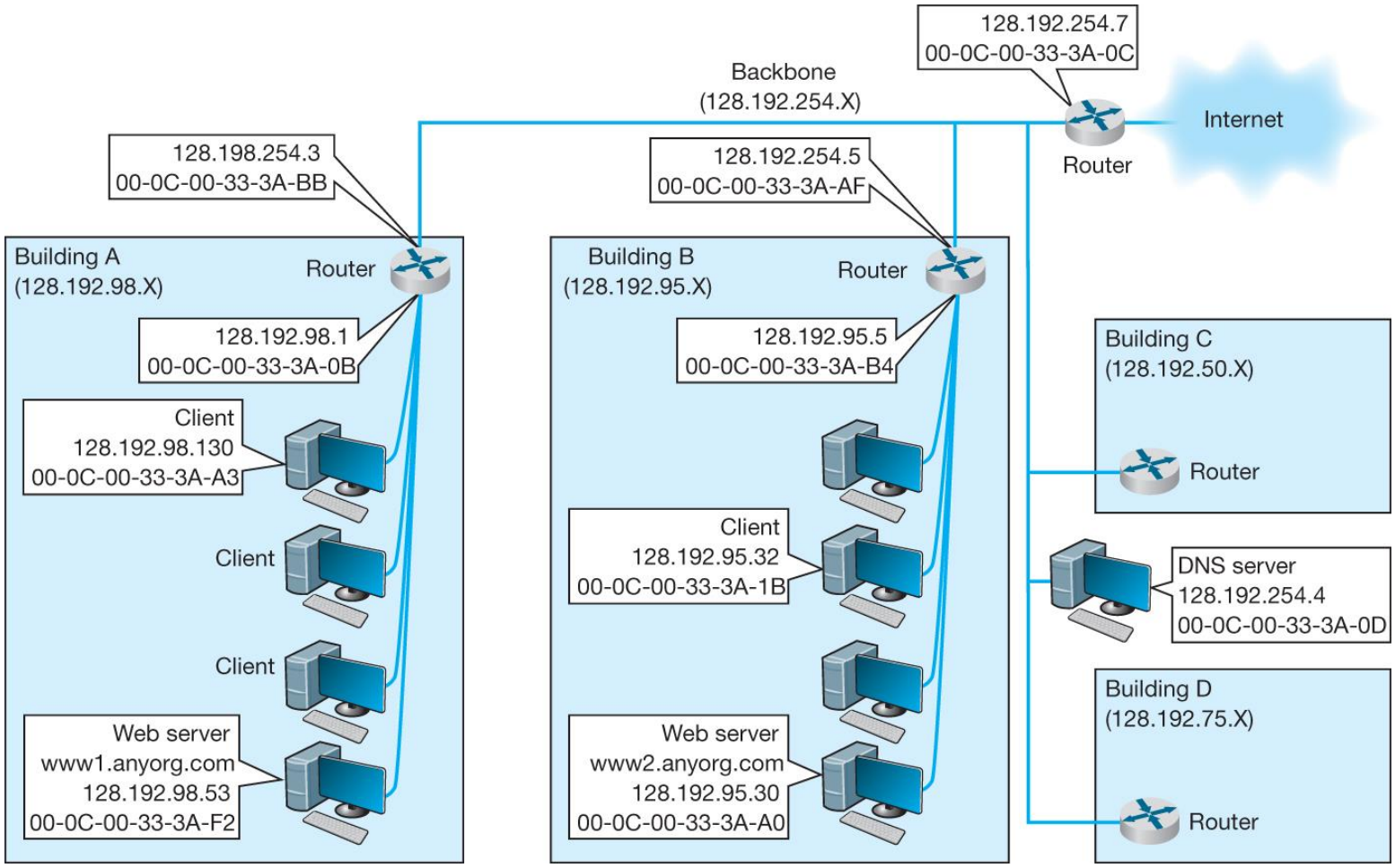
- Multi-switch VLAN enables to create subnets based on **who** you are rather than on **where** you are
- We can create e.g. an accounting subnet and a marketing subnet rather than a Building A and Building B subnets
- VLANs make it simpler to **manage the broadcast traffic**, hence improving the overall performance.
- VLANs offer the ability to prioritize traffic.



