

# Chapter 7

## Network



### 7.1 What is a Network

A network refers to connections between nodes, where each node represents an element or thing. There are various types of networks, including information networks, railway networks, and logistics networks. An information network consists of multiple information devices like telephones and computers connected by communication channels. While the terms “network” and “information network” are not identical, “network” often refers to an information network in many contexts. In this textbook, unless otherwise stated, the term “network” specifically refers to information network.

### 7.2 Methods of Switching

Information networks can be categorized based on their switching methods [1]. There are two main types: circuit-switched networks, represented by the telephone network, and packet-switched networks, represented by computer networks. In the following, we will provide detailed explanations of each type.

In a telephone network, each telephone is connected to a cable, which is, in turn, connected to an exchange station (see Fig. 7.1). The number of cables between an exchange station and a relay station might be less than the cables between the exchange station and telephone terminals. Consequently, the simultaneous usage of telephones may be limited by the availability of cables between the exchange station and the relay station.

Since each terminal exclusively uses a cable, a circuit-switched network is ideal for transmitting continuous information like voice. However, the limited number of cables restricts the simultaneous use of terminals.

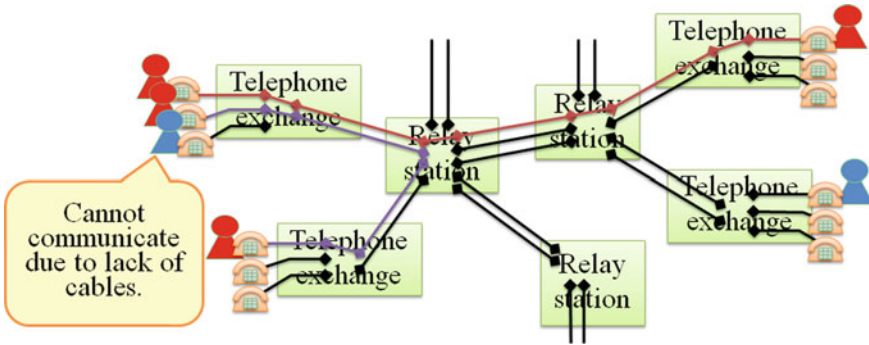


Fig. 7.1 Circuit-switched network

Unlike circuit-switched networks that primarily handle continuous data like voice, computer networks transmit a variety of data types. Using a switching system where each communication exclusively occupies a cable would result in low efficiency. Therefore, computer networks use a packet-switched system, where data is divided into fixed-size packets. In a packet-switched network, multiple communications can share a cable simultaneously, allowing for a high degree of concurrent communication.

In Fig. 7.2, each host represents a personal computer (PC) user. Communication data from user A to user B passes through three routers before reaching user B, while communication data from user C to user D traverses four routers before reaching user D. The cable connecting the central router and the upper-right router is shared by both communications. Packets from A to B are shown in brown, and packets from C to D are shown in yellow.

