

# Chapter Nine

Introduction to Metropolitan Area  
Networks and Wide Area Networks

Data Communications and Computer  
Networks: A Business User's Approach  
Seventh Edition

After reading this chapter,  
you should be able to:

- Distinguish local area networks, metropolitan area networks, and wide area networks from each other
- Identify the characteristics of metropolitan area networks and compare to LANs and WANs
- Describe how circuit-switched, datagram packet-switched, and virtual circuit packet-switched networks work
- Identify the differences between connection-oriented and connectionless networks

After reading this chapter,  
you should be able to:

- Describe the differences between centralized and distributed routing
- Describe the differences between static and adaptive routing
- Document the main characteristics of flooding and use hop count and hop limit in a simple example
- Discuss the basic concepts of network congestion, including quality of service

# Introduction

- As we have seen, a **local area network** covers a room, a building or a campus.
- A metropolitan area network (**MAN**) covers a city or a region of a city.
- A wide area network (**WAN**) covers multiple cities, states, countries, and even the solar system.

# Metropolitan Area Network Basics

- MANs **borrow technologies** from LANs and WANs.
- MANs support high-speed disaster recovery systems, real-time transaction backup systems, interconnections between corporate data centers and Internet service providers, and government, business, medicine, and education high-speed interconnections.
- Almost exclusively fiber optic systems

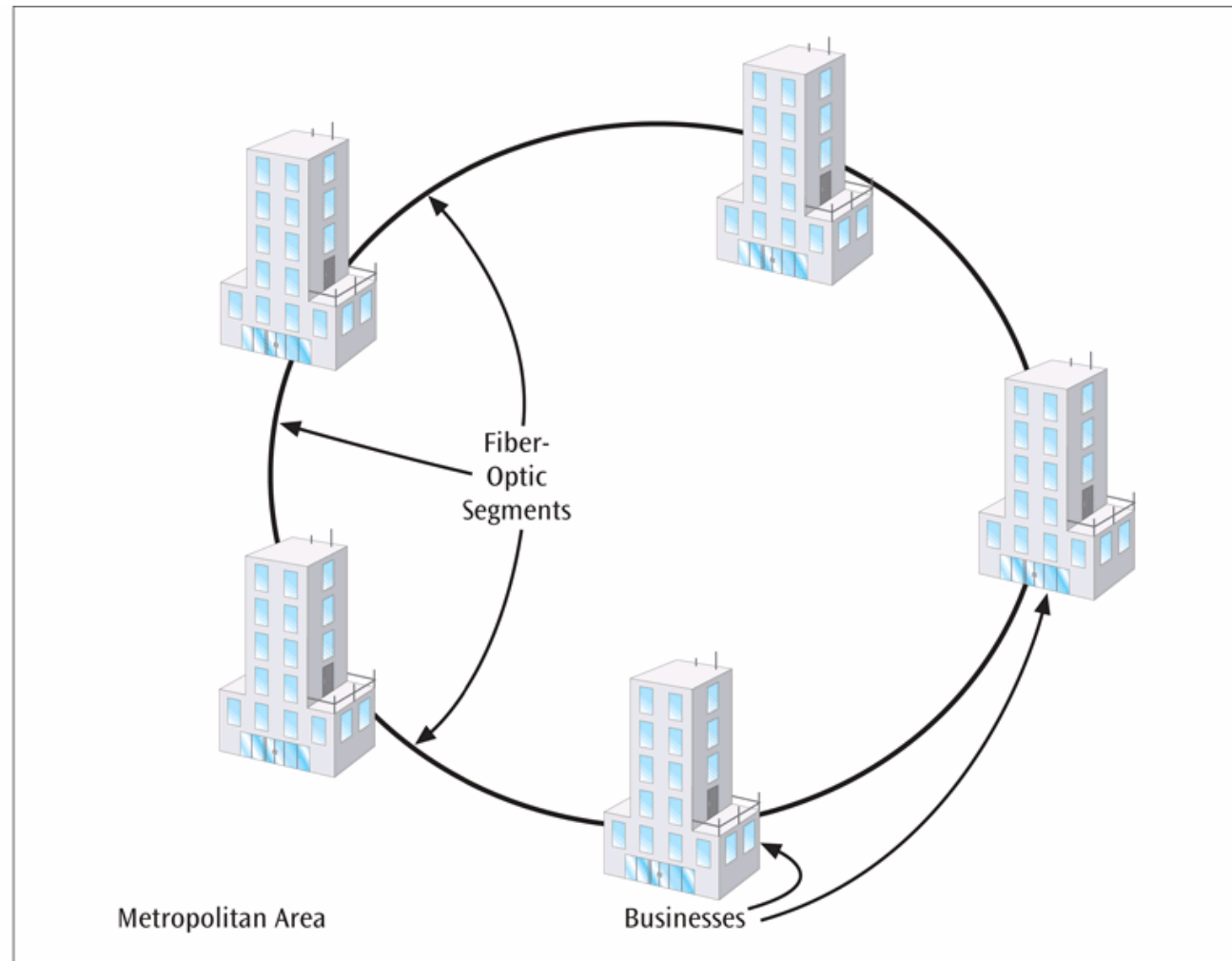
# Metropolitan Area Network Basics

- MANs have **very high** *transfer speeds*
- MANs can recover from network faults very quickly (failover time)
- MANs are very often a **ring** topology (not a star-wired ring)
- Some MANs can be provisioned dynamically

# Metropolitan Area Network Basics

**Figure 9-1**

*A physical ring  
used to support a  
metropolitan area  
network*



# SONET versus Ethernet MANs

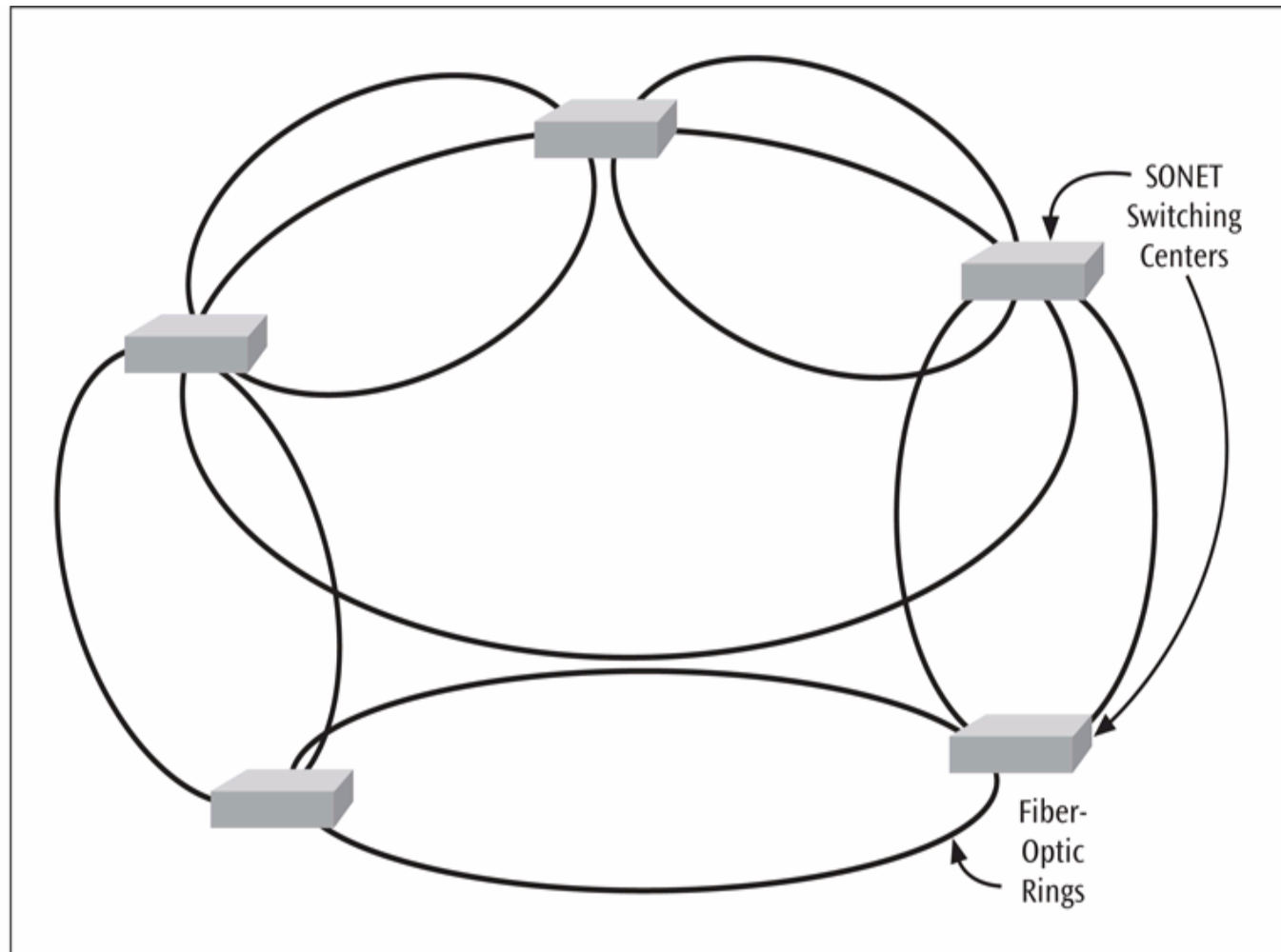
- Most MANs are SONET network built of multiple rings (for failover purposes)
- SONET is well-proven but complex, fairly expensive, and cannot be provisioned dynamically.
- SONET is based upon T-1 rates and does not fit nicely into 1 Mbps, 10 Mbps, 100 Mbps, 1000 Mbps chunks, like Ethernet systems do.
- Ethernet MANs generally have high failover times