- In the example there are three VLANs with VIDs 10, 20 and 30
- VIDs are matched with three subnets:

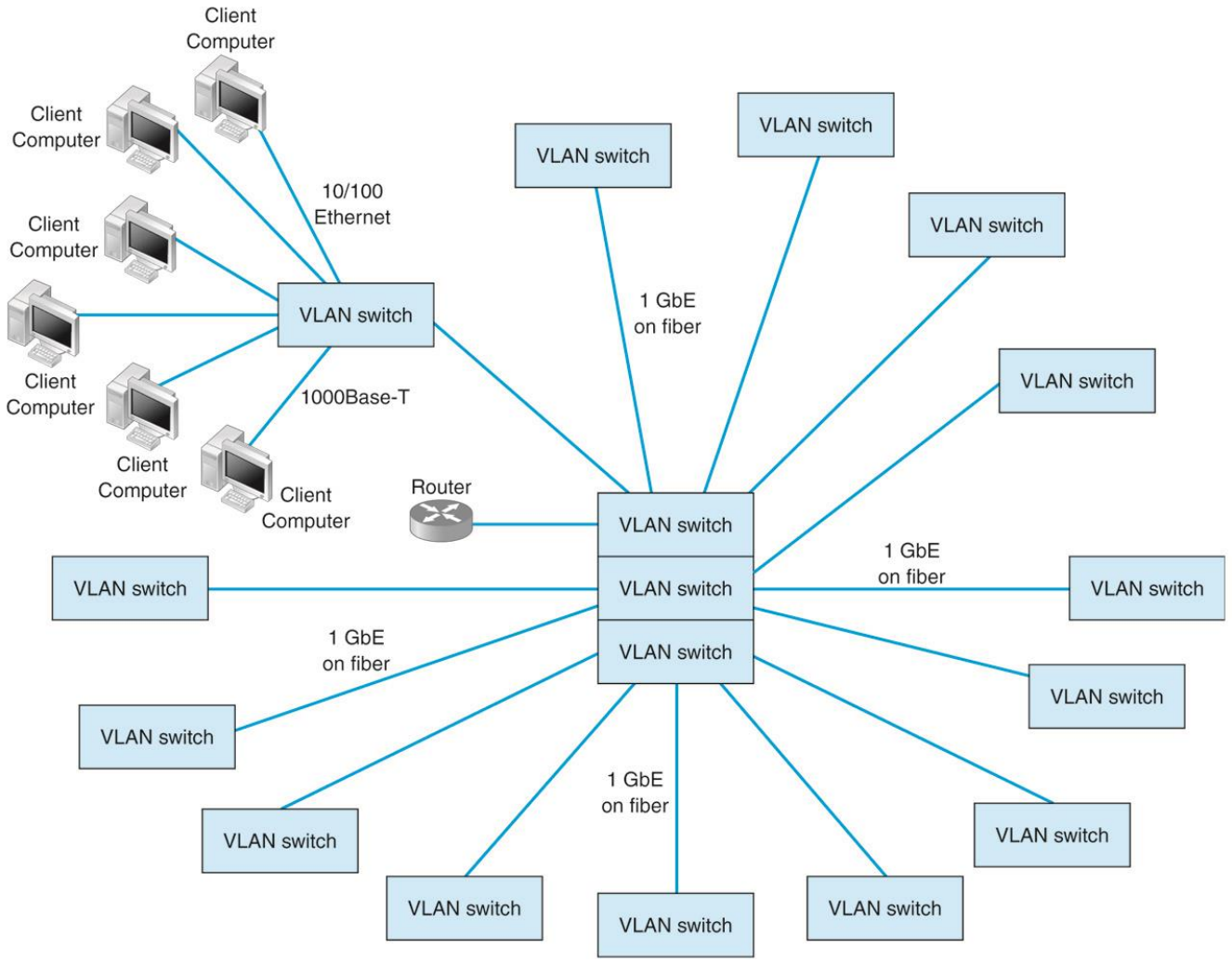
  10 - 179.58.10.x, 20 - 179.58.11.x, 30 - 179.58.7.x,
- There are also three VLAN switches using the 802.1Q tagging protocol
- The router connected to one of the VLAN switches routes the traffic for all three subnets

