SAMPLE CHAPTER

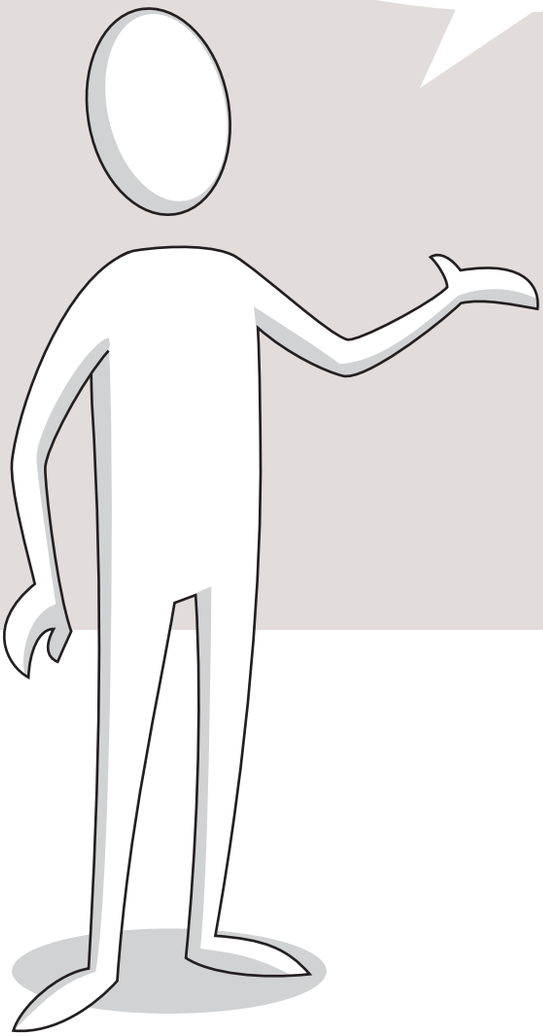
Level Up

Through **Digital Discoveries** 12

Mc Graw Hill | binarylogic

Contents

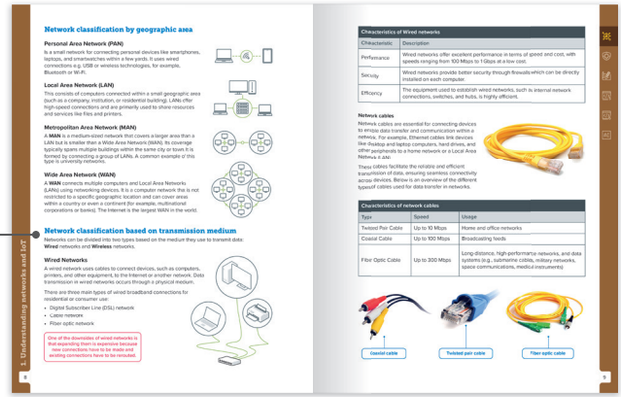
Welcome!
You're about to embark on
a journey that goes beyond just using
technology—you'll learn how it really works
and how you can shape the future with it.
From coding challenges to real-world
applications, this course will help you sharpen
your skills and spark new ideas.
Let's level up together!



Key Features

An innovative approach to building digital competencies, developed by expert educators.

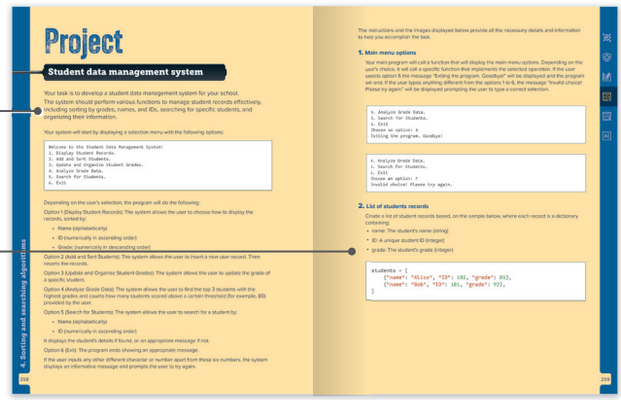
Each unit offers straightforward explanations and contemporary examples, making technology concepts accessible and relevant.



Curriculum aligns with the latest industry standards, preparing students for certifications and future careers.

Every unit includes a variety of tasks and activities designed to help students build essential digital competencies.

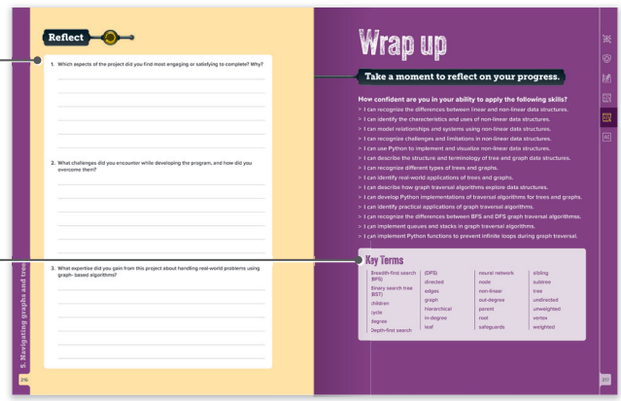
Projects and exercises throughout the course reinforce students' understanding and practical application of digital skills in real-world scenarios.



Well-defined learning goals and hands-on, applicable digital skills.

Students learn about platform diversity, expanding their digital toolkit and adaptability.

Each unit organizes key terms that are crucial for digital literacy, equipping students for today's technology-driven workplace.



1. Understanding networks and IoT

Imagine a world where networks—wired, wireless, mobile, and satellite—work together to make life easier. This unit focuses on how these networks enable the Internet of Things (IoT) to connect everyday devices seamlessly. Get ready to uncover the technologies powering our smart and connected world.

Learning Objectives

In this unit, you will:

> investigate how wired and wireless networks work.
> evaluate the advantages and limitations of various network topologies.
> trace how mobile networks evolved from 1G to 5G.
> describe the functions of satellites in communication networks.
> identify what IoT is and its key components.
> explore how IoT systems connect and share information.
> discover how IoT platforms manage devices.
> examine how data flows within an IoT system.
> analyze examples of IoT applications in different fields.
> address the challenges of implementing IoT systems.

LESSON 1

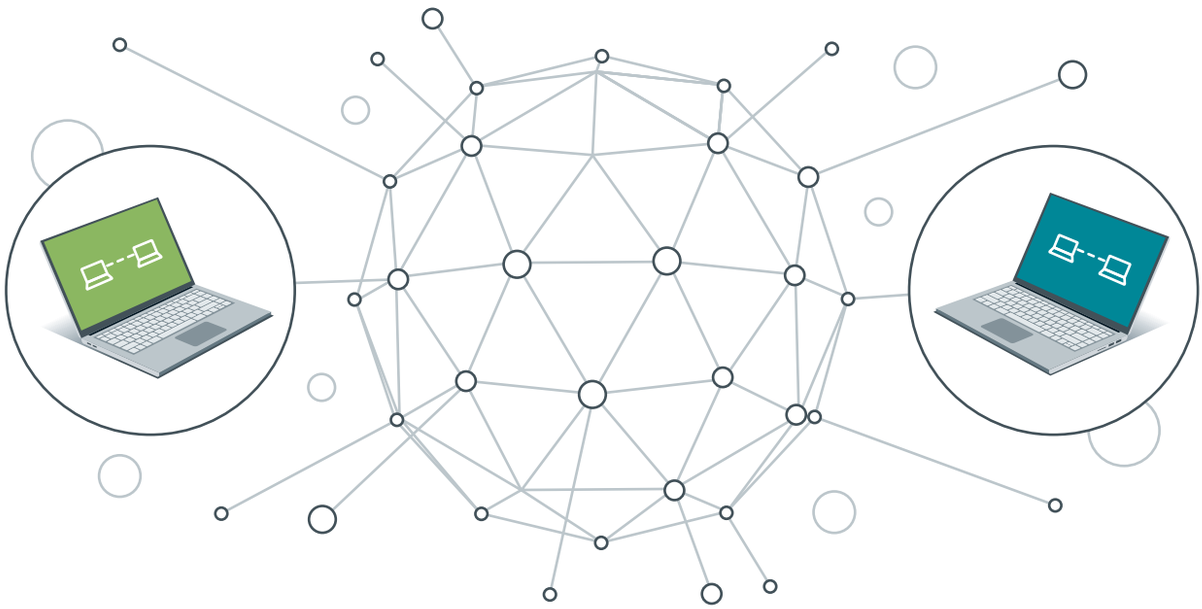
Wired and wireless networks

Do you know what a computer network is? Can you think of devices in your home that are connected to a wired or wireless network?

Networks are categorized into different types based on geographic area, transmission medium, network topology, and the use of wired and wireless networks in communications. This lesson introduces the classification of networks, their concepts, and their characteristics.

Computer networks

A computer network is a collection of computers that are interconnected to share resources such as data and devices. It is made up of two main components: peripheral devices and the communication media that transfer data between these devices.



Network classification

Networks can be classified into several main categories based on the following features:

- The geographic area covered by the network (Personal Area Network, Local Area Network, Metropolitan Area Network, Wide Area Network).
- The transmission medium for data (Wired or Wireless).
- The network topology (Bus, Ring, Star, Mesh, Hybrid).

Network classification by geographic area

Personal Area Network (PAN)

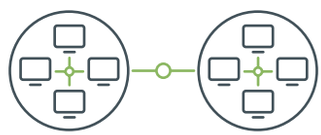
A **PAN** is a small network for connecting personal devices, like smartphones, laptops, and smartwatches, within a few yards. It uses wired connections (e.g., USB) or wireless technologies (e.g., Bluetooth or Wi-Fi).

Local Area Network (LAN)

A **LAN** consists of computers connected within a small geographic area, such as a company, institution, or residential building. LANs offer high-speed connections and are primarily used to share resources and services like files and printers.

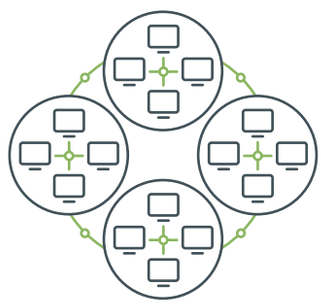
Metropolitan Area Network (MAN)

A **MAN** is a medium-sized network that covers a larger area than a LAN but is smaller than a Wide Area Network (WAN). Its coverage typically spans multiple buildings within the same city or town. It is formed by connecting a group of LANs. A common example of this type is university networks.



Wide Area Network (WAN)

A **WAN** connects multiple computers and Local Area Networks (LANs) using networking devices. It is a computer network that is not restricted to a specific geographic location and can cover areas within a country or even a continent, such a multinational corporations or banks. The Internet is the largest WAN in the world.



Network classification based on transmission medium

Networks can be divided into two types based on the medium they use to transmit data: **wired** networks and **wireless** networks.

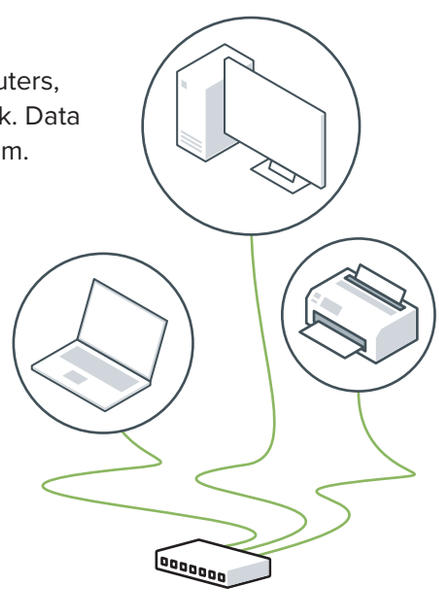
Wired networks

A wired network uses cables to connect devices, such as computers, printers, and other equipment, to the Internet or another network. Data transmission in wired networks occurs through a physical medium.

There are three main types of wired broadband connections for residential or consumer use:

- Digital Subscriber Line (DSL) network
- Cable broadband network
- Fiber optic network

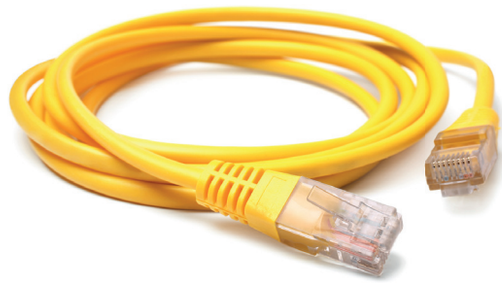
One of the downsides of wired networks is that expanding them is expensive, because new connections have to be made and existing connections have to be rerouted.



Characteristics of wired networks	
Characteristic	Description
Performance	Wired networks offer excellent performance in terms of speed and cost, with speeds ranging from 100 Mbps to 1 Gbps at a low cost.
Security	Wired networks provide better security through firewalls, which can be directly installed on each computer.
Efficiency	The equipment used to establish wired networks, such as internal network connections, switches, and hubs, is highly efficient.

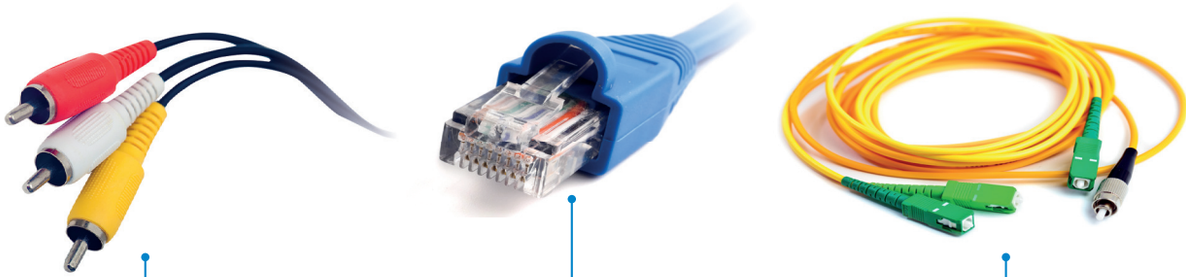
Network cables

Network cables are essential for connecting devices to enable data transfer and communication within a network. For example, Ethernet cables link devices like desktop and laptop computers, hard drives, and other peripherals to a home network or a Local Area Network (LAN).



These cables facilitate the reliable and efficient transmission of data, ensuring seamless connectivity across devices. The following table provides an overview of the different types of cables used for data transfer in networks.