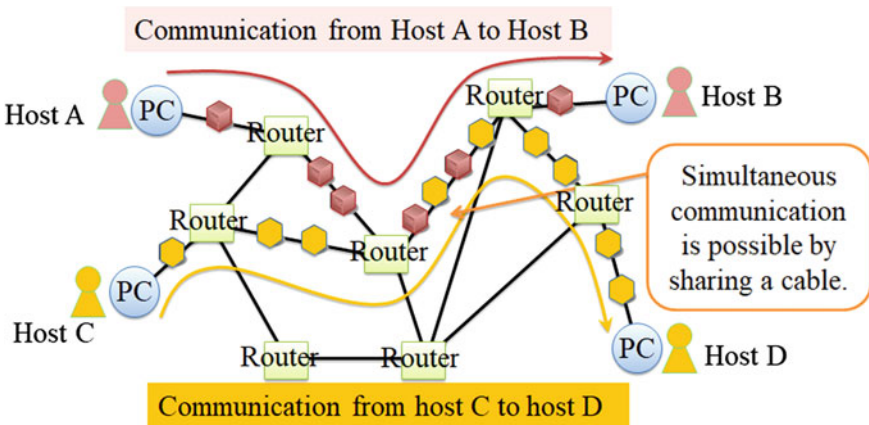


Fig. 7.2 Packet-switched network

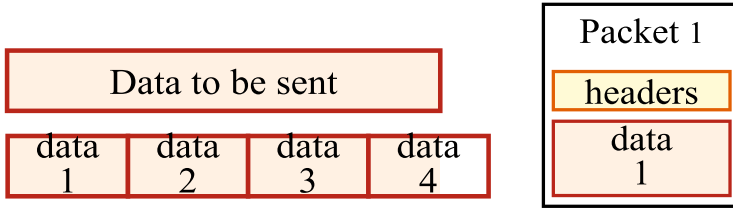


Fig. 7.3 Relation between data to be sent and a packet

Figure 7.3 illustrates the relation between data to be sent and a packet in a packet-switched network. The data is divided into the packet size, which is smaller than the data size [1]. Each packet consists of a portion of the data and headers containing information to identify the data, including sender, destination, type, serial number, and size. A detailed explanation of header structure will be provided in Sect. 7.5.1.

### 7.3 Network Topologies

Network topologies define the network’s connection type or configuration. In the early days, when computers were expensive, networks were developed to allow multiple terminals to share a single computer. The predominant topology at that time was the star topology, known for its efficient cable usage but vulnerable to network-wide failure if the central device malfunctions.

Other network topologies include bus, line, ring, tree, and mesh types. Bus topology was common in early Ethernets. Line topology suits smaller systems but is vulnerable to network-wide failure if any device malfunctions. Ring topology offers redundancy with minimal cables. Table 7.1 provides a summary of different network topologies along with their respective characteristics. The selection of a network topology should align with the specific type and intended purpose of the network.




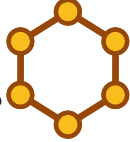


### 7.4 Physical Configuration

Based on the physical configuration, networks can be categorized into two main types: wired local area network (LAN) and wireless LAN.

#### 7.4.1 Wired LAN (Ethernet)

A wired LAN is commonly referred to as Ethernet [1]. Ethernet standards consist of three components, as depicted in Fig. 7.4: the number on the left side indicates the

Table 7.1 Network topologies

Type	Characteristics
Star 	A network configuration where multiple devices are connected to a central hub or switch. It offers efficient cable usage. If a cable fails, only one node is affected. However, a central device failure can bring down the entire network
Bus 	A network configuration where multiple devices are connected to a single shared bus, with terminators at both ends to prevent signal reflection and noise. This configuration was prevalent in the early days of Ethernet
Line 	A network configuration where multiple devices are connected in a linear series. This configuration is simple, but if any of the devices experiences a failure or goes offline, it can disrupt the entire network's functionality
Ring 	A network configuration where device connections create a circular data path. Each networked device is connected to two others, forming a circular data path resembling points on a circle. One advantage of this configuration is that it allows for cable redundancy while minimizing the number of cables required
Tree 	A network configuration where connected devices are arranged like the branches of a tree
Mesh 	A network configuration where each device is interconnected with every other device. This configuration ensures maximum transmission reliability, even if one connection fails. However, it requires a significant number of cables due to its high redundancy

**Fig. 7.4** An example of Ethernet standards

$$\begin{pmatrix} 10 \\ 100 \\ 1000 \\ 10G \end{pmatrix} \text{Base} \begin{pmatrix} 2 \\ 5 \\ T \\ TX \\ FX \\ \text{etc} \end{pmatrix}$$

maximum data rate, “Base” or “Fast” in the middle refers to the signaling type, and the number or letters on the right side denote the type of cable used. For example, in the “10BASE-T” standard, “10” indicates a maximum data rate of 10 Mbps (10 million bits per second); “Base” signifies the use of baseband signaling, and “T” means the network is wired using twisted pair copper cables.