Example of a traditional network

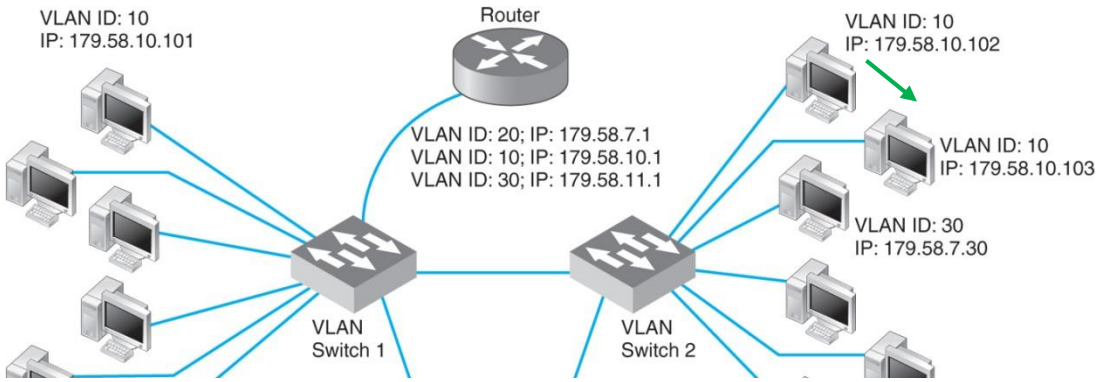


- Subnets are geographically located: Buildings A, B, C, D
- Each subnet has its own router

Another VLAN Backbone Network Example



VLAN in action



- We'll assume this network uses the first three bytes to specify the IP subnet (/24)

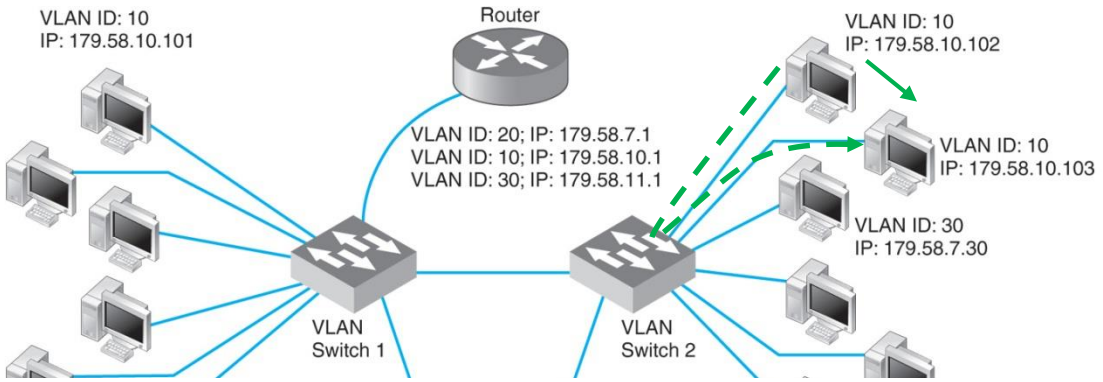
- We have three VLAN switches with three IP subnets (179.58.10.x, 119.58.7.x, and 179.58.11.x) and three VLANs (10,20,30).
- A router is used to enable communication among the different IP subnets.

Case 1: Same subnet same switch:

- Suppose a computer connected to switch 2 (IP 179.58.10.102) sends a message to a computer on the same IP subnet that is also connected to switch 2 (IP 179.58.10.103).
- The sender recognizes that the destination computer is in the same IP subnet.
- It creates an Ethernet frame with the destination computer's Ethernet address (using ARP if needed to find the Ethernet address), and transmit the frame to its VLAN switch 2.

