Business Data Communications & Networking:

12th Edition

Chapter 7: Wired and Wireless LANs

Sadiq M. Sait, PhD
Professor
College of Computer Sciences and Engineering
Director, Industry Collaboration

Fall 2022

OBJECTIVES

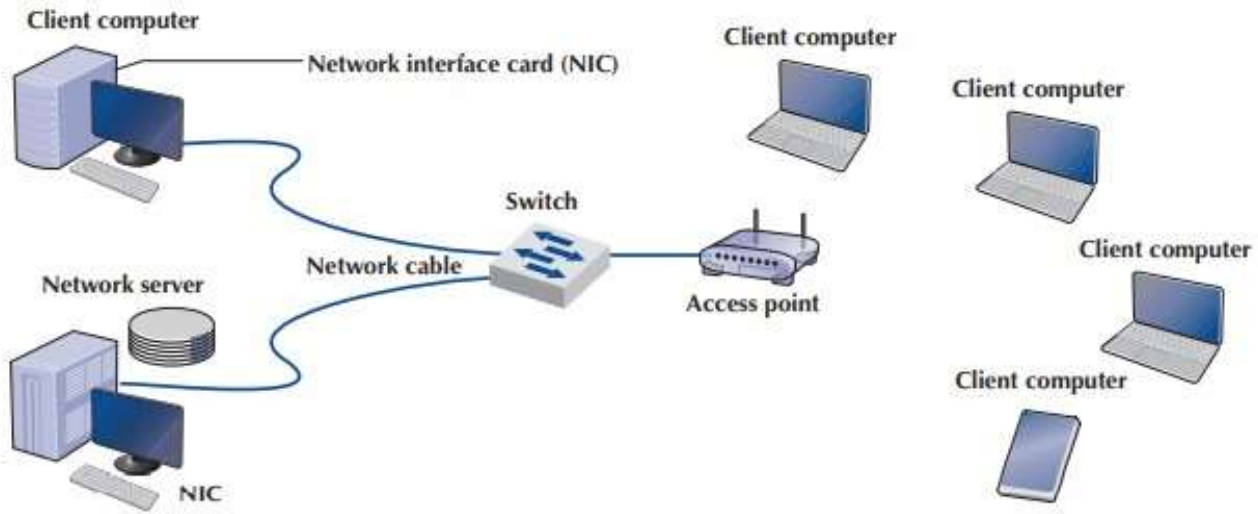
- In this chapter we examine the 3 major network architecture components that use Local Area Networks (LANs):
  - the LANs that provide network access to users,
  - the data center, and
  - the e-commerce edge.
- We focus on the LANs that provide network access to users as these are more common.
- Learn how wired and wireless LANs work.
- What are the major components of LANs?
- The two most commonly used **LAN technologies: wired and wireless Ethernet**.
- How to design LANs and **improve their performance?**

- Objectives:
  a) Understand the major components of LANs
  b) Understand the best practice recommendations for LAN design
  c) Be able to design wired Ethernet LANs
  d) Be able to design wireless Ethernet LANs
  e) Be able to improve LAN **performance**

7.2 LAN Components t

- There are several components in a traditional LAN (Figure 7-1 below).
- **The first two are the client computer and the server.**
- **The other components are network interface cards (NICs), network circuits, hubs/switches/access points, and the network operating system.**
- The network interface card (**NIC**) is used to connect the computer to the network cable in a wired network and is one part of the physical layer connection among the computers in the network.
- **In a wireless network, the NIC is a radio transmitter** that sends and receives messages on a specific radio frequency.
- **All desktop computers have a wired NIC built in, while virtually all laptops have both a wired NIC and a wireless NIC.**
- You can purchase a **wireless NIC for a desktop computer (often a USB device).**