Notably, Fig. 7.4 is an example of Ethernet standards. The figure does not include all Ethernet standards, and not all data rates on the left side can be paired with the numbers or letters on the right side.

In an Ethernet standard, the key element is the “maximum data rate” on the left side. Currently, Ethernet networks with a maximum data rate of only 10 Mbps are uncommon. Most Ethernet networks offer a maximum data rate of 100 Mbps or 1000 Mbps. While Ethernet networks with a maximum data rate of 10 Gbps (10,000 Mbps) are available, they are not yet widely adopted.

Ethernet connections can be established using either copper cabling or fiber optic cabling. In a copper cabling Ethernet, data is transmitted through copper cables. Previously, ADSL was primarily used for broadband Internet access over traditional copper telephone lines. It offers a maximum downstream (download) data rate of up to 24 Mbps. Upstream (upload) speeds are lower than downstream speeds. One advantage of ADSL is its ability to carry both voice communication (telephone service) and data communication (Internet service) over the same copper cable simultaneously. This is achieved by using different frequency bands for voice and data, allowing both services to coexist without interference. However, ADSL has been largely replaced by faster and more capable broadband technologies. Currently, one of the most prevalent forms of copper cabling Ethernet is twisted pair cabling Ethernet including Fast Ethernet (100 Mbps) and Gigabit Ethernet (1 Gbps).

Copper cabling has its drawbacks, including vulnerability to interference, lower quality for voice communication, and decrease in data rate as the distance from the closest exchange station increases. For example, an ADSL Ethernet may achieve the maximum data rate when the customer’s location is within 100 m of the nearest exchange station. As the distance from the exchange station increases, the data rate gradually decreases due to signal attenuation and other factors. Beyond a certain distance, the achievable data rate may significantly decrease.

In contrast, fiber optic cabling Ethernet offers distinct advantages, including high data rates over long distances. This technology relies on optical fibers for data transmission. With a maximum data rate exceeding 10 Gbps and a reach of over 40 km,

fiber optics excel in providing high-speed connectivity over considerable distances. They are also known for their resilience against external interference, even in challenging environments with high levels of noise. However, fiber optic cables are vulnerable to physical damage, including scratches, bends, and stains. If the optical fibers suffer from such issues, it can lead to a sudden network outage.

### 7.4.2 Wireless LAN (Wi-Fi)

Wireless LANs, also known as Wi-Fi, are standardized by IEEE 802.11 [1, 2]. Their standards have gone through multiple iterations and revisions. At present, the most commonly known ones among the IEEE 802.11 family include IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax.

Table 7.2 displays the frequency bands, maximum data rates, and characteristics of these Wi-Fi standards. For example, the 802.11a Wi-Fi operates in the 5 GHz frequency band and offers a maximum data rate of 54 Mbps. It is unlikely to be interfered by electronic devices like microwave ovens and Bluetooth devices, but has limited ability to go through obstacles.

Comparing the Wi-Fi standards listed in Table 7.2 with the Ethernet standards shown in Fig. 7.4, it can be known that Wi-Fi can match or even surpass Ethernet in terms of data speed. For example, the maximum data rate of an 802.11ax Wi-Fi reaches 9.6 Gbps, significantly faster than many common Ethernet standards with maximum rates of 100 Mbps or 1 Gbps.

**Table 7.2** Details of commonly known IEEE802.11 standards

x	Frequency band	Maximum data rate	Characteristics	
			Likelihood to be interfered	Ability to go through obstacles
a	5 GHz	54 Mbps	Low	Weak
b	2.4 GHz	11 Mbps	High	Strong
g	2.4 GHz	54 Mbps	High	Strong
n	2.4 GHz	600 Mbps	High	Strong
	5 GHz	600 Mbps	Low	Weak
ac	5 GHz	6.9 Gbps	Low	Weak
ax	2.4 GHz	9.6 Gbps	High	Strong
	5 GHz	9.6 Gbps	Low	Weak

**• Questions**

1. According to the details of the Wi-Fi standards in Table 7.2, which item determines the characteristics of a Wi-Fi network?

