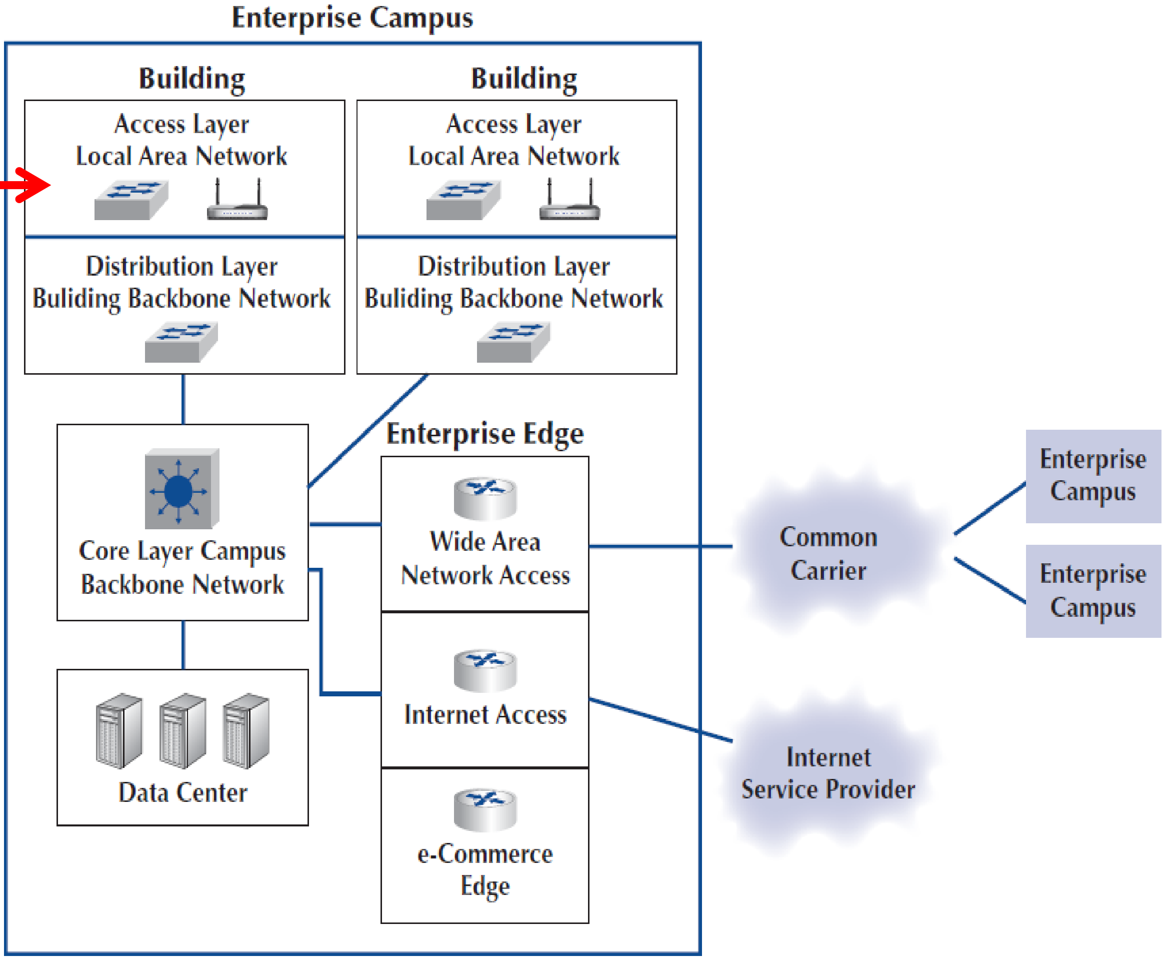
CIS 375
CHAPTER 7

Wired and Wireless
Local Area Networks(LAN)

Outline

- Why use a LAN?
- LAN components
- Wired Ethernet
- Wireless Ethernet
- Best Practice in LAN design
- Improving LAN performance
- Implications for Cyber Security

Focus of
this lecture

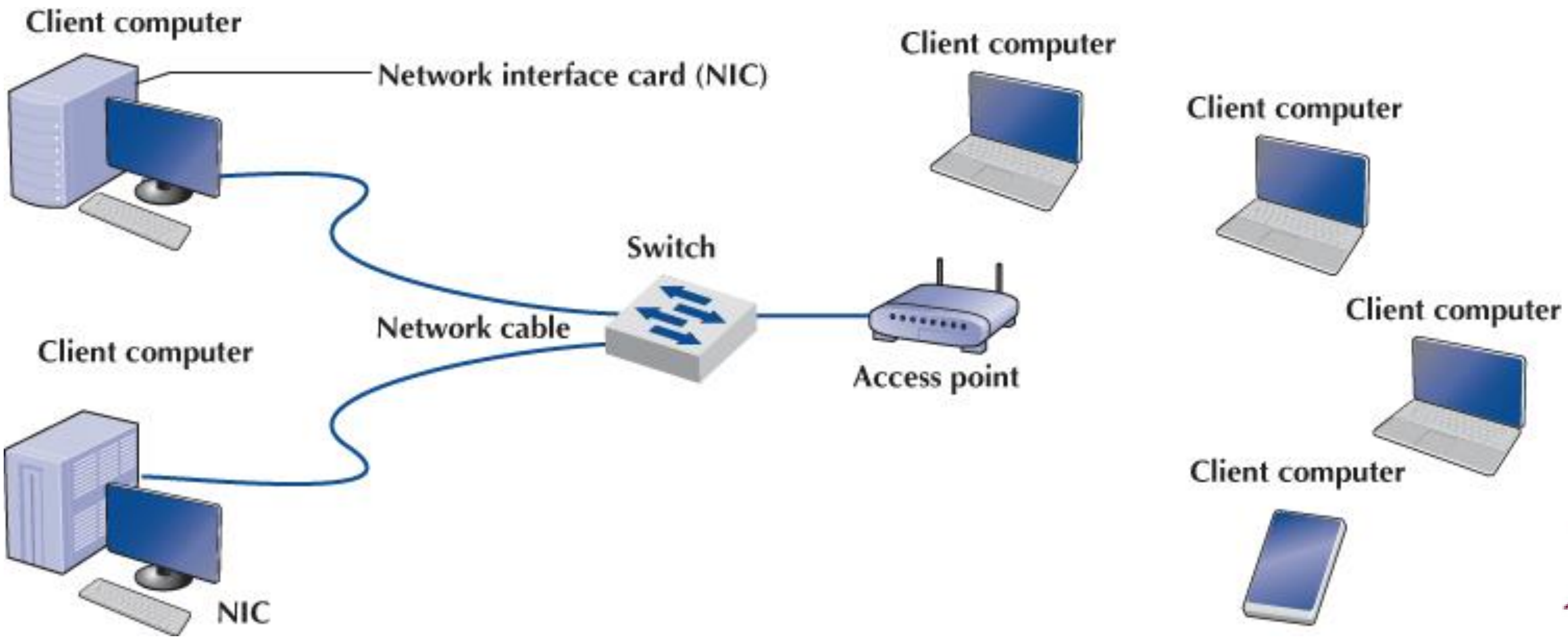


Why use a LAN?