FIGURE 7-1
Local area network components



7.2.2 Network Circuits (Wireless LANs)

- **Wireless LANs (WLANs) use radio transmissions to send data between the NIC and the access point (AP). [ALOHA]**
- Most countries (but not all) permit WLANs to operate in two frequency ranges: the **2.4 and 5 GHz range.**
  - These same frequency ranges can be used by **cordless phones** and **baby monitors**, which means that your WLAN and your cordless phone may **interfere** with each other.
- Under **ideal** conditions, the radio transmitters in the NICs and APs can **transmit 100–150 meters (300–450 feet).**
- In practice, the range is much shorter as walls absorb (**attenuate**) the radio waves.
- The other problem is that as the distance from the AP increases, the maximum **speed drops, often very dramatically**. **When we design a WLAN, each AP is set to transmit on a different channel, very much like the different channels on your TV. Each channel uses a different part of the 2.4 or 5GHz frequency range.**
- **When a computer first starts using the WLAN, its NIC searches all available channels within the appropriate frequency range and then picks the channel that has the strongest signal.**

7.2.3 Network Hubs, Switches, and Access Points

- **First**, a hub or a switch can be thought of as a **junction box**, permitting new computers to be connected to the network as easily as plugging a power cord into an electrical socket.

- **Each connection point where a cable can be plugged in is called a port. Each port has a unique number.**

- Switches can be designed for use in small-office, home-office (SOHO) environments (see Figure 7-2a) or for large enterprise environments (see Figure 7-2b).

- **Second**, hubs and switches act as **repeaters**. All LAN cables are rated for the maximum distance they can be used (typically 100 meters for twisted-pair cable, and, 400 meters to several Kilometers for fiber-optic cable).

7.2.3 Network Hubs, Switches, and Access Points (contd)

- A wireless access point is a radio transceiver that plays the same role as a hub or switch in wired Ethernet LANs.

- It enables the computers near it to communicate with each other and it also connects them into wired LANs, typically using 100Base-T or 1000Base-T.

- **All NICs in the WLAN transmit their frames to the AP, and then the AP retransmits the frames over the wireless network or over the wired network to their destination.**
  - AP for use in SOHO environments has a separate power supply while an AP for use in large enterprises uses **Power Over Ethernet (POE),** the power is provided from a POE switch over the unused wires in a category 5/5e cable.
  - POE APs are more expensive, but can be located anywhere you can run Cat 5/5e cable, even if there are no power outlets nearby.

7.2.4 Network Operating Systems (NOS)

- The network operating system (NOS) is the software that controls the network.
  - Every NOS provides two sets of software: one that runs on the network server(s) and one that runs on the network client(s).
  - The server version of the NOS provides the software that performs the functions associated with the **data link, network, and application layers and usually the computer's own operating system.**
  - The client version of the NOS provides the software that performs the functions associated with the **data link and the network layers and must interact with the application software and the computer's own operating system.**
  - Most NOSs provide **different versions** of their client software that run on different types of computers, so that Windows computers, for example, can function on the same network as Apple computers.
  - In most cases (e.g., Windows and Linux), the client NOS software is included with the operating system itself.

7.2.4 Network Operating Systems (NOS) (contd).

- One of the most important functions of a NOS is a directory service.
  - **Directory services** provide **information about resources** on the network that are available to the users, such as shared printers, shared file servers, and application software.
- **A common example of directory services is Microsoft's Active Directory Service** (ADS).
- Active Directory Service works in much the same manner as **TCP/IP's DNS** service, and in fact ADS servers, called domain controllers, can also act as DNS servers.