## 7.5 Internet

In a broad sense, the term “Internet” refers to a network in which multiple networks are interconnected. However, when we use the term “Internet” in a narrow sense, we are typically referring to the vast global-scale interconnected network that originated from ARPANET, a military network of the US Department of Defense. ARPANET was designed to withstand damage and continue functioning even if parts of it were destroyed. Today, when we say “the Internet”, we are usually referring to this global network, which is much more extensive and widely used than a generic “internet”.

### 7.5.1 Internet Protocols

A communication protocol is a set of predetermined rules for transmitting and processing information. It serves as the essential framework for ensuring correct information exchange between senders and receivers. It is similar to sending a postal letter, where one must write the recipient’s address, place the letter in an envelope, and affix a stamp.

For information communication on the Internet, a great number of protocols are needed. These include protocols for the cables connecting devices and protocols for processing different types of data, such as text, voice, and images. If only one protocol is used as a single system to meet all these needs, it can be imagined that this single protocol would become very large in scale and, consequently, difficult to maintain. Therefore, a hierarchical model is employed to facilitate the development and modification of protocols.

There are two hierarchical models of protocols. One is the Open Systems Interconnection (OSI) model developed by the International Organization for Standardization (ISO), and the other is the TCP/IP model, which is currently in use [2]. The term “TCP/IP” collectively refers to the two most widely used protocols: TCP, which stands for Transmission Control Protocol, and IP, which stands for Internet Protocol.

Table 7.3 provides a comparison of the two models. The OSI model comprises 7 layers, which are, from layer 1 to layer 7: the physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer. This model is not intended for practical implementation and is referred to as a reference model. It serves as a foundation for the development of multilayered protocols

**Table 7.3** OSI model versus TCP/IP model

OSI model	TCP/IP model
<b>Application layer (Layer 7)</b> Provides communication function for applications	<b>Application layer (Layer 4)</b> Provides services to the application being used by the user
<b>Presentation layer (Layer 6)</b> Unifies formats of data expression	
<b>Session layer (Layer 5)</b> Manages data sequence	
<b>Transport layer (Layer 4)</b> Achieves reliable data transmission	<b>Transport layer (Layer 3)</b> Ensures reliability in data transmission
<b>Network layer (Layer 3)</b> Determines the transmission route and destination of data	<b>Internet layer (Layer 2)</b> Provides end-to-end data transmission
<b>Data link layer (Layer 2)</b> Controls data transmission to neighboring devices	<b>Network interface layer (Layer 1)</b> Provides methods of data transmission in the physical parts of a network
<b>Physical layer (Layer 1)</b> Provides methods of transmission in electronic and mechanical parts	

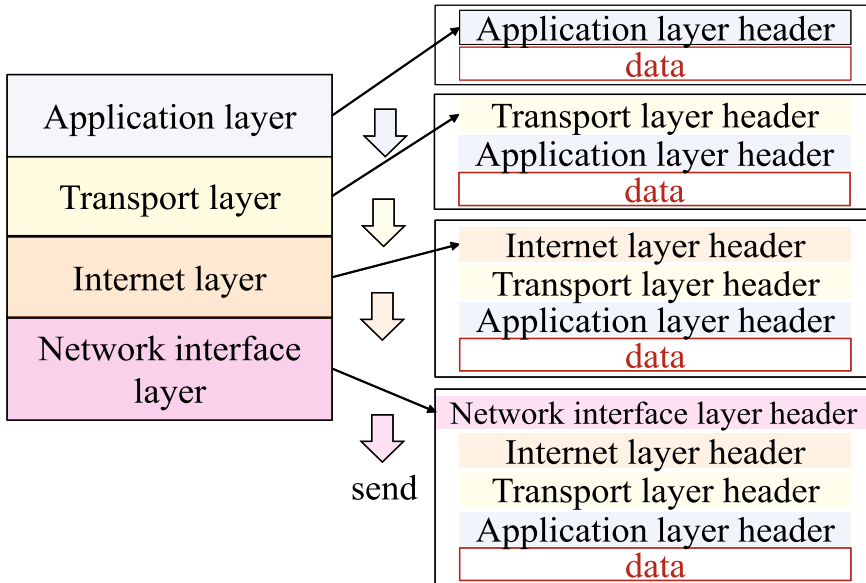
The TCP/IP model is currently in use and consists of 4 layers. In the model, layers 1 and 2 in the OSI reference model are combined into layer 1, known as the network interface layer, and layers 5 to 7 in the OSI reference model are combined into layer 4, known as the application layer.