- Information sharing
  - Improved decision making
  - May reduce data duplication and inconsistency
- Resource sharing
  - Devices such as printers can be shared by many clients
- Software sharing
  - Some software can be purchased on a per-seat basis and resides on server
  - Reduces costs, simplifies maintenance and upgrades
- Device Management
  - Software updates and configuration are easier

LAN Components

1. Clients
2. Servers
3. Network interface cards (NICs)
4. Network cables
5. Hubs / switches / access points
6. Software



LAN Components

1. **Clients**
   - Devices on the network that request information from servers
2. **Servers**
   - Devices on the network that deliver information or provide services to clients
3. **Network interface cards (NIC)**
   - Also called network cards and network adapters
   - Operate at layers 1 and 2
   - Commonly built into motherboards
   - Ethernet NICs contain unique MAC address

LAN Components

4. Network Cables

Name	Type	Maximum Data Rate	Used by
Category 3	UTP	10 Mbps	10BASE-T
Category 5	UTP/STP	100 Mbps	100BASE-T
Category 5e	UTP/STP	1 Gbps	1000BASE-T
Category 6/6a	UTP/STP	10Gbps	10GBASE-T
OM1 (62.5/125 µm)	Fiber	1-10 Gbps*	1000BASE-SX
OM3 (50/125 µm)	Fiber	10-100 Gbps*	10GBASE-SR

* Speed depends on circuit length

LAN Components

5. **Hubs** and **switches**
   - Link cables from different devices, sometimes more than one type of cabling
   - Act as repeaters, reconstructing and strengthening incoming signals

(a) Small-Office, Home-Office (SOHO) switch
with five 10/100/1000 Mbps ports

http://homestore.cisco.com/en-us/Switches/
linksys-EZXS55W_stcVVproductId53934575VVcatId543809VVviewprod.htm

(b) Data center chassis switch with 512 10 Gbps ports

Source: newsroom.cisco.com/dlls/2008/prod_012808b.html

LAN Components

5. **Access points (APs)** use radio waves to connect wireless clients to the wired network (instead of connecting using hubs/switches)
   - Many APs use power over Ethernet (PoE) for electricity
   - No external power is needed
   - Power flows over unused twisted pair wires
   - Also used by some IP cameras and phones

LAN Components

(a) AP for SOHO use

(b) A power-over-Ethernet AP for enterprise use

LAN Components

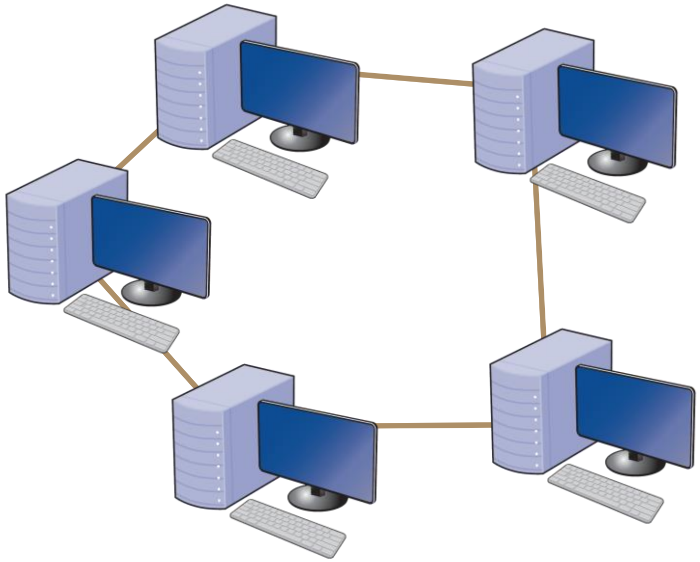
6. **Software**
   - Network Operating System (NOS)
     - Runs on devices and manage networking functions
     - E.g., Novel NetWare, Microsoft Windows Server, Linux
     - E.g., Cisco IOS or JUNOS on routers
   - Clients devices typically have network software components included with OS installation
     - E.g., TCP/IP included in Windows, OS X, and Linux
     - Allows clients to view and access available network resources
   - Provides **directory services** about LAN resources
   - **Network profiles** specify resources that devices and users can access

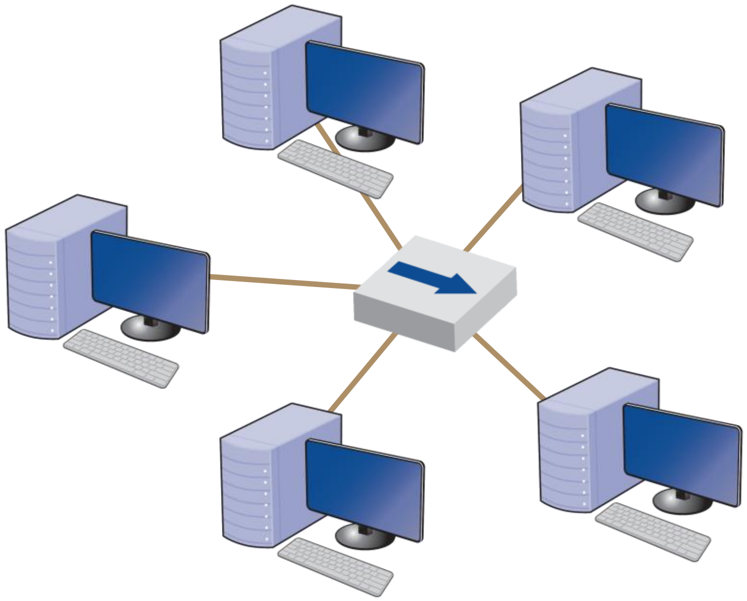
Wired Ethernet

- IEEE 802.3 standards
- Used by nearly all LANs today
- Originally developed at Xerox PARC and standardized by a consortium of Digital Equipment Corp., Intel and Xerox (DIX)
- Layer 2 protocol, but physical layer must meet protocol requirements