Characteristics of network cables		
Type	Speed	Usage
Coaxial Cable	Up to 100 Mbps	Broadcasting feeds
Twisted Pair Cable	Up to 10 Mbps	Home and office networks
Fiber Optic Cable	Up to 300 Mbps	Long-distance, high-performance networks, and data systems (e.g., submarine cables, military networks, space communications, medical instruments)



Coaxial cable

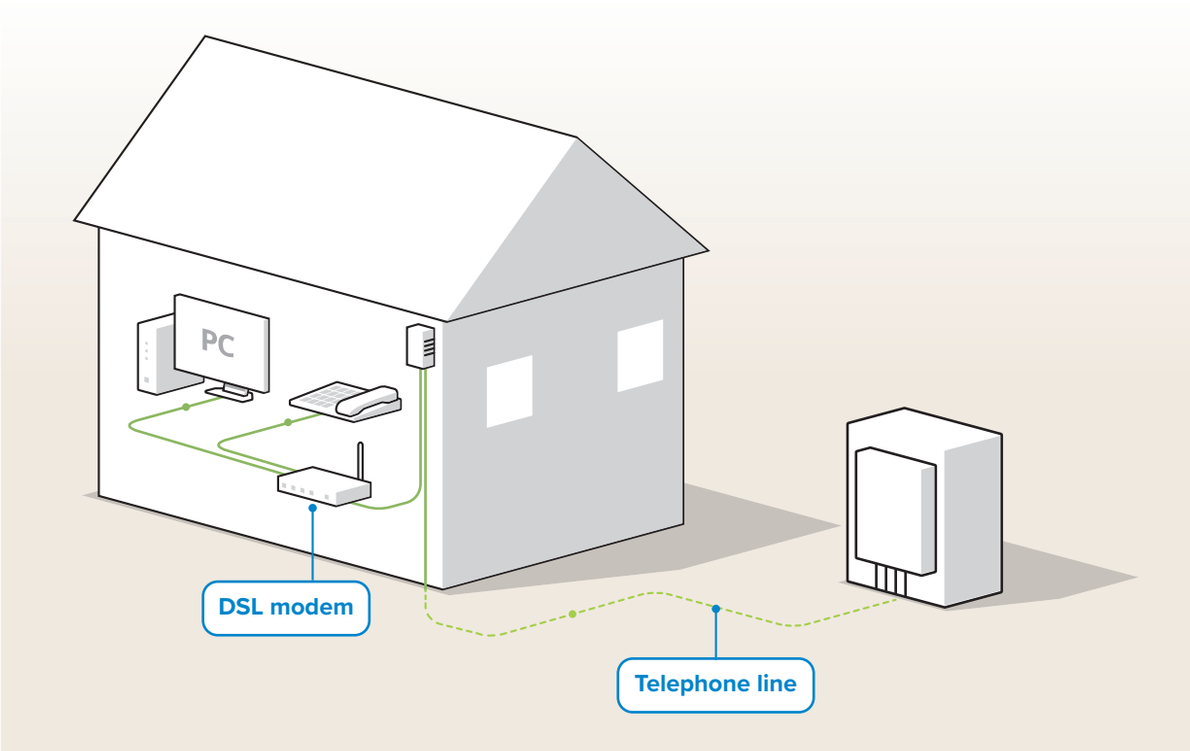
Twisted pair cable

Fiber optic cable

Digital Subscriber Line (DSL)

Digital Subscriber Line (DSL) is a wired communication technology that uses existing telephone lines to transmit high-bandwidth data, such as multimedia and video, to service subscribers. DSL provides dedicated, point-to-point access to the public network.

With **DSL**, both voice and Internet data can flow simultaneously over the same line, allowing users to utilize the Internet and phone services without interruptions. This requires a specialized modem called a DSL modem, which connects to a traditional telephone line.



There are various types of DSL networks, including:

Asymmetric Digital Subscriber Line (ADSL)

With ADSL, download speeds are significantly faster than upload speeds. This type of DSL allows for a maximum download speed of 24 Mbps and an upload speed of 1 Mbps.

Very High-Speed Digital Subscriber Line (VDSL)

VDSL is one of the fastest DSL types, offering average download speeds of up to 50 Mbps and upload speeds of up to 2 Mbps. This type of connection requires copper wires or fiber optic cables to transmit data to homes or offices.

Very High-Speed Digital Subscriber Line 2 (VDSL2)

VDSL2 is an enhanced version of VDSL and is ideal for services such as high-definition television (HDTV), video streaming, voice services, and online gaming.

- Download Speeds: Up to 100 Mbps (can exceed 200 Mbps over short distances).
- Upload Speeds: Between 50 and 100 Mbps.

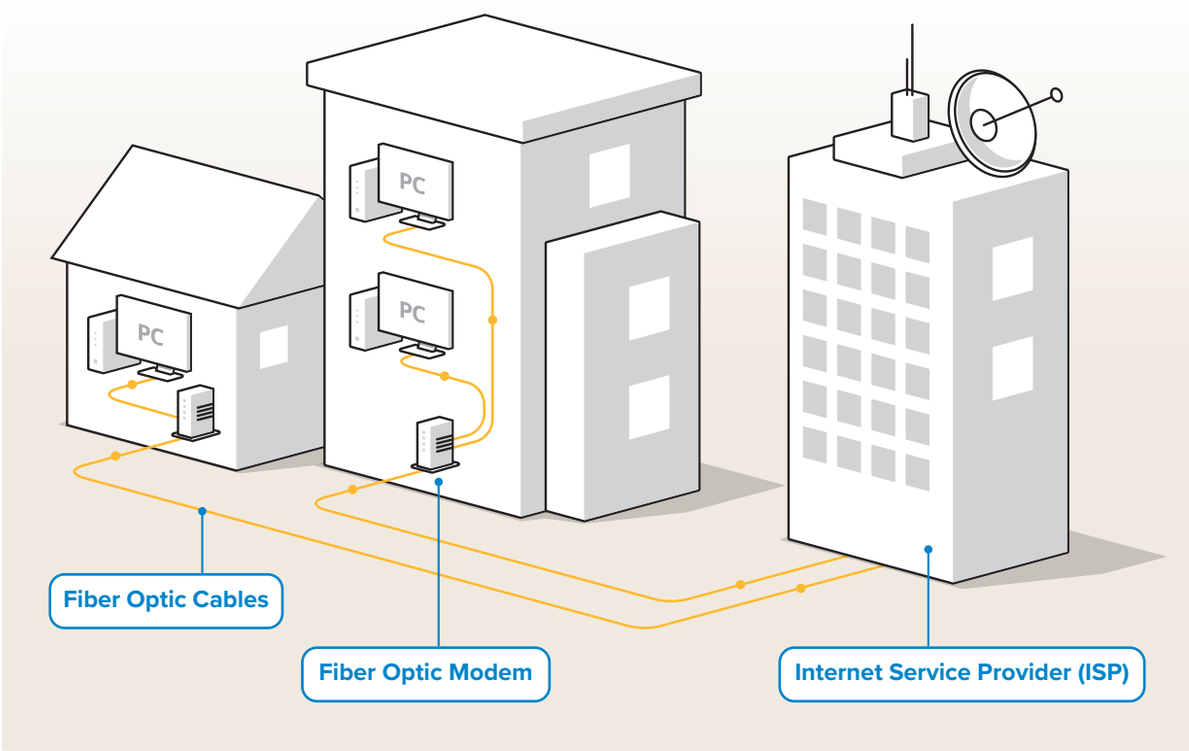
VDSL2 is designed to meet the demands of modern multimedia and interactive services.

Fiber Optic Network

Fiber optic technology provides the fastest Internet speeds available today, as it uses light to transmit data through fiber optic cables. Download and upload speeds can reach up to 2.5 Gbps (Gigabits per second). This connection is also capable of transmitting data over much longer distances than DSL or wired Internet.

The service requires a specialized modem called a **Fiber Optic Modem**. Homes and businesses can be directly connected to fiber optic cables, but this often requires replacing existing infrastructure, such as copper telephone wires and coaxial cables.

Fiber to the home (FTTH) and **Fiber to the business (FTTB)** deliver communication signals using fiber optic cables, replacing older copper cables to connect directly from the provider to the home or business.



Wireless networks

A wireless network connects devices without the need for physical wires. It uses radio wave technology to transmit information and link devices to the network or applications. Common types of wireless networks include:

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

When referring to the wireless version of a network type, we add the letter 'W' to indicate that the network is wireless. For example, a Local Area Network (LAN) becomes a Wireless Local Area Network (WLAN).

Key characteristics of wireless networks	
Characteristic	Description
Performance	The performance of Wi-Fi wireless networks primarily depends on distance. As the distance between devices and the wireless access point increases, network speed decreases. Additionally, the performance of the wireless network diminishes as the number of devices using it increases.
Security Concerns	Data can be intercepted and eavesdropped upon, which is why advanced encryption techniques are used to enhance security. Authentication mechanisms are also applied for the same reason, although some encryption methods currently in use can be easily breached.
Signal Interference	Some wireless networks rely on radio waves for communication, making their signals susceptible to interference from other electronic devices. Moreover, the constant movement of network users causes signal instability, making network management more challenging.
Scalability	Wireless networks are very easy to expand. A new user can be added by issuing a password and updating it on the server.

Classifying wireless networks

Wireless networks are classified by signal range and technology, which determine their coverage area and intended use. These classifications help define the purpose, scale, and applications of different wireless technologies.

Classification of wireless networks based on the range of their signal		
Network type	**Signal range**	**Technology used**
Personal Area Network (PAN)	About 10 cm for NFC, 10 meters for Bluetooth	Bluetooth, NFC (Near-Field Communication)
Local Area Network (LAN)	Within a building or organization	Wi-Fi
Metropolitan Area Network (MAN)	City-wide coverage	WiMAX
Wide Area Network (WAN)	Worldwide coverage	Cellular Networks

Hot spots

The term **hot spot** refers to wireless local networks that provide users with access to the Internet, either for free or for a fee. These are commonly found in public places, such as libraries, airports, and government offices.

Access points

Signal strength is an important aspect of wireless networks. The signal weakens as the distance from the transmitter increases. This problem can be solved by using access points to strengthen the wireless signal. However, factors such as building structure, geography, and interference from other devices operating on similar frequencies—like microwave ovens or mobile phones—can affect the efficiency of access points.

Wireless network technologies

Several wireless technologies have been developed to support wireless networks. Among the most common are Wi-Fi, Bluetooth, Near Field Communication (NFC), and IEEE 802.15.4.

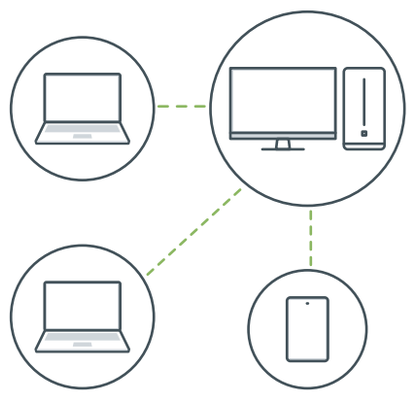
Bluetooth is a wireless technology for short-range data exchange. It is used in a variety of devices, including cell phones, keyboards, mice, wireless headsets, gaming controllers, tracking devices, and location finders.

Wi-Fi is one of the most popular and widely used wireless technologies. It is commonly used in computers, smartphones, gaming consoles, IP cameras, smart TVs, printers, and many other devices.

NFC (Near Field Communication) is a technology that enables short-range communication between compatible devices using radio waves, most commonly found in smartphones. It allows NFC-enabled devices to store credit card information, enabling phones to be used for payments while shopping.

While NFC ensures secure data transmission that cannot be easily intercepted wirelessly, it has some limitations, including a very short range (up to 4 inches) and slower data transfer speeds compared to Bluetooth.

IEEE 802.15.4 is a wireless access technology designed for low-cost, low-data-rate devices powered by electricity or batteries. It is inexpensive and can support a longer battery life.



This networking technology is easy to set up due to its small protocol stack, simplicity, and flexibility, making it ideal for applications requiring minimal energy consumption and low complexity.

Network classification based on topology

In the world of computer networks, the term topology refers to the physical or logical layout of how devices are connected. Here are some basic network topologies:

Bus Topology

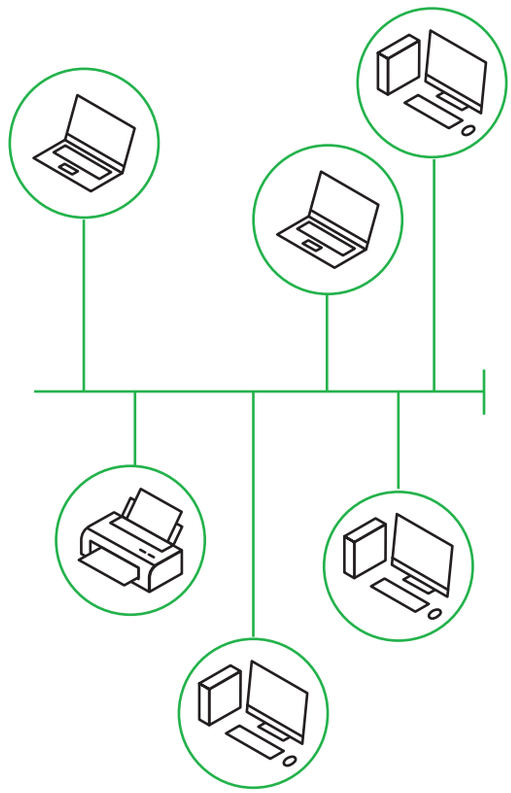
In a Bus Topology, all devices are connected to a central backbone, which serves as the "spine" of the network.

Advantages:

- It is the simplest network topology for connecting peripherals or computers in a linear layout.
- It is highly cost-effective compared to other topologies.

Disadvantages:

- Troubleshooting and fixing issues can be difficult.
- All devices share the same backbone, leading to collisions when multiple devices attempt to transmit data simultaneously.
- Collisions disrupt data transfer across the network.



Ring Topology

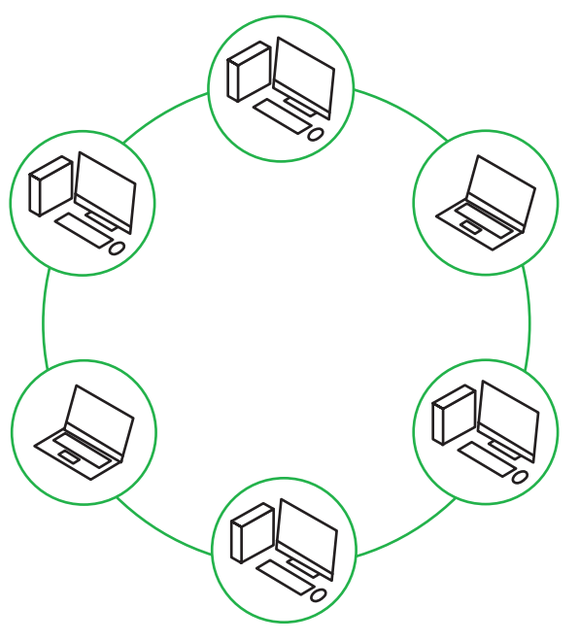
In a Ring Topology, devices are connected in a circular loop, and data packets travel in one direction until they reach their destination.

Advantages:

- Reduces data collisions by ensuring one-directional flow.
- Devices don’t need direct connections to communicate.
- New devices can be added without impacting the network’s performance.

Disadvantages:

- All data must pass through every point in the network, which can create a bottleneck.



Star Topology

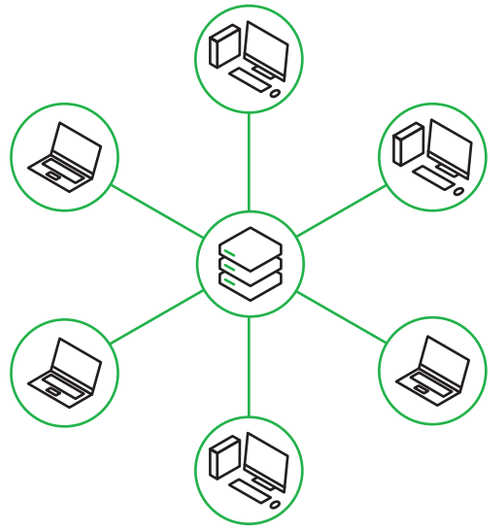
In a Star Topology, all devices are connected to a central device, such as a switch or hub.

Advantages:

- Easy to manage and expand the network by adding new devices.
- Failure of one device, that is not the central device, doesn't affect the rest of the network.

Disadvantages:

- Failure of the central device causes the entire network to fail.