# SONET versus Ethernet MANs

**Figure 9-2**

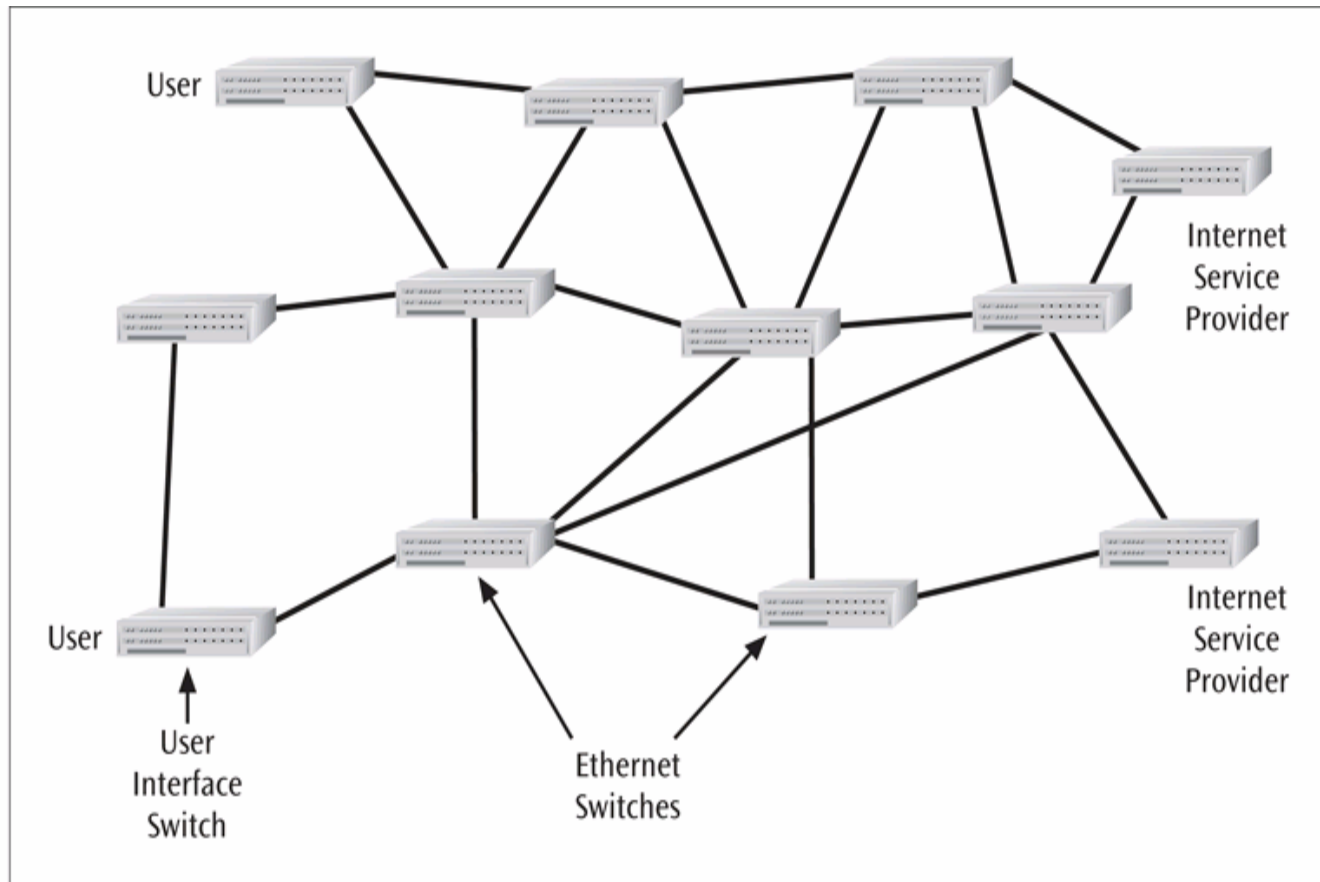
*SONET systems are comprised of multiple rings*



# SONET versus Ethernet MANs

**Figure 9-3**

*The Ethernet MAN topology*

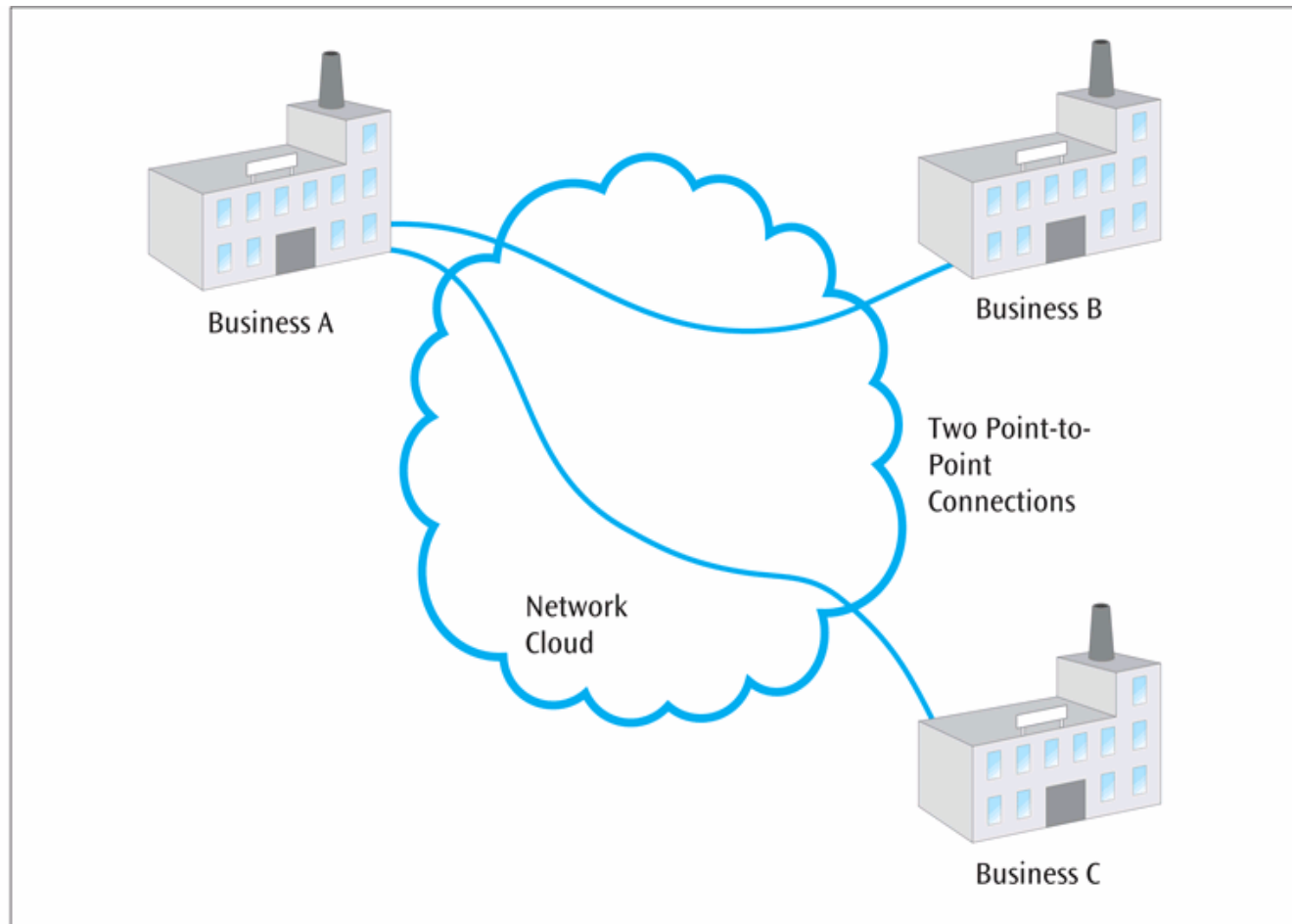


# Metro Ethernet

- One of the latest forms of the metropolitan area network is *metro Ethernet*
- Metro Ethernet is a service in which the provider creates a door-to-door Ethernet connection between two locations
- For example, you may connect your business with a second business using a point-to-point Ethernet connection (Figure 9-4a)

