MANs and WANs (1 of 2)

- A **WAN (wide area network)** is a group of LANs that spread over a wide geographical area
- A **MAN (metropolitan area network)** is a group of connected LANs in the same geographical area
  - Also known as a **campus area network (CAN)**
- MANs and WANs often use different transmission methods and media than LANs
- **PAN (personal area network)** is a much smaller network of personal devices
  - A network of personal devices such as your smartphone and your computer
- Other network types:
  - **BAN (body area network)**
  - **SAN (storage area network)**
  - **WLAN (wireless local area network)**

MANs and WANs (2 of 2)

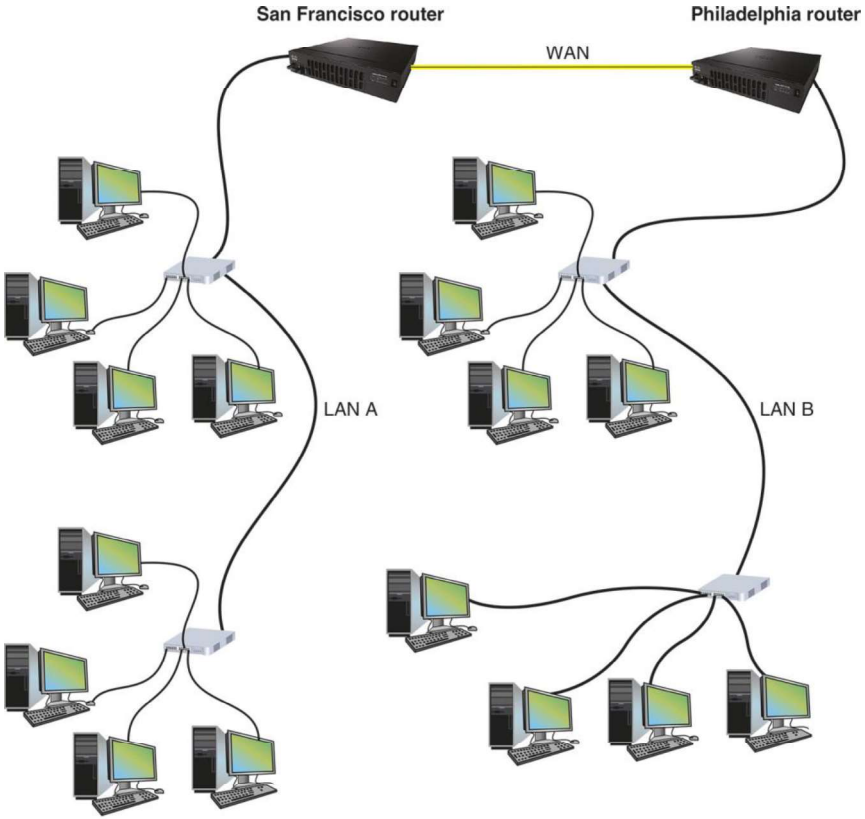

Figure 1-17 A WAN connects two LANs in different geographical areas

Figure 1-17 A WAN connects two LANS in different geographical areas

The Seven-Layer OSI Model (1 of 2)