Mesh Topology

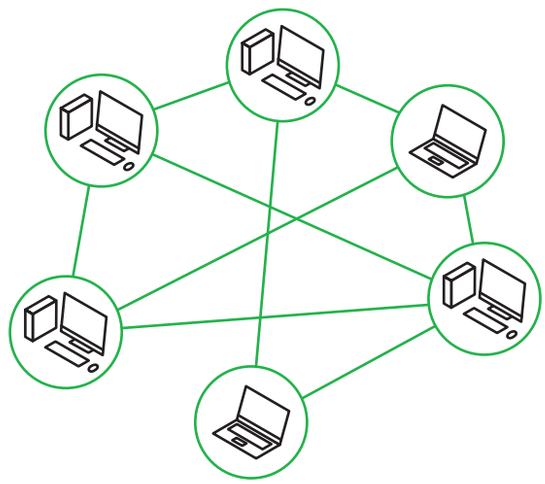
In a Mesh Topology, every device is connected to every other device.

Advantages:

- Supports simultaneous data transfer between devices.
- The network remains operational even if one or more connections fail.

Disadvantages:

- Costly and complex to set up due to the large number of connections required.



Hybrid Topology

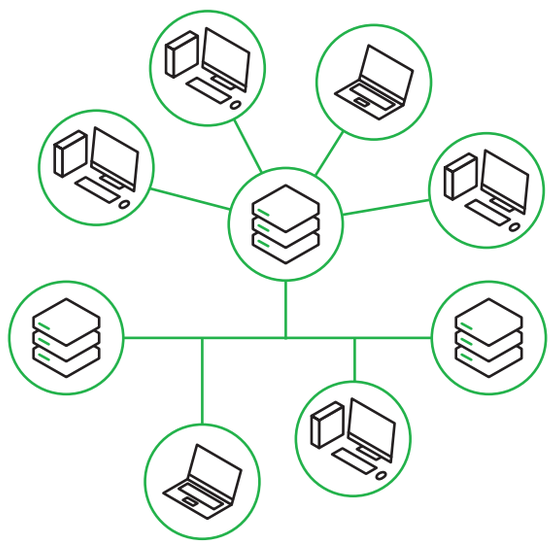
A Hybrid Topology combines two or more types of topologies (e.g., Star, Ring, Bus, Mesh). This layout is often used when integrating two different networks.

Advantages:

- Flexible and can be upgraded by adding new devices without impacting performance.
- Provides optimal performance by adapting to specific network needs.

Disadvantages:

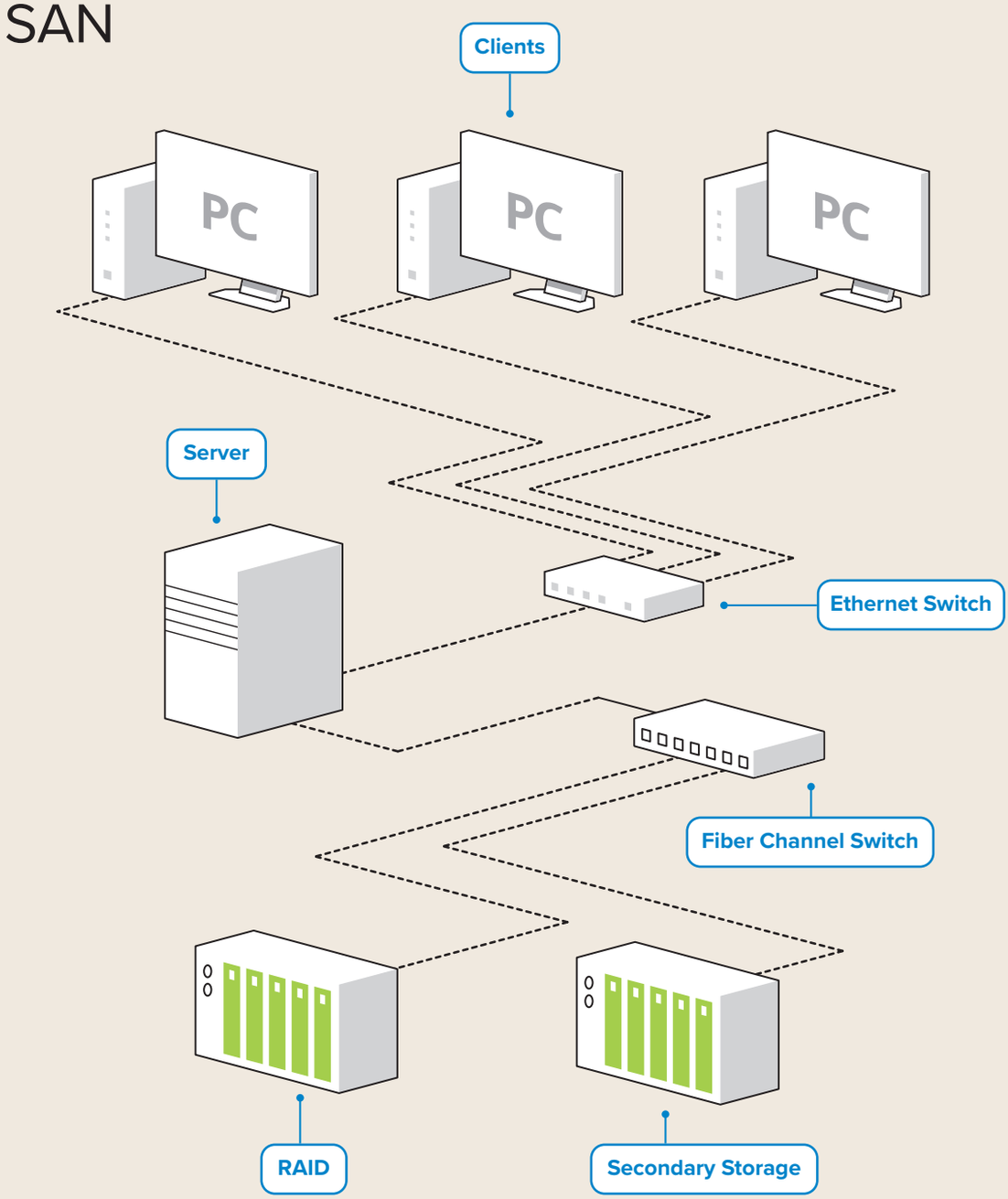
- Costly to implement due to the large number of connections and components required.



Storage Area Network (SAN)

A **Storage Area Network (SAN)** is a specialized type of network that allows servers to access shared data stored on network devices. Typically, a SAN is a dedicated network for storage devices that cannot be accessed by other devices through the Local Area Network (LAN).

As illustrated in the following diagram, SANs usually consist of clients, switches, storage media, and storage devices interconnected using various technologies, topologies, and protocols. Microsoft SQL Server databases are an example of SAN use. These databases store an organization's most valuable data, requiring the highest levels of performance and availability.



Hands on!

1. Read the following sentences and put a check mark for True or False.

	True	False
1. A Wide Area Network (WAN) is limited to a single building or institution.		
2. Wired networks use cables as the medium to transmit data, offering better security through firewalls.		
3. Twisted pair cables are typically used for high-performance, long-distance data systems like submarine cables.		
4. Fiber optic networks have slower upload and download speeds compared to DSL networks.		
5. Wireless networks use radio wave technology to transmit information and connect devices without physical wires.		
6. Wi-Fi allows communication between devices over very short distances, typically up to 4 inches.		
7. In a Star Topology, the failure of one device that is not the central device does not affect the rest of the network.		
8. In a Ring Topology, data packets travel in multiple directions simultaneously to reach their destination.		
9. A Storage Area Network (SAN) is a dedicated network for storage devices that cannot be accessed by other devices through the LAN network.		

2. Read the questions and put a check mark for the correct answer.

1. Which of the following is a primary characteristic of fiber optic networks?
   - a. They use copper cables to transmit data over short distances.
   - b. They rely on radio waves for data transmission.
   - c. They use light to transmit data over long distances at high speeds.
   - d. They are limited to speeds of up to 10 Mbps.

2. What is the primary purpose of an access point in a wireless network?
   - a. To increase the data encryption level.
   - b. To reduce the number of connected devices.
   - c. To strengthen the signal in areas with weak coverage.
   - d. To allow devices to connect using coaxial cables.

3. What is a key advantage of a Mesh Topology?
   - a. It is cost-effective to set up and maintain.
   - b. It supports simultaneous data transfer between devices.
   - c. It eliminates the need for access points.
   - d. It simplifies the process of troubleshooting network issues.

4. Which of the following is true about Hybrid Topology?
   - a. It is the most cost-effective network topology.
   - b. It is used to integrate multiple topologies, such as Star and Ring.
   - c. It cannot adapt to specific network needs.
   - d. It does not support the addition of new devices.

5. Which topology connects devices in a circular loop where data packets travel in one direction?
   - a. Star Topology
   - b. Mesh Topology
   - c. Bus Topology
   - d. Ring Topology

6. In which network topology are all devices connected to a central backbone?

- a. Bus Topology
- b. Mesh Topology
- c. Ring Topology
- d. Hybrid Topology

3. List two advantages and two disadvantages of wired networks compared to wireless networks.

4. Explain the difference between ADSL, VDSL, and VDSL2.

5. Imagine your school is upgrading its network system. Should it implement a wired network, a wireless network, or a combination of both? Provide reasons to support your decision, considering factors like cost, coverage, and performance.

LESSON 2

The evolution of mobile networks

Do you know what a mobile network is? Have you ever wondered how the Global Positioning System (GPS) functions?

Humans have created many technologies that make life easier and improve communication and transportation around the world. Mobile networks are important in daily life and have evolved over time. Satellite networks and the Global Positioning System (GPS) are also very useful and have many everyday applications.

Mobile networks

After the development of landline phones for communication, technology continued to evolve, leading to the widespread use of mobile phones. Mobile phones rely on mobile networks to support their functions. A mobile network is a cellular network composed of base stations (antennas), cell phones, and digital switching centers.

Base stations

Base stations provide connectivity between mobile devices and the public telephone network. They consist of:

- Microwave antennas
- Transmission towers
- Equipment stations

Each tower covers a specific geographic area called a "cell," which is why it is referred to as a cellular network. These cells are designed to ensure that users remain within the coverage area. The size and range of each cell are determined after considering factors such as obstacles (trees, mountains, buildings) and the number of users.

Every base station has a maximum frequency range available for Internet and data usage. Service providers increase bandwidth to accommodate the growing number of users.

Generations of Mobile Networks

First Generation (1G)

The first generation (1G) of wireless telephone and mobile communication technologies appeared in the 1980s and gained widespread use in the early 1990s. It introduced cellular technology, a key innovation compared to earlier systems. 1G relied on the Advanced Mobile Phone System (AMPS), an analog communication standard. While it allowed voice calls between subscribers within the same country, data transfer speeds were limited to 24 Kbps. Analog systems like 1G are no longer in use and have been replaced by modern digital technologies.

Second Generation (2G)

The second generation (2G) marked a significant advancement by replacing analog systems with digital technology. Developed in Finland in 1991, the Global System for Mobile Communications (GSM) became the new standard, enabling features such as SMS (Short Message Service), MMS (Multimedia Messaging Service), and picture messaging. Data encryption improved privacy, while digital signals consumed less power, leading to longer battery life for mobile devices. However, 2G required strong digital signals for reliable operation. Data transfer speeds reached up to 64 Kbps.

Third Generation (3G)

The third generation (3G) brought further innovation by building on 2G standards and introducing technologies like the Universal Mobile Telecommunications System (UMTS) and Code Division Multiple Access 2000 (CDMA2000). 3G combined the features of 2G with new protocols, offering faster data transfer speeds of up to 2 Mbps. This generation enabled high-speed Internet access, video calls, and mobile TV, making it a major step forward in multimedia communication.

Fourth Generation (4G)

The fourth generation (4G) represented a pivotal milestone in wireless communications. Offering significantly higher speeds than 3G, 4G reduced latency and allowed data transfer rates of up to 1 Gbps. This improvement made 4G ideal for high-quality voice calls and transformed smartphones into versatile devices capable of replacing computers in certain tasks. Its high-speed capabilities proved particularly useful in areas with limited broadband connectivity.

Fifth Generation (5G)

The fifth generation of mobile networks is the latest in cellular technology. Mobile communications are now faster and more efficient, meeting the growing demand for Internet-connected devices.

5G uses a new type of mobile network with redesigned antenna systems. This technology is built on three pillars: higher speeds, broader networks, and lower latency. These new networks can transfer data at extremely high speeds (up to 10 or 20 Gbps) to multiple users with high precision and minimal delay. While 5G offers speeds up to 20 Gbps in ideal conditions, real-world speeds can vary due to factors like network congestion or device limitations.

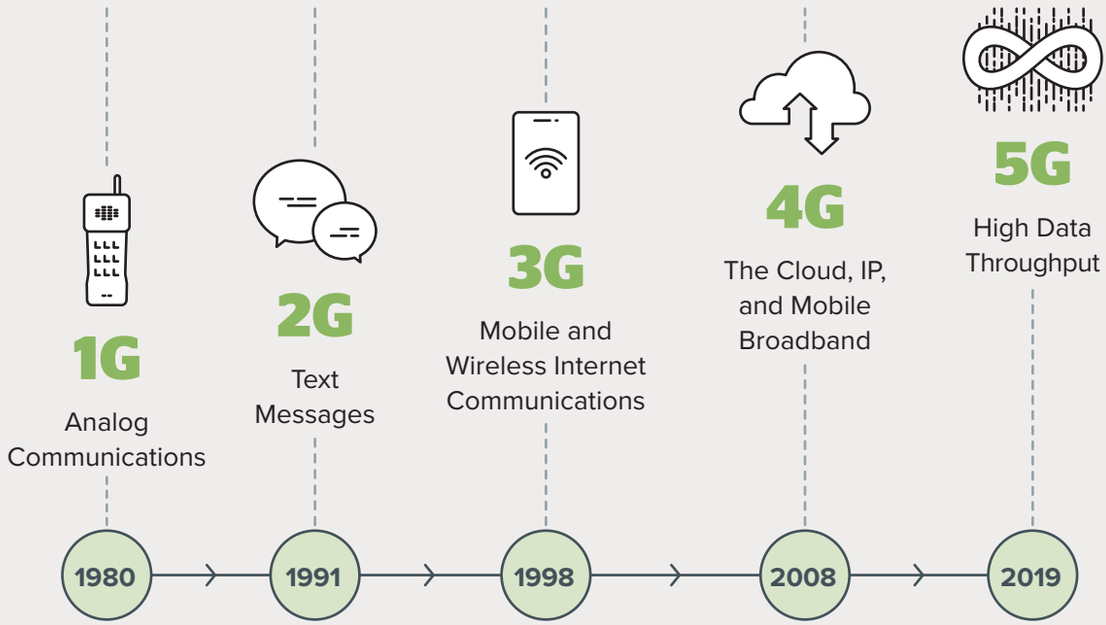
This technology will revolutionize the world, enabling and expanding the spread of technologies that constitute the Internet of Things (IoT), such as self-driving cars, virtual reality glasses, automated systems, and other smart technologies.

5G networks and services are now available in many countries around the world. Meanwhile, some tech companies and research labs have already started testing sixth-generation (6G) models, as the innovation journey never stops.

There are two numbers that indicate data transfer speed: one is ideal, and the other is real.

The ideal number represents the speed that a particular technology can support, measured in a lab under perfect conditions. In contrast, the real number reflects the real-world speed experienced by the user when using their device.