Wired Ethernet

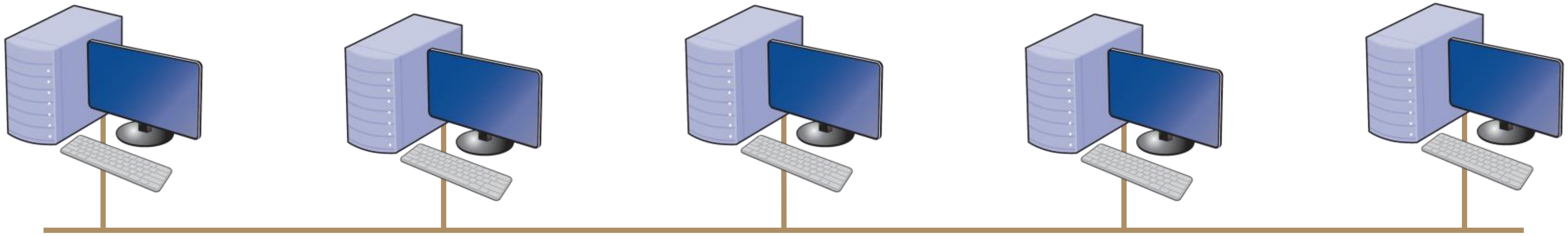
- Topology: Basic geographic layout of a network
- Types
  - **Logical**: How the network works conceptually
  - **Physical**: How the network is physically installed





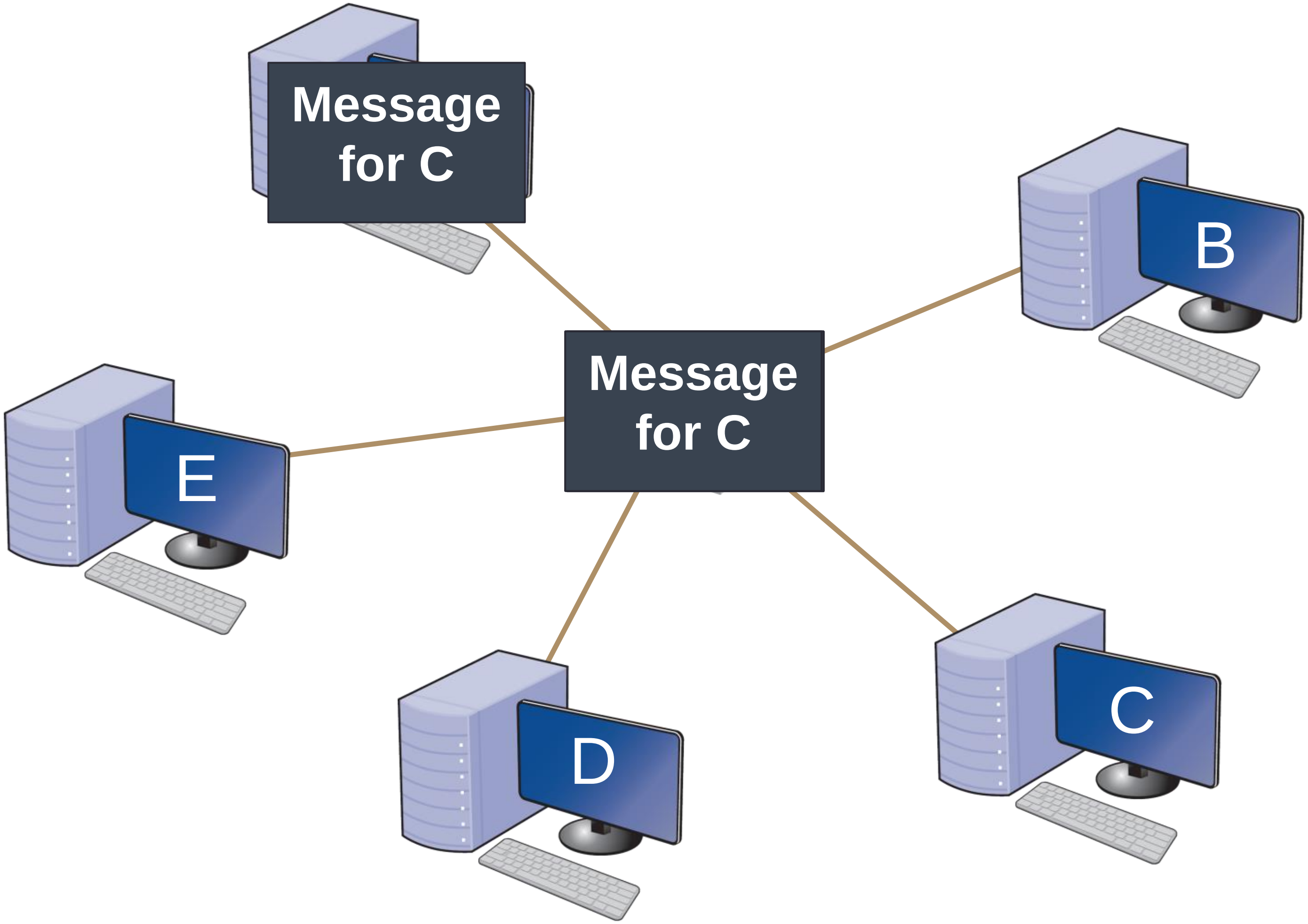
Wired Ethernet

- Hub-based Ethernet
  - Also called shared or traditional Ethernet
  - Logical **bus topology** means that all devices receive every frame as if they were connected to the same circuit
  - The hub is a multiport repeater



