Chapter 2
Network Devices
Objectives

• Explain the uses, advantages, and disadvantages of repeaters, hubs, wireless access points, bridges, switches, and routers
• Define the standards associated with wireless media
• Explain basic wireless connection parameters, security, and troubleshooting
• Define network segmentation
Objectives (continued)

• Explain network segmentation using bridges, switches, routers, brouters, and gateways
• Explain Ethernet operations
• Define Fast Ethernet and Gigabit Ethernet
Repeaters

- The number of **nodes** on a network and the length of cable used
  - Influence the quality of communication on the network
- **Attenuation**
  - The degradation of signal clarity
- **Repeaters**
  - Work against attenuation by repeating signals that they receive on a network
    - Typically cleaning and regenerating the digital transmission in the process

![Diagram of Repeaters in a network](image)
Repeater (continued)

- Note that on analog networks, devices that boost the signal are called amplifiers.
- These devices do not have the same signal regeneration capabilities as repeaters.
  - Because they must maintain the shape of the received signal.
- Repeaters work in the Physical layer (layer 1).
- On optical networks, signal amplification is handled by optical repeaters.
- Some repeaters can be used to connect two physically different types of cabling.

![Diagram of Optical Amplifier Function]

![Diagram of Optical Repeater Function]
Repeaters (continued)

Figure 2-2  Repeater in the network
Hubs

• **Hub**
  – Generic connection device used to tie several networking cables together to create a link between different stations on a network

• **Active hubs**
  – Amplify or repeat signals that pass through them

• **Passive hub**
  – Merely connects cables on a network and provides no signal regeneration

• **Topology** refers to the physical layout of network cable and devices

### Attenuation

An analog signal distorted by noise and then amplified

A digital signal distorted by noise and then repeated
Hubs (continued)

Figure 2-3  Star topology
Advantages and Disadvantages of Repeaters and Hubs

• **Advantages**
  – Can extend a network’s total distance
  – Do not seriously affect network performance
  – Certain repeaters can connect networks using different physical media
Advantages and Disadvantages of Repeaters and Hubs (continued)

• Disadvantages
  – Cannot connect different network architectures, such as Token Ring and Ethernet
  – Do not reduce network traffic
    • They repeat everything they receive
  – Do not segment the network
  – Do not reformat data structures
    • Cannot connect networks that require different types of frames
Advantages and Disadvantages of Repeaters and Hubs (continued)

- Repeaters do not segment a network
  - Frames that are broadcast on a given segment may collide
- Devices that “see” the traffic of other devices are said to be on the same collision domain
Wireless Access Points

- **Wireless access points**
  - Provide cell-based areas where wireless clients such as laptops and PDAs can connect to the network
    - By associating with the access point
- Operate at the **Physical** and **Data Link layers** of the OSI model
  - In most respects, a wireless access point functions exactly like a hub
Figure 2-4  Wireless access point in the network
# Wireless Standards and Organizations

<table>
<thead>
<tr>
<th>Standard</th>
<th>Frequency Band (GHz)</th>
<th>Transmission Method</th>
<th>Data Rates (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original 801.11</td>
<td>2.4</td>
<td>infrared, frequency hopping spread spectrum, direct sequence spread spectrum</td>
<td>1, 2</td>
</tr>
<tr>
<td>802.11b</td>
<td>2.4</td>
<td>direct sequence spread spectrum</td>
<td>1, 2, 5.5, 11</td>
</tr>
<tr>
<td>802.11a</td>
<td>5</td>
<td>orthogonal frequency division multiplexing</td>
<td>6, 9, 12, 18, 24, 36, 48, 54</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4</td>
<td>direct sequence spread spectrum and orthogonal frequency division multiplexing</td>
<td>1, 2, 5.5, 11 and 6, 9, 12, 18, 24, 36, 48, 54</td>
</tr>
</tbody>
</table>

*Table 2-1  802.11 Standards*
Wireless Network Components

- **In ad hoc mode**
  - Wireless clients can connect and communicate directly with each other
  - There is no access point
- **In infrastructure mode**
  - Wireless clients attach wirelessly to an access point
  - Involves the access point wired back into a switch
- **Basic Service Set (BSS)**
  - When a single access point is available in infrastructure mode
Wireless Network Components (continued)

- **Extended Service Set** (ESS)
  - Involve multiple access points connected to various switches in the network
  - Allows users to roam around the building and remain connected to the WLAN as well as the LAN and WAN
Wireless Connectivity

- Access points typically broadcast their network name
- The **Service Set Identifier** (SSID)
  - The network name
- When wireless clients are powered on, they begin scanning the airspace for available access points
- They detect the broadcasted SSID of the various access points in the area
  - Attempt to associate with the one that has the highest signal level and the lowest error rate
Wireless Connectivity (continued)

• If the system is open, the client is accepted by the access point and begins communications

• When SSID is not broadcasted
  – Wireless clients must already be configured with the correct SSID

• The client will send out a probe request with:
  – Configured SSID
  – Access point with that SSID configured will allow the client to associate
Wireless Security Measures