Development of the Fifth Generation (5G)



Bridge mode

Bridge mode is a networking technique that integrates existing network infrastructures with wireless technology to enhance connectivity. It is especially valuable in areas with slow broadband services. By using devices like 4G routers, Bridge Mode can act as a gateway to provide high-speed Internet access. Additionally, it can serve as a backup solution in case the primary broadband connection fails. This approach ensures reliable and consistent connectivity for both residential and commercial applications.

Satellites

Satellites can be divided into two types: **natural satellites** and **artificial satellites**. The natural satellite of Earth is the Moon, which is visible in the sky. On the other hand, an artificial satellite is a human-made device launched into space to orbit Earth or other planets in a specific orbit.

Satellite networks

Satellite networks use artificial satellites for communication functions. Unlike land-based networks, they cover larger distances and have a completely different shared bandwidth, network design, setup, operation, operating costs, and supported applications.

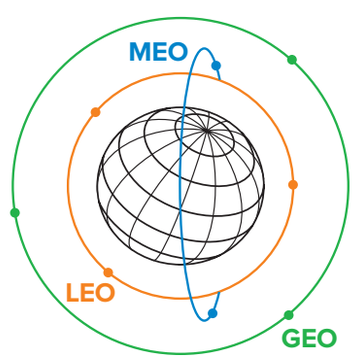
The primary role of satellite networks is to extend access to telecommunication, television applications, and high-speed Internet in areas where installing and maintaining cable networks is challenging. These networks also provide services to ships, airplanes, vehicles, and locations beyond the reach of land-based networks. Satellites play a significant role in monitoring space, Earth, and weather conditions. They are also highly beneficial in military communication applications, GPS systems, mobile communication networks, and broadcast services.

There are three categories of orbits around Earth:

High Earth Orbit (Geostationary Orbit - GEO)

Medium Earth Orbit (MEO)

Low Earth Orbit (LEO)



Satellite Internet access

Satellite Internet serves individuals who cannot access land-based service provider systems, enabling them to connect to the Internet via satellites. This requires a satellite dish on the ground and a continuous connection to the satellite. Satellite Internet is generally more expensive than land-based connections and can be slower at times. A notable feature of this connection is latency, which refers to the time it takes for information to complete a round trip via satellite communication.

History

According to the United Nations Office for Outer Space Affairs (UNOOSA), as of April 2021, there were 7,389 satellites orbiting Earth.

Global Positioning System (GPS)

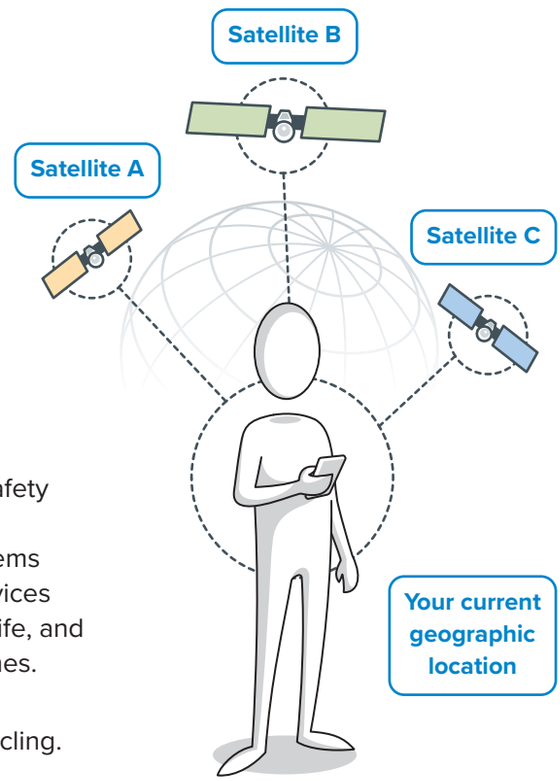
The **Global Positioning System (GPS)** is a satellite navigation system developed by the U.S. Department of Defense in the 1970s. Initially designated for military purposes, it was made available for civilian use in the 1980s.

GPS provides precise location capabilities 24 hours a day, anywhere in the world. The GPS network consists of approximately 30 satellites orbiting Earth twice daily. The orbits are designed so that six satellites are visible from most locations on Earth at any time. These satellites broadcast radio signals with their location, status, and precise time from onboard atomic clocks.

A GPS device receives these radio signals and calculates its distance from each visible satellite. By determining the distances to at least four satellites, a GPS device can calculate its position on Earth in three dimensions. For two-dimensional positioning, signals from at least three satellites are required. The process used to determine a location is called **triangulation**, a mathematical method for measuring distances.

GPS tracking technology

The Global Positioning System (GPS) is a method for accurately locating objects. This system is embedded in many devices, such as cell phones and vehicles. Examples of its uses include locating vehicles for their owners to track their routes across the country or the world, tracking people such as children or the elderly, or monitoring and studying animals. However, the person or object to be tracked must carry a tracking device.



There are two types of tracking devices: **active** and **passive**.

- Active tracking devices are used for security and safety purposes. They can monitor elderly people with conditions such as Alzheimer's and lost or stolen items like bags, cars, laptops, and cell phones. These devices can also be used for tracking pets, monitoring wildlife, and conducting research or playing location-based games.
- Passive tracking devices are used for measuring distances during activities like skiing, running, or cycling.

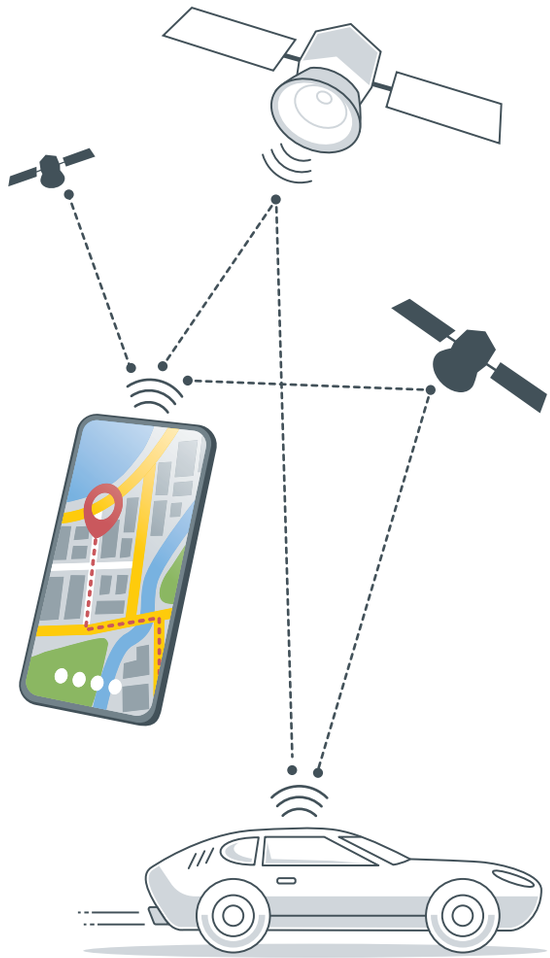
Comparison of tracking devices	
Active trackers	**Passive trackers**
No continuous real-time tracking	Continuous real-time tracking
Monitors and stores data in its internal memory for later uploading to the computer for analysis	Immediate data transmission to central devices such as servers
Low cost	High cost
No paid subscription required	Requires a paid subscription

Galileo Navigation System

The European Union, through the European Space Agency, developed the Galileo Navigation System, designed primarily for civilian purposes. The system is named after the Italian astronomer Galileo Galilei. According to the European Space Agency, the fully deployed Galileo system will consist of 24 operational satellites and six spare satellites in Earth's medium orbits (MEO), positioned at an altitude of 14,429 miles.

The system uses two ground operation centers, one in Germany and the other in Italy, to manage the satellites. Galileo aims to provide European users with independence from other navigation systems such as the American GPS or the Russian GLONASS.

Galileo is widely used in search and rescue operations. The satellites are equipped with transceivers that track distress signals from emergency beacons and relay them to rescue coordination centers, which then initiate rescue operations. This new system provides location accuracy within three feet under optimal conditions, with most of its services offered free of charge. Most new generations of cell phones now support Galileo.



Electronic Tracking

The electronic tracking industry has developed in both fascinating and concerning ways. Many people dislike the idea of being tracked or having their data monitored, such as visited websites, email content, or personal devices. Web browser developers are addressing deceptive data monitoring practices, and some governments are enacting strict policies against electronic tracking.

The primary information collected by tracking services includes "mouse click data," which gathers insights into users' browsing habits and patterns, including what they click on and their basic data.

Cameras have become smaller, making them easy to conceal. People now have cameras on their cell phones and, more recently, in their glasses. As a result, a photo or video of you could be posted online without your knowledge.

Smart Tip

In addition to GPS, other navigation systems are currently in use or under development. Examples include the BeiDou Navigation Satellite System (China), NAVIC (India), and the Quasi-Zenith Satellite System (Japan).

Hands on!

1. **Read the following sentences and put a check mark for True or False.**

	True	False
1. Bridge Mode can act as a gateway to provide high-speed Internet access.		
2. A base station provides connectivity between mobile devices and the public telephone network.		
3. 1G technology allowed data transfer speeds of up to 64 Kbps.		
4. Each base station covers a specific geographic area called a "cell."		
5. 4G reduced latency and allowed data transfer rates up to 10 Gbps.		
6. Satellite Internet is generally faster and less expensive than land-based Internet connections.		
7. GPS provides precise location information 24 hours a day, anywhere in the world.		
8. Triangulation requires signals from at least four satellites for two-dimensional positioning.		
9. Passive tracking devices transmit data immediately to a central server.		
10. Electronic tracking only collects data about email content and ignores browsing habits.		

2. Read the questions and put a check mark for the correct answer.

1. Which innovation did 2G technology introduce compared to 1G?
   - [ ] a. Analog voice communication
   - [ ] b. Cellular coverage for rural areas
   - [ ] c. Digital signals for improved privacy and data services
   - [ ] d. Support for real-time video streaming

2. What does a GPS device require to determine its position in three dimensions?
   - [ ] a. Signals from at least three satellites
   - [ ] b. Signals from one powerful satellite
   - [ ] c. Data transmitted through cellular networks
   - [ ] d. Triangulation from two satellites

3. Which of the following is a characteristic of 5G networks?
   - [ ] a. Only supports voice calls and SMS
   - [ ] b. Analog technology for greater efficiency
   - [ ] c. Support for Internet of Things (IoT) devices
   - [ ] d. Maximum speed of 64 Kbps

4. What distinguishes active tracking devices from passive ones?
   - [ ] a. Continuous real-time tracking
   - [ ] b. Low cost and no subscription required
   - [ ] c. Immediate data transmission to central servers
   - [ ] d. Requires a paid subscription

3. For each mobile network generation, complete the table by specifying the key technology or standard associated with it and its corresponding maximum data transfer speed.

Mobile network generation	Technology/standard	Speed
1G		
2G		
3G		
4G		
5G		

4. Explain how the GPS determines a device's location using satellites. In your answer, describe the role of satellites, the signals they send, and how the GPS device calculates its position.

5. What is one key difference between active trackers and passive trackers?

6. You are tasked with designing a communication system for a small village that is far from cities and lacks access to modern infrastructure. Would you recommend mobile networks, satellite networks, or a combination of both? Consider the village's needs, challenges, and available technologies, and explain your choice.

LESSON 3

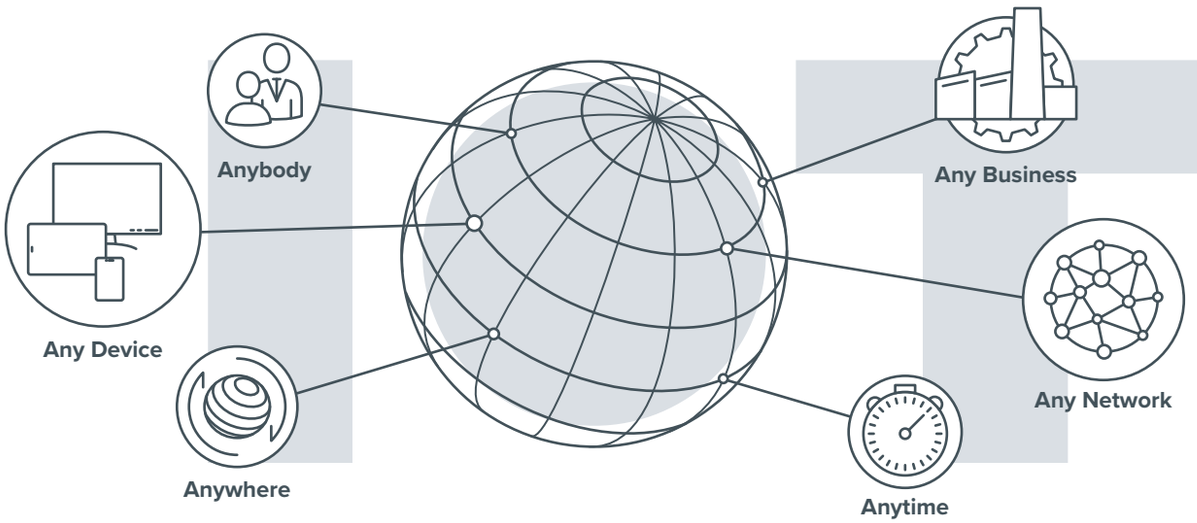
The fundamentals of IoT

Can you name devices such as smartwatches or voice assistants that connect to the Internet?
How do you think they work together?

What is the Internet of Things?

We currently live in a world where virtually anything imaginable can be online, communicate with other devices or people, and facilitate new services that improve our lives. The world is undergoing a significant technological transformation, from self-driving drones carrying food orders to wearable sensors monitoring our health. This progression is collectively known as the **Internet of Things (IoT)**.

The main objective of the IoT is to connect devices not already part of a computer network, whether private or public, like the Internet, so that they may share data and interact with people and other objects. The IoT is an evolution in technology that will enable devices to perceive and manage the physical environment by making objects autonomous and integrating them into an intelligent network.

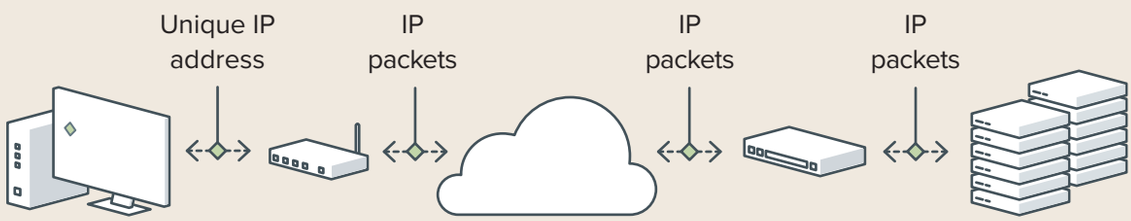


The history of the Internet of Things

The idea of using sensors on physical objects to interact over a network dates back to the 1980s. For example, university students experimented with remotely tracking the contents of a soda vending machine. At the time, technology was limited, and the Internet was not yet available. As networks became global, hardware companies developed smaller chips, CPUs, and sensors, leading to new applications. The Internet evolved from ARPAnet (created in 1969) into the modern Internet based on IP (Internet Protocol) and TCP (Transmission Control Protocol). By 1995, the U.S. government decommissioned the network backbone, creating an open framework for global connectivity.

Unique IP addresses became the foundation of today's connected world, allowing devices like smartphones, gaming consoles, and washing machines to connect to networks. Routers manage these devices and their data requests using public or private IP addresses.