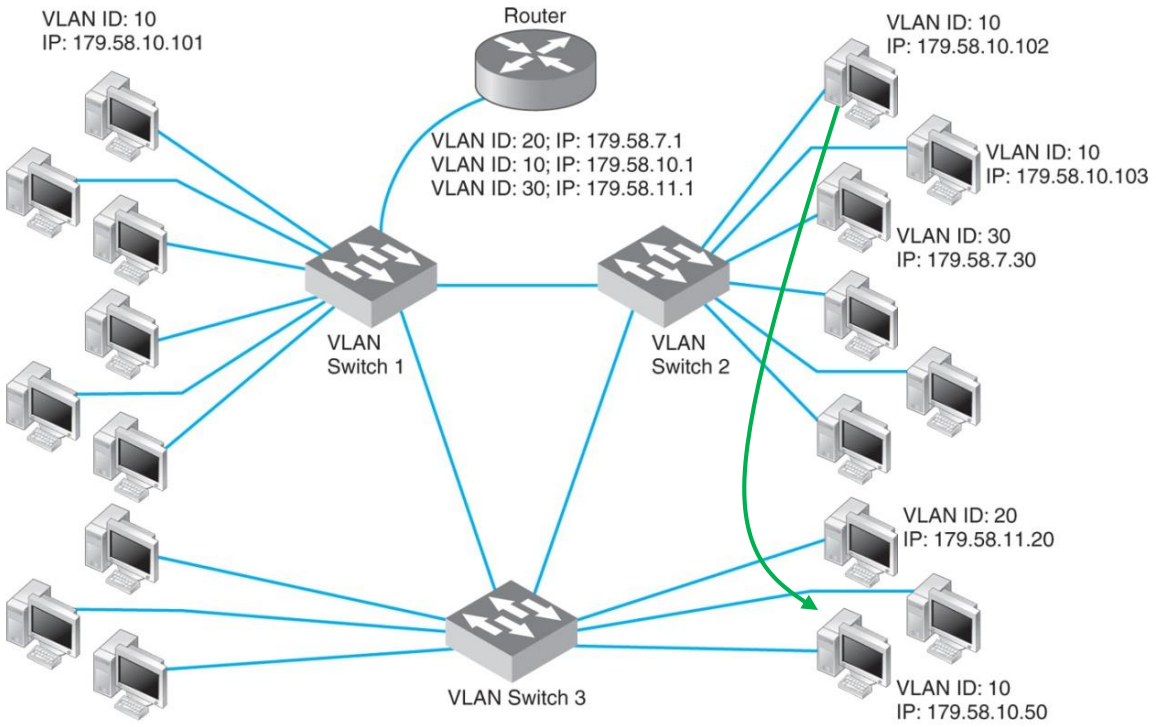
VLAN example

Same subnet same switch



- When a VLAN switch receives a frame that is destined for another computer in the same subnet on the same VLAN switch, the switch acts as a traditional layer-2 switch:
  - it forwards the frame unchanged to the correct computer.
- Recall that switches build a **forwarding table** that lists the Ethernet address of every computer connected to the switch.
- When a frame arrives at the switch, the switch looks up the Ethernet address in the forwarding table, and if it finds the address, then it forwards the frame to the correct computer.

Case 2: Same subnet different switch (1):