# Metro Ethernet

**Figure 9-4 (a)**  
*Two point-to-point connections*

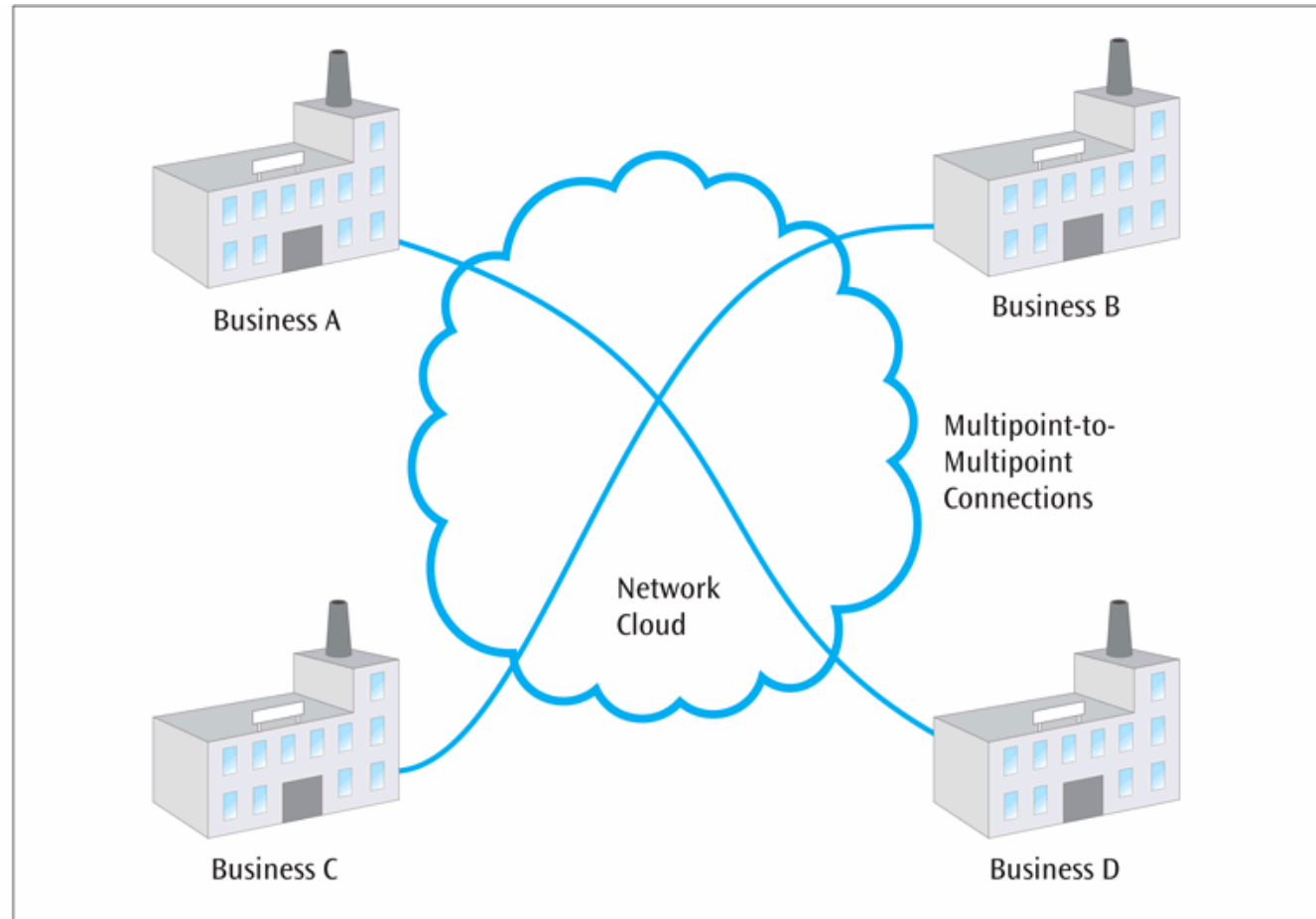


# Metro Ethernet

- You may also connect your business with multiple businesses using a connection similar to a large local area network (Figure 9-4b)
- Thus, by simply sending out one packet, multiple companies may receive the data
- Neat thing about metro Ethernet is the way it seamlessly connects with a company's internal Ethernet network(s)

# Metro Ethernet

**Figure 9-4 (b)**  
*Multipoint-to-multipoint connections*



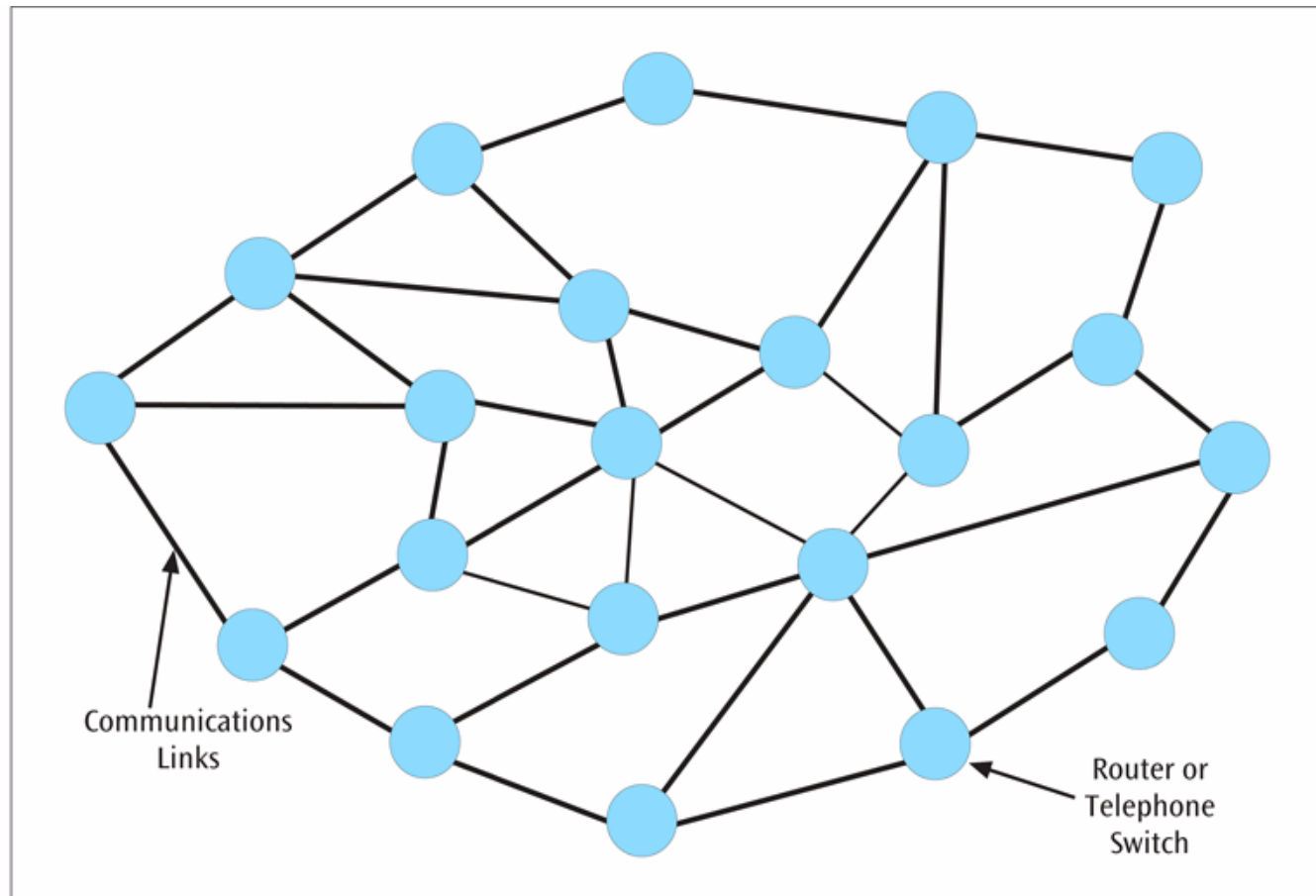
# Wide Area Network Basics

- WANs used to be characterized with **slow**, **noisy** lines.
- Today WANs are **very high speed** with very **low error rates**.
- WANs usually follow a **mesh** topology.