IP routing process over the Internet

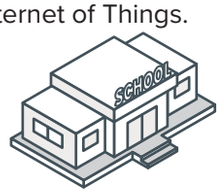


The rise of the Internet of Things (IoT)

In recent years, electronic devices have become smaller, more powerful, and more versatile. For instance, people who once relied on desktop computers now use smartphones, which are faster, have more memory, and can connect to wireless networks while running on battery power. Modern smartphones integrate several sensors, such as cameras, microphones, GPS, accelerometers, and gyroscopes. Advancements in miniaturization have also made it possible for devices to become so small that they can be embedded into other physical objects, expanding the possibilities for connected technologies.

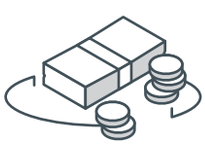
The evolution of the Internet of Things

The evolution of the Internet went through four phases, which also defined the development of the Internet of Things.



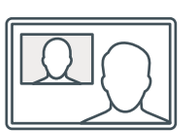
1. **Connectivity phase**

   In the early years of the Internet, only organizations and schools had Internet connectivity. Internet connection was uncommon for the typical individual. During the connectivity phase, more and more individuals gained access to the Web.



2. **Networked economy**

   With the advancement of technology, connection speeds continued to increase, and connectivity was no longer the primary obstacle. This phase focused on maximizing efficiency and profit through networking.



3. **Immersive experiences**

   The era of immersive experiences is defined by the emergence of social media, collaboration, and widespread device availability. Human interactions have been digitized, and applications are gradually transitioning to cloud infrastructure.

4. **Internet of Things**

   The final phase concerns the communication and transaction of data between almost every device connected to the Internet to provide solutions and experiences for various industries.

Applications enhanced through IoT

As the IoT becomes an integral part of technology solutions, it is increasingly combining with other technologies like artificial intelligence and robotics, either using them to improve IoT applications or enhancing them with IoT-enabled objects. The result is that a collection of existing and emerging technologies is applied to solve old or new problems in the most efficient way. The following table shows applications of emerging technologies that are enhanced through IoT technologies.

Applications enhanced through IoT	
Application	**Description**
Automation	Machines and technologies that aid in automation can be found throughout history. The capacity to automate an activity frequently results in increased speed, efficiency, and safety and reduced cost. Today, automation is what enables intelligent homes, intelligent buildings, and intelligent factories. It includes lighting controls, smart speakers, security systems, intelligent home products, and robots.
Computer vision	Sensors paired with AI algorithms enable computers to understand photos and videos, often better than humans can. Face recognition, helping drones and vehicles steer and avoid collisions, and improving machine learning models for assessing the accuracy of chemotherapy and other treatments through the analysis of photos and scans are all current applications of the technology. In industrial applications, this approach can increase the fault detection rate by 90% or more in various processes.
Natural Language Processing (NLP)	This field employs linguistics, computing, and Artificial Intelligence to understand and implement human language. Alexa, Siri, and Google Assistant are exemplary NLP user interfaces and voice interfaces are becoming increasingly prevalent on linked devices and equipment. This technology is also applied to chatbots and automated web services requiring typing or speaking. Nowadays, researchers are developing methods for systems to recognize emotions and intentions.
Machine Learning	This technology, a subfield of AI, interprets and predicts future outcomes for various scenarios using mathematical models trained on training data. Machine Learning helps globally distributed systems within the Internet of Things complete tasks without explicit programming. It is particularly beneficial for monitoring, forecasting, and telemetry applications.
Edge AI	Increasing numbers of digital devices are capable of performing local processing. Edge AI allows data processing to be carried out on the device itself or on a local server (at the "edge" of the network), rather than in a centralized data center. This architecture enables devices to run faster, more intelligently, and with less energy. It drastically alters the operation of autonomous devices and extends the battery life of sensors by years.

Application	Description
Advanced Analytics	Because data is frequently dispersed, the IoT alters how analytic procedures are carried out. This implies that software must be able to assemble and interpret the appropriate data. Manufacturing, healthcare, transportation, financial services, energy, telecommunications, and home automation are among the industries that benefit from IoT-centered analytics.
Robotics	Autonomous machines, such as drones, mobile robots, and autonomous vehicles, are improving rapidly due to onboard artificial intelligence and powerful sensor technology. A new concept has been introduced: the Internet of Robotic Technologies (IoRT), which refers to systems that observe events around them, calculate the data onboard and via the cloud, and then use this information to act in the real world.
Augmented Reality (AR)	AR's strength lies in its capacity to integrate, modify, and augment the virtual and actual worlds. In the consumer market, AR smartphone apps are used to improve images, digitally try on clothing, and play games. Various glasses and goggles aid in various jobs, from training to engineering. Text and graphics are generated by a rendering engine that receives the appropriate data from the IoT and delivers it to a device.
Virtual Reality (VR)	Immersive and intuitive, 3D computer-generated VR simulations require an IoT infrastructure. Today's videoconferencing systems, for instance, are transforming into VR places where individuals from all over the world can join a meeting, participate in a webinar, or attend a virtual conference through a 2D screen such as a laptop or smartphone or dedicated headgear. VR enables the assembly of elements from various physical locations to form a single virtual world.
Blockchain	The distributed ledger technology, which was first developed for digital currency, plays a crucial role in the Internet of Things. It can monitor and authenticate data as it traverses devices, databases, and microservices. Thus, it can aid with automation and detect infractions such as tampering. This is particularly beneficial in a highly decentralized IoT context, where data continually passes through organizations, servers, and systems.

Smart objects

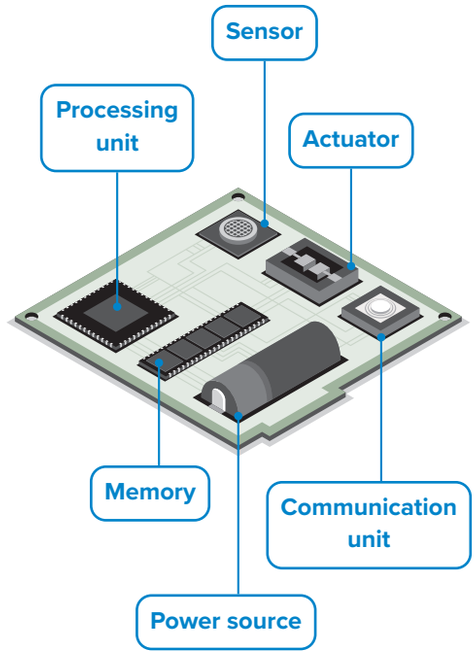
Connected objects, or **smart objects**, are the objects that exchange data over a network. The user interface can vary in complexity, ranging from a simple thermostat switch to a more complex interface in a modern car or an app on a smartphone with multiple features. However, there will also be many cases where the smart object does not have any "user interface," but instead has autonomous **sensors** and **actuators** interacting with their environment without human intervention. A sensor learns and measures its environment, and an actuator can alter the physical world.

The main components of a smart object

A smart object is a device with at least the four components listed below. The smart object may have just one sensor or one actuator, more than one sensor or more than one actuator, or a combination of sensors and actuators, depending on the IoT application.

Processing unit

A smart object contains a processing unit for gathering data, processing and analyzing information received by the sensor(s), coordinating control signals to the actuator, and operating a variety of systems, including communication and power systems. Depending on the processing requirements of a given application, the type of processing unit employed can vary significantly. Microcontrollers are the most prevalent due to their compact size, versatility, programming ease, low power consumption, and low cost.



Sensors and actuators

A smart object is able to interact with the physical world via its sensors and actuators. As discussed in the preceding sections, a sensor learns and measures its environment, but an actuator can alter the physical world. It is not necessary for a smart object to incorporate both sensors and actuators. Depending on the application, a smart object may contain one or more sensors and/or actuators.

Communication unit

The communication unit is responsible for linking a smart item to other smart objects and the outside world (via the network). Smart object communication devices can be either wired or wireless. In IoT networks, smart items are interconnected wirelessly for a variety of reasons, including cost, limited infrastructure availability, and ease of implementation. There are numerous communication protocols for smart items.

Power source

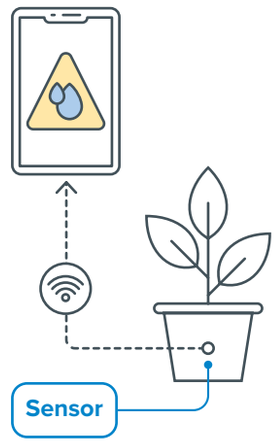
Smart objects have components that require a power source. Interestingly, the communication unit of a smart item typically consumes the greatest amount of energy. As with the other three elements of smart objects, the power needs vary substantially between applications. Smart objects typically have limited power, are deployed for an extended period of time, and are difficult to access.

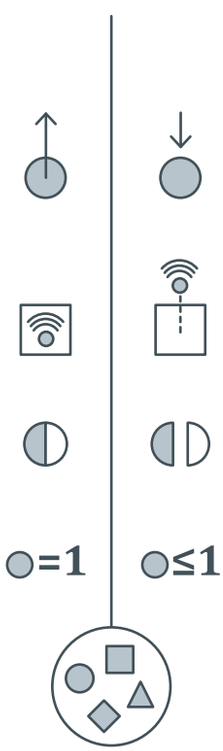
This combination necessitates power efficiency, prudent power management, sleep modes, ultra-low power consumption hardware, etc., especially when the smart object relies on battery power. For long-term installations when smart items are, for all intents and purposes, unavailable, scavenging sources are typically used to provide power.

Sensors

A sensor does exactly what its name indicates: it senses. More specifically, a sensor measures a physical quantity, converts that measurement into data, and passes it on to be used by smart devices or humans. Sensors are not limited to gathering human-like sensory data. They provide a wide spectrum of measurement data with greater precision than human senses. Sensors can be embedded in any physical object and connected to the Internet by wired or wireless networks.

A modern car has an impressive collection of sensors that provide an immense amount of data that can be consumed by smart systems as well as shared with other vehicles on the road. The driver can check and control everything in the car with sensors of all types, like water and oil temperature, location, tire pressure, and velocity, which provide relevant data to improve safety and vehicle maintenance.





Classifying sensors

Active or passive

Sensors can be classified according to whether they need an external power source. Active sensors must use energy to detect changes in the environment (for example, an IR proximity sensor), while passive sensors can detect change without using energy (for example, a gyroscope).

Invasive or non-invasive

Sensors can be a part of the environment they are measuring (invasive) or external component (non-invasive).

Contact or no-contact

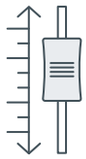
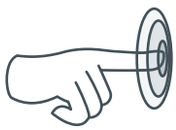
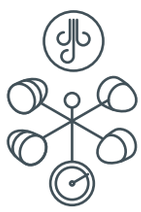
Sensors may require physical contact with the object being measured (contact) or not (no-contact).

Absolute or relative

Sensors can gather data on an absolute scale or relative to a reference value.

Area of application

Sensors can be categorized according to the specific industry in which they are utilized.

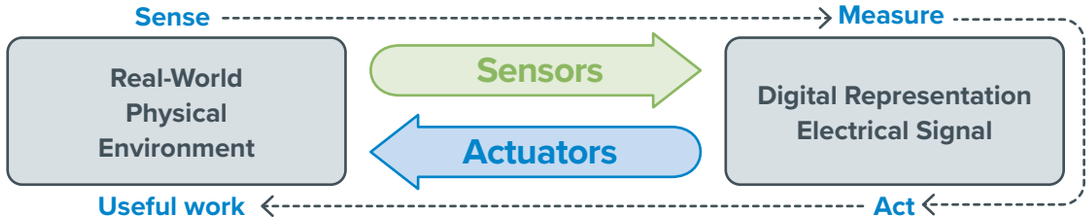
Sensor types with examples		
Sensor type	**Description**	**Examples**
 Position	A position sensor measures the position of an object; the measurement can be in absolute or relative terms. There are three types of position sensors: linear, angular, and multi-axis.	Potentiometer, inclinometer, and proximity sensor
 Occupancy and motion	In a surveillance area, occupancy sensors detect the presence of people and animals, while motion sensors detect the movement of people and objects. In contrast to motion sensors, occupancy sensors generate a signal even when a person is inactive.	Electric eye, and radar
 Velocity and acceleration	Velocity sensors may be linear or angular, indicating how quickly an object moves in a straight line or how quickly it rotates. Acceleration sensors measure velocity changes.	Accelerometer, and gyroscope
 Force	Force sensors determine if a physical force is applied.	Force gauge, viscometer, and touch sensor
 Pressure	Similar to force sensors, pressure sensors measure the force exerted by liquids or gases.	Barometer, and piezometer
 Flow	Flow sensors detect the fluid flow rate.	Anemometer, mass flow sensor, and water meter

Sensor type	Description	Examples
 Acoustic	Acoustic sensors measure sound levels in the environment.	Microphone, geophone, and hydrophone
 Humidity	Humidity sensors measure the amount of humidity in the air or in a mass.	Hygrometer, humidity sensor, and soil moisture sensor
 Light	Light sensors are capable of detecting the presence of light.	Infrared sensor, photodetector, and flame detector
 Radiation	Radiation sensors detect environmental radiation.	Geiger-Müller counter, and neutron detector
 Temperature	Temperature sensors quantify the amount of heat or cold within a system. Contact temperature sensors must be in physical contact with the target object. Non-contact temperature sensors measure temperature from a distance.	Thermometer, calorimeter, and temperature gauge
 Chemical	Chemical sensors determine the chemical concentration within a system.	Breathalyzer, and smoke detector
 Biosensor	Biosensors can detect biological properties in living organisms.	Blood glucose biosensor, pulse oximetry, and electrocardiograph

Actuators

Actuators are the complement of sensors

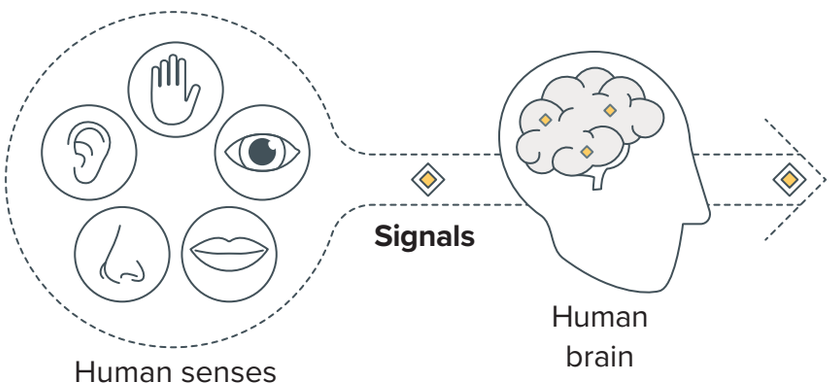
Actuators receive a control signal, most commonly an electrical signal or digital command, that triggers a physical effect in the system.

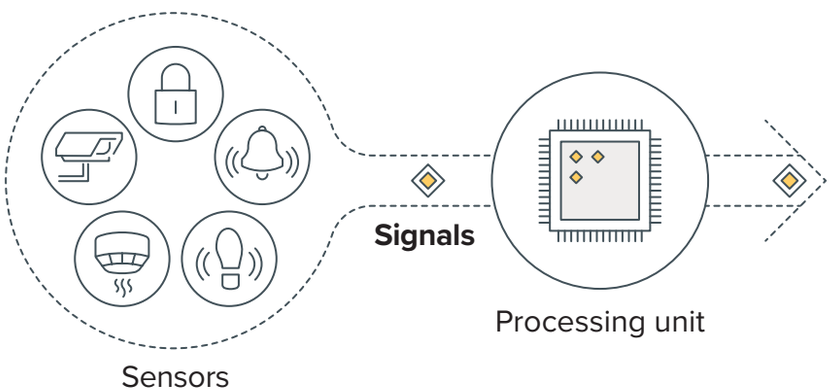


Human analogy

Humans use their five senses to sense and measure their environment. The sensory organs convert this information into electrical pulses that the nervous system sends to the brain for processing. Likewise, IoT sensors are devices that sense and measure the physical world and send their measurements as electrical signals to a microprocessor or microcontroller for additional processing.