Wired Ethernet

- Hub-based Ethernet uses **physical star** topology

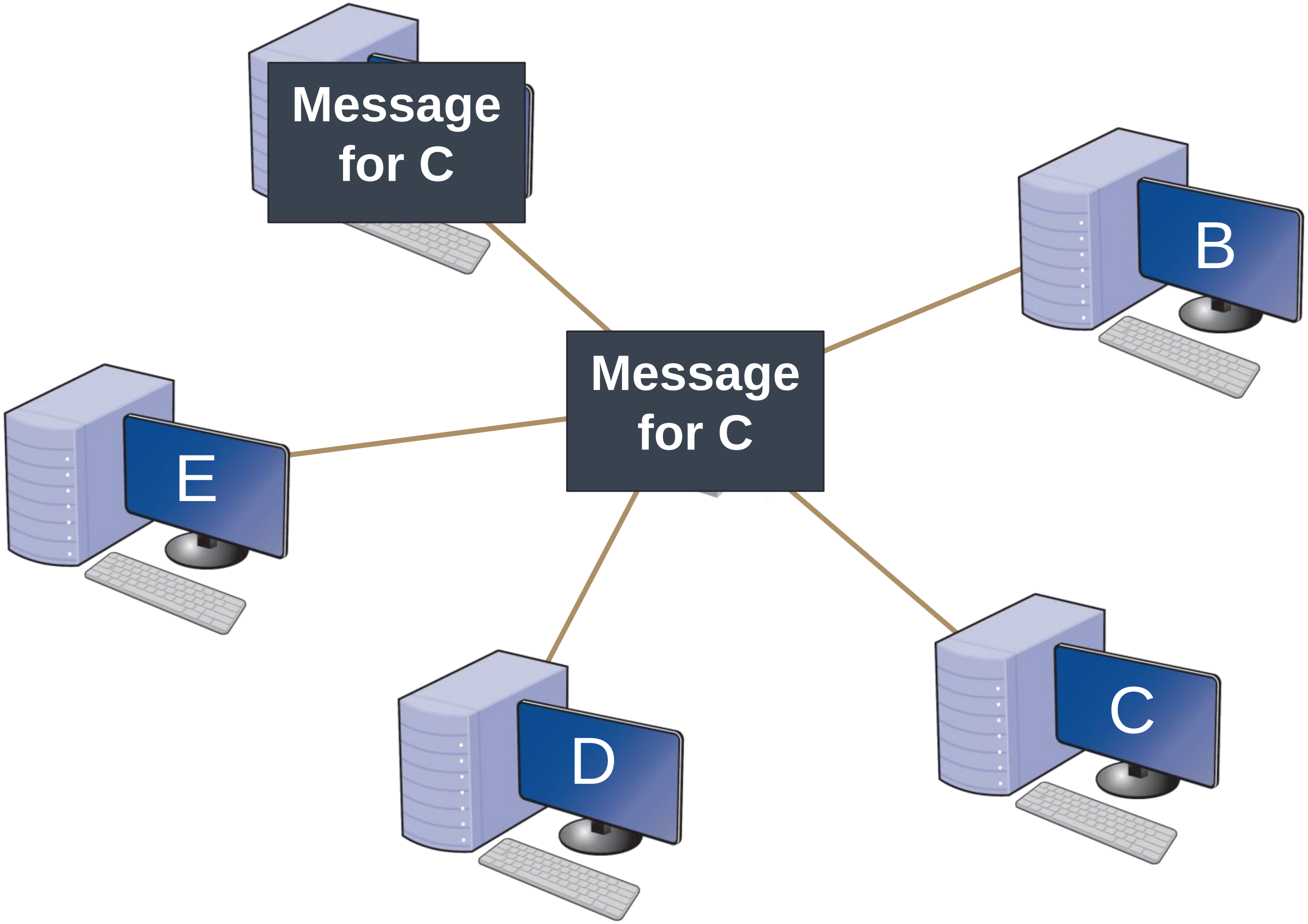


Wired Ethernet

- Switch-based Ethernet
  - Logical **star topology** means that only the destination receives the frame
    - Switch reads destination address of the frame and only sends it to the interface (physical port) connected to a circuit
    - Uses forwarding tables (also called MAC or CAM tables), which are similar to routing tables
    - Breaks up the **collision domain**
  - Physical **star topology**

Wired Ethernet

- Switch-based Ethernet



Wired Ethernet

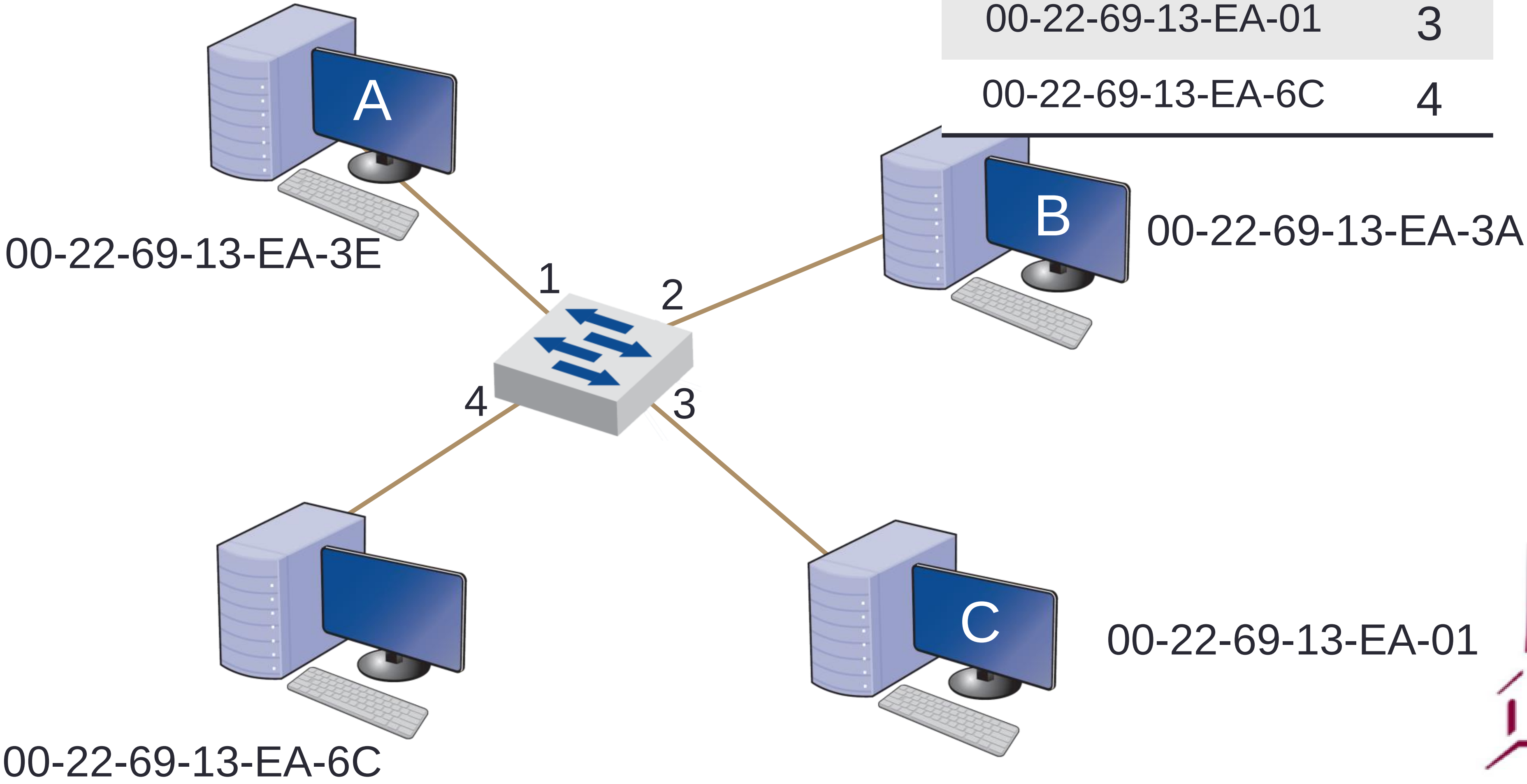
- Switch operation
  - Switches learn which MAC address is associated with an interface (physical port) by reading the source address on a frame
  - When a new frame is received, the switch reads the destination MAC address
  - Looks up destination address in the forwarding table
    - If found, forwards frame to the corresponding interface
    - If not found, broadcasts frame to all devices (like a hub)

