

Unit II: Hardware and Software**Chapter 9: Networks and the Internet****9.1: Goal:**

In this chapter, you will discover how computers communicate with one another to share information and resources across homes, schools, businesses, and around the world. You will learn how networks and the Internet work, explore common networking technologies, and understand how data travels from one device to another. By the end of this chapter, you will have a solid foundation for understanding the connected world in which we live and work.

9.2: Objectives:

- Explain the purpose of computer networks.
- Differentiate between LANs, WANs, and the Internet.
- Identify common networking devices, including routers, switches, and modems.
- Describe how data travels across the Internet using packets.
- Explain the purpose of IP addresses and domain names.
- Compare wired and wireless networking technologies.
- Describe cloud computing and online collaboration tools.
- Identify common Internet services, including the World Wide Web, email, streaming, and file sharing.
- Recognize common network security practices.
- Explain how emerging networking technologies continue to change the way people communicate and work.

9.3: Think About It

Imagine waking up tomorrow and discovering that the Internet has disappeared. Your phone cannot send text messages, online classes are unavailable, streaming services won't load, credit card payments fail, and navigation apps stop working.

How many activities in your daily routine would be affected? Which ones would surprise you the most?

9.4: Opening Scenario

Emma is studying at a local coffee shop before her biology exam. She connects her laptop to the café's Wi-Fi, opens her college's learning management system, joins a virtual study group, edits a shared presentation stored in the cloud, and messages her instructor with a question. As she leaves, her work automatically synchronizes to her tablet so she can continue studying on the bus home.

Although these tasks seem routine, they depend on a complex network of devices working together behind the scenes. Wireless access points, routers, Internet service providers, cloud servers, and data centers all cooperate to move information around the world in just seconds.

This chapter explores how these networks make modern communication, learning, and entertainment possible.

9.5: Why This Chapter Matters

Nearly every profession depends on computer networks. Nurses access electronic health records, engineers collaborate with colleagues across continents, teachers conduct virtual classes, businesses rely on online commerce, and families stay connected through messaging and video calls.

Understanding how networks operate helps you become a more informed technology user. It also enables you to make better decisions about security, privacy, troubleshooting, and selecting the technologies that best meet your needs. Whether you are sending an email, streaming a movie, or participating in an online meeting, you are relying on one of the world's largest technological achievements: the Internet.

Understanding Computer Networks

A **computer network** is a group of two or more computers and other devices connected so they can communicate and share resources. Networked devices can include desktop computers, laptops, smartphones, printers, servers, smart TVs, and other connected devices. Networks may use **wired connections**, such as Ethernet cables, or **wireless connections**, such as Wi-Fi.



Networks allow users to **share files, printers, applications, and Internet connections** and to communicate through services such as email, messaging, and video conferencing. Networks can range from a small home network connecting a few devices to large networks connecting thousands of computers across schools, businesses, and government organizations. The **Internet** is the world's largest computer network: a global system of interconnected networks that allows devices around the world to communicate and exchange information.

Types of Networks

Computer networks can be classified by the **geographic area they cover** and the devices they connect. A small network might connect computers and printers within one room or building, while a much larger network can connect devices across cities, countries, or the world.

PAN: Personal Area Network

Connects devices within a very short distance, such as a smartphone connected to wireless earbuds or a smartwatch.



LAN: Local Area Network

Connects devices within a limited area such as a home, classroom, office, or college building.



WLAN: A wireless LAN that uses Wi-Fi

MAN: Metropolitan Area Network covers a city or large campus



WAN: A Wide Area Network connects networks across large geographic areas, such as different states or countries.

The **Internet** is the largest example of a WAN because it connects millions of smaller networks around the world.



Network Hardware

Network hardware consists of the physical devices that allow computers and other devices to connect and communicate over a network. Some devices connect individual computers to a network, while others direct data between devices or connect one network to another. Network hardware can support both **wired and wireless connections**.

Common network hardware includes a **network interface controller (NIC)**, which allows a device to connect to a network; a **switch**, which connects devices within a local network and directs data to the appropriate device; and a **router**, which connects different networks and directs data between them. A **wireless access point** provides Wi-Fi connectivity, while a **modem** connects a home or organization to an Internet service provider. Networks may also use **Ethernet cables, fiber-optic cables, and other communication equipment** to transmit data.

ROUTER	SWITCH	MODEM
		
Connects networks and routes data	Connects devices on a network	Connects to the Internet service

How the Internet Works

The **Internet** is a worldwide system of interconnected computer networks. When you use a web browser, send an email, stream a video, or use an online application, your device communicates with other computers through these networks. Your **Internet service provider (ISP)** provides the connection between your local network and the larger Internet. **Routers** help direct data from one network to another until it reaches its destination.

Information traveling across the Internet is usually divided into small pieces called **packets**. Each packet contains part of the data along with information that helps it reach the correct destination. Packets may travel through different routes before arriving, where they are reassembled into the original information. Internet communication relies on agreed-upon rules called **protocols**, including **TCP/IP**, which help devices exchange data reliably.