Based on the information received from the senses, the brain sends signals to direct motor function and movement, and the nervous system carries that information to the appropriate part of the muscular system. Correspondingly, a processor can send an electrical signal to an actuator that converts the signal into physical action and has a measurable impact on its environment. This interaction between sensors, actuators, and processors and the similar functionality in biological systems is the basis for the fields of robotics and biometrics.





Classifying actuators

Type of motion

Actuators can be classified according to the type of motion they produce.

Examples: Linear, rotary, and one/two/three-axes

Force output

Actuators can be categorized according to the force exerted.

Examples: High power, low power, and micro power

Output type

Actuators can be classified according to the number of stable-state outputs.

Examples: Binary, and continuous

Area of application

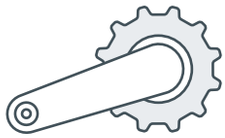
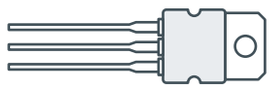
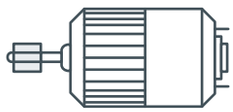
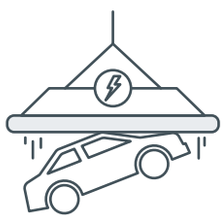
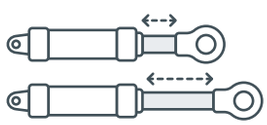
Actuators can be categorized according to the specific industry in which they are used.

Examples: Manufacturing, automotive, and medicine

Type of energy

Actuators can be categorized based on the type of energy they utilize.

Examples: Electrical, chemical, and kinetic

Actuator types with examples	
Actuator type	Examples
 Mechanical actuator	Lever, screw jack, and hand crank
 Electrical actuator	Thyristor, bipolar transistor, and diode
 Electromechanical actuator	AC motor, DC motor, and step motor
 Electromagnetic actuator	Electromagnet, and linear solenoid
 Hydraulic and pneumatic actuator	Hydraulic cylinder, pneumatic cylinder, piston, and pressure control valve
 Thermal and magnetic actuators	Magnetorestrictive material, bimetallic strip, and piezoelectric bimorph
 Microactuators and nanoactuators	Electrostatic motor, microvalve, and comb drive

Hands on!

1. Read the following sentences and put a check mark for True or False.

	True	False
1. Unique IP addresses are not necessary for devices such as smartphones and washing machines to connect to networks.		
2. The evolution of the Internet of Things (IoT) went through four phases, starting with the connectivity phase.		
3. Edge AI refers to processing data exclusively in centralized data centers.		
4. Advanced Analytics in IoT improves the analysis of data in industries like manufacturing, healthcare, and transportation.		
5. All smart objects must include both sensors and actuators to function effectively.		
6. A sensor in a smart object measures its environment, while an actuator alters the physical world.		
7. Passive sensors require an external power source to detect changes in the environment.		
8. Velocity sensors measure how quickly an object moves in a straight line or how quickly it rotates.		
9. Actuators receive a control signal and convert it into a physical effect in the system.		

2. Read the questions and put a check mark for the correct answer.

1. Which phase of the Internet's evolution focused on maximizing efficiency and profit through networking?
   - a. Connectivity phase
   - b. Networked economy
   - c. Immersive experiences
   - d. Internet of Things

2. What does Natural Language Processing (NLP) in IoT focus on?
   - a. Improving drone navigation
   - b. Understanding and implementing human language
   - c. Enhancing photo and video analysis
   - d. Controlling smart appliances

3. Which of the following is NOT a component of a smart object?
   - a. Processing unit
   - b. Sensors and actuators
   - c. Communication unit
   - d. Centralized server

4. How can sensors be classified?
   - a. Active or passive
   - b. Wired or wireless
   - c. Internal or external
   - d. Digital or analog

5. What is an example of an electric actuator?
   - a. Lever
   - b. Thyristor
   - c. Hydraulic cylinder
   - d. Electromagnet

3. Name the most critical technological advancement in recent history that made the IoT possible.

4. Select three types of sensors that are important for measuring the environment and describe their uses.

5. How does the analogy between human senses, the brain, and actuators help us better understand the relationship between sensors, processors, and actuators in IoT systems? Think of a real-world example where this analogy applies, and explain how the components work together to achieve a specific task.

LESSON 4

IoT infrastructure

What do you think happens when a smart device collects data? Where do you think this data goes, and how is it processed to make decisions?

The Internet in the Internet of Things

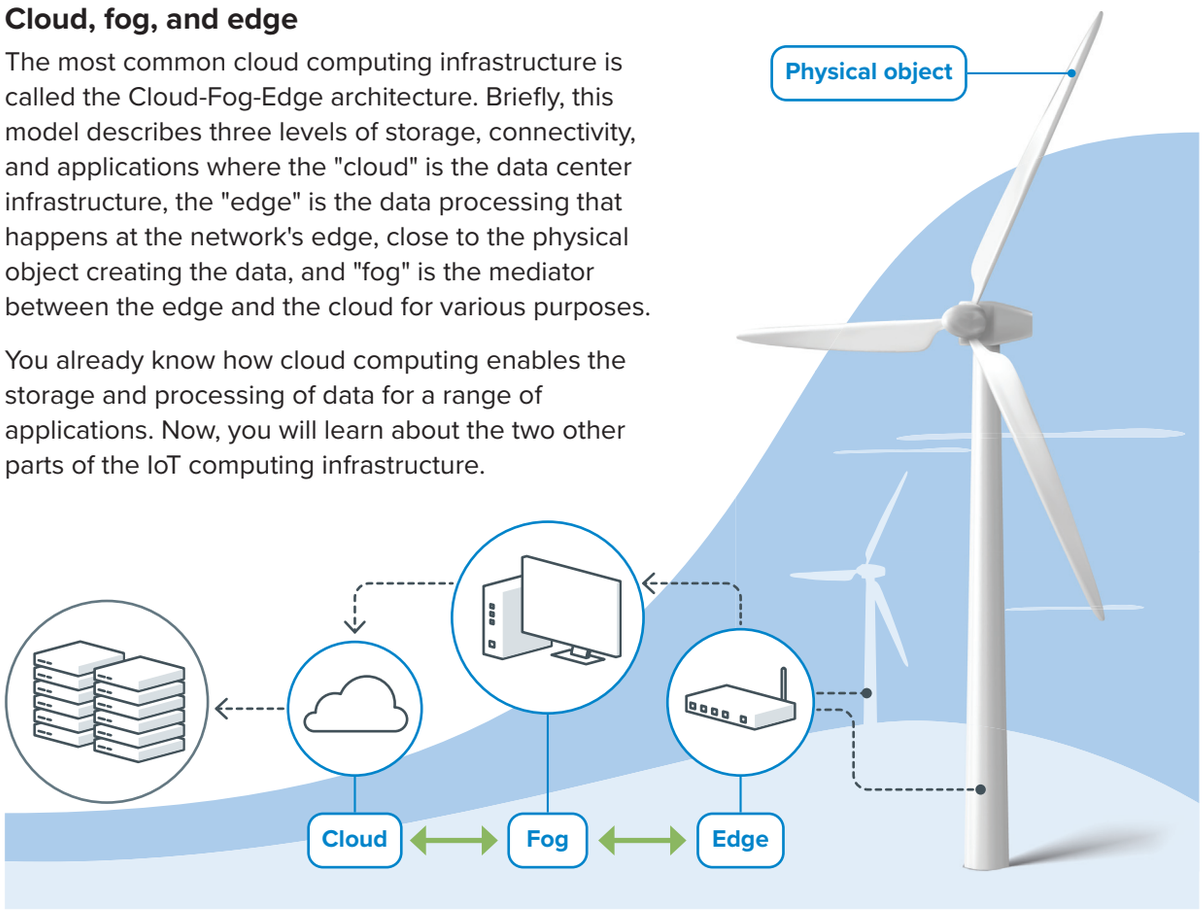
The term Internet of Things contains two keywords: Internet and Things. We have explained what Things (smart devices) are, and now we will explore the Internet part of an IoT solution. Cloud connectivity and cloud services allow the data gathered by a smart object's sensors to undergo high-level processing and enable sophisticated actuator control based on large-scale data analysis. IoT devices are usually connected to a cloud **IoT service** using a communication protocol, and through this service, the main IoT application will make decisions based on the collected data.

This lesson covers the Cloud-Fog-Edge architecture, the networks and protocols utilized, and the types of data exchanged to support an effective IoT solution.

Cloud, fog, and edge

The most common cloud computing infrastructure is called the Cloud-Fog-Edge architecture. Briefly, this model describes three levels of storage, connectivity, and applications where the "cloud" is the data center infrastructure, the "edge" is the data processing that happens at the network's edge, close to the physical object creating the data, and "fog" is the mediator between the edge and the cloud for various purposes.

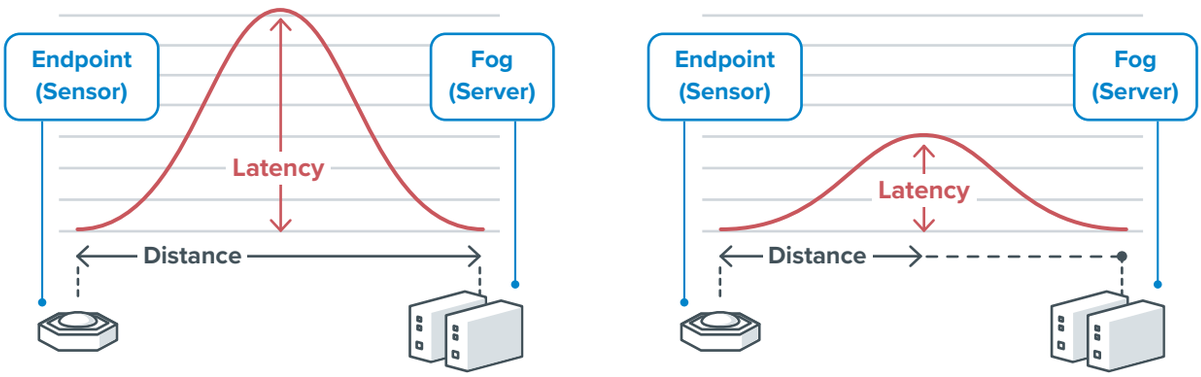
You already know how cloud computing enables the storage and processing of data for a range of applications. Now, you will learn about the two other parts of the IoT computing infrastructure.



Fog computing fundamentals

A constant technological goal of IoT systems is to distribute data management as close as possible to the sensor/actuator nodes. **Fog computing** is the most well-known example of using edge services in the IoT to move processing closer to the devices that generate the IoT data. A fog node can be any device with computing, storage, and network connectivity. Some examples are industrial controllers, switches, routers, embedded servers, and IoT gateways. A gateway enables connectivity for devices that cannot connect directly to the Internet. A Wi-Fi hotspot is an example of a gateway. The fog node is close to the edge endpoint, which is a data routing service that can receive and send data to and from other services. It can be a program on a computer or a dedicated hardware device. The fog node can gather and process data from several edge endpoints and act as a gateway and a filter for data sent to the cloud.

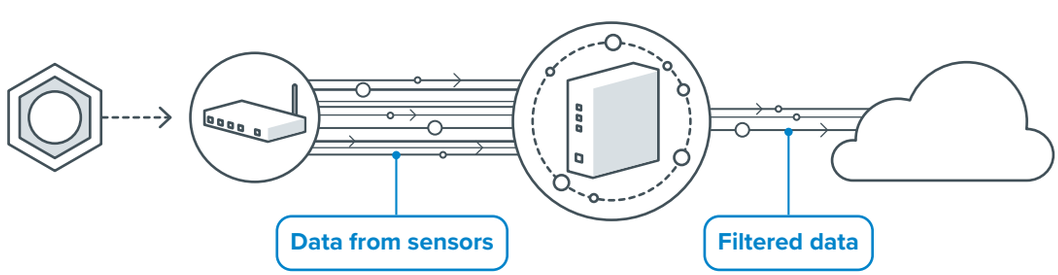
Analyzing IoT data close to its origin reduces latency, which is the delay in the processing of data over a network connection or the delay between a user action and the response. This approach offloads gigabytes of network traffic from the core network and keeps sensitive data within the local network.



The role of fog nodes in IoT systems

Typically, fog services are performed very close to the IoT device, as close to the edge endpoints as possible. One significant benefit is that the fog node has contextual awareness of the sensors it manages due to its geographic proximity to those sensors. Because the fog node can analyze data from all the sensors on that section, it can provide contextual analysis of the messages it receives and may choose to send only relevant data to the cloud. As a result, the volume of data sent upstream is significantly reduced and the data sent is more useful to cloud-based applications and analytics servers.

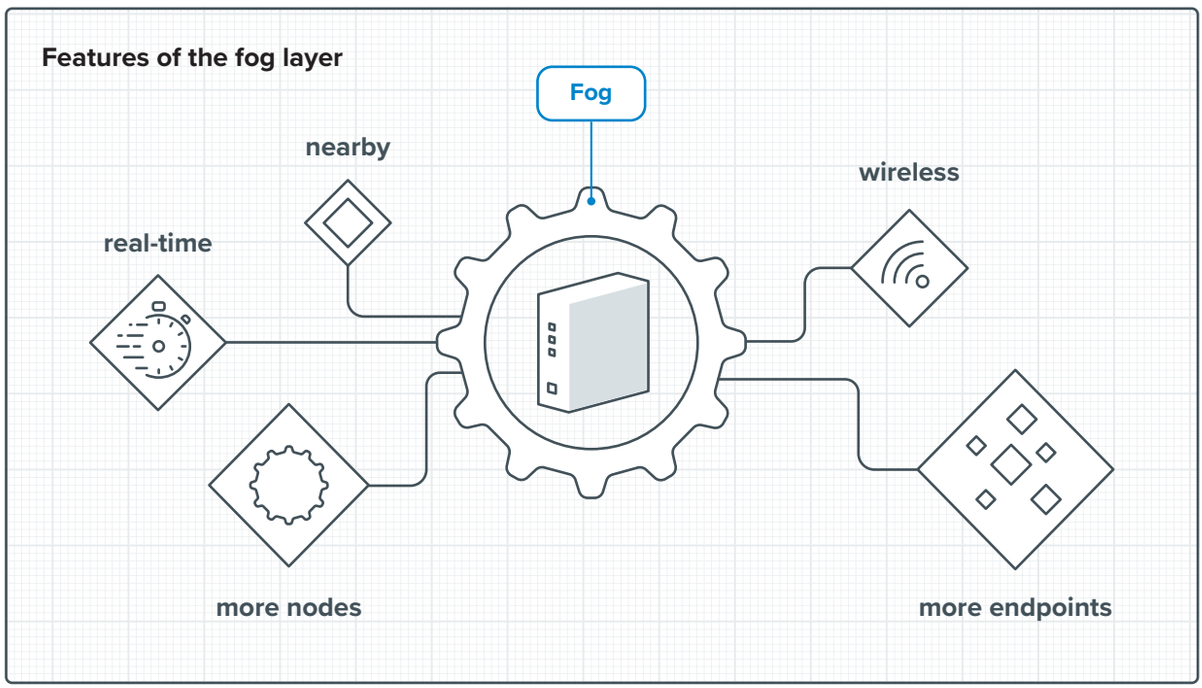
Furthermore, having contextual awareness allows fog nodes to respond to events in the IoT network much faster than the traditional cloud model, which would likely cause higher latency and slower response times. Thus, the fog layer provides a distributed network capability, allowing devices to be monitored, controlled, and analyzed in real-time without waiting for communication from the cloud's central application and analytics servers.