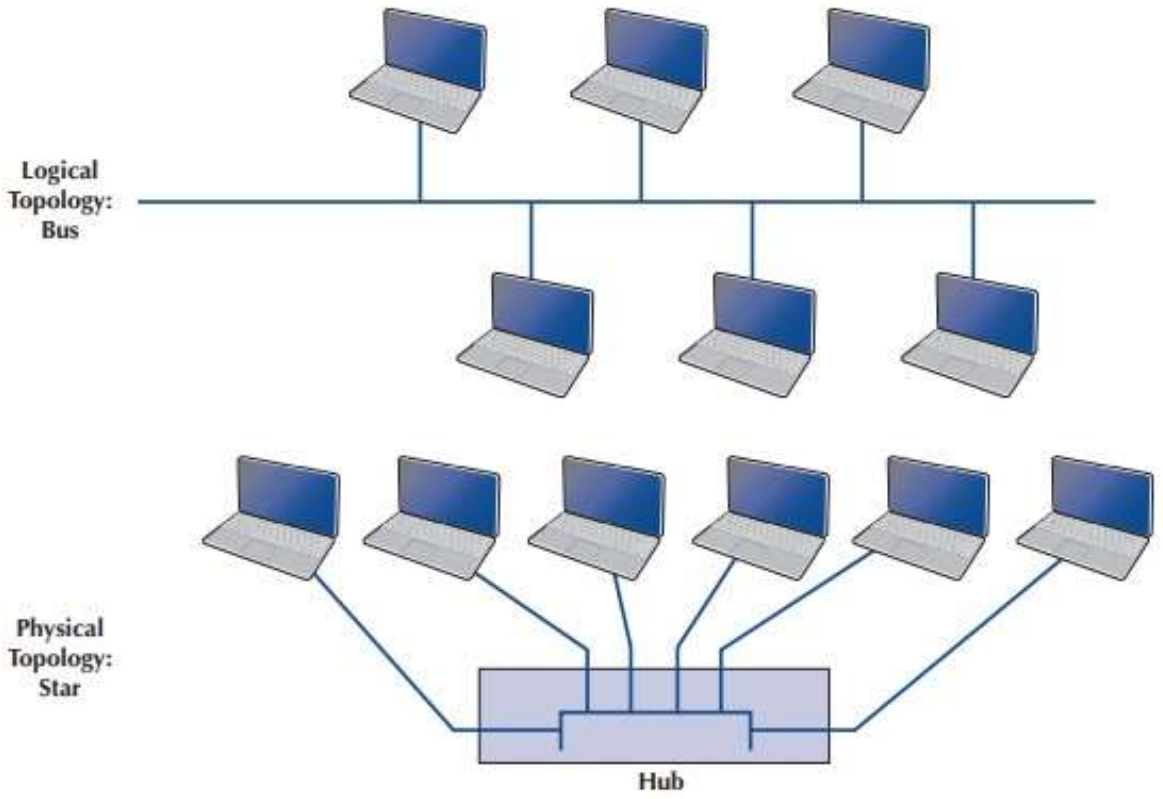
7.3.1 WIRED ETHERNET --- Topology

- **Topology is the basic geometric layout of the network**—the way in which the computers on the network are interconnected.
- It is important to distinguish between a **logical topology and a physical topology**.

7.3.1 WIRED ETHERNET --- Hub Based Ethernet

- When we use hubs, Ethernet's logical topology is a **bus** topology.
- All computers are connected to one half-duplex circuit running the length of the network which is called the bus.
- The top part of Figure 7-4 shows Ethernet's logical topology.
  - All frames from any computer flow onto the central cable (or bus) and through it to all computers on the LAN.
- Every computer on the bus receives all frames sent on the bus, even those intended for other computers.
- Before processing incoming frames, **the Ethernet software on each computer checks the data link layer address** and processes only those frames addressed to that computer.
- The bottom part of Figure 7-4 shows the physical topology of an Ethernet LAN when a hub is used.
- From the outside, an Ethernet LAN appears to be a **star topology**, nonetheless, it is logically a bus.
- With hubs, all computers share the same **multipoint circuit (called collision domain)** and must take turns using it.
- When one computer transmits, other computers wait, which is inefficient (all frames are sent to all computers in the same collision domain.
- Security is a problem because any frame can be read by any computer.
- Wireless Ethernet works much the same as hub-based Ethernet.