# Wide Area Network Basics

**Figure 9-5**

*A simple mesh network*





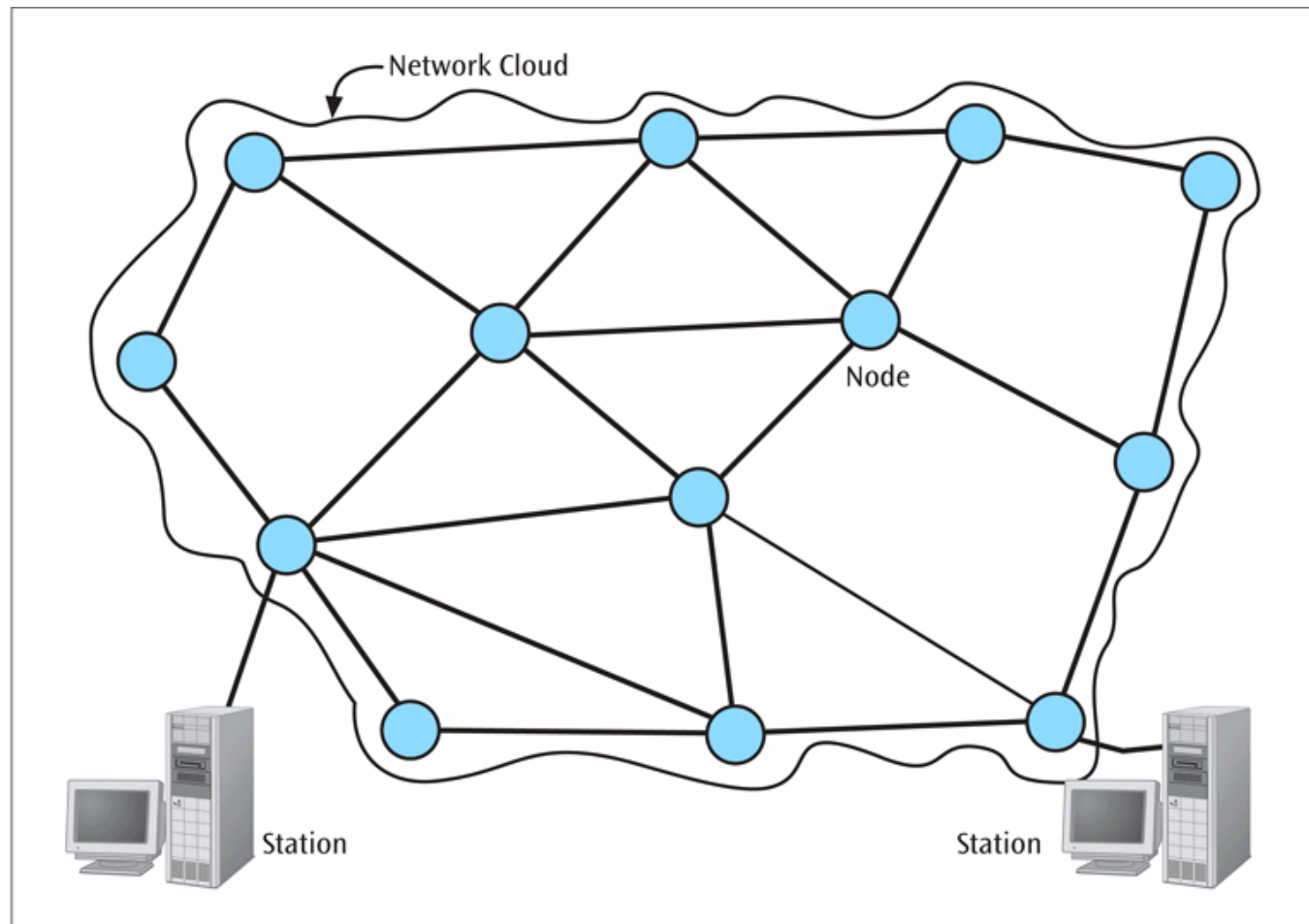
# Wide Area Network Basics

- A **station** is a device that interfaces a user to a network.
- A **node** is a device that allows one or more stations to access the physical network and is a transfer point for passing information through a network.
- A node is often a computer, a router, or a telephone switch.
- The **sub-network** or physical network is the underlying connection of nodes and telecommunication links.

# Wide Area Network Basics

**Figure 9-6**

*Network cloud, nodes, and two end stations*



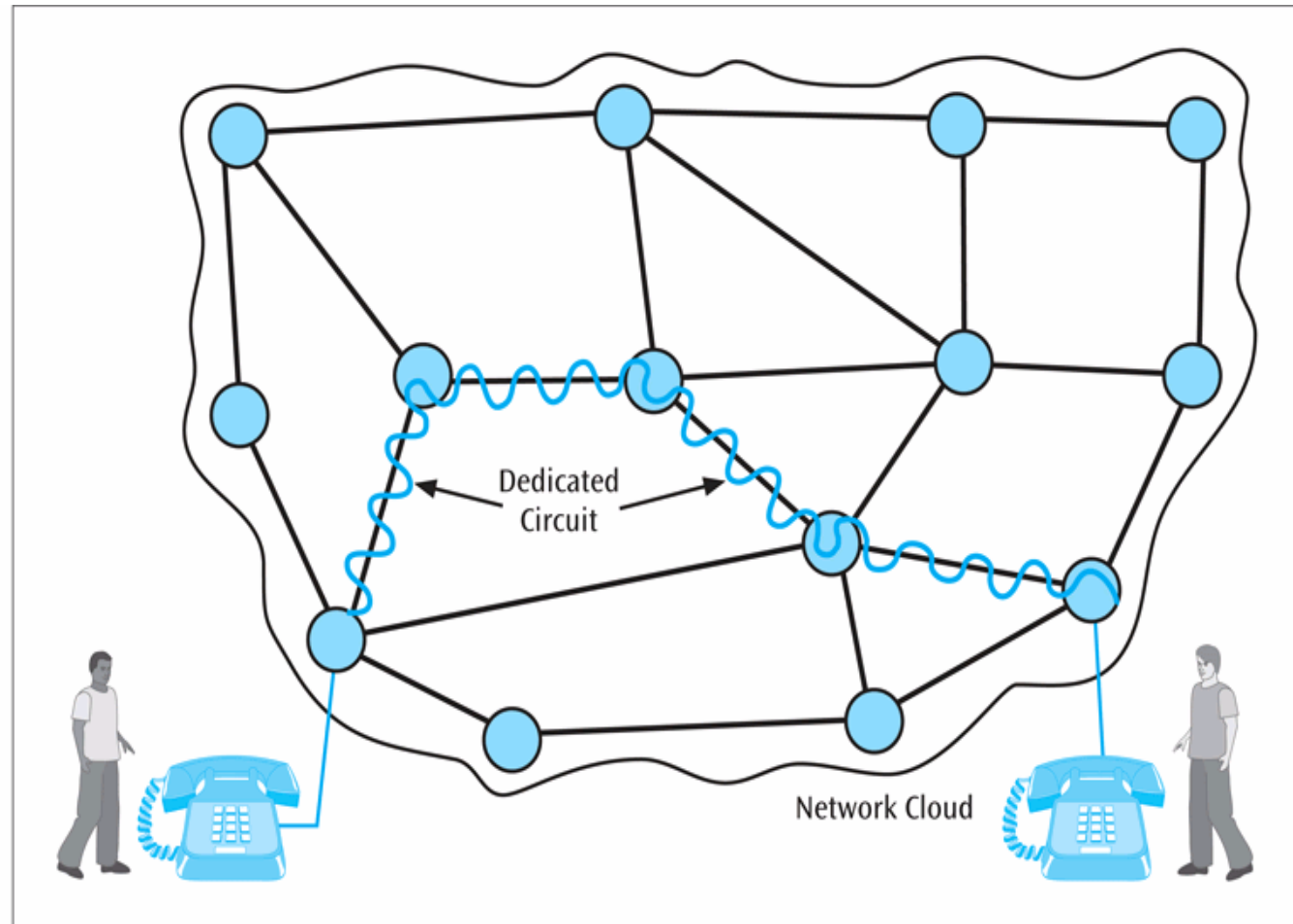
# Types of Network Structures

- **Circuit switched network** - a sub-network in which a dedicated circuit is established between sender and receiver and all data passes over this circuit.
- The telephone system is a common example.
- The connection is **dedicated** until one party or another terminates the connection.
- AT&T announced end of 2009 that they will begin phasing out their switched networks

# Types of Network Structures

**Figure 9-7**

*Two people carrying on a telephone conversation using a circuit-switched network*



# Types of Network Structures

- ***Packet switched network*** - a network in which all data messages are transmitted using fixed-sized packages, called packets.
- More efficient use of a telecommunications line since packets from multiple sources can **share** the medium.
- One form of packet switched network is the ***datagram***. With a datagram, each packet is on its own and may follow its own path.
- ***Virtual circuit*** packet switched network create a logical path through the subnet and all packets from one connection follow this path.

# Types of Network Structures

- **Broadcast network** - a network typically found in local area networks but occasionally found in wide area networks.
- A workstation transmits its data and all other workstations “connected” to the network hear the data. Only the workstation(s) with the proper address will accept the data.

# Summary of Network Structures

**Table 9-1**

*Summary of network cloud characteristics*

| Characteristic                              | Circuit-Switched | Datagram<br>Packet-Switched | Virtual Circuit<br>Packet-Switched | Broadcast            |
|---------------------------------------------|------------------|-----------------------------|------------------------------------|----------------------|
| Path setup time?                            | Yes              | No                          | Yes                                | No                   |
| Routing decision for each packet?           | No               | Yes                         | No                                 | Typically no routing |
| Dedicated path?                             | Yes              | No                          | No                                 | No                   |
| Can dynamically reroute if problems occur?  | No               | Yes                         | No                                 | Typically no routing |
| Connection dedicated to your transfer only? | Yes              | No                          | No                                 | No                   |

# Connection-oriented versus Connectionless

- The network structure is the underlying physical component of a network. What about the software or application that uses the network?
- A network application can be *either* **connection-oriented** *or* **connectionless**.