Fog computing advantages

Fog applications are as diverse as the IoT itself. Their typical responsibilities include data reduction, monitoring, and analyzing real-time data from network-connected devices.

Fog computing advantages	
Advantage	Description
Contextual location awareness and low latency	The fog node is located as close as possible to the IoT endpoint to provide distributed computing.
Geographic distribution	Fog-based applications use a complex distributed network which means that security threats can be localized, whereas in a more centralized network, such threats would affect the whole system.
Deployment near IoT endpoints	Typically, fog nodes are deployed in the presence of several IoT endpoints. Typical metering deployments typically consist of 3,000 to 4,000 nodes per gateway, which also serves as a fog computing node.
Wireless communication between the fog and the IoT device	Although it is possible to connect wired nodes, the benefits of fog are greatest when a large number of endpoints are involved, and wireless access is the simplest way to achieve scalability.
Use for real-time interactions	Important fog applications involve interactions in real-time, as opposed to batch processing. The preprocessing of data in fog nodes enables upper-layer applications to process a subset of the larger data packets.



Edge computing endpoints

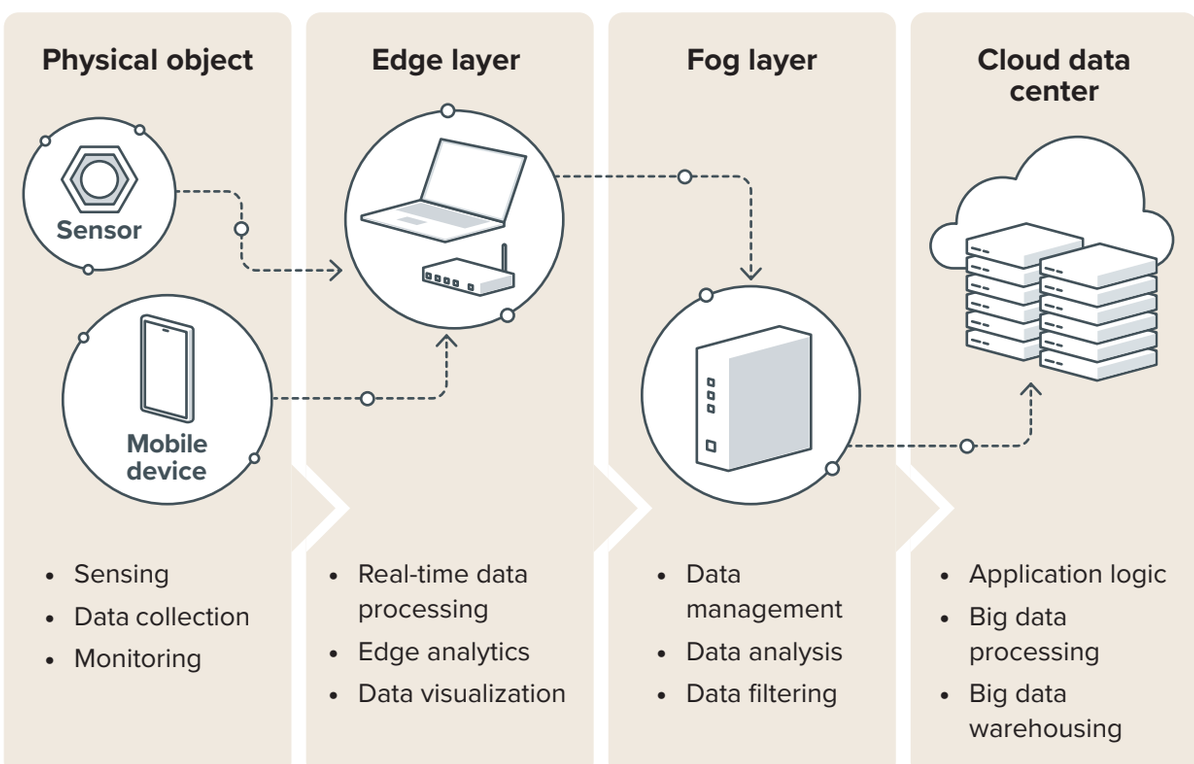
Newer types of IoT endpoints have sufficient computing power to perform low-level analytics and filtering. These are called **edge computing** endpoints or **edge devices**. This layer in the cloud-fog-edge architecture provides more efficiency to the IoT solution. The cloud is not replaced by edge or fog computing. Instead, all these layers complement one another. The edge and fog computing layers assist in filtering, analyzing, and managing data.

They prevent the cloud from being queried for each event by each IoT device. This model requires that network bandwidth, computation and data storage resources are organized hierarchically. Data is collected, analyzed, and sent at each stage based on the capabilities of the resources at each layer. The latency decreases as more data is sent to edge endpoints closer to the IoT devices. The benefit of this hierarchy is that responses to events from resources close to the IoT device are quick, with immediate results. At the same time, big data storage and processing resources in cloud data centers are available when needed.

Edge and fog working together

Edge and fog computing necessitates using an abstraction layer to enable applications to communicate with one another. The abstraction layer uses standardized Application Programming Interfaces (APIs) for monitoring, provisioning, and controlling physical resources. To support flexibility and consistency across the IoT system, the abstraction layer also requires a mechanism to support virtualization, with the ability to run multiple operating systems or service containers on physical devices. Regarding architecture, fog nodes closest to the network edge receive data from IoT devices. The fog IoT application then directs various data types to the best location for analysis.

The most time-sensitive data is analyzed closest to the smart objects generating the data on the edge or fog node. Data that can be acted on in seconds or minutes is routed to an aggregation node for analysis and action. Less time-critical data is sent to the cloud for historical analysis, big data analytics, and long-term storage.



Networking protocols

Basic networking protocols

The fundamental Internet networking protocols, **Internet Protocol** (**IP**), **Transmission Control Protocol** (**TCP**), and **User Datagram Protocol** (**UDP**), also provide connectivity for IoT networks. Data transmission between smart objects and any other system in an IoT application is handled via higher-level protocols. These new protocols have been developed to address the requirements of IoT data transfer. Some IoT networks rely on a push model, such as a sensor reporting at regular intervals or responding to a local trigger. Others rely on a pull model, such as an application that queries the sensor for data across the IoT network.

How TCP and UDP protocols work	
Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
This connection-oriented protocol needs the formation of a session between the source and destination prior to data transmission. It can be compared to a standard telephone conversation, in which two phones must be connected and a communication link established before the two parties can communicate.	With this protocol, data can be sent quickly from source to destination, but there is no guarantee that it will get there. This is like sending mail, in which a letter is mailed to the right person but it is not known for sure whether this letter is received until another letter is sent to the initial sender as a response.

IoT networking protocols

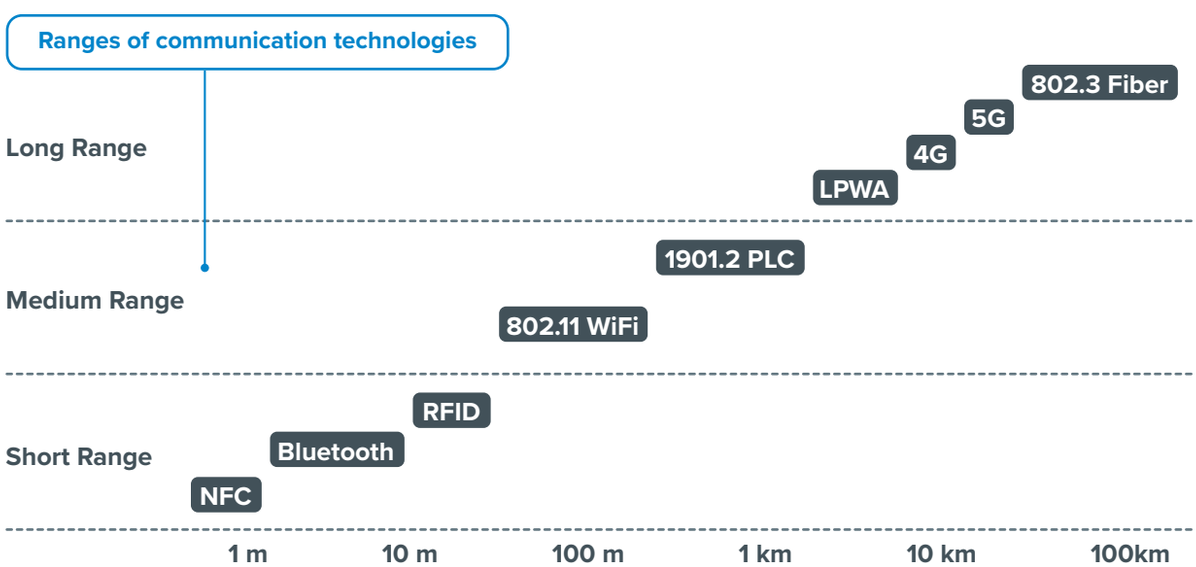
The table below contains some of the latest networking protocols that IoT devices use to communicate with each other and the Internet. These protocols build upon the basic Internet networking protocols.

IoT networking protocols		
Protocol name		Features
6LoWPAN	6LoWPAN	6LoWPAN is an acronym for **IPv6** over Low-Power Wireless Personal Area Networks. This protocol delivers low-cost and secure IoT communications.
ZigBee	ZigBee	ZigBee is an evolution of 6LoWPAN and provides a simpler and less expensive means of communication than Bluetooth and WiFi. Common applications include building automation, home automation, and healthcare.
ISA100 WIRELESS	ISA100.11a	ISA100.11a protocol is a standard for industrial automation of wireless systems which is used for process control.
WirelessHART	WirelessHART	WirelessHART is a protocol stack for creating a time-synchronized, self-organizing, and self-healing mesh architecture.
THREAD	Thread	Thread is a set of protocols for making a safe and reliable mesh network for connecting and controlling devices, mainly at home.

IoT communication technologies

The various communication technologies for IoT solutions are classified by the range of information and data transmitted through them. Keep in mind that devices that use long-range communication technologies consume much more energy than their short-range counterparts.

IoT communication technologies classified by distance	
Distance	**IoT communication technologies**
Short range	A serial cable is a classic example of a wired system. Wireless short-range solutions, with a maximum distance of tens of meters between two devices, are usually a replacement for serial cables. Short-range wireless technologies include Bluetooth, Near-Field Communication (NFC), and **Radio Frequency IDentification** (**RFID**).
Medium range	This is the most common type of IoT access technology. There are various implementations in the tens to hundreds of meters range. The maximum distance between two devices is frequently less than one kilometer, but Radio Frequency (RF) technologies have no predetermined maximum distance as long as the radio signal is broadcast and received properly. Medium-range wireless technologies include IEEE 802.11 Wi-Fi. Wired technologies such as IEEE 802.3 Ethernet and IEEE 1901.2 Narrowband Power Line Communications (PLC) may also be classified as medium range.
Long range	Long-range technologies are required for distances larger than one kilometer between two devices. Cellular (2G, 3G, 4G, and 5G) and Low-Power Wide-Area (LPWA) technologies are examples of long-range wireless technologies. LPWA communications may communicate over a broad area while requiring little power. As a result, these technologies are appropriate for battery-powered IoT sensors. IEEE 802.3 via optical fiber and IEEE 1901 Broadband Power Line Communications are both categorized as long range but are not considered IoT access technologies.



Hands on!

1. **Read the following sentences and put a check mark for True or False.**

	True	False
1. Fog computing is designed to bring data processing closer to the devices generating IoT data.		
2. A Wi-Fi hotspot is an example of a fog node that processes IoT data directly at the source.		
3. Fog nodes can analyze data from multiple sensors in their region and provide contextual analysis.		
4. Fog nodes rely entirely on the cloud to respond to IoT events in real-time.		
5. Fog-based applications use a centralized network, which means that a single security threat can impact the entire system.		
6. UDP (User Datagram Protocol) guarantees that all data sent is delivered to the intended recipient without any loss.		
7. TCP (Transmission Control Protocol) ensures data delivery by establishing a session between the source and destination before transmitting.		
8. IoT communication technologies with a long range, such as LPWA and cellular networks, are ideal for low-power, battery-operated IoT devices.		
9. Short-range IoT communication technologies, such as Bluetooth and NFC, are typically used for distances of tens of yards between devices.		

2. Read the questions and put a check mark for the correct answer.

1. Which of the following is a function of a gateway in IoT systems?
   - [ ] a. Acts as a direct processor for all cloud data
   - [ ] b. Enables connectivity for devices that cannot connect directly to the Internet
   - [ ] c. Stores all IoT data indefinitely
   - [ ] d. Eliminates the need for edge endpoints

2. How does fog computing ensure scalability?
   - [ ] a. By eliminating the need for wireless communication
   - [ ] b. By reducing the number of IoT endpoints
   - [ ] c. By supporting wireless communication between the fog and IoT devices
   - [ ] d. By relying entirely on cloud-based systems

3. Which IoT networking protocol is an evolution of 6LoWPAN and is commonly used in building automation and healthcare?
   - [ ] a. ZigBee
   - [ ] b. WirelessHART
   - [ ] c. ISA100.11a
   - [ ] d. Thread

4. Which IoT communication technology is categorized as short range?
   - [ ] a. 5G
   - [ ] b. NFC
   - [ ] c. LPWA
   - [ ] d. IEEE 802.11 Wi-Fi

5. Which protocol is designed for creating a reliable mesh network for connecting and controlling devices, mainly at home?
   - [ ] a. Thread
   - [ ] b. 6LoWPAN
   - [ ] c. WirelessHART
   - [ ] d. ISA100.11a

3. Describe how adding a fog layer in IoT applications improves their effectiveness.

4. Draw a diagram to visualize the relationship between the cloud, fog, and edge layers of the IoT architecture.

5. Imagine you are designing a smart home system with IoT devices, like smart lights, security cameras, and door locks. Which communication technology (short-range, medium-range, or long-range) would you choose for each device, and why? Consider the distance between devices, power usage, and the amount of data each device needs to transfer.

LESSON 5

IoT applications and challenges

Can you think of a device you use that makes life easier or safer? How might it be improved with IoT technologies?

IoT Applications

The IoT is one of the fastest-growing technologies, and as we move from the age of products to the age of services, the IoT plays a major role in this technological revolution. The day is not too far when you will go home in a self-driving car and the entrance door will auto-detect your presence and open automatically. The following are some examples of areas where the IoT changes how we live and work:

Wearables

Wearables such as smartwatches, are a very popular item on the market, but many people consider them simple gadgets. In fact, these devices are IoT devices offering a variety of functions, ranging from medical monitoring to wellness and fitness tracking. They can communicate with cloud services to provide real-time health insights to their user and even provide alerts for potential health problems.

Telemedicine

Telemedicine, or telehealth, has not yet reached its full potential. IoT-enabled telemedicine is exemplified by always-connected medical devices that healthcare professionals can monitor. Remote medical diagnosis happens proactively, saving valuable time for the proper treatment of patients. For example, heart attack detection systems can sense a person's heartbeat in real-time and send potentially life-saving messages to a doctor.