- While security is always necessary in WLANs due to the broadcast nature of the medium
  - These devices are not designed to handle the most complex and highest levels of security
- The most important reason to implement security on your WLAN at home
  - Others in your neighborhood do not use your bandwidth for free
Wireless Security Measures (continued)

- Workspace situations call for security that not only requires the client device to authenticate
  - But that also prompts the device user to enter a username and password
- **802.1x** is used at the physical layer to block ports
- The **Extensible Authentication Protocol (EAP)** is used at layer 2 to transfer the authentication frames
## Wireless Security Protocols (continued)

<table>
<thead>
<tr>
<th>802.11 Security Option</th>
<th>Type of Encryption</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP (Wired Equivalent Privacy)</td>
<td>Lower-level encryption: RC4 algorithm, static key</td>
<td>Home</td>
</tr>
<tr>
<td>WPA (Wi-Fi Protected Access)</td>
<td>Higher level encryption: TKIP algorithm, dynamic keys, user authentication also supported (802.1x)</td>
<td>Home and small office</td>
</tr>
<tr>
<td>WPA2 (Wi-Fi Protected Access version 2)</td>
<td>Highest level of encryption: AES algorithm, dynamic keys, user authentication also supported (802.1x)</td>
<td>Home and small office</td>
</tr>
<tr>
<td>802.11i (The IEEE standard based on WPA2)</td>
<td>Highest level of encryption: AES algorithm, dynamic keys, user authentication with 802.1x/EAP</td>
<td>Businesses</td>
</tr>
</tbody>
</table>

*Table 2-2  802.11 Security*
Advantages and Disadvantages of Wireless Access Points

• **Advantages**
  – Provide the ability to work anywhere within range of your access points
  – Extends the range of your network without running additional wires

• **Disadvantages**
  – Introduces serious security concerns
  – 802.11 provides much less bandwidth than wired devices
  – Many situations exist where 802.11 will not function well due to serious interference from various sources
Network Segmentation

- **Segmentation**
  - The breaking down of a single heavily populated network segment into smaller segments, or collision domains, populated by fewer nodes

- **Segment**
  - Part of a network that is divided logically or physically from the rest of the network

- When network administrators place too many nodes on the same network segment
  - Causes the number of collisions to increase
**Figure 2-5** Network segmentation
Bridges

- **Bridges**
  - Operate at the Data Link layer of the OSI model
  - Filter traffic between network segments by examining the destination MAC address
    - Based on the destination MAC address, the bridge either forwards or discards the frame
  - Reduce network traffic by keeping local traffic on the local segment

- **Broadcast frame**
  - Frame destined for all computers on the network
Figure 2-6 Bridge
Transparent Bridges

• Also called learning bridges
  – Because they build a table of MAC addresses as they receive frames
• They “learn” which addresses are on which segments
• The bridge uses the source MAC addresses to determine which addresses are on which segments
  – By determining a frame’s origin, the bridge knows where to send frames in the future
• Ethernet networks mainly use transparent bridges
Source-Routing Bridges

• Rely on the source of the frame transmission to provide the routing information
  – The source computer determines the best path by sending out explorer frames
• The source includes the routing information returned by its explorer frames in the frame sent across the network
  – The bridge uses this information to build its table
Translation Bridges

- Can connect networks with different architectures, such as Ethernet and Token Ring
- These bridges appear as:
  - Transparent bridges to an Ethernet host
  - Source-routing bridges to a Token Ring host
Advantages and Disadvantages of Bridges

• **Advantages**
  – Can extend a network by acting as a repeater
  – Can reduce network traffic on a segment by subdividing network communications
  – Increase the available bandwidth to individual nodes because fewer nodes share a collision domain
  – Reduce collisions
  – Some bridges connect networks using different media types and architectures
Advantages and Disadvantages of Bridges (continued)

• Disadvantages
  – Slower than repeaters and hubs
    • Extra processing by viewing MAC addresses
  – Forward broadcast frames indiscriminately, so they do not filter broadcast traffic
  – More expensive than repeaters and hubs

• Broadcast storm
  – When two or more stations engage in the transmission of excessive broadcast traffic
Switches

• **Switches**
  – Operate at the Data Link layer of the OSI model
  – Increase network performance by reducing the number of frames transmitted to the rest of the network

• **Switch** opens a **virtual circuit** between the source and the destination
  – Prevents communications between just two computers from being broadcast to every computer on the network or segment
  – Called **microsegmentation**
Switches (continued)

- When two machines have a virtual circuit
  - They do not have to share the bandwidth with any other computers
- Multiple virtual circuits can be in use at the same time, each with its own full **bandwidth**
  - Called “switched bandwidth”
- When machines must share a wire and compete for available bandwidth with other machines, they experience **contention**
Figure 2-7  Star topology using a switch
Advantages and Disadvantages of Switches