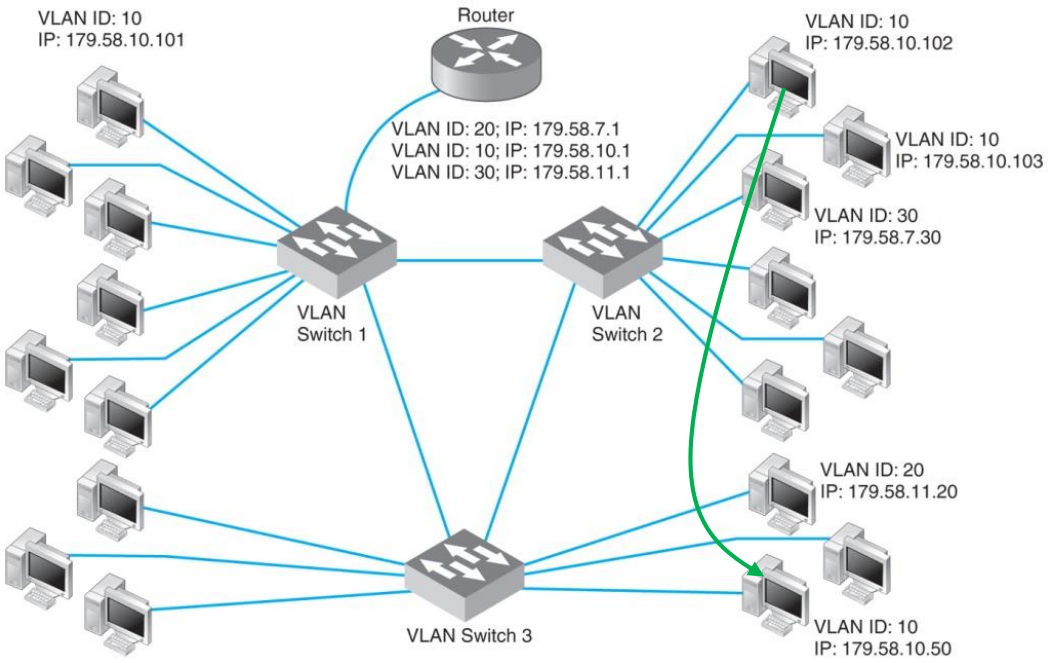


- Suppose that the computer on switch 2 (179.58.10.102) sends a message to a computer on switch 3 (179.58.10.50).

- The sending computer will act exactly as before because to it, the situation is the same:
  - It doesn't know where the destination computers is; it just knows that the destination is on its own subnet.
- The sending computer will create an Ethernet frame with the destination computer's Ethernet address (using ARP if needed to find the Ethernet address) and transmit the frame to VLAN switch 2.

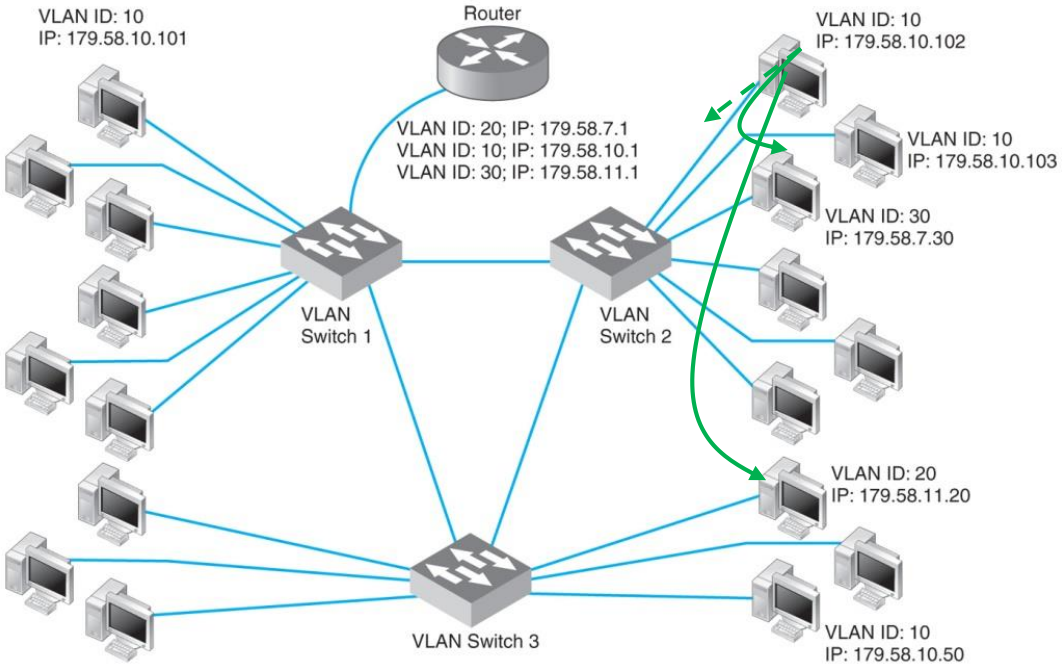
Same subnet, different switches (2):

- Switch 2 receives the frame, looks up the destination Ethernet address in its forwarding table, and sends the frame over the **trunk** to switch 3.
- It changes the frame by inserting the VLAN ID and priority code into the tag field and transmits the frame over the trunk to switch 3.



- Switch 3 receives the frame, looks the Ethernet address up in its forwarding table, and identifies the specific computer the frame needs to be sent to.
- The switch removes the VLAN tag information and transmits the revised frame to the destination computer.
- In this way, neither the sending computer nor the destination computer are aware that the VLAN exists. The VLAN is transparent.