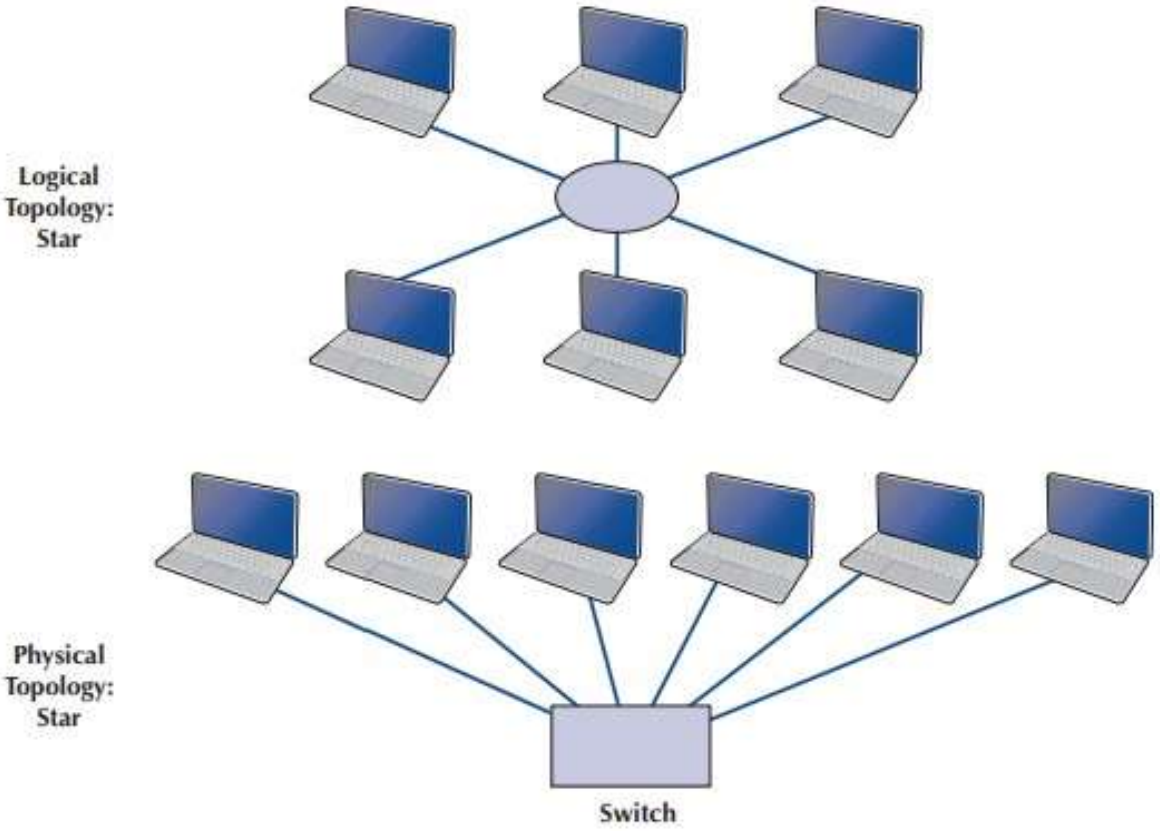
FIGURE 7-4
Ethernet topology using hubs



7.3.1 WIRED ETHERNET --- Switch Based Ethernet

- When we use switches, Ethernet's topology is a logical star and a physical star (Figure 7-5).
- From the outside, the switch looks almost identical to a hub, **but inside, it is very different**.
- A switch is an intelligent device with a small computer built in that is designed to manage a set of separate point-to-point circuits.
- That means that each circuit connected to a switch is **not shared** with any other devices; only the switch and the attached computer use it.
- The physical topology looks essentially the same as Ethernet's physical topology: a star. On the inside, the logical topology is a set of separate point-to-point circuits, also a star.
- **Many switches support full duplex circuits.** When a switch receives a frame from a computer, it looks at the address on the frame and retransmits the frame only on the circuit connected to that computer, not to all circuits as a hub would.
  - Therefore, no computer needs to wait because another computer is transmitting; every computer can transmit at the same time, resulting in much faster performance.
  - Today, no one buys a hub unless she or he can't afford a switch.
  - So how does a switch know which circuit is connected to what computer?