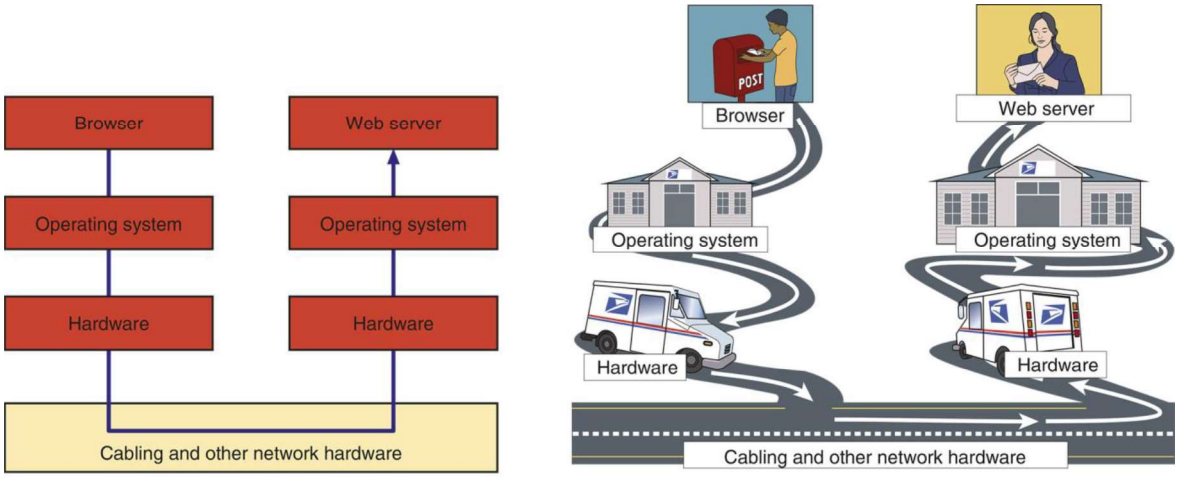

Figure 1-18 A browser and web server communicate by way of the operating system and hardware, similar to how a letter is sent through the mail using the U.S. Postal Service and the road system

Figure 1-18 A browser and web server communicate by way of the operating system and hardware, similar to how a letter is sent through the mail using the U.S. Postal Service and the road system

The Seven-Layer OSI Model (2 of 2)

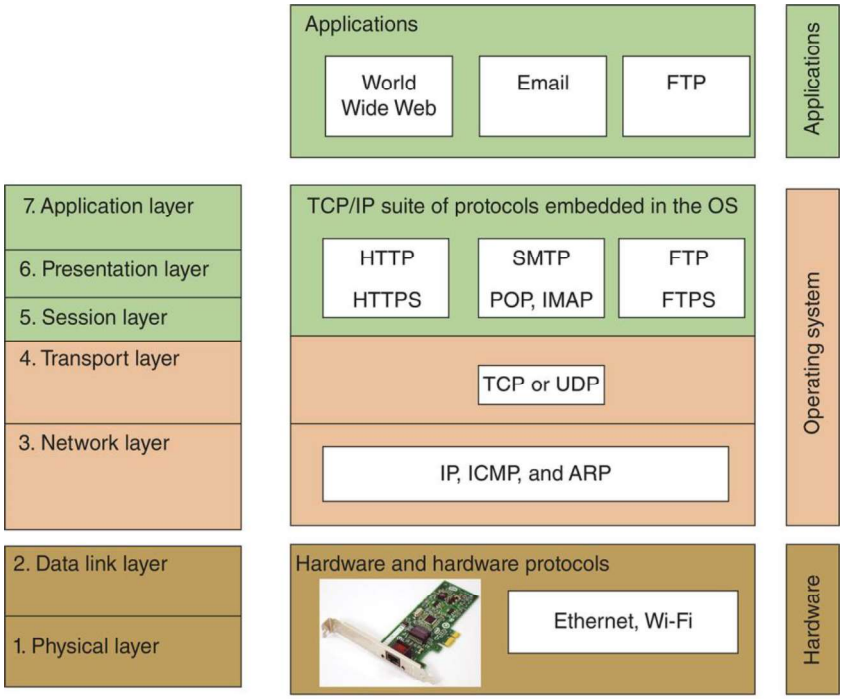

Figure 1-19 How software, protocols, and hardware map to the seven-layer OSI model

Figure 1-19 How software, protocols, and hardware map to the seven-layer OSI model

Layer 7: Application Layer

- The **application layer** describes the interface between two applications, on separate computers
- Application layer protocols are used by programs that fall into two categories:
  - Provide services to a user, such as a browser and Web server
  - Utility programs that provide services to the system, such as **SNMP (Simple Network Management Protocol)** programs that monitor and gather information about network traffic
- **Payload** is the data that is passed between applications or utility programs and the OS

Layer 6: Presentation Layer

- The **presentation layer** is responsible for reformatting, compressing, and/or encrypting data in a way that the receiving application can read
- Example:
  - An email message can be encrypted at the Presentation layer by the email client or by the OS