Case 3: Different subnets, different switches (1)

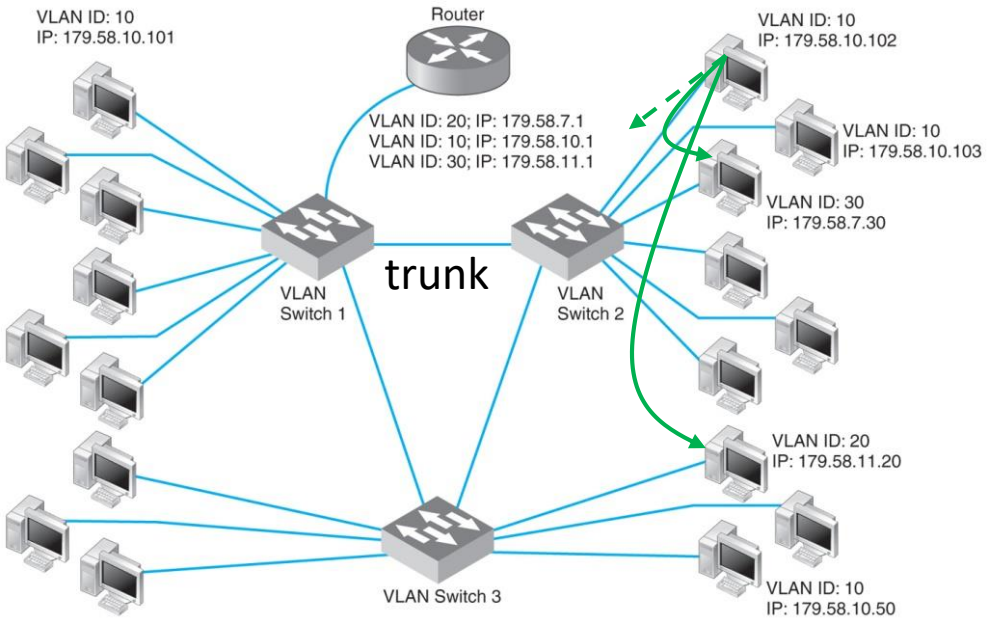


- Suppose the computer (179.58.10.102) connected to a VLAN switch 2 wants to send a message to a computer on a different subnet e.g., either

  to 179.58.7.30 on the same switch 2, or to 179.58.11.20 on switch 3.

- The sending computer recognizes that the destination is on a different subnet, and therefore creates an Ethernet frame with a destination Ethernet address of its router (179.58.10.1, MAC address not shown), and sends the frame to switch 2.
- At this point, everything works the same as in the previous example.
- Switch 2 looks up the destination Ethernet address in its forwarding table,
- recognizes that the frame needs to go to switch 1 because the router's Ethernet address is listed in the forwarding table as being reachable through switch 1.

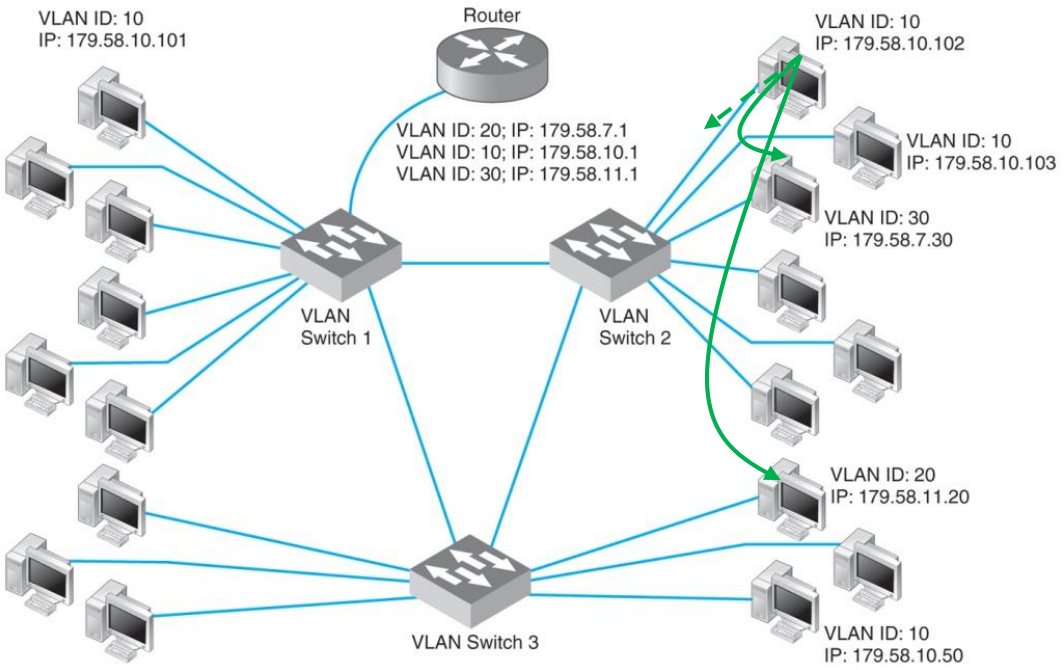
Different subnets, different switches (2)