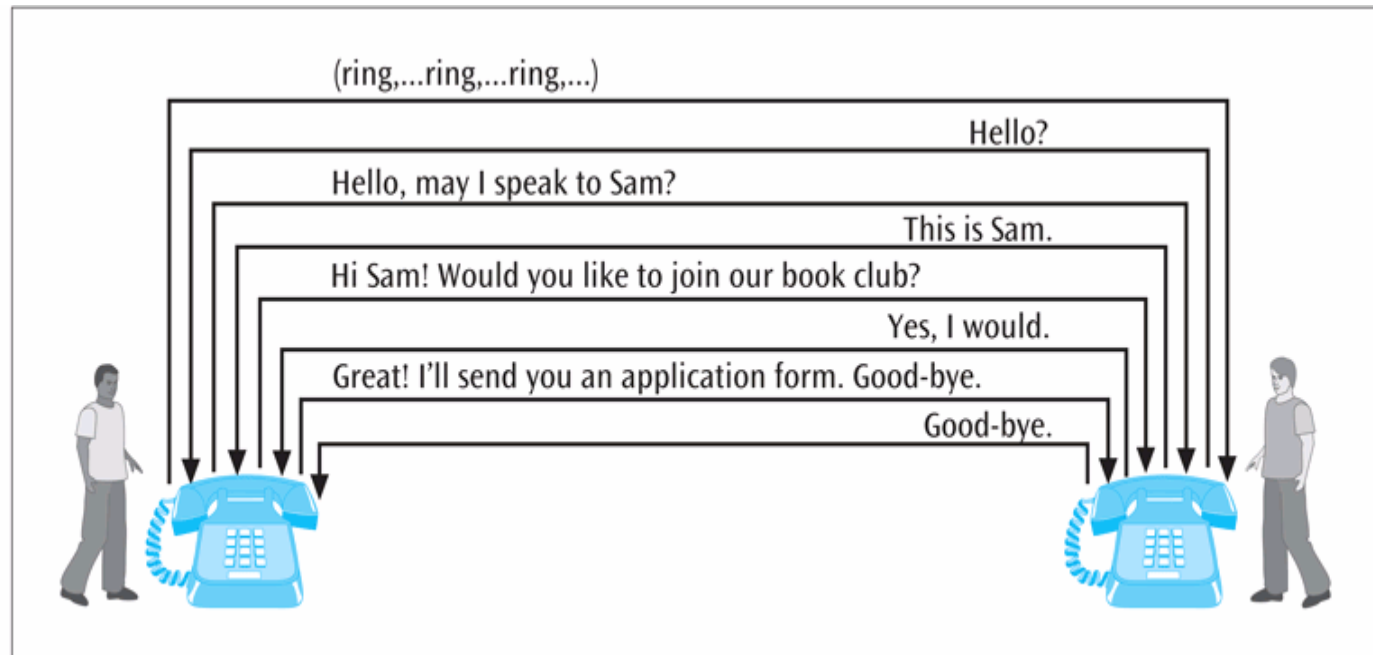
# Connection-oriented versus Connectionless

- A **connection-oriented application** requires both sender and receiver to **create** a connection before any data is transferred.
- Applications such as large file transfers and sensitive transactions such as banking and business are typically connection-oriented.
- A connectionless application does not create a connection first but simply sends the data. Electronic mail is a common example.

# Connection-oriented versus Connectionless

**Figure 9-8**

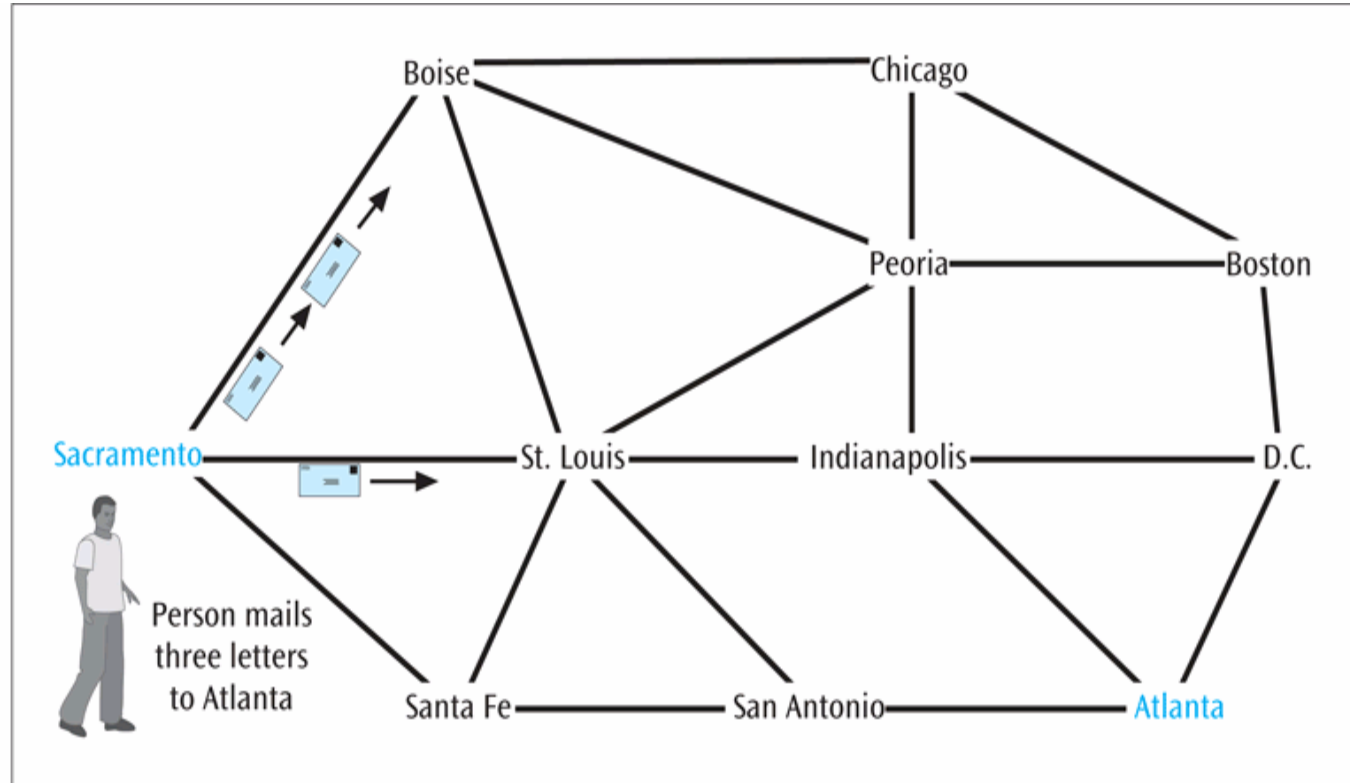
*Connection-oriented  
telephone call*



# Connection-oriented versus Connectionless

**Figure 9-9**

*Connectionless postal network*



# Connection-oriented versus Connectionless

- A connection-oriented application can operate over both a circuit switched network or a packet switched network.
- A connectionless application can also operate over both a circuit switched network or a packet switched network but a packet switched network may be more efficient.