- **Advantages**
  - Switches increase available network bandwidth
  - Switches reduce the workload on individual computers
  - Switches increase network performance
  - Networks that include switches experience fewer frame collisions because switches create collision domains for each connection (a process called microsegmentation)
  - Switches connect directly to workstations
Advantages and Disadvantages of Switches (continued)

• **Disadvantages**
  – Switches are significantly more expensive than bridges
  – Network connectivity problems can be difficult to trace through a switch
  – Broadcast traffic may be troublesome
Routers

- **Routers**
  - Operate at the Network layer of the OSI model
  - Provide filtering and network traffic control on LANs and WANs
  - Can connect multiple segments and multiple networks

- **Internetworks**
  - Networks connected by multiple routers

- Similar to switches and bridges in that they segment a network and filter traffic
  - Routers use the logical address
Physical vs. Logical Addresses

• MAC address
  – Found at the Data Link layer of the OSI model
  – Used by bridges and switches to make forwarding decisions within a network or subnetwork

• IP address
  – Logical address when TCP/IP is used on an internetwork

• Routers use the IP address to route packets to the correct network segment
Physical vs. Logical Addresses (continued)

Figure 2-8  Router
Advantages and Disadvantages of Routers

• Advantages
  – Can connect different network architectures, such as Ethernet and Token Ring
  – Can choose the best path across an internetwork using dynamic routing techniques
  – Reduce network traffic by creating collision domains
  – Reduce network traffic by creating broadcast domains
Advantages and Disadvantages of Routers (continued)

• Disadvantages
  – Routers work only with routable network protocols; most but not all protocols are routable
  – Routers are more expensive than other devices
  – Dynamic router communications (inter-router communication) cause additional network overhead, which results in less bandwidth for user data
  – Routers are slower than other devices because they must analyze a data transmission from the Physical through the Network layer
Figure 2-9  Router connecting network to the Internet
Brouters

- **Brouter**
  - Hybrid device
  - Functions as both a bridge for nonroutable protocols and a router for routable protocols
  - Provides the best attributes of both a bridge and a router
  - Operates at both the Data Link and Network layers and can replace separate bridges and routers
Gateways

- **Gateway**
  - Usually a combination of hardware and software
  - Translates between different protocol suites
  - Has the most negative effect on network performance
    - Packets must be rebuilt not just at the lower levels but at the very upper levels
      - So that actual data content can be converted into a format the destination can process
  - Creates the most **latency**
Ethernet Operations

• Ethernet
  – A network access method (or media access method) originated by the University of Hawaii
  – Later adopted by Xerox Corporation, and standardized as IEEE 802.3 in the early 1980s
• Today, Ethernet is the most commonly implemented media access method in new LANs
CSMA/CD

- **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**
  - Used by Ethernet to prevent data packets from colliding on the network
  - Allows any station connected to a network to transmit anytime there is not already a transmission on the wire
- After each transmitted signal, each station must wait a minimum of 9.6 microseconds before transmitting another frame
  - Called the **interframe gap (IFG)**, or **interpacket gap (IPG)**

![Diagram of CSMA/CD](image-url)
CSMA/CD (continued)

- **Collisions**
  - Two stations could listen to the wire simultaneously and not sense a carrier signal
    - In such a case, both stations might begin to transmit their data simultaneously
      - A collision would occur on the network wire
    - The first station to detect the collision transmits a 32-bit *jam signal*
      - Tells all other stations not to transmit for a brief period
    - The two stations enter a backoff period
CSMA/CD (continued)

• Collision domain
  – The physical area in which a frame collision might occur
  – Routers, switches, bridges, and gateways do segment networks
    • And thus create separate collision domains
Fast Ethernet

• **Fast Ethernet** (100BaseT)
  – Uses the same network access method (CSMA/CD) as common 10BaseT Ethernet
  – Provides ten times the data transmission rate

• When you upgrade from 10BaseT to Fast Ethernet
  – All the network cards, hubs, and other connectivity devices that are now expected to operate at 100 Mbps must be upgraded

• Fast Ethernet is defined under the **IEEE 802.3u** standard
Gigabit Ethernet

• **Gigabit Ethernet** (1000BaseX)
  – The next iteration of Ethernet, increasing the speed to 1000 Mbps
  – Defined in the **IEEE 802.3z** standard

• Gigabit Ethernet can work in half-duplex mode through hubs
  – Not typical
  – Almost all applications of the standard are full-duplexed through switches

• 10 Gigabit Ethernet (10GBaseX, 10GbE or 10GigE) is the fastest of the Ethernet standards
Half- and Full-Duplex Communications

- **Half-duplex** communications
  - Devices can send and receive signals, but not at the same time
- **Full-duplex** communications
  - Devices can send and receive signals simultaneously
- Most Ethernet networks can use equipment that supports half- and full-duplex communications
- Full-duplex communications use one set of wires to send and a separate set to receive
Half- and Full-Duplex Communications (continued)

• Benefits of using full-duplex:
  – Time is not wasted retransmitting frames, because there are no collisions
  – The full bandwidth is available in both directions because the send and receive functions are separate
  – Stations do not have to wait until other stations complete their transmissions