FIGURE 7-5
Ethernet topology using switches



7.3.1 WIRED ETHERNET --- Switch Based Ethernet

- So how does a switch know which circuit is connected to what computer? **The switch uses a forwarding table that is very similar to the routing tables.**
- The table lists the **Ethernet address** of the computer connected to each port on the switch.
- When the switch receives a frame, it compares the destination address on the frame to the addresses in its forwarding table to find the port number on which it needs to transmit the frame (hence called a layer-2 switch)
- **Switches learn addresses to build the forwarding table.**
- If a switch receives a frame with a destination address that is not in the forwarding table, the switch must still send the frame to the correct destination. In this case, it must retransmit the frame to **all** ports, except the one on which the frame was received.
- The attached computers, being Ethernet and assuming they are attached to a hub, will simply ignore all frames not addressed to them.
- The one computer for whom the frame is addressed will recognize its address and will process the frame, which includes sending an acknowledgement (ACK) or a negative acknowledgement (NAK) back to the sender.

7.3.1 WIRED ETHERNET --- Switch Based Ethernet

- There are three modes in which switches can operate. The **first** is cut-through switching, the switch begins transmitting before it has received the entire frame.
  - The advantage is low latency (the time it takes a device from receiving a frame to transmitting it) which results in a very fast network.
  - The disadvantage is that the switch begins transmitting before it has read and processed the **frame check sequence**.
  - Can only be used when the incoming data circuit has the same data rate as the outgoing circuit.
- With the **second** switching mode, called **store and forward** switching.
  - Here the switch does not begin transmitting the outgoing frame until it has received the **entire incoming frame and has checked** to make sure it contains no errors.
  - **If errors are found, the switch simply discards the frame.**
  - This mode has higher latency and thus results in a slower network (unless many frames contain errors).
  - Store and forward switching can be used **regardless** of whether the incoming data circuit has the same data rate as the outgoing circuit

7.3.1 WIRED ETHERNET --- Switch Based Ethernet

- The final mode, called **fragment-free switching**, lies **between** the extremes of cut-through switching and store and forward switching.
  - With fragment-free switching, **the first 64 bytes of the frame are read and stored**. **The switch examines the first 64 bytes** (which contain all the header information for the frame), **and if all the header data appear correct, the switch presumes that the rest of the frame is error free and begins transmitting.**
  - Fragment-free switching is a **compromise** between cut-through and store and forward switching because it has higher latency and better error control than cut-through switching, but lower latency and worse error control than store and forward switching.
    - **Most switches today use cut-through or fragment-free switching**

7.3.2. Media Access Control (MAC)

- What is MAC?
  - **When several computers share the same collision domain (i.e., multipoint circuit), it is important to control their access to the media.**
  - If two computers on the same circuit transmit at the same time, their transmissions will become **garbled**.
  - These collisions must be prevented, or if they do occur, there must be a way to recover from them.
  - This is called media access control.
- Ethernet uses **Carrier Sense Multiple Access with Collision Detection (CSMA/CD).**
- CSMA/CD, like all contention-based techniques, is very simple in concept: **wait until the circuit is free and then transmit**.
- Ethernet's CSMA/CD protocol can be termed "**ordered chaos**."
- **As long as no other computer attempts to transmit at the same time, everything is fine.**

7.3.2. Media Access Control (MAC) (contd)

- However, it is possible that two computers located some distance from one another begin sending simultaneously (this is called a collision).
- The two frames collide and destroy each other.
- The solution to this is to **listen while transmitting**, better known as **collision detection (CD).**
- If the NIC detects any signal other than its own, it presumes that a collision has occurred and sends a **jamming** signal.

7.4 WIRELESS ETHERNET (WiFi)

- **Wireless Ethernet** is the commercial name for a set of standards developed by the IEEE 802.11 standards group.
- The 802.11 family of technologies is much like the Ethernet family.
- Just as there are several different types of Ethernet (e.g., 10Base-T, 100Base-T, and 1000Base-T), there are several different types of 802.11.

7.4 WIRELESS ETHERNET (WiFi)

- **Topology: Same as hub-based wired ethernet**
- Media Access Control: CSMA/CD. But detection of collision is more difficult in radio.
  - This is why WiFi attempts to avoid a collision.
  - ***Before a computer can transmit in a WLAN, it must first establish an association with a specific AP, so that the AP will accept its transmissions.***
- Searching for an available AP is called **scanning**.
  - Two types of scanning: **Active and Passive.**
    - During active scanning **NIC sends** a ***probe frame***.
    - During passive scanning, the **NIC listens** on all channels for a special frame called a ***beacon frame*** that is sent out by an access point.
  - The beacon frame contains all the necessary information for a NIC to associate with it.