Table 7.4 provides a list of widely used protocols in each layer of the TCP/IP model. In the network interface layer, protocols for Ethernet standards and Wi-Fi standards introduced in Sect. 7.4 are used. In the transport layer and the Internet layer, TCP and IP are used, respectively. In the application layer, HTTP is used for viewing web pages, and SMTP and POP are used for sending and receiving emails

**Table 7.4** Examples of protocols in TCP/IP model

TCP/IP model	Examples of protocols
<b>Application layer</b> Provides services according to the application being used by the user	<ul style="list-style-type: none"> <li>• Web: HTTP</li> <li>• E-mail: SMTP, POP, IMAP</li> </ul>
<b>Transport layer</b> Ensures reliability in data transmission	TCP, UDP, ICMP
<b>Internet layer</b> Provides end-to-end data transmission	IP
<b>Network interface layer</b> Provides methods of data transmission in the physical parts of a network	<ul style="list-style-type: none"> <li>• Ethernet: 10/100/1000 Base-T/ FX</li> <li>• Wi-Fi: IEEE 802.11a/b/g/n/ac/ax</li> </ul>





**Fig. 7.5** Procedure of sending data to the Internet in TCP/IP model

In the TCP/IP model, data intended for transmission over the Internet flow downward from the upper layers to the lower layers. Initially, data is sent to the topmost layer, which then appends a layer header to the data before passing it down to the next lower layer. Each successive layer follows this process, receiving data from the layer above, adding its own layer header, and forwarding the modified data to the layer below. Finally, the data destined for Internet transmission contains four headers, each added by one of the layers, as illustrated in Fig. 7.5.

Accordingly, the headers in the packet introduced in Sect. 7.2 (Fig. 7.3) consist of headers from the application layer, transport layer, Internet layer, and network interface layer.

In contrast, data received from the Internet moves upward from lower layers to upper layers. Initially, the data is received by the lowest layer, which checks whether the data is addressed to it. If it is, the layer removes its own header from the data and then forwards the data to the layer above. Each subsequent layer follows this process, receiving data from the layer below, checking for addressing, and, if correct, removing its own layer header before forwarding the data to the layer above. Ultimately, the processed data contains no headers, as depicted in Fig. 7.6.

When verifying the destination of data, each layer employs a specific type of address. Among these addresses, the IP address used in the Internet layer is the most well-known. Aside from its role in transmitting and receiving data within the Internet layer, IP addresses are widely used for various other purposes.