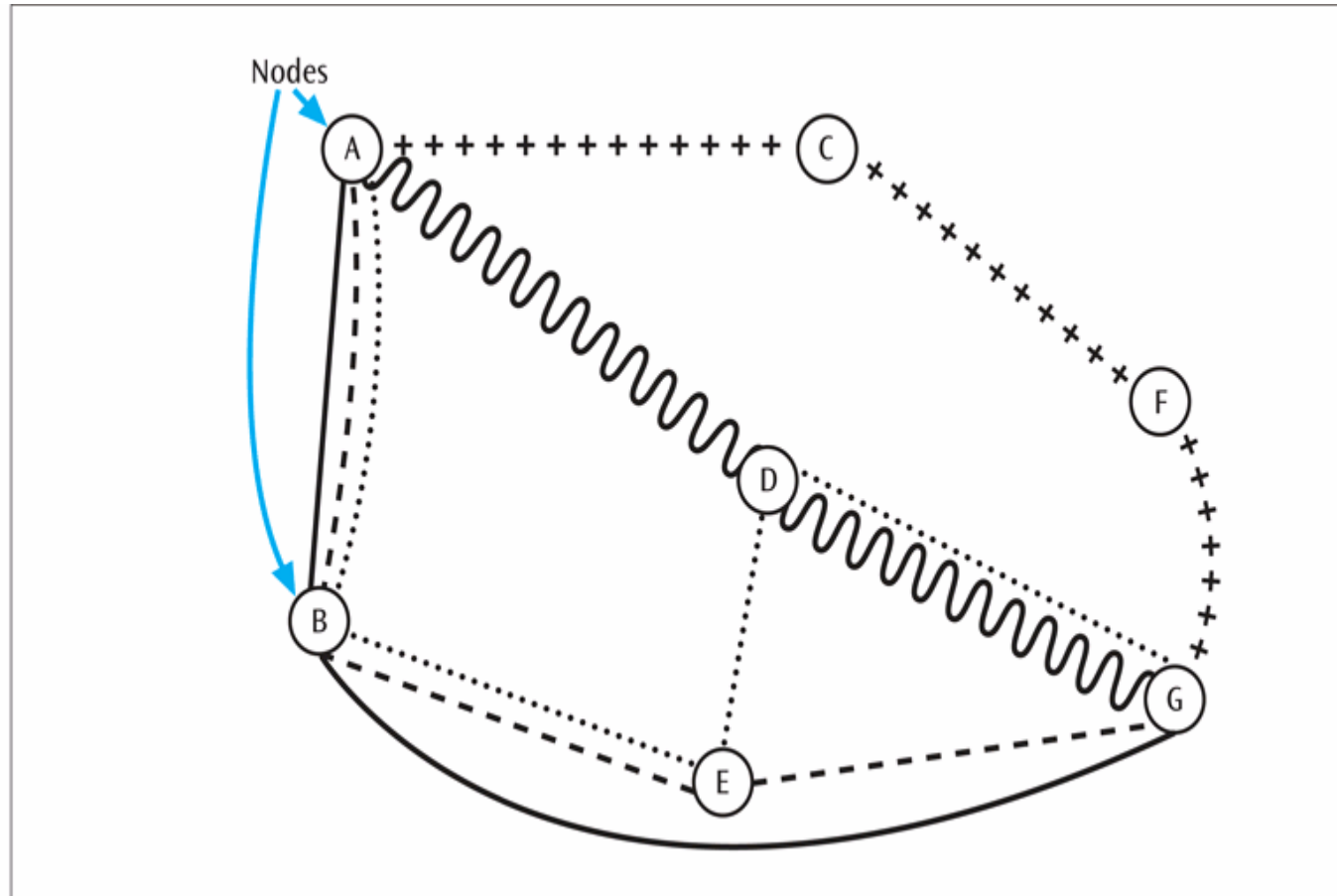
# Routing

- Each node in a WAN is a router that accepts an input packet, examines the destination address, and forwards the packet on to a particular telecommunications line.
- How does a router decide which line to transmit on?
- A router must select the one transmission line that will best provide a path to the destination and in an optimal manner.
- Often many possible routes exist between sender and receiver.

# Routing

**Figure 9-10**

*A seven-node network showing multiple routes between nodes*



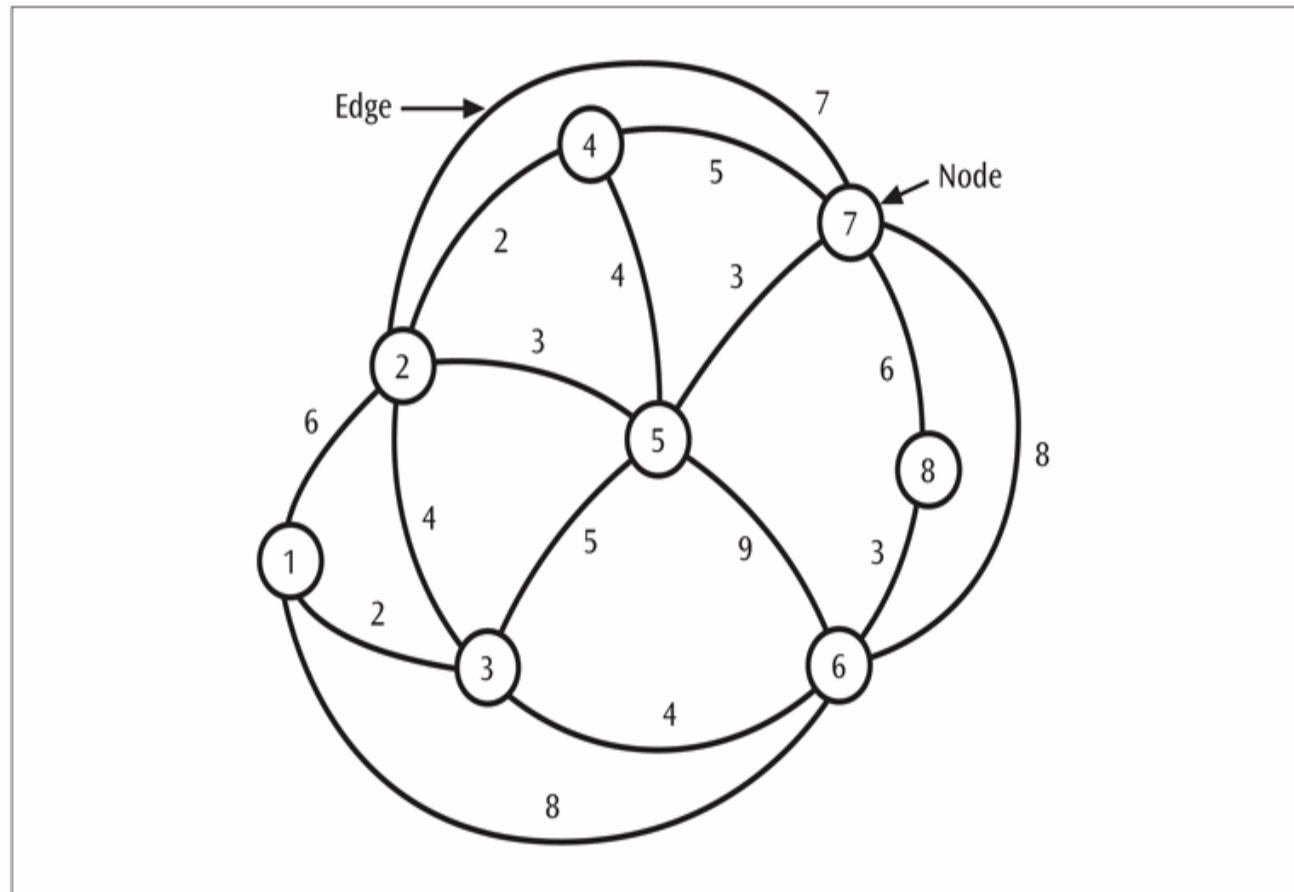
# Routing

- The communications network with its nodes and telecommunication links is essentially a weighted network graph.
- The edges, or telecommunication links, between nodes, have a cost associated with them.
- The cost could be a delay cost, a queue size cost, a limiting speed, or simply a dollar amount for using that link.

# Routing

**Figure 9-11**

*A simple example of  
a network graph*





# Routing

- The routing method, or algorithm, chosen to move packets through a network should be:
- Optimal, so the least cost can be found
- Fair, so all packets are treated equally
- Robust, in case link or node failures occur and the network has to reroute traffic.
- Not too robust so that the chosen paths do not oscillate too quickly between troubled spots.

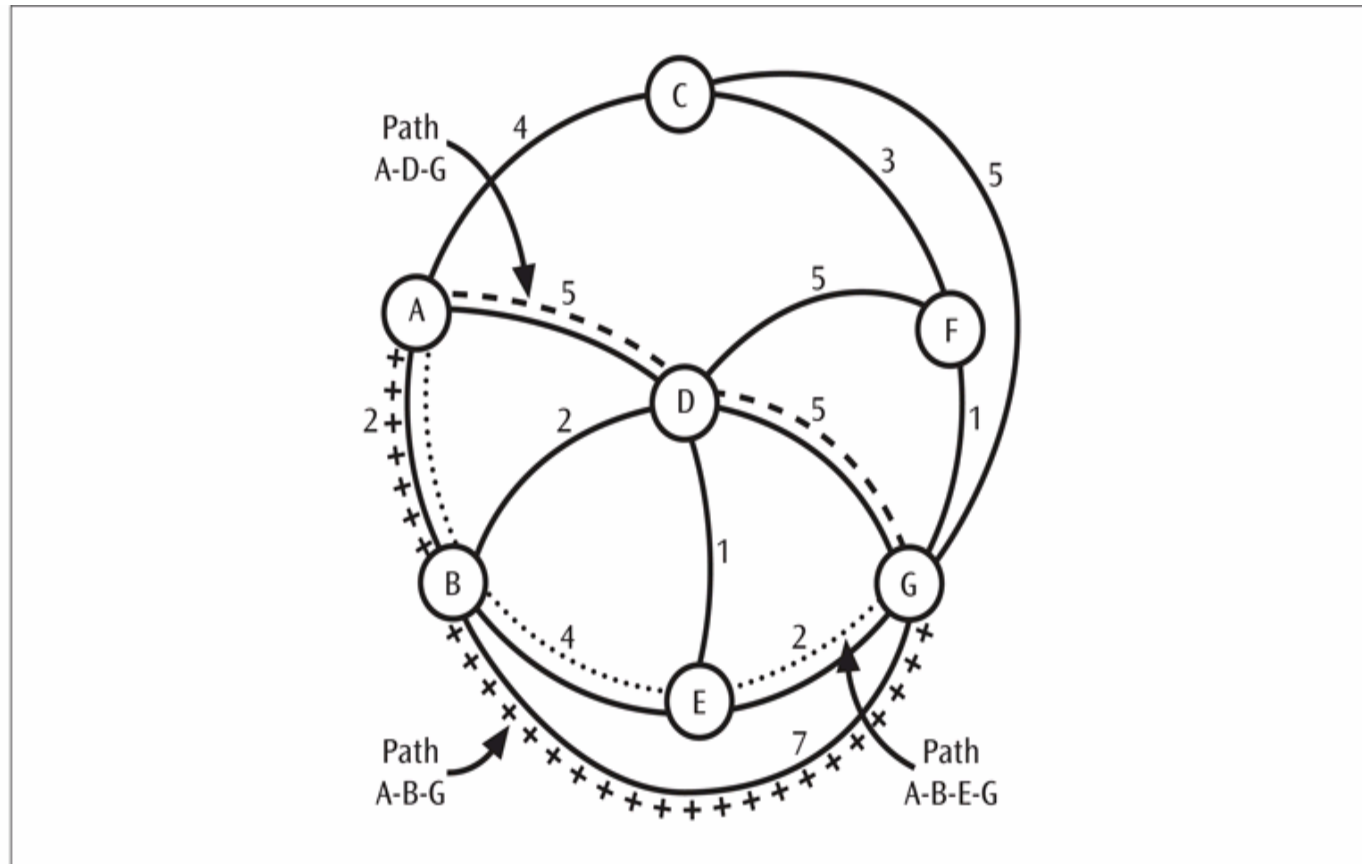
# Least Cost Routing Algorithm

- Dijkstra's least cost algorithm finds all possible paths between two locations.
- By identifying all possible paths, it also identifies the least cost path.
- The algorithm can be applied to determine the least cost path between any pair of nodes.