7.5 THE BEST PRACTICE LAN DESIGN

- **Today, we still believe the best practice is to use wired Ethernet for the primary LAN, with Wi-Fi as an overlay network.**
- Many organizations today install switched 100Base-T or 1000Base-T over category 5e wiring for their wired LANs. It is relatively low cost and fast.
- Selecting the best practice wireless technology is usually simple. **You pick the newest one, cost permitting.**
- The physical WLAN design begins with a site survey which determines the
  - feasibility of the desired coverage
  - potential sources of interference
  - current locations of the wired network into which the WLAN will connect, and
  - an estimate of the number of APs required to provide coverage.

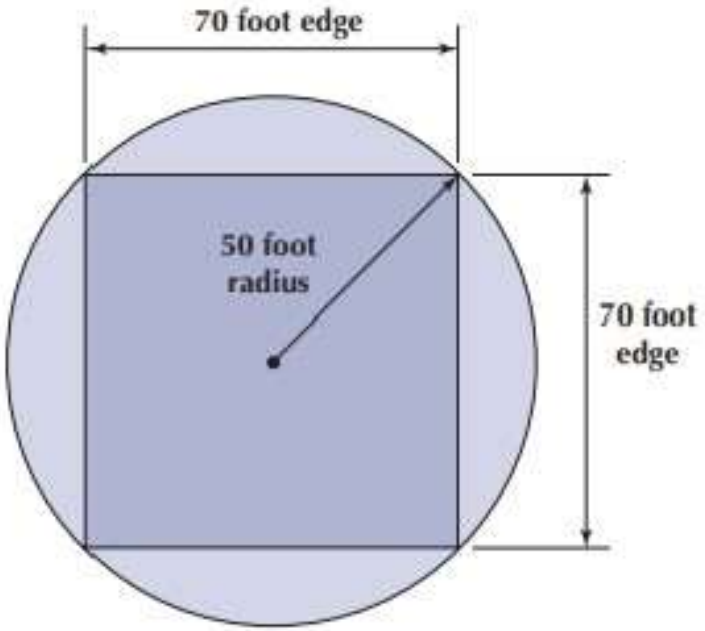
7.5.2 Designing User Access with Wireless Ethernet (contd) EXTRA

- WLANs work very well when there is a clear line of sight between the AP and the wireless computer.
- The more walls there are between the AP and the computer, the weaker the wireless signal becomes (attenuation).
- An access point with an **omnidirectional** antenna broadcasts in all directions. **Its coverage area is a circle with a certain radius.**
- Wi-Fi has a long-range, but real-world tests of Wi-Fi in typical office environments have shown that data rates slow down dramatically when the distance from a laptop to the AP exceeds **50 feet**.
- It is also expensive because **many** APs will need to be purchased.
- Costs may be reduced by using a longer radius (e.g., 100 feet), so that fewer APs are needed, but this may result in slower data rates.
- One may design wireless LANs using this 50-foot radius circle, but because most buildings are **square**, it is usually easier to design using squares.

7.5.2 Designing User Access with Wireless Ethernet (contd) EXTRA

- Figure 7-8 shows that a 50-foot radius translates into a square that is approximately 70 feet on each edge. Smaller squares in areas where there are more walls that can cause more interference and larger squares in areas with fewer walls

FIGURE 7-8
Design parameters for Wi-Fi access point range



7.5.2 Designing User Access with Wireless Ethernet (contd) EXTRA

- Below is a sample building. The lower left corner is a 150 feet sq, while the rest of the building is a 150 feet×450 feet rectangle. Assume that the large rectangle part is an open office environment (we can use 75-ft square), while the smaller part uses drywall (use 50-ft square).
- It is important to ensure that the APs don't interfere with each other.
- Each AP is set to transmit on a different channel, (3 commonly used are 1, 6, and 11) so there is minimal overlap between APs using the same channel.
- After the initial design is complete, a site survey is done using a temporary APs.