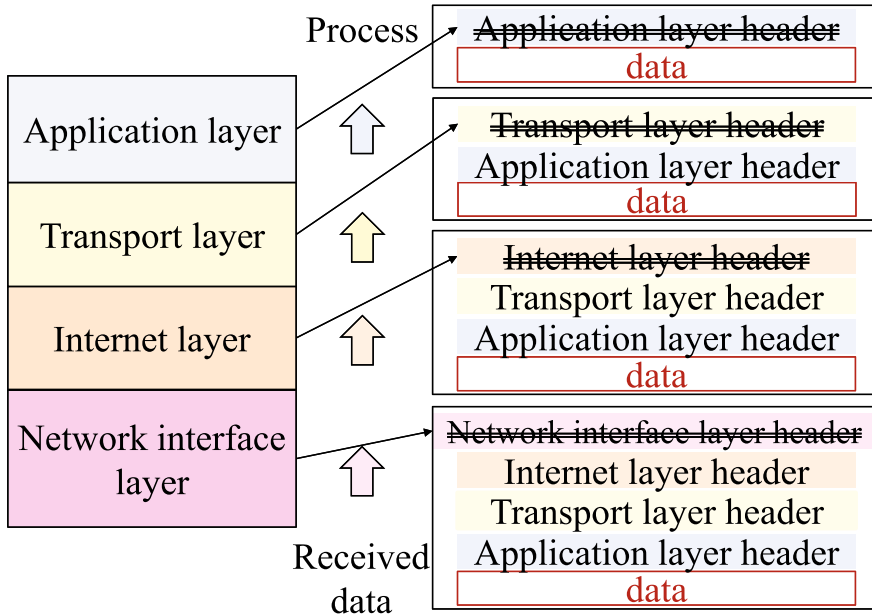


Fig. 7.6 Procedure of processing data received from the Internet in TCP/IP model

### 7.5.2 IP Address

An IP address serves as an identifier for a unique terminal connected to the Internet. Figure 7.7 illustrates an IP address, where 133.28.10.100 represents the IP address itself, and 80 is the port number. Typically, the port number is used to identify the software or application. For example, port number 80 is commonly associated with web browsers.

The range of IP addresses allocated to each country and region worldwide is pre-established and remains constant. For example, the IP addresses allocated for Kanazawa University start from 133.28.xx.xx [3]. Similarly, the IP address ranges for individual buildings and departments are also predetermined and fixed [3]. In other words, there is a direct correlation between an IP address and a location. As a result, if you know the IP address of a terminal device, you can know its location.

IP addresses can be divided into two categories: global addresses and private addresses. A global address is unique worldwide and does not duplicate anywhere else in the world. For example, the IP address shown in Fig. 7.7 is a global address. On the other hand, a private address is managed independently within an internal

Fig. 7.7 An example of IP address and port number



network, such as a company’s or a home network. Private addresses typically begin with either “10.” or “192.168.”

There are two versions of IP addresses: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). IPv4 has been in use since the early days of the Internet, while IPv6 was developed as the next-generation protocol. IPv4 uses a 32-bit address format, allowing for a total of  $2^{32} = 4,294,967,296$  (more than 4.2 billion) addresses. With the global population approaching this number, IPv4 address exhaustion is a foreseeable issue. In contrast, IPv6 employs a 128-bit address format, capable of accommodating an astonishing  $2^{128} = 340,282,366,920,938,463,463,463,374,607,431,768$  (more than 340 decillion) addresses, making it virtually inexhaustible. IPv6 also brings various improvements over IPv4. However, the challenge lies in its incompatibility with IPv4, which has hindered its widespread adoption despite its standardization in 1995.

### 7.5.3 Domain Name

An IP address is made up of digits, which are not easy to remember and use. To make it easier to remember and use, domain names, which are made up of characters, are used. Figure 7.8 shows an illustrative URL, where the portion beginning with “example” represents the domain name. A domain name has a hierarchical structure that is separated by “.”. The hierarchy begins with a top-level domain (TLD) situated at the far right, followed by a second-level domain (SLD). The top-level domain can encompass either a generic TLD (gTLD) or a country code TLD (ccTLD). Examples of gTLDs include .com (for companies), .org (for organizations), and .gov (for U.S. government entities).

When a user enters a domain name, such as a website address, the address needs to be converted into its corresponding IP address before it can be used by computers on the Internet. This automatic conversion between domain names and IP addresses is made possible through a mechanism known as the Domain Name System (DNS). DNS servers play a crucial role in managing lists of domain names and their corresponding IP addresses. When a user inputs a domain name, a DNS server translates that name into the corresponding IP address, allowing computers on the Internet to process it. Similarly, when an IP address needs to be converted back into its corresponding domain name, the DNS server handles this translation before presenting the result to the user. Due to the vast number of domain names and IP addresses on the Internet, a single DNS server cannot manage them all effectively. Instead, a

Fig. 7.8 An example of domain name



distributed hierarchical structure is used, with the root DNS server situated at the top.