Smart homes

Smart homes, one of the best and most practical implementations of the IoT, significantly enhance convenience and home security. There are a variety of IoT applications for smart homes, but the most effective combine intelligent utility systems and entertainment. Home security is strengthened with improved locking systems and networked surveillance systems.

As the IoT evolves, we can be confident that our homes will become more intelligent. For example, an automatic lighting system will know when we are not home and conserve energy.

Education

An IoT-enabled school or campus can assist teachers and administrators to record daily attendance. The system can also notify parents of absent students automatically. Other IoT devices used in the education sector are smart whiteboards, door locks and fire or security systems.

Smart grids

The electricity grid is a complex and critical system, as it provides electricity to homes, industries, transportation, and almost everything in our daily life.

A **smart grid** is an electricity grid that uses IoT technologies to reduce electricity waste, enhance electricity transmission efficiency, improve restoration time, and reduce operating costs.

Self-driving cars

The big technology companies are developing versions of self-driving cars or other vehicles. Multiple sensors and embedded devices connected to the cloud generate massive data for decision-making based on machine learning algorithms.

However, since human lives are on the streets, we must ensure that the technology is ready to improve road safety. Achieving this goal requires rigorous testing and continuous refinement to minimize the risk of accidents and errors in autonomous vehicles.

Additionally, regulatory bodies and industry standards must evolve in tandem with this advancing technology to establish a robust framework for its safe deployment.

Retail stores

A new type of retail store bridges the gap between online and physical stores. The IoT-enabled store adds products to your shopping cart in real-time as you select them from the shelves and facilitates cashless transactions by deducting funds from your digital wallet on your smartphone.

If you change your mind and add another item to your cart, the prior item is removed and replaced with the new one. There is no cashier to charge you for your purchases, and you do not need to wait in line to pay.

Smart supply-chain management

Supply networks must be efficient and optimized otherwise, they increase the cost of goods. IoT solutions for tracking items with electronic tags while in warehouses or on the road provide real-time information, reduce errors, and minimize delays in the supply chain.

Industrial IoT

The Industrial IoT, or IIoT, consists of sensors, instruments, and other IoT devices linked to production and energy management applications. Industry experts anticipate that IIoT will have the greatest potential of all IoT applications as it can improve product quality and production efficiency.

For example, a commercial jetliner manufacturer has integrated sensors into tools and machines and given workers smart glasses to reduce errors and enhance safety in the workplace.

Smart agriculture

The IoT holds great potential for transforming the agricultural industry, promising a bright future ahead. Tools for drip irrigation, recognizing crop patterns, water distribution, and drones for farm surveillance are being continuously developed.

These innovations enable farmers to become more productive and address problems more effectively.

Smart transportation

Many urban centers around the world are investing in advanced public transportation systems. These systems often incorporate IoT-enabled driverless vehicles and innovative solutions to facilitate seamless city navigation.

These modern transportation networks aim to enhance the overall commuting experience while also prioritizing safety. In addition, central control centers equipped with state-of-the-art technology play a crucial role in monitoring and managing the surveillance systems for stations, routes, and other critical infrastructure components.

Traffic management

With the help of IoT technologies, traffic management in large cities can be enhanced. Using mobile phones as smart objects with their GPS sensors and apps such as Google Maps, and information from our vehicles through cloud systems like the Local Hazard Information system, IoT technologies can improve traffic and road safety.

Long-term analysis of traffic patterns is another IoT application. Commuters will be better equipped to avoid traffic and delays if they are informed of alternative routes during busy hours.

Intelligent transport systems

To improve road safety and traffic management, various transportation authorities worldwide are actively pursuing the implementation of intelligent transport systems on their highways. These initiatives involve equipping road and highway networks with IoT systems to control the flow and efficiency of traffic.

The respective plans of these authorities define the primary framework for the future implementation of intelligent transport systems, aiming to enhance road safety and optimize transportation infrastructure.

Water/waste management

Numerous municipalities are implementing water recycling through the use of water treatment units. Using an IoT application, it is possible to determine how much water is consumed in a particular location, how much wastewater is being created, and how waste production has changed over time.

With a smart waste management system, authorities can forecast, among other things, how much waste will be generated in a particular region, how it will be processed, when it will be cleared, and how to evaluate data for future planning. Similarly, the volume of garbage generated in each neighborhood over time can be analyzed. All this information can be utilized to plan the city's improvement initiatives.

Data analytics systems enable optimal trash collection planning and forecasting of future trends.

IoT security issues

One of the biggest issues arising from the universal use of the Internet, the rapid increase of devices in the IoT, and the use of the cloud is the security of this entire digital global environment. Data networks have existed for decades, but most were publicly inaccessible, with special security protocols and access devices. The connection of billions of devices on data networks that are connected to the Internet is the reason for increased security breaches.

IoT devices may simply switch on and off lights to conserve energy, but they may also interact with sensitive data like personal medical data. It is imperative to address these security concerns from the beginning of the system design. IoT networks are exposed to a greater variety of attacks than other networks, and the quality and complexity of these attacks are increasing daily.

IoT systems should ensure user interactions are conducted in a secure environment. To avoid unwanted access to private data, IoT security experts should consider the following:

- Trustworthy and decentralized authentication models
- Technologies for encryption and data protection that save energy
- Cloud computing security and trustworthiness
- Data control
- Legal and liability concerns
- Communication and networking vulnerabilities
- Access and user rights and rules for sharing value additions
- Secure, inexpensive hardware
- Privacy policy management

Examples: Security issues with RFID technologies

Radio-Frequency Identification is one of the most commonly used communication protocols for processing identification data for smart objects. RFID employs radio frequency waves to interact and exchange data without needing physical contact. Two components comprise an RFID system: a transponder (RFID tag) and a transceiver (RFID reader). The **Electronic Product Code** (**EPC**) is the unique identifier of the smart object. RFID tags are characterized as either active or passive.

The inbuilt battery of an active tag permits the remote interaction of its unique EPC with surrounding EPCs at a limited distance. Passive tags operate without a battery, and data is read only when a transceiver within a short range activates the tag. Unfortunately, the data within the RFID is vulnerable to tampering, corruption, and deletion, although cryptographic techniques are used to ensure privacy and proof of originality of the transferred data.

Examples of security vulnerabilities of IoT systems through RFID exploitation	
Security vulnerability	Attack example
Attack on authenticity **Unauthorized Tag Disabling**	The IoT connects billions of small devices, each of which must have a unique IP address. Only IPv6 can support the current number of IoT devices. The migration to the new IP standard delays the rapid development of the Internet of Things ecosystem, and it will result in an increase in network security vulnerabilities.
Attack on integrity **Unauthorized Tag Cloning**	IoT sensors must be autonomous. Changing batteries on the billions of deployed devices is time-consuming, and the sensors must also be power-efficient to avoid rising energy costs.
Attack on confidentiality	Utilizing IoT devices causes several legal complications and magnifies numerous Internet-related privacy issues. One issue includes the transmission of data across international borders.
Attack on availability **Denial of Service (DoS) Attack**	Every day sensors and devices continue to expand their capabilities. This results in the development of new, enhanced services. Modern apps with an intuitive user experience that support these services are becoming more complex and demanding for developers and user experience designers.

Security issues with Wireless Sensor Network technologies

Wireless Sensor Networks (WSN) are responsible for transferring data and information between smart objects in IoT systems. They are composed of autonomous nodes that communicate with limited frequency and capacity. The communication node consists of a battery, sensor, memory, radio transceiver, and microprocessor. Due to the limited communication range of each sensor node, information is relayed between the source and the base station in multiple stages.

Wireless sensors gather and transmit the required data in coordination with other nodes for routing to the central system. Wireless sensors have limited power and computing capabilities, making many traditional security methodologies difficult or impossible to implement.

Security concerns based on IoT system levels	
IoT system levels	Security concerns
 **Device level**	IoT devices must prove their identity to maintain authenticity and limit locally stored data to protect privacy. Because IoT devices are present everywhere in the environment, physical security is also important. This creates the need to design resistance to device breaches so that it is difficult to extract sensitive items such as personal data, cryptographic keys, or credentials. To support a long service life, software updates must be frequently applied.
 **Network level**	Connectivity and messaging between IoT devices and cloud services occurs at the network level. Internet communications usually use a combination of private and public networks, so securing traffic is critical. Many IoT devices also communicate through protocols other than Wi-Fi. The IoT gateway is responsible for maintaining confidentiality, integrity, and availability when translating between different wireless protocols.
 **Service level**	This level represents the IoT management system and is responsible for managing devices and users, implementing policies and rules, and coordinating automation across devices. Role-based access control to manage the identity of users and devices and the actions they are authorized to take are critical at this level. Action tracking must be enabled to ensure that potentially compromised devices can be identified when abnormal behavior is detected.
 **Data level**	Large-scale analysis of aggregated data generated in the IoT is often described as the most valuable aspect of the IoT for service providers. Maintaining data privacy is a top priority for government agencies such as the Federal Trade Commission (FTC) in the USA and the Network and Information Security Agency (ENISA) in the European Union, which release the corresponding privacy-related security requirements guidelines.

Approaches to solving security challenges

Security is a major consideration during the design phase of an IoT system. Building security throughout the design phase begins at the hardware level and continues with communication infrastructure, the operating system level, and the application design level, and this should be extended until application deployment. Companies and state organizations should enforce data protection policies and comply with their national legislation. Specialized network and security engineers with experience in IoT systems design test and secure IoT devices and networks by implementing best practices in cybersecurity. These engineers must combine technical knowledge and field experience from various computing domains.

Privacy concerns

The concept of privacy varies across cultures and has evolved and transformed over time. Initially, installing surveillance cameras was considered intrusive; however, this practice is now a widespread and broadly accepted data transfer. The Internet of Things is a blend of public and commercial applications, and who will have access to and authority over the collected data is a concern. In IoT systems, privacy should be enforced over personally identifiable information, and storage and disclosure restrictions should be imposed. An adequate privacy and protection framework must be in place, and consumers must be guaranteed that their data is private and secure.

As we navigate the digital global environment, the security challenges arising from the universal use of the Internet, the exponential growth of IoT devices, and the integration of cloud services have become paramount. While data networks have been in existence for decades, they were often characterized by restricted access and robust security protocols. However, the rapid growth of IoT devices, numbering in the billions, interconnected through data networks that ultimately link to the Internet, has given rise to a heightened risk of security breaches. IoT devices, ranging from simple streetlight controllers to collectors of personal medical data, demand a proactive approach to security right from the system's inception.

The IoT ecosystem is especially susceptible to a broad range of cyber threats, and the sophistication and frequency of these attacks continue to increase. To combat this evolving threat landscape, it is essential to adhere to IoT security best practices. This includes the integration of security measures from the hardware level to application deployment, the selection of secure communication infrastructures, compliance with data protection regulations, and the employment of specialized network and security engineers who are well-versed in IoT system design and cybersecurity.

In this expanding realm of IoT, the pursuit of innovative solutions and the protection of privacy and security must ultimately go hand in hand. By addressing these security concerns, it is possible to maximize the IoT's potential while maintaining the confidentiality and integrity of the data it processes.

Hands on!

1. **Read the following sentences and put a check mark for True or False.**

	True	False
1. Wearables such as smartwatches can provide real-time health insights and alerts for potential health problems.		
2. Self-driving cars rely only on human control and do not use IoT or embedded devices for decision-making.		
3. Traffic management systems with IoT do not use GPS or mobile apps to analyze and optimize traffic flow.		
4. IoT applications in smart agriculture help farmers monitor water distribution, crop patterns, and soil conditions in real-time.		
5. RFID systems are completely secure and cannot be tampered with or cloned.		
6. Wireless Sensor Networks (WSN) are responsible for transferring data and information between smart objects in IoT systems.		
7. IoT devices must prove their identity to maintain authenticity and protect locally stored data.		
8. Maintaining data privacy in IoT systems is only a concern for individual users, not government agencies.		
9. Action tracking at the service level can help identify potentially compromised devices when abnormal behavior is detected.		
10. Security for IoT systems starts at the hardware level during the design phase.		

2. Read the questions and put a check mark for the correct answer.

1. How do IoT-enabled smart grids improve electricity systems?
   - a. By completely eliminating electricity transmission
   - b. By reducing electricity waste and improving restoration times
   - c. By generating unlimited power automatically
   - d. By focusing only on residential areas

2. What is one primary benefit of IoT-enabled retail stores?
   - a. Enhanced employee training programs
   - b. Automated shelf stocking
   - c. Cashless transactions and no need to wait in line
   - d. Integration with industrial IoT systems

3. What is the primary impact of a Denial of Service (DoS) attack on IoT systems?
   - a. Improves device security
   - b. Increases user privacy
   - c. Disrupts device availability and new service development
   - d. Enhances wireless communication

4. Which IoT system level focuses on securing traffic between IoT devices and cloud services?
   - a. Device level
   - b. Network level
   - c. Service level
   - d. Data level

3. Compare and contrast IoT-enabled self-driving cars and smart public transportation. Are these IoT applications distinct, or do they complement each other?

4. Solar or wind renewable energy sources introduce variability in power generation. Do you think smart grid technologies can make the distribution and management of renewable energy more efficient?

5. Search the Internet for an event where a security vulnerability led to a cyberattack on an IoT system. Explain what damage was caused and how it could have been prevented.

6. What are two security concerns associated with IoT devices? Explain why these concerns are significant and provide an example of how they could impact users or businesses.

Project

Exploring IoT in daily life

Now it's time to explore how IoT is transforming various aspects of your daily life and present your findings in a PowerPoint presentation to the class.

1. Investigate

Investigate how IoT is currently used and its potential future applications in areas such as:

- Smart homes
- Healthcare
- Transportation
- Environmental management

2. Collect examples

Use class materials and reliable online sources to collect examples, benefits, and challenges of IoT in these areas.

3. Examples of IoT applications

Define IoT and explain why it's important. Create 3–4 slides with specific examples of IoT applications in different areas. Use visuals like images, diagrams, or graphs to illustrate your points.

4. Summarize

Use 1–2 slides to discuss the potential challenges (for example, security and privacy) and your ideas for how IoT might evolve. Summarize what you've learned about IoT's role in everyday life.

5. Be prepared

Deliver your presentation to the class and be prepared to answer a few questions from classmates or your teacher.

Reflect

1. What did you enjoy the most about learning how IoT is used in everyday life?

2. What challenges did you face when researching real-world IoT examples, and how did you address them?

3. What did you find most surprising about the current and potential applications of IoT in everyday life?

Wrap up

Take a moment to reflect on your progress.

How confident are you in your ability to apply the following skills?

> I can describe different network types.
> I understand how wired and wireless networks function.
> I understand the development of mobile networks and their impact.
> I know the roles of different satellite systems.
> I can explain how IoT systems work.
> I know the advantages and challenges of IoT systems.
> I know the components and role of an IoT platform.
> I understand how IoT platforms manage data and devices.
> I understand how IoT is applied in different industries.
> I know the challenges IoT systems face.

Key Terms

actuator
Bluetooth
Denial of Service (DoS) Attack
Digital Subscriber Line (DSL)
edge computing
edge device
Electronic Product Code (EPC)
endpoint
fiber optic network
fog computing
gateway
Global Positioning System (GPS)
Internet of Things (IoT)
Internet Protocol (IP)
IoT device
IoT service
latency
Local Area Network (LAN)
Metropolitan Area Network (MAN)
Near-Field Communication (NFC)
Personal Area Network (PAN)
protocol
Radio Frequency IDentification (RFID)
satellite network
sensor
smart grid
smart object
Storage Area Network (SAN)
topology
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)
Wide Area Network (WAN)
wired network
wireless network
wireless sensor network