ELEC S212

Network Programming and Design

Unit 1

Introduction to computer networking and the Internet

香港公開大學
THE OPEN UNIVERSITY OF HONG KONG
科技學院 School of Science and Technology

Course team

Developers: Jacky Mak, Consultant
John Wu, Consultant

Designer: Ross Vermeer, ETPU

Coordinator: Dr Philip Tsang, OUHK

Member: Dr Steven Choy, OUHK

External Course Assessor

Prof. Cheung Kwok-wai, The Chinese University of Hong Kong

Production

ETPU Publishing Team

The Open University of Hong Kong
Ho Man Tin, Kowloon
Hong Kong

This course material is printed on environmentally friendly paper.

Contents

Overview

We begin our study of network programming and design by making sure you have a solid foundation in basic networking concepts, the Open Systems Interconnect (OSI) model and the Internet model, the Internet and its services, and major networking standards and standards organizations.

The first section of this unit provides you with an overview of basic networking concepts. You'll learn about the two basic models for networks, i.e. peer-to-peer and client/server, and you'll be introduced to a range of common network types such as local area networks (LANs), wide area networks (WANs) and so on.

In the second section of this unit, we explore how and why we implement a layering structure in the OSI model and the Internet architecture. Layering structures and the corresponding functions of each layer are discussed, in order to identify the differences between the OSI model and the Internet architecture.

In the third section, we discuss what the Internet is and describe its architecture. A brief history of the Internet is presented, along with some of the common uses of the Internet.

In general, networks (and especially the Internet) are comprised of vastly heterogeneous computers and devices. Protocols must be adopted to ensure that data are transferred in a standard method or format such that the communicating devices can understand how to process the data. The final section of this unit therefore discusses what a protocol is, and briefly describes several popular networking protocols. It also introduces the major networking standards and standards organizations.

In short, this unit:

- explains what a computer network is, and why computer networks are used;
- describes the basic network topologies, their usages and benefits;
- describes, compares and contrasts the characteristics of circuit-switched networking and packet-switched networking;
- describes, compares and contrasts the characteristics of connection-oriented and connectionless services; and
- explains what the Internet is, and describes its infrastructure and services that are available on the Internet.

This unit should take you four weeks (or approximately 30 hours) to complete.

Basic computer networking concepts

This section presents an overview of computer networking. It also sets the stage for the rest of the unit by introducing many key concepts and important terminology. You will explore many of the topics discussed in more detail later in the course.

What is a computer network?

A network is a group of computers and other devices (such as printers) that are connected by some type of transmission media for the purpose of communicating and sharing resources. Networks may be as small as two computers connected by a cable in a home office, or as large as several thousand computers connected across the world via a combination of cables, phone lines and satellite links. In addition to connecting personal computers, networks can link mainframe computers, printers, plotters, fax machines and phone systems. Computers on a network may communicate through copper wires, fibre-optic cable, radio waves, infrared or satellite links.

將一堆既電腦，用某種方式連埋一齊

Computer networks enable multiple users to share devices and data that are referred to as the networks' resources or services. The two fundamental network models are peer-to-peer and client/server. You'll learn more about these models later in this topic.

Activity 1.1

Different authors may have different definitions of a computer network.

Conduct a simple search for definitions of a computer network. You can of course search the Internet, but you might also want to look through any computing textbooks you may own, or that you can find in the library.

What different 'flavours' can you identify in these definitions? Do the definitions seem to change over time?

After you've completed your search, try to summarize the key characteristics of computer networks you've identified.

What advantages do networks offer?

In general, networks offer numerous advantages relative to using a standalone computer. These advantages include the following:

- enabling resource sharing Printers ,fax ...
- enhancing communication and collaboration between people Facebook, ig, Twitter
- allowing both the remote and central management of resources and computers 網上訂飛, TaoBao
- enabling distributed systems.

Enabling resource sharing

Networks allow resources to be shared without regard to the physical locations of the resources and the user. Such resources that can be shared include (but are not limited to):

- **equipment** — expensive colour laser printers, scanners, fax gateways and so on.
- **information** — data files, multimedia files, database, program libraries and so on.
- **storage** — file servers in a corporate environment
- **computational resources** — emerging technologies such as grid computing that allow unused computational resources (for example, idle processing power) to be shared over a network.

Resource sharing saves money because expensive resources can be better utilized. In addition, sharing information can also increase productivity because large data files can be transferred much faster over a network than by using floppy disks.

Enhancing communication and collaboration between people

Networks allow and enhance communication and collaboration between people without regard to their geographical separation. For example, we can use electronic mail, video conferencing, Internet telephony, and instant messaging applications to communicate with our friends, relatives, customers, and co-workers on the other side of the globe any time at no or minimal cost. This is especially important for organizations and projects that span national boundaries.

Allowing remote and central management of resources and computers

Networks allow an organization's administrator to remotely manage and administer computers and other resources from a central location. For example, the administrator of a multinational bank can initiate a database backup on multiple database servers that are located around the globe from his or her own desktop computer. Again, this is especially important for organizations and projects that span national boundaries.