### • Questions

2. What is the mechanism of a Web page accessible from only inside an institution, i.e. a Web page that cannot be accessed even if you enter your user name and password when you are outside that institution?

Hint: think about how you can know whether a terminal device is inside the institution.

## 7.6 Various Information Systems

In recent years, there has been rapid development in information and communication systems, resulting in the popularity of various new systems. In this book, we will provide brief descriptions of some of these systems.

### (1) Cloud computing

Cloud computing refers to the use of devices or services over the Internet. The term “cloud” symbolizes the Internet, because Internet is often depicted as a cloud in images.

Traditionally, we have used computers with locally installed software and applications. Cloud computing, however, entails the use of software, applications, and services via the Internet, eliminating the need for installation on local devices. For example, using online services or storing files in online storage are examples of cloud computing.

Cloud computing includes Software as a Service (SaaS), which provides use of software, and Infrastructure as a Service (IaaS), which provides use of computer resources (CPU, memory, storage, etc.) via virtualization technologies.

### (2) Sensor network

A sensor network is a type of network in which sensors are interconnected. Originally, the term “network” referred to a system of interconnected computers. In a sensor network, sensors replace the traditional computers. Sensors typically serve specific functions and are simpler than computers. As a result, most sensor networks are wireless and use low-power protocols like ZigBee.

### (3) Ubiquitous computing

The word “ubiquitous” derives from the Latin word “ubique”, which means “everywhere, anytime, and any place”. Accordingly, ubiquitous computing refers

to an information environment in which computers are accessible everywhere at any time.

In recent years, the development of smartphones and wearable computers has made it possible for users to own and carry multiple computing devices. As a result, the vision of a ubiquitous networked society based on ubiquitous computing is becoming a reality.

#### (4) **Internet of Things (IoT)**

The Internet of things (IoT) is often seen as the successor to ubiquitous computing. IoT has gathered attention because it enables information exchange and control between various things, including home appliances, machines, and portable devices, by assigning them IP addresses directly. IoT facilitates remote control of devices like television recorders and air conditioners, as well as remote monitoring, such as tracking a machine's status or a pet's location. Moreover, it enables seamless communication between things, as they can send and receive data. Furthermore, sensors attached to these things can collect substantial amounts of data, which can open the door to new values and services.

#### (5) **Industry 4.0**

Industry 4.0 represents a transformative approach to digitizing and computerizing the manufacturing industry through the integration of AI and IoT. Its primary goal is to enhance productivity by harnessing AI technologies, such as machine learning, for predicting equipment malfunctions and abnormalities. Additionally, it leverages IoT to collect real-time data on machine operations and captures big data like temperature and humidity datasets at various machine locations.

### **Exercises**

1. What may cause a computer network to be slow?

**• Guidance**

Think about various possibilities, primarily based on the content in this book.

2. What may cause a computer network to go down?

**• Guidance**

Think about various possibilities, primarily based on the content in this book.

3. Describe what you expect in your future life and work from technologies such as AI and IoT.

**• Guidance**

Give some detailed examples of your expectations. A poor example might be “use AI to raise work efficiency” because it is unclear how to use AI, raise what kind of efficiency, and in what type of work. It would be better to give more details.

4. Create a flowchart to illustrate your idea for using AI and IoT to realize one of the expectations.

**• Guidance**

You are encouraged to create a clear and user-friendly flowchart for an innovative idea. Flowchart is the topic of Chap. 2, and you may review it if you need a refresher. The notes on flowcharting will help you improve the quality of your flowchart.

## References

1. Andrew ST, David JW (2010) Computer networks, 5th edn. <https://csc-knu.github.io/sys-prog/books/Andrew%20S.%20Tanenbaum%20-%20Computer%20Networks.pdf>
2. Forouzan BA (2005) Data communications and networking. McGraw-Hill Education, New Delhi, India
3. <https://www.med.kanazawa-u.ac.jp/inside/net/shinsei/listip.html>