- Switch 2 sets the VLAN tag information and sends the frame over the trunk to switch 1.

- Switch 1 looks up the destination Ethernet address in its forwarding table, and sees that the router is attached to it.
- Switch 1 removes the VLAN tag field and sends the frame to the router.
- The router is a layer-3 device, so when it receives the message, it strips off the Ethernet frame and reads the IP packet.
- The router looks in its routing table and sees that the destination IP address is within a subnet it controls (either 179.58.7.x or 179.58.11.x depending on which destination computer the packet was sent to).

Different subnets, different switches (3)



- The router creates a new Ethernet frame and sets the destination Ethernet address to the destination computer (using an ARP if needed) and sends the frame to switch 1.
- Switch 1 reads the Ethernet address and looks it up in its forwarding table.
- It discovers the frame needs to go to switch 2 (for 179.58.7.30) or switch 3 (for 179.58.11.20), sets the VLAN tag field, and forwards the frame over the trunk to the correct switch.
- The destination switch **removes the VLAN tag** information and sends the frame to the correct computer.

Broadcasting in VLAN

- Up to this point we've been talking about unicast messages – messages from one computer to another – that are the majority of network traffic.
- How the broadcast messages such as ARPs are sent to all computers in the same subnet?
- Each computer on a VLAN switch is assigned into a subnet with a matching VLAN ID.
- When a computer issues a broadcast message, the switch identifies the VLAN ID of the sending computer and then sends the frame to all other computers that have the same VLAN ID.
- These computers may be on the same switch or on different switches.

ARP processing

- For example, suppose computer 179.58.10.102 issues an ARP to find an Ethernet address (e.g., the router address).
- Switch 2 would send the broadcast frame to all attached computers with the same VLAN ID (e.g., 179.58.10.103).
- Switch 2's forwarding table also tells it than VLAN 10 spans switch 1 and switch 3, so it sends the frame to them.
- Switches 1 and 3 use their tables to send it to their attached computers that are in the same VLAN (which includes the router).
- The router has multiple lP addresses and VLAN IDs because it is connected to several different VLANs and subnets (three, in our example here).

Learning in VLAN switches

- We have also assumed that the VLAN switch has a complete forwarding table – a table that lists all the Ethernet addresses of all the computers in the network.
- Just like a layer-2 switch, the VLAN switch learns Ethernet addresses as it sends and receives messages.
- When the VLAN switch is first turned on, the forwarding table is empty, just like the forwarding table of a layer-2 switch; however, its VLAN ID and trunk tables are complete because these are defined by the network administrator.
- Suppose the switch has just been turned on and has an empty forwarding table.
- It receives an Ethernet frame, looks up the destination address in the forwarding table, and does not find where to send it.

Learning and broadcasting in VLAN switches

- If the VLAN switch were a layer-2 switch, it would send the frame to all ports.
- A VLAN switch is smarter than this.
- Note that an Ethernet frame is *always* sent to a computer in the same IP subnet as the sending computer.
- Any time a frame needs to move to a different subnet, it goes through a router which sits on both subnets.
- Therefore, any time the VLAN switch cannot find a destination Ethernet address in the forwarding table, it treats the frame as a broadcast frame and sends it to all the computers in the same subnet, which in VLAN terms means all the computers with the same VLAN lD.
- This means that a VLAN architecture can improve performance by reducing traffic in the network compared with a switched backbone architecture.
- Since a switched backbone uses layer-2 switches, all the computers are in the same subnet, and a broadcast traffic goes to all computers.
- By using a VLAN we can limit where broadcast traffic flows by dividing the network into separate subnets, so that broadcast messages only go to computers in the same subnet.