Enabling distributed systems

In the past, a computer system was usually based on a centralized mainframe computer. In contrast, a modern distributed system is based on a number of less powerful computers connected by a network. Since these networks connect multiple computers together, we can build distributed systems that provide services that are more efficient in several ways. A distributed system can be more:

- *available* and *reliable*, because the failure of one or a few of the component computers will not bring down the whole system
- *scalable*, because additional computers can be added with relative ease to cope with the growth of the system.

Activity 1.2

Read the Wikipedia article on the World Community Grid (WCG) at:

http://en.wikipedia.org/wiki/World_Community_Grid

Can you think of any other uses for the WCG that would benefit humanity?

On the other hand, from a user's point of view, what potential problems might hinder you from participating in such an effort?

What services can networks provide?

The features provided by a network are usually called **services**. Electronic mail is the most visible network service in a company. Other services such as printing, file sharing, Internet access, remote dial-in capabilities, communication and management services are all critical business functions that can be provided through networks. In large organizations, separate servers may be dedicated to performing each of these functions. In a small company that has only a few users, however, one server can perform all functions.

After completing the following reading, you should be able to list and describe several specific services that networks can provide.

Reading

Dean (2012) 1–3, 12–16.

At this point, you should be ready to tackle your first self-test. Answer the following questions as accurately and completely as you can before checking the feedback provided at the end of the unit.

Self-test 1.1

1 What is a computer network?

2 List the major advantages that computer networks have over a standalone computer.

3 List the major categories of network services.

Peer to Peer (processing power 差啲多). 宜家好少了(岩極細型公司)， eg. Work

Client/server and peer-to-peer networks

Computers can be positioned on a network in different ways relative to each other, and can be granted different levels of control over shared resources. They can also be made to communicate and share resources according to different schemes.

In a **peer-to-peer** network, every computer can communicate directly with every other computer. In a **client/server** network, a central computer is used to facilitate communication and resource sharing between computers on the network.

Server = 集中，提供服務比人（hardware 層面比較勁）
Eg. Sharing , active directory

The following reading describes these two fundamental network models.

Reading

Dean (2012) 3–7.

In reality, many networks are **hybrid** networks. Hybrid networks provide centralized services based on servers, but they also allow users to share and manage their own resources within the workgroup.

In recent years, many new peer-to-peer (P2P) network applications have appeared. These applications link thousands — even millions — of

computers over the Internet to share files between each other. Unlike the traditional peer-to-peer networks that Dean discusses, however, these new P2P applications use specialized networking algorithms and protocols to make them *very* scalable. Examples of such applications include BitTorrent, eMule, and PPLive, just to name a few.

Activity 1.3

Search the Internet to find out what PPTV is. Can you find any other, similar P2P applications?

Elements common to client/server networks

In general, any server-based network, regardless of network architecture, requires the following components:

定義

- **Client** — A computer on the network that requests resources or services from another computer on the network. Most clients are workstation computers.
- **Server** — A computer on the network that manages shared resources or services. It usually has more processing power, memory and hard disk space than clients.
- **Network interface card (NIC)** — The device that enables a workstation to connect to the network and communicate with other computers.
- **Network operating system (NOS)** — The software that runs on a file server and enables the server to manage data, users, groups, security, applications and other networking functions.
- **Central wiring concentrator** — A device that serves as a connection point for all attached network devices.
- **Transmission media** — The means through which data are transmitted and received. Transmission media can be via wires or wireless.

The following reading introduces you to some basic elements common to all client/server networks. You will learn much more about these elements later in this unit, and throughout the course.

Reading

Dean (2012) 9–12.

PANs, LANs, MANs, CANs and WANs

以size 分類

Networks can be classified into broad categories according to their relative sizes. These categories, from the smallest to the largest, are:

- **Personal area network (PAN)** — A PAN is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one person. Its reach is typically just a few metres. PANs can be used for communication among the personal devices themselves, or for connecting to higher level networks and the Internet. PANs may be wired with computer buses such as USB and FireWire. A wireless PAN (WPAN) can also be made possible using network technologies such as IrDA, Bluetooth and ZigBee.

= 屋企既network

- **Local area network (LAN)** — A LAN is a network of computers and other devices that is confined to a relatively small space, such as one building or even one office. The defining characteristics of LANs, in contrast to Wide Area Networks (WANs), include their much higher data transfer rates, smaller geographic range, and lack of a need for leased telecommunication lines. The prevalent LAN technology is Ethernet.

- **Metropolitan area network (MAN)** — A MAN is a network that is larger than a LAN, typically connecting clients and servers from multiple buildings, but that still is confined to a limited geographic area. For example, a MAN could connect multiple city government buildings around a city's centre. MANs can span up to a few tens of kilometres, and the devices used are typically modems and wires/cables. The typical network technologies used for MANs are ATM and FDDI, although they are in the process of being displaced by Gigabit Ethernet in many areas.

- **Campus area network (CAN)** — A CAN is another type of network that connects local area networks (LANs) within a limited geographical area, i.e. a campus. It can be considered to be a form of a metropolitan area network, but one that is specific to an academic setting.