FIGURE 7-9
A Wi-Fi design (the numbers indicate the channel numbers)

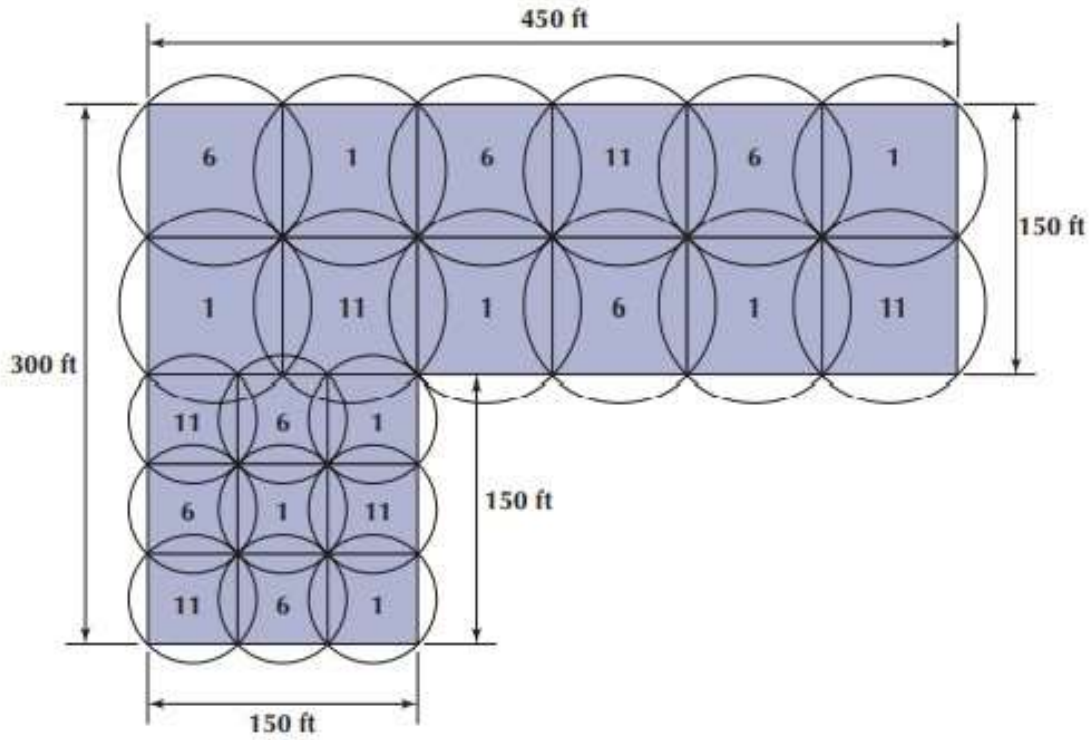
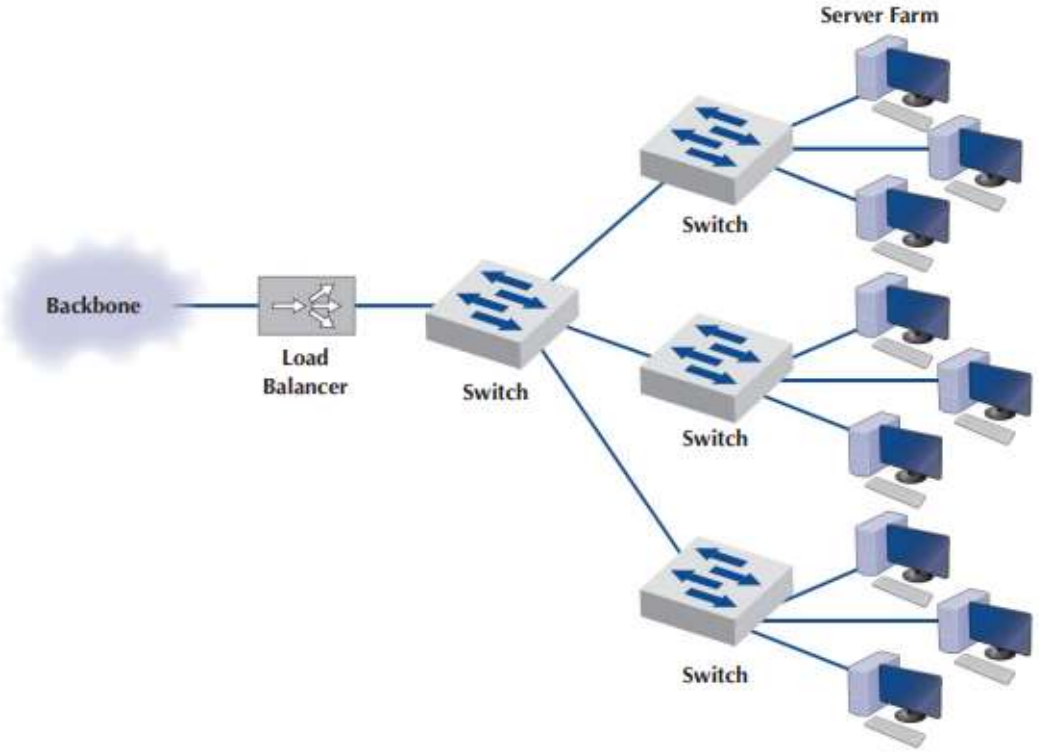