Layer 5: Session Layer

- The **session layer** describes how data between applications is synched and recovered if messages don't arrive intact at the receiving application
- The application, presentation, and session layers are intertwined
  - It is often difficult to distinguish between them
- Most tasks are performed by the OS when an application makes an API call to the OS
  - An API (application programming interface) call is the method an application uses when it makes a request of the OS

Layer 4: Transport Layer

- The transport layer is responsible for transporting Application layer payloads from one application to another
- Two main Transport layer protocols are:
  - **TCP (Transmission Control Protocol)** - makes a connection with the end host, checks whether data was received; called a connection-oriented protocol
  - **UDP (User Datagram Protocol)** - does not guarantee delivery by first connecting and checking whether data is received; called a connectionless protocol
- Protocols add control information in an area at the beginning of the payload (called **header**)
- **Encapsulation** is the process of adding a header to the data inherited from the layer above
- The Transport layer header addresses the receiving application by a number called a **port**
- If a message is too large, TCP divides it into smaller messages called **segments**
  - In UDP, the message is called a **datagram**

Layer 3: Network Layer

- The network layer is responsible for moving messages from one node to another until they reach the destination host
- The principal protocol used by this layer is **IP (Internet Protocol)**
- IP adds its own network layer header to the segment or datagram
  - The entire network layer message is called a **packet**
- An **IP address** is an address assigned to each node on a network
  - The network layer uses it to uniquely identify each host
- IP relies on several routing protocols to find the best route for a packet to take to reach destination
  - ICMP and ARP are examples
- Network layer protocol will divide large packets into smaller packets in a process called **fragmentation**

Layer 2: Data Link Layer

- Layers 2 and 1 are responsible for interfacing with physical hardware on the local network
  - Protocols at these layers are programmed into firmware of a computer's NIC and other hardware
- Type of networking hardware or technology used on a network determine the data link layer protocol used
  - Ethernet and Wi-Fi are examples
- The data link layer puts control information in a data link layer header and at the end of the packet in a trailer
  - The entire data link layer message is called a **frame**
- A **MAC (Media Access Control) address** is also called a physical address, hardware address, or data link layer address
  - It is embedded on every network adapter

Layer 1: Physical Layer

- The physical layer is responsible for sending bits via a wired or wireless transmission
- Bits can be transmitted as:
  - Wavelengths in the air
  - Voltage on a copper wire
  - Light (via fiber-optic cabling)

Protocol Data Unit or PDU

- Protocol data unit (PDU) is the technical name for a group of bits as it moves from one layer to the next and from one LAN to the next
  - Technicians loosely call this group of bits a message or a transmission

Summary of How the Layers Work Together

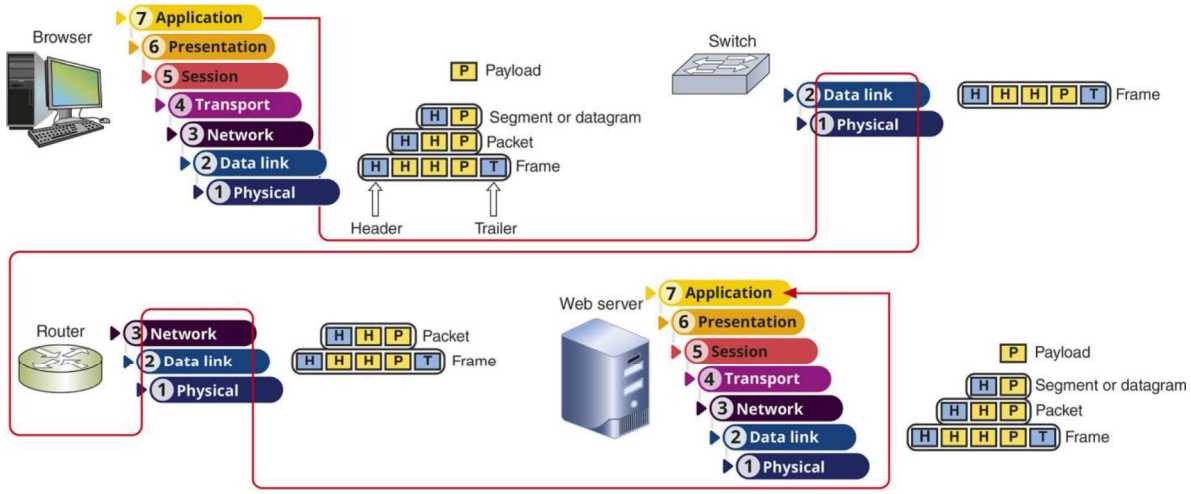

Figure 1-20 Follow the red line to see how the OSI layers work when a browser makes a request to a web server