# Least Cost Routing Algorithm

**Figure 9-12**

*Network with costs associated with each link*



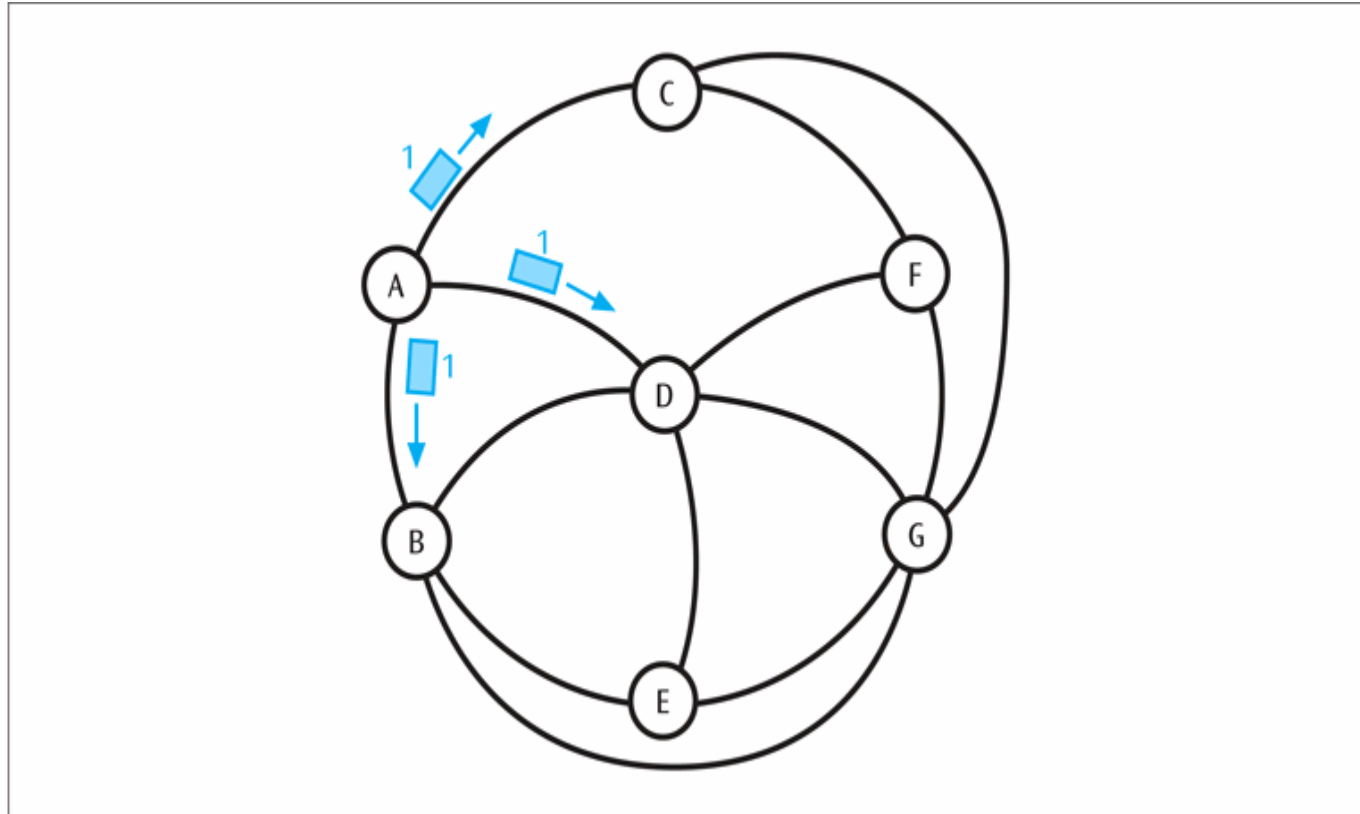
# Flooding Routing

- When a packet arrives at a node, the node sends a copy of the packet out every link except the link the packet arrived on.
- Traffic grows very quickly when every node floods the packet.
- To limit uncontrolled growth, each packet has a hop count. Every time a packet hops, its hop count is incremented. When a packet's hop count equals a global hop limit, the packet is discarded.

# Flooding Routing

**Figure 9-13**

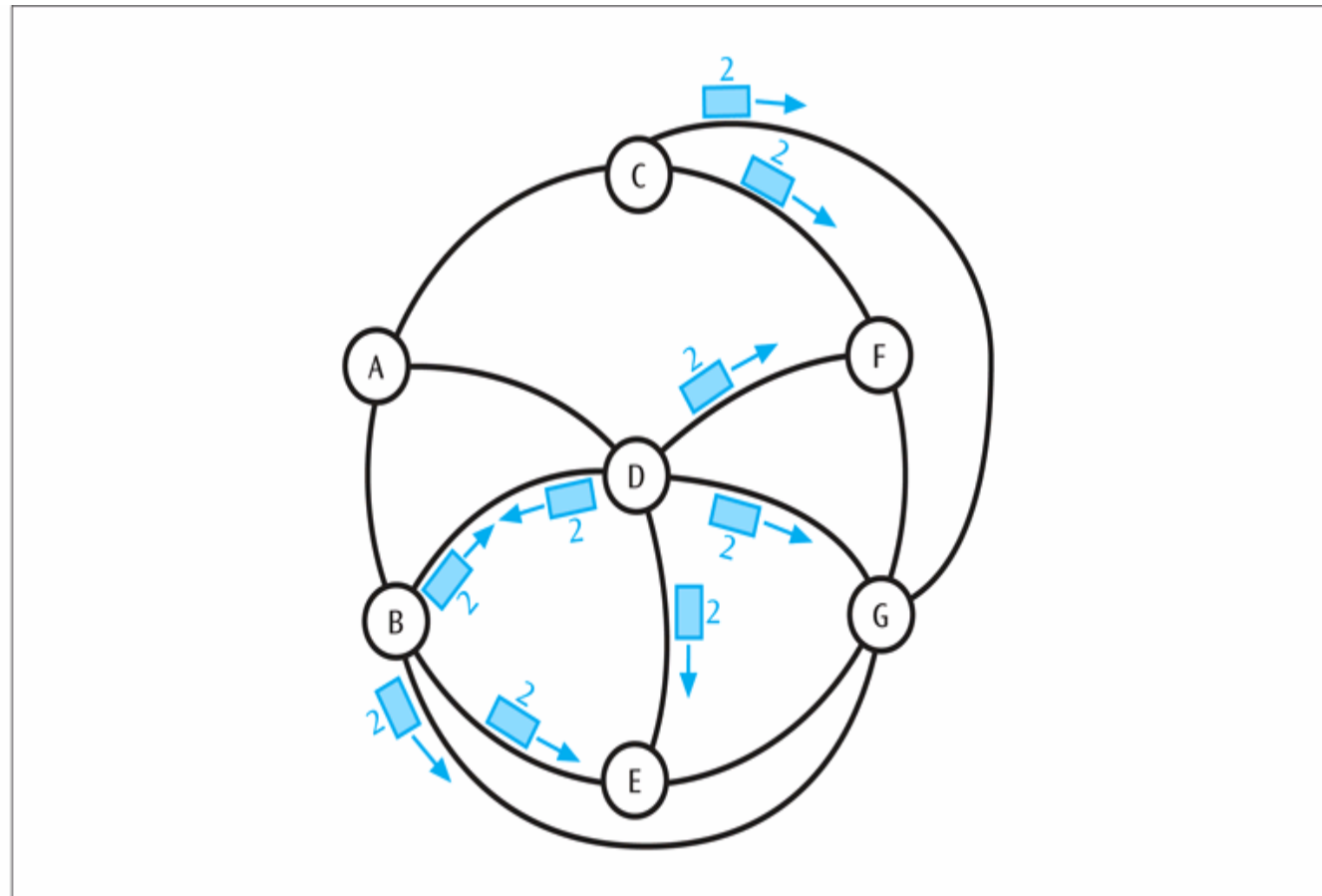
*Network with flooding,  
starting from Node A*



# Flooding Routing

**Figure 9-14**

*Flooding has continued to Nodes B, C, and D*



# Centralized Routing

- One routing table is kept at a “central” node.
- Whenever a node needs a routing decision, the central node is consulted.
- To survive central node failure, the routing table should be kept at a backup location.
- The central node should be designed to support a high amount of traffic consisting of routing requests.