Wired Ethernet

- Switch-based Ethernet

Switch Forwarding Table

MAC	Port
00-22-69-13-EA-3E	1
00-22-69-13-EA-3A	2
00-22-69-13-EA-01	3
00-22-69-13-EA-6C	4



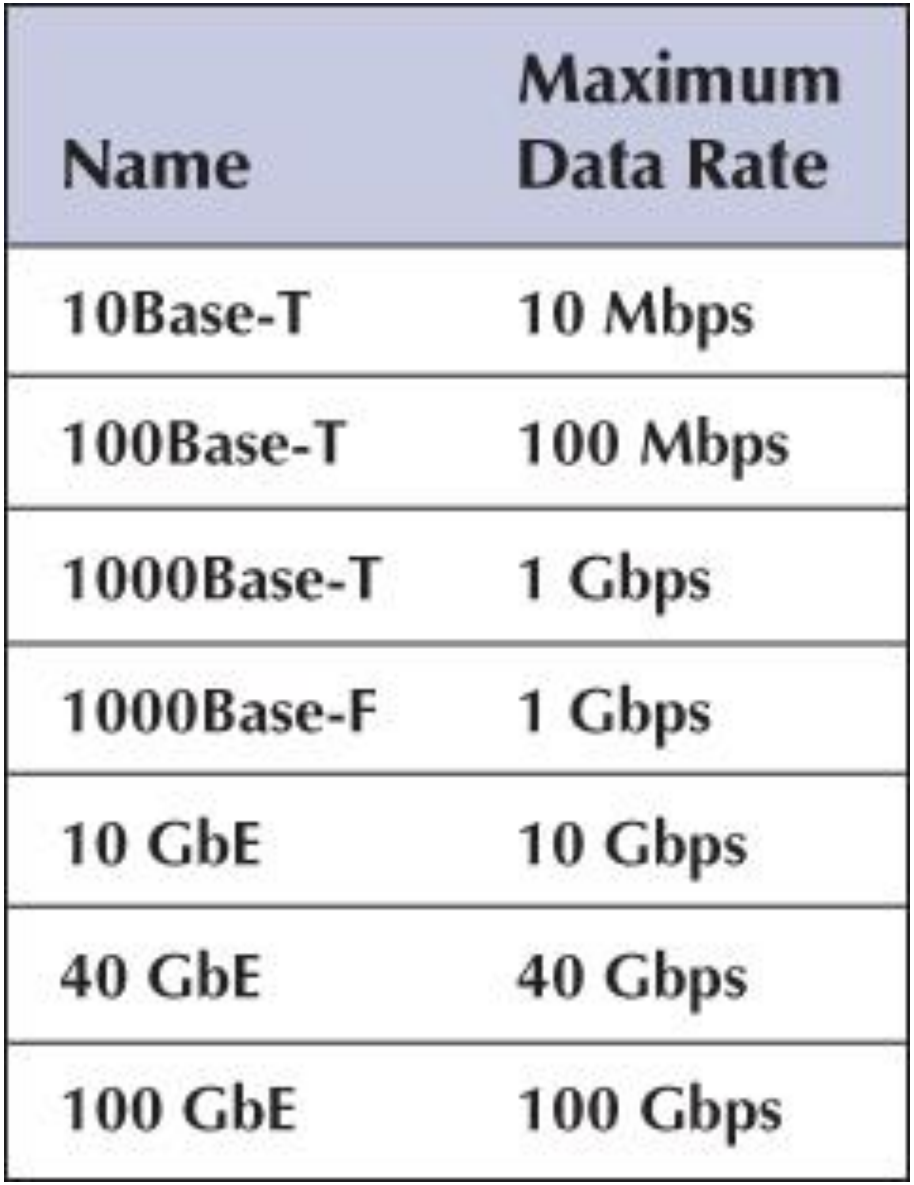
Wired Ethernet

- Switching modes
  - **Store and forward switching –** frames retransmitted after entire frame is received and error check is complete
    - Slower, but fewer errors
  - **Cut-through switching –** frames retransmitted as soon as destination address read
    - Low latency, but some capacity wasted
  - **Fragment-free switching –** frames retransmitted once the header (first 64 bytes) is received and has no errors
    - Compromise between store and forward and cut-through

Wired Ethernet

- Media access control
  - Wired Ethernet uses a contention-based technique called **carrier sense multiple access with collision detection (CSMA/CD)**
    - Carrier Sense (CS):
      - A device “listens” to determine if another computer is transmitting
      - Only transmit when no other computer is transmitting
    - Multiple Access (MA):
      - Many devices have access to transmit on the network medium
    - Collision Detection (CD):
      - Collisions occur when multiple devices transmit simultaneously
      - If a collision is detected, wait a random amount of time and resend
  - Relies on collision detection rather than avoidance

Types of Ethernet



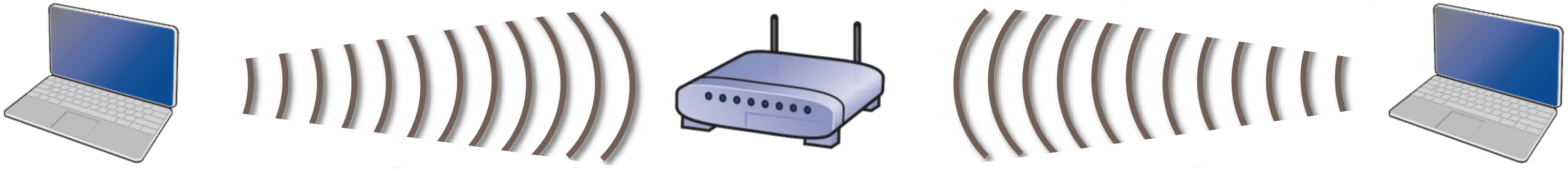
Name	Maximum Data Rate
10Base-T	10 Mbps
100Base-T	100 Mbps
1000Base-T	1 Gbps
1000Base-F	1 Gbps
10 GbE	10 Gbps
40 GbE	40 Gbps
100 GbE	100 Gbps

Wireless Ethernet

- Commonly called Wi-Fi
- A family of standards developed by IEEE formally called 802.11
- Uses radio frequencies to transmit signals through the air (instead of cables)
- Wi-Fi has many benefits
  - Provides network connections where cabling is impossible or undesirable
  - Allows device and user mobility
  - Potentially more economical than wired networks

Wireless Ethernet

- Components
  - Access points (APs)
    - Antenna type
      - Omnidirectional
      - Directional
    - AP ≠ Router
    - Association with AP
      - Active vs. passive scanning
  - Wireless NICs