Figure 7-12: Network with Load Balancer EXTRA

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



7.6 IMPROVING LAN PERFORMANCE

- When LANs had only a few users, performance was usually very good.
- Today, however, when most computers in an organization are on LANs, performance can be a problem.
- Performance is usually expressed in terms of
  - throughput (the total amount of user data transmitted in a given time period) or
  - in response time (how long it takes to get a response from the destination).
- how to improve throughput?
  - Let us focus on dedicated-server networks because they are the most commonly used type of LANs,
- To improve performance, you must locate the bottleneck, the part of the network that is restricting the data flow.
- Generally speaking, the bottleneck will lie in one of two places.
  - The first is the network server.
  - The second location is a network circuit

7.6 IMPROVING LAN PERFORMANCE (contd).

- The first is the network **server**.
  - In this case, the client computers have no difficulty sending requests to the network **server**, but the server **lacks sufficient capacity** to **process** all the requests it receives in a timely manner.
- The second location is a network **circuit**
  - Either the access LAN, the building backbone, the campus backbone, or the circuit into the data center (server can easily process all the client requests it receives, but a **circuit lacks enough capacity to transmit all the requests to the server.**
- The first step in improving performance is to identify whether the bottleneck lies in a circuit or the server. How?
  - To do so, you simply **watch the utilization of the server during periods of poor performance.**
    - If the server utilization is high (e.g., 80–100%), then the bottleneck is the server; it cannot process all the requests it receives in a timely manner.
    - If the server utilization is low during periods of poor performance, then the problem lies with a network circuit;
  - Most organizations focus on ways to improve the server and the circuits to remove bottlenecks.
  - These actions address the supply side of the equation—The other way is to attack the demand side: reduce the amount of network use by the clients.

7.6.3 REDUCING NETWORK DEMAND

- One way to **reduce network demand is to move files to client computers.**
- Heavily used software packages that continually access and load modules from the network can place unusually heavy demands on the network.
- Placing even one or two such applications on client computers can greatly improve network performance (although this can create other problems, **such as**?).
- Most organizations now provide **both wired and wireless networks**, so another way to reduce demand is to shift it from wired networks to wireless networks, or vice versa, depending on which has the problem.
  - For example, you can encourage wired users to go wireless or install wired Ethernet jacks in places where wireless users often sit.
- Because the demand on most LANs is uneven, network performance can be improved by attempting to move user demands from peak times to off-peak times.
  - For example, early morning and after lunch are often busy times when people check their email.
  - Telling network users about the peak times and encouraging them to change their habits may help (easier said than done).
  - Finding one application that places a large demand on the network and moving it can have a significant impact (e.g., printing several thousand customer records after midnight).