Figure 1-20 Follow the red line to see how the OSI layers work when a browser makes a request to a web server

Knowledge Check Activity 1-2

Which OSI layer adds both a header and a trailer?

a. Transport layer
b. Network layer
c. Data link layer
d. Physical layer

Knowledge Check Activity 1-2: Answer

Which OSI layer adds both a header and a trailer?

Answer: c. Data link layer

The data link layer puts its control information in a data link layer header and also attaches control information to the end of the packet in a trailer

Safety Procedures and Policies

- Network and computer technicians need to know how to protect themselves
  - As wells as protect sensitive electronic components
- This section takes a look at some best practices for safety

Emergency Procedures

- Know the best escape route or emergency exit
- Fire Suppression Systems - have a fire suppression system in the data center that includes:
  - Emergency alert system
  - Portable fire extinguishers
  - Emergency power-off switch
- Ask yourself: Does the security system allow access during a failure (fail open) or deny access during the failure (fail close)?
- An **SDS (safety data sheet)** explains how to properly handle substances such as chemical solvents and how to dispose of them
  - Includes information such as identification, first-aid measures, fire-fighting measures, accidental release measures, handling and storage guidelines, exposure controls, and physical and chemical properties

Safety Procedures (1 of 4)

- Electrical and tool safety is generally regulated by **OSHA (Occupational Safety and Health Administration)**
- OSHA guidelines when using power tools:
  - Wear **PPE (personal protective equipment)**
  - Keep all tools in good condition and properly store tools not in use
  - Use the right tool for the job and operate the tool according to the manufacturer's instructions
  - Watch out for trip hazards, so you and others don't stumble on a tool or cord

Safety Procedures (2 of 4)

- Lifting Heavy Objects - follow these guidelines:
  - Decide which side of object to face so load is most balanced
  - Stand close to the object with your feet apart
  - Keep your back straight, bend knees and grip load
  - Lift with your legs, arms, and shoulders (not your back or stomach)
  - Keep the load close to your body and avoid twisting your body while you're holding it
  - To put the object down, keep your back as straight as possible and lower object by bending your knees

Safety Procedures (3 of 4)

- Protecting Against Static Electricity
  - Computer components are grounded inside a computer case
  - **Grounding** means that a device is connected directly to the earth
- Sensitive electronic components can be damaged by **ESD (electrostatic discharge)**
- Static electricity can cause two types of damage:
  - Catastrophic failure - destroyed beyond use
  - Upset failure - shorten the life of a component

Safety Procedures (4 of 4)

- Before touching a component, ground yourself by:
  - Wearing an ESD strap around your wrist that clips onto the chassis or computer case
  - Touching the case before touching any component inside the case
  - Storing a component inside an antistatic bag
- In addition to protecting against ESD, always shut down and unplug a computer before working inside it

Troubleshooting Network Problems

- Troubleshooting steps used by most expert networking troubleshooters:
  - Step 1: Identify the problem and its symptoms
  - Step 2: Establish theory of probable cause
  - Step 3: Test your theory to determine cause
  - Step 4: Establish a plan for resolving the problem
  - Step 5: Implement the solution or escalate the problem
  - Step 6: Verify full functionality and implement preventative measures
  - Step 7: Document findings, actions, outcomes

Self-Assessment

What networking hardware devices have you used in the past?

What type of network or computer safety issues have you (or a friend or another student) experienced? How did you troubleshoot those issues?

Summary

Now that the lesson has ended, you should be able to:

- Distinguish between peer-to-peer and client-server networks
- Identify types of applications and protocols used on a network
- Describe various networking hardware devices and the most common physical topologies
- Describe the seven layers of the OSI model
- Explain best practices for safety when working with networks and computers
- Describe the seven-step troubleshooting model for troubleshooting network problems