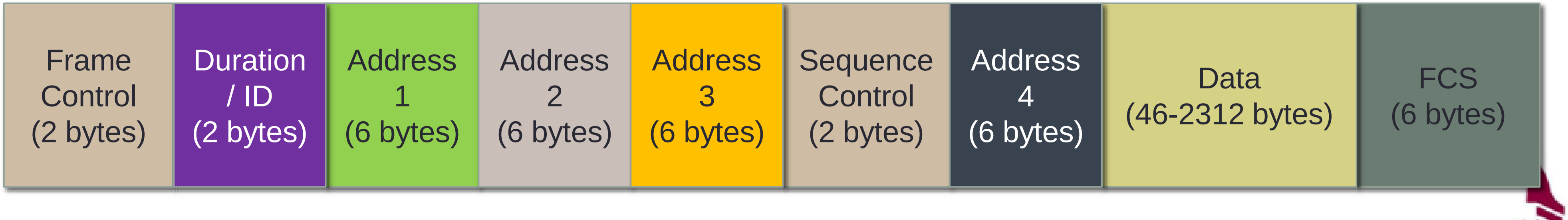


Wireless Ethernet

- Topology
  - Physical **star**
  - Logical **bus**
- Media access control
  - Uses **CSMA/CA** (CSMA with collision avoidance)
  - Two methods
    - Distributed coordination function (DCF)
    - Point coordination function (PCF)
      - Solves hidden node problem
      - Not widely implemented

Wireless Ethernet

- 802.11 Frame
  - Includes four address fields
    - Two addresses have the same meaning as in wired Ethernet, the others are used communicating with APs and other devices



Frame Control (2 bytes)	Duration / ID (2 bytes)	Address 1 (6 bytes)	Address 2 (6 bytes)	Address 3 (6 bytes)	Sequence Control (2 bytes)	Address 4 (6 bytes)	Data (46-2312 bytes)	FCS (6 bytes)

Wireless Ethernet

- Wi-Fi devices transmit and receive within **frequency ranges**
  - These frequency ranges are divided into “channels”
- Frequency ranges (in the United States)
  - 2.4 GHz range
    - 2.412-2.462 Ghz
    - 3 non-overlapping channels
  - 5 GHz range
    - 5.180-5.320 and 5.745-5.825 Ghz
    - 12 non-overlapping channels
- Larger frequency range → higher potential bandwidth
- Higher frequency → greater attenuation (i.e., shorter range)
- Overlapping channels should be minimized

Wireless Ethernet

- Types of Wi-Fi:

Type	Date Published	Max Tx Speed	Frequency (Ghz)	Official Status
802.11a	1999	54 Mbps	5, 3.7	Obsolete (Superseded)
802.11b	1999	11 Mbps	2.4	Obsolete (Superseded)
802.11g	2003	54 Mbps	2.4	Obsolete (Superseded)
802.11n	2009	600 Mbps	2.4/5	Obsolete (Superseded)*
802.11ac	2013	6.77 Gbps	5	Current
802.11ad	2012	~7 Gbps	2.4, 5, 60	Current
802.11ax	Est. 2019	?	2.4, 5	In-Progress

*Still widely used in 2014

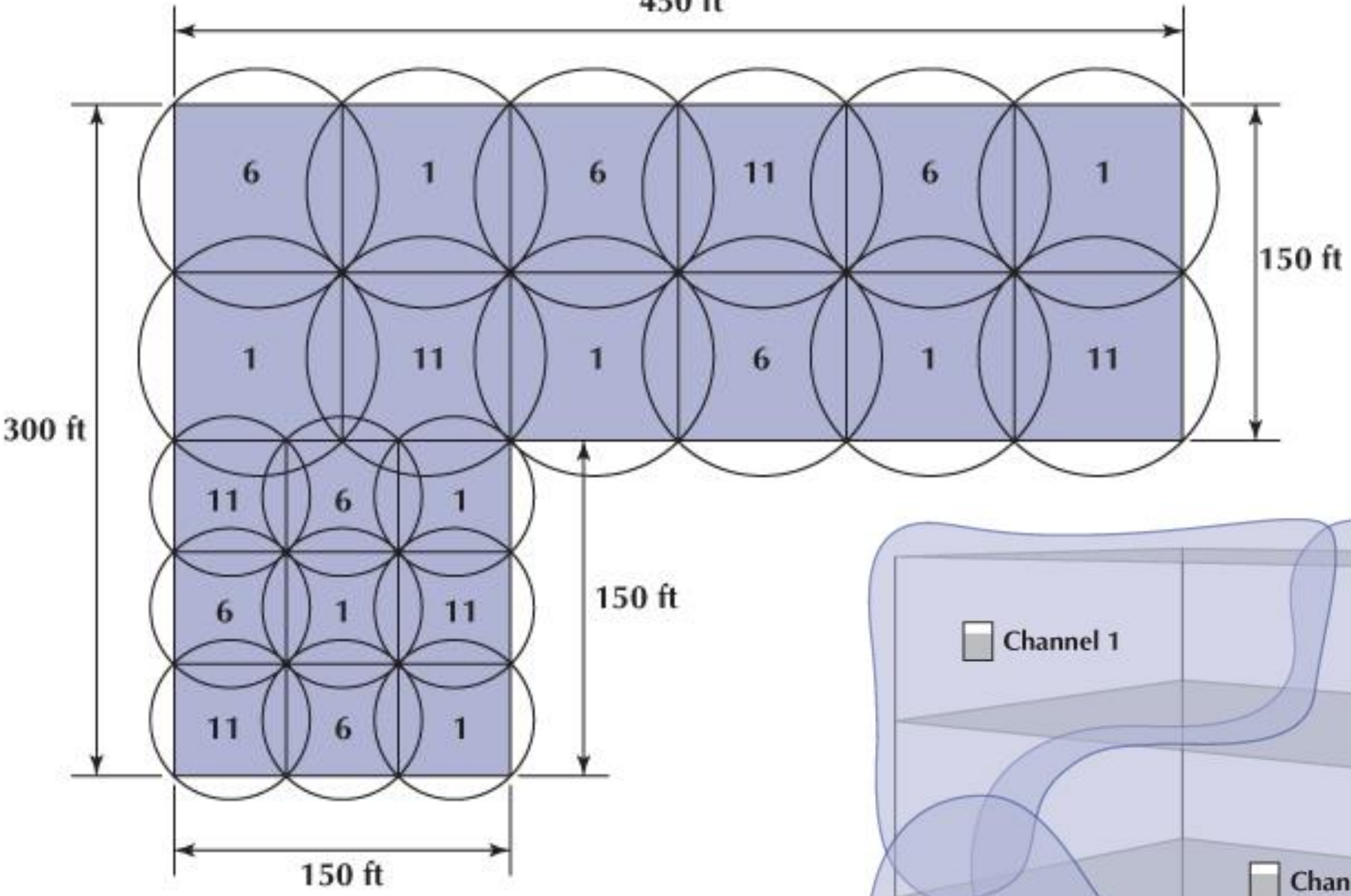
Wireless Ethernet Security

- Security is particularly important for WLANs because they are easy to discover - **wardriving**
- Security protocols:
    - Wired Equivalent Privacy (WEP)
        - Insecure and easy to bypass
    - WPA – Wi-Fi Protected Access – key
        - Key is changed for every frame that is transmitted to the client
        - Stronger than WEP
    - WPA2 (802.11i) – master key
        - Uses AES (Advanced Encryption Standard)
            - WPA2 is currently recommended
        - Client and AP negotiate a new key
- MAC address filtering
    - May prevent casual users from connecting