# Centralized Routing

**Table 9-2**

*Routing table kept at a centralized network site*

|                  |   | Destination Node |   |   |   |   |   |   |
|------------------|---|------------------|---|---|---|---|---|---|
|                  |   | A                | B | C | D | E | F | G |
| Origination Node | A | -                | B | C | B | B | C | B |
|                  | B | A                | - | A | D | D | D | D |
|                  | C | A                | A | - | A | F | F | F |
|                  | D | B                | B | F | - | E | E | E |
|                  | E | D                | D | G | D | - | G | G |
|                  | F | C                | G | C | G | G | - | G |
|                  | G | E                | E | F | E | E | F | - |



# Distributed Routing

- Each node maintains its own routing table.
- No central site holds a global table.
- Somehow each node has to share information with other nodes so that the individual routing tables can be created.
- Possible problem with individual routing tables holding inaccurate information.

# Distributed Routing

**Table 9-3**

*Local routing table for Node C*

|                  |   | Destination Node |   |   |   |   |   |   |
|------------------|---|------------------|---|---|---|---|---|---|
|                  |   | A                | B | C | D | E | F | G |
| Origination Node | C | A                | A | - | A | F | F | F |

# Adaptive Routing versus Static Routing

- With adaptive routing, routing tables can change to reflect changes in the network
- Static routing does not allow the routing tables to change.
- Static routing is simpler but does not adapt to network congestion or failures.

# Routing Examples - RIP

- Routing Information Protocol (RIP) - First routing protocol used on the Internet.
- A form of distance vector routing. It was adaptive and distributed
- Each node kept its own table and exchanged routing information with its neighbors.

## Routing Examples - RIP

- Suppose that Router A has connections to four networks (123, 234, 345, and 789) and has the following current routing table:

| • | <b>Network</b> | <b>Hop Cost</b> | <b>Next Router</b> |
|---|----------------|-----------------|--------------------|
| • | 123            | 8               | B                  |
| • | 234            | 5               | C                  |
| • | 345            | 6               | C                  |
| • | 789            | 10              | D                  |

## Routing Examples - RIP

- Now suppose Router D sends out the following routing information (note that Router D did not send Next Router information, since each router will determine that information for itself):
  - **Network    Hop Cost**
  - 123            4
  - 345            5
  - 567            7
  - 789            10

## Routing Examples - RIP

- Router A will look at each entry in Router D's table and make the following decisions:
  - 1. Router D says Network 123 is 4 hops away (from Router D). Since Router D is 1 hop away from Router A, Network 123 is actually 5 hops away from Router A. That is better than the current entry of 8 hops in Router A's table, so Router A will update the entry for Network 123.
  - 2. Router D says Network 345 is 5 hops away. Add one hop to get to Router D and Network 345 is 6 hops away. That is currently the same hop count as shown in Router A's table for Network 345, so Router A will not update its table.

## Routing Examples - RIP

- Router A will look at each entry in Router D's table and make the following decisions:
- 3. Router D says Network 567 is 7 hops away. Add 1 hop to get to Router D, giving 8 hops. Since Router A has no information about Network 567, Router A will add this entry to its table. And since the information is coming from Router D, Router A's Next Router entry for network 567 is set to D.
- 4. Router D says Network 789 is 10 hops away. Add 1 hop to get to Router D. The value of 11 hops is worse than the value currently in Router A's table. Since Router A currently has information from Router D, and Router D is now saying it takes more hops to get to Network 789, then Router A has to use this information.



## Routing Examples - RIP

- Router A's updated routing table will thus look like the following:

- **Network Hop Cost Next Router**

- |       |    |   |
|-------|----|---|
| • 123 | 5  | D |
| • 234 | 5  | C |
| • 345 | 6  | C |
| • 567 | 8  | D |
| • 789 | 11 | D |

# Routing Examples - OSPF

- Open Shortest Path First (OSPF) - Second routing protocol used on the Internet
- A form of link state routing
- It too was adaptive and distributed but more complicated than RIP and performed much better

# Network Congestion

- When a network or a part of a network becomes so saturated with data packets that packet transfer is noticeably impeded, network congestion occurs.
- What can cause network congestion? Node and link failures; high amounts of traffic; improper network planning.
- When serious congestion occurs buffers overflow and packets are lost.

# Network Congestion

- What can we do to reduce or eliminate network congestion?
- An application can observe its own traffic and notice if packets are disappearing. If so, there may be congestion. This is called *implicit congestion control*.
- The network can inform its applications that congestion has occurred and the applications can take action. This is called *explicit congestion control*.

# Congestion Avoidance

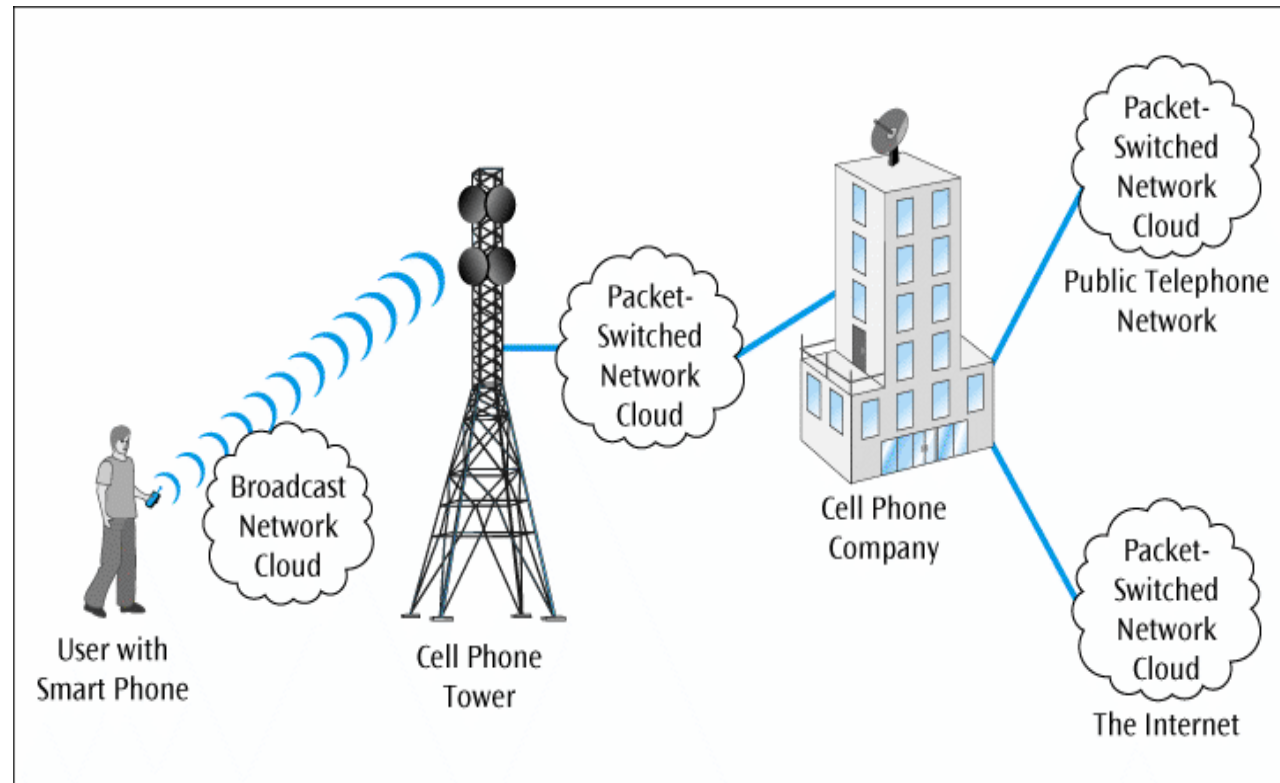
- Before making a connection, user requests how much bandwidth is needed, or if connection needs to be real-time
- Network checks to see if it can satisfy user request
- If user request can be satisfied, connection is established
- If a user does not need a high bandwidth or real-time, a simpler, cheaper connection is created
- This is often called *connection admission control*
- Asynchronous transfer mode is a very good example of this (Chapter Eleven)

# WANs In Action: The Smart Phone

- The network structure that support cell phones and smartphones is growing more complex every day
- All phones within transmission distance of a cell tower are participating in a broadcast network

# WANs In Action: The Smart Phone

**Figure 9-15**  
*Interconnection  
of network  
clouds*



## WANs In Action: The Smart Phone

- Once your data/signal reaches the cell tower, the data becomes part of a packet-switched network within the telephone company
- If the data moves from the telephone company into the Internet, then your data is passed from one packet switched network to another



# Summary

- A metropolitan area network is fast, fiber-based, has very small failover times, and is often dynamically provisional
- Early MANs were SONET-based, but Ethernet-based MANs are becoming very popular
- SONET-based MANs are rings, while Ethernet-based MANs are meshes
- Metro Ethernet is a popular form of MAN

## Summary (continued)

- Wide area networks cover states, countries, the world
- User connects to a station and the station interfaces to a network node
- A WAN cloud is based upon nodes (routers/switches) and high-speed links
- WANs can be circuit-switched (fading away) or packet switched (datagram and virtual circuit)
- RIP and OSPF are two routing protocols