When you enter a website address, the **Domain Name System (DNS)** helps translate the human-readable domain name into an **IP address** that identifies the appropriate computer or server. Your browser can then request the webpage from that server, and the server sends the necessary data back across the Internet to your device.



Wired Communication

Wired communication transmits data between devices through physical cables. Wired networks are commonly used in homes, schools, offices, and data centers because they can provide **fast, stable, and reliable connections**. Unlike wireless signals, wired connections are generally less affected by distance within their designed limits, physical obstacles, or interference from nearby wireless devices.

Ethernet is one of the most common technologies used for wired local networks and typically uses copper cables to connect computers, switches, routers, and other network equipment. **Fiber-optic cable** transmits data using pulses of light rather than electrical signals and can carry large amounts of data at very high speeds over long distances. Wired networks require physical cabling and may provide less mobility than wireless networks, but their **speed, reliability, security advantages, and consistent performance** make them important parts of modern computer networks.



Wireless Communication

Wireless communication allows devices to exchange data without being connected by physical cables. Instead, information travels through the air using **radio waves and other forms of electromagnetic signals**. Wireless technology makes it possible for laptops, smartphones, tablets, smartwatches, and other devices to communicate while users move from place to place.

Common wireless technologies include **Wi-Fi**, which connects devices to local networks and the Internet; **Bluetooth**, which provides short-range connections between devices such as headphones, keyboards, and smartphones; and **cellular networks**, which provide mobile voice and data services over larger geographic areas. Other wireless technologies include **NFC (Near Field Communication)**, used for very short-range communication such as contactless payments. Wireless communication offers convenience and mobility, but users should also consider **security, signal strength, interference, range, and connection speed** when using wireless networks.



Wireless Technologies

- Wi-Fi
- Bluetooth
- Cellular networks (4G/5G)
- Satellite Internet
- Hotspots

Internet Services and Cloud Computing

The Internet provides many **services** that people use for communication, information, entertainment, education, and work. Common Internet services include the **World Wide Web, email, instant messaging, video conferencing, streaming media, online shopping, social media, and file sharing**. These services rely on networks of computers and servers that exchange information across the Internet.

Common Uses

- Web
- Email
- Streaming
- Social media
- Video Conferencing
- Cloud storage
- Online collaboration

Many Internet services now depend on **cloud computing**, which provides applications, storage, and computing resources from remote data centers. For example, a student might use a web-based application to create a document, store it in cloud storage, and share it with classmates for collaboration. Streaming services, online games, AI applications, and video-conferencing platforms also frequently rely on cloud infrastructure.

Although the **Internet and cloud computing are closely related, they are not the same thing**. The Internet is the global network that connects devices and networks, while cloud computing uses that network to deliver computing resources and services. In simple terms, **the Internet provides the connection; the cloud provides many of the services and resources accessed through that connection**.

Staying Safe Online

Staying safe online means protecting your devices, accounts, personal information, and privacy while using the Internet. Online threats can include **phishing, malware, scams, identity theft, account theft, and fraudulent websites**. Users should be cautious about unexpected messages, links, attachments, and requests for personal or financial information. A message that creates urgency, such as claiming that an account will immediately be closed, should be verified before taking action.

Staying Safe Online

- Secure websites (HTTPS)
- Strong passwords
- Multi-factor authentication
- Public Wi-Fi
- VPN overview
- Phishing review
- Responsible online behavior

Good security habits can greatly reduce online risks. Use **strong, unique passwords** for important accounts and enable **multi-factor authentication (MFA)** whenever possible. Keep operating systems, browsers, and applications updated so that known security vulnerabilities are corrected. Users should also review privacy and sharing settings, use secure networks when accessing sensitive information, and think carefully before posting personal information online.

AI has made online safety more challenging because convincing **fake images, voices, videos, messages, and websites** can be created quickly. Rather than trusting content simply because it looks or sounds authentic, users should consider the source, verify unusual requests through another method, and pause before sending money, passwords, verification codes, or sensitive information.



Chapter Summary

Computer networks connect computers and other devices so they can **communicate, exchange data, and share resources**. Networks range from small personal and local networks to wide area networks that connect devices across large geographic areas. The **Internet** is the world's largest network, connecting millions of smaller networks around the globe.

Networks depend on hardware such as **network interface controllers (NICs), switches, routers, modems, wireless access points, and communication media**. Data can travel through **wired connections**, including Ethernet and fiber-optic cable, or through **wireless technologies**, including Wi-Fi, Bluetooth, cellular networks, and NFC. Information sent across the Internet is divided into **packets**, while protocols such as **TCP/IP** provide rules for communication. **IP addresses** identify devices, and the **Domain Name System (DNS)** helps translate familiar domain names into IP addresses.

Networks make many familiar Internet services possible, including the **World Wide Web, email, messaging, video conferencing, streaming, social media, and cloud computing**. Cloud computing uses Internet connections to provide applications, storage, and computing resources from remote data centers.

Because networks connect devices and information, **security is an important responsibility for every Internet user**. Strong passwords, multi-factor authentication, software updates, careful sharing, and awareness of phishing, scams, malware, and AI-generated deception can help users protect their devices, accounts, privacy, and personal information.