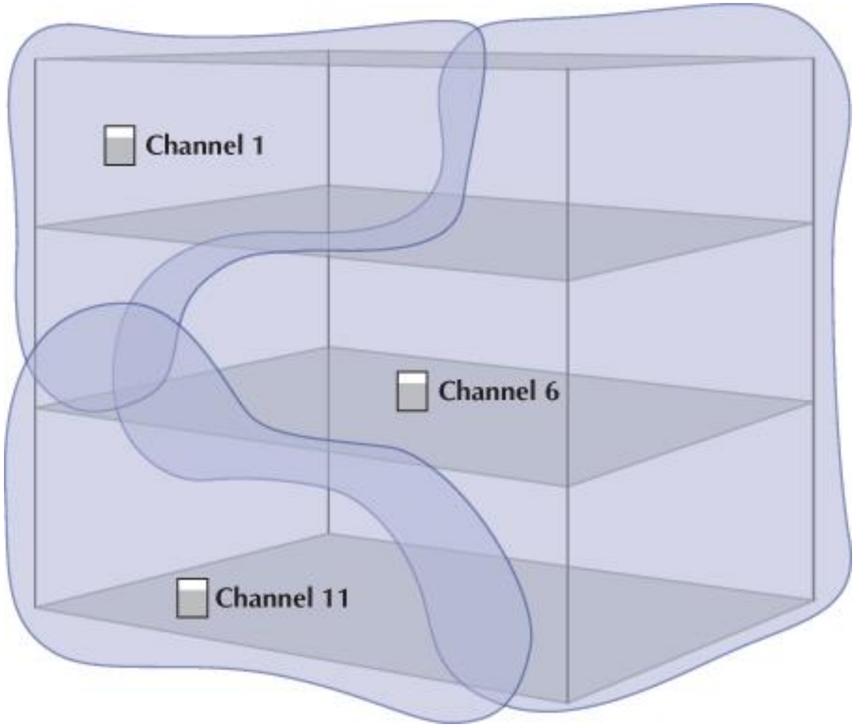
LAN Design

- Current best practice is to use wired LANs for primary network and wireless as an overlay network
- Select fastest stable technology, cost permitting
  - e.g., choose 802.11ac over 802.11n or 1000BASE-T over 100BASE-T
- Physical WLAN design
  - More challenging than LANs because of interference
  - Start with **site survey** to determine:
    - Coverage required
    - Potential sources of interference
    - Locations of wired hubs/switches and power sources
    - Number of APs needed

LAN Design



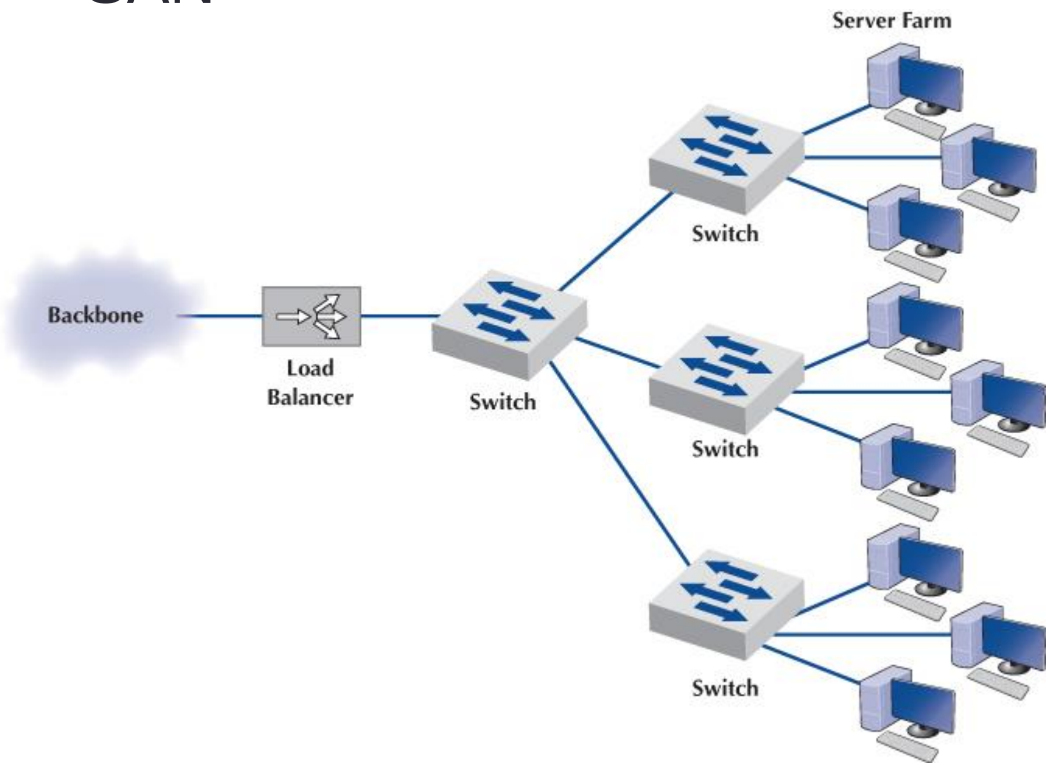
450 ft
6 1 6 11 6 1
150 ft
1 11 1 6 1 11
300 ft
11 6 1
6 1 11
150 ft
11 6 1
150 ft

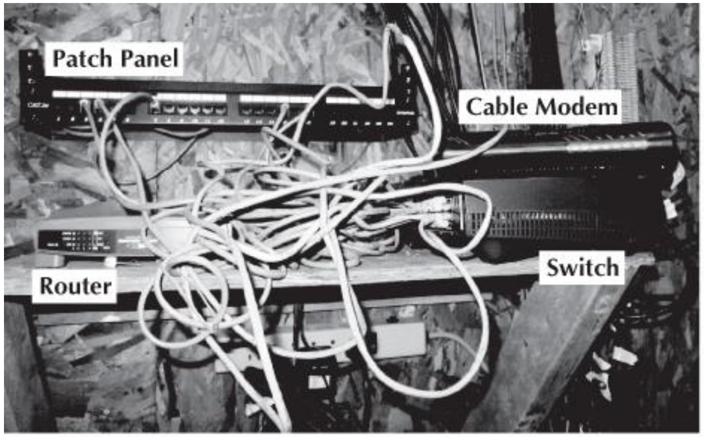


Channel 1
Channel 6
Channel 11

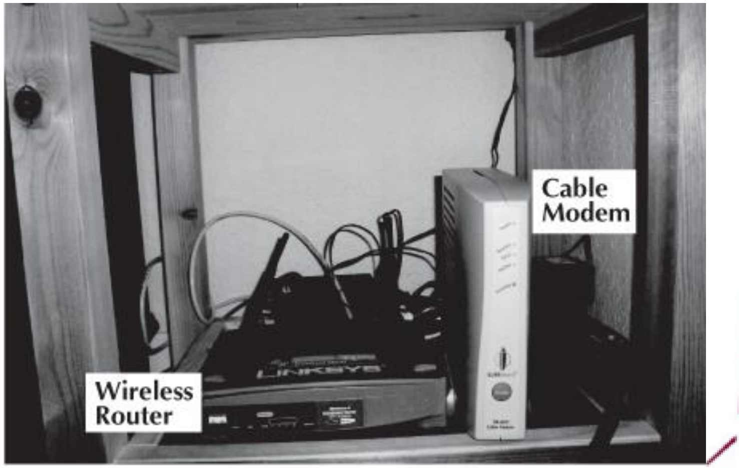
LAN Design

- LANs may have very different requirements
  - Load balancers
  - Virtualization
  - Security
  - SAN





(a) Alan's home network



(b) Alexandra's home network

Improving LAN Performance

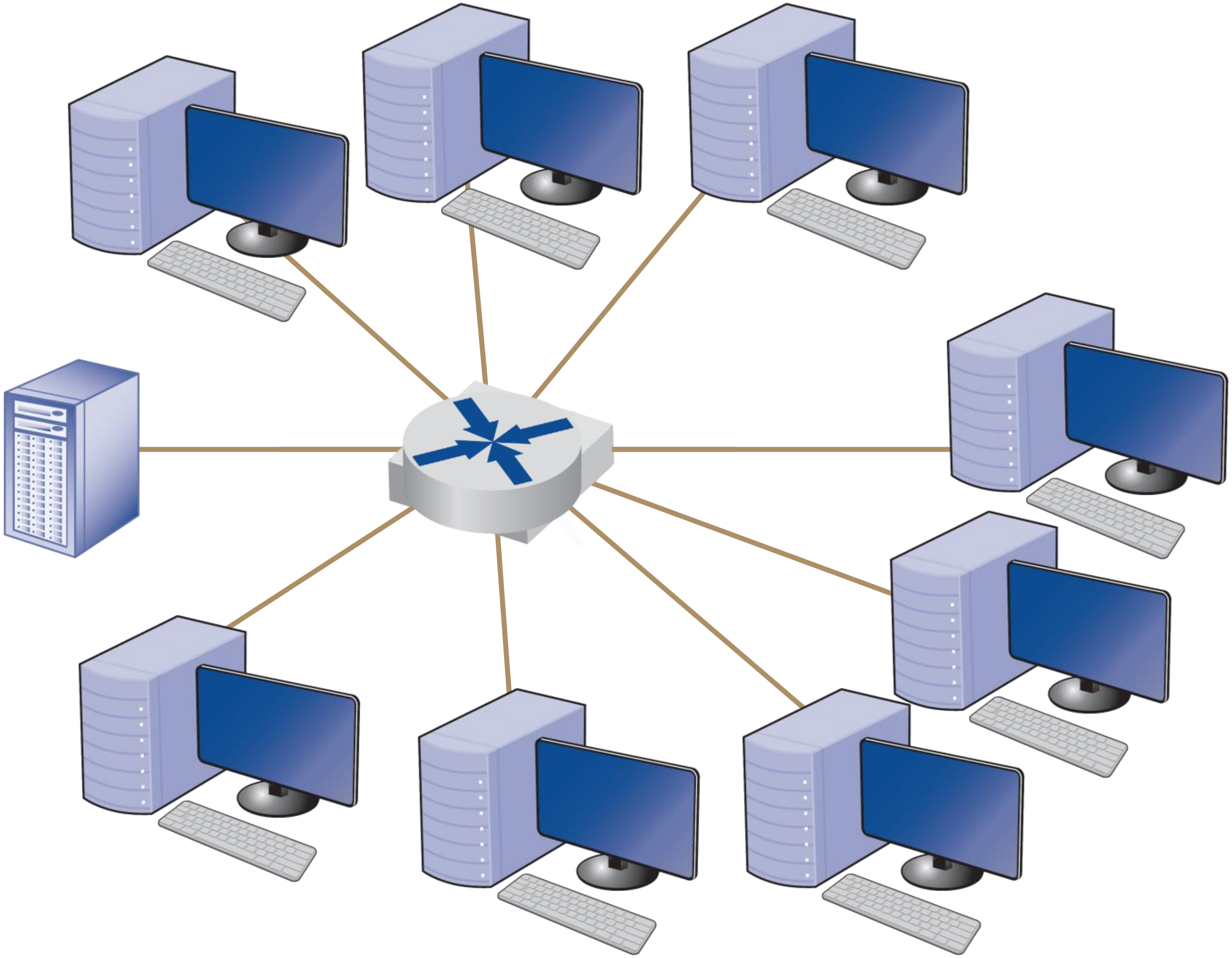
- How can we improve **throughput**, the total data transmitted in a given period of time?
  - Identify **bottlenecks**
    - The parts of the network restricting data flow
    - **Devices**
      - Servers (check CPU and disk performance)
      - Clients
      - Networking devices
    - **Circuits**
    - **Demand**

Improving LAN Performance

- Devices
    - Upgrade server
        - Software and hardware (CPU, memory, disks)
        - Redundant array of inexpensive disks (RAID)
    - Add a new server
    - Upgrade clients
- Circuits
    - Buy faster circuit (e.g., 100BASE-T to 1000BASE-T)
    - Add circuits
    - Add access points on different channels
    - Segment network

Improving LAN Performance

Network Segmentation



Improving LAN Performance

- Reducing network demand
  - Move files to client computers
  - Encourage off-peak usage
  - Consider blocking or throttling unnecessary network traffic

Implications for Management

- Enterprise LAN equipment is quickly becoming a commodity
- SOHO users are primarily moving to wireless
  - Speeds have increased
  - Dramatic growth of WiFi-enabled devices
- The Internet of Things will influence LAN design

Implications for Cyber Security

- Securing LAN

- Securing WLAN