- **Wide area network (WAN)** — A WAN is a network that spans a long distance (typically across metropolitan, regional or national boundaries) and that connects two or more LANs. Since they carry data over longer distances than LANs, WANs require slightly different transmission methods and media and often use a greater variety of technologies than LANs. The largest and most well-known example of a WAN is of course the Internet.

In the following reading you will learn more about LANs and WANs.

> ***Reading***
>
> Dean (2012) 7–8.

Self-test 1.2

1 Compare and contrast client/server networks against peer-to-peer networks.

2 Compare and contrast LANs against WANs.

Network topologies

The physical layout of a network's nodes, i.e. the way computers in a network are arranged and connected, is defined by its **physical topology**, which greatly affects the network performance and reliability. Along with the physical medium chosen for implementing the links, a network's topology determines its speed and communication efficiency. Its selection depends on the geographic environment, the kinds of applications running on the network and the implementation costs.

Bus = fallout

而家係用 **Star = Ethernet Toplogogy

Ring = IBM 整出黎，network card 要收license

The three basic physical topologies are **bus**, **star** and **ring**. Each has its own relative advantages and disadvantages.

The way in which a network accesses media and transmits packets across it is its **logical topology**. At a first glance, you may *think* that a network's logical topology is just the same as its physical topology. However, the way in which data travels across a network may indeed be different from the physical layout of its nodes.

You will learn about network topologies in detail in *Unit 2*.

Circuit-switching, message switching and packet switching

Switching is the component of a network's logical topology that determines how connections are created between nodes. There are three methods for switching: **circuit switching**, **message switching** and **packet switching**. Every network transport system relies on one of these switching mechanisms.

You will also learn more about switching in *Unit 2*.

Connection-oriented and connectionless services

When data is transmitted in **connection-oriented communication**, the devices at the end points use a preliminary protocol to establish an end-to-end connection before any data is sent. Connection-oriented protocol services are often — but not always — 'reliable' network services that guarantee that data arrive in the proper sequence.

The alternative to connection-oriented communication is **connectionless communication**, also known as **datagram communication**, in which data is sent from one end point to another without any prior arrangement, and no guarantees provided. In datagram communication, each data packet must contain complete address information, since packets are routed individually. The packets in any given communication may be delivered along different paths and without any guarantees, according to a best-effort policy.

Connectionless protocols are usually described as **stateless** because the end points have no protocol-defined way to remember where they are in a 'conversation' of message exchanges. Because they can keep track of a conversation, connection-oriented protocols are sometimes described as **stateful**.

You will learn about connection-oriented and connectionless services and how they are applied in the transport layer protocols in *Unit 3*.

Network transport systems

A network transport system describes the network's logical interconnection between nodes rather than its physical interconnection. A network transport system depends on electrical pulses carried by the physical layer of the OSI model (which you will learn about later in this unit). Currently, Ethernet and Wi-Fi are the two most common network transport systems, but ARCNET, Token Ring and many others have been used in the past.

Ethernet, standardized as IEEE 802.3, was developed in the mid-1970s by Bob Metcalfe and David Boggs at Xerox PARC. Ethernet has quickly become the standard for wired LAN technology. It is also a working example of the more general **Carrier Sense Multiple Access with Collision Detect** (**CSMA/CD**) technology. Figure 1.1 shows Metcalfe's historical schematic for his invention.

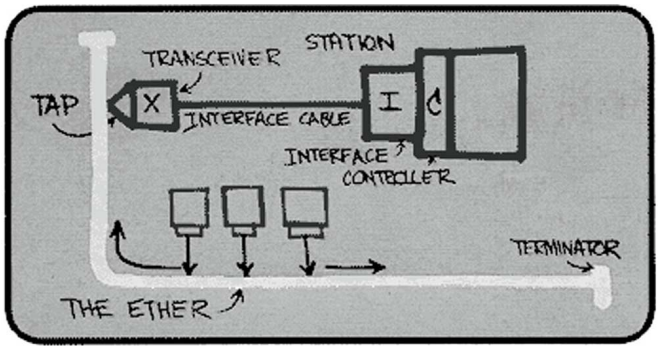

Figure 1.1 The original Metcalfe design that led to the 10BASE5 Ethernet standard

In recent years, Wi-Fi, the wireless LAN system standardized by IEEE 802.11, has become prevalent in home and small office networks and is augmenting Ethernet in large installations.

You will learn more about Ethernet and Wi-Fi in *Unit 2*.

Network operating systems

Network operating systems enable servers to share resources with clients. They also facilitate other services such as communications, security and user management. The prevalent network operating systems today include Windows Server 2003/2008, Unix, Linux, Solaris, Mac OS X Server, and Novell Netware/OES. You will learn more about network operating systems in *Unit 4*.

Network security

The availability of resources in open systems, coupled with the tremendous network growth in wireless networks, combine to raise severe security concerns for computer networks. It is the responsibility of network service providers to protect corresponding resources. If a system does not have proper protection, malicious intruders may steal or modify data. Some attacks can even cause the system to crash, or to lose data. Network security is a vast subject, but we will cover the basics in *Unit 8*.

The OSI model and the Internet reference model

In the first topic you learned the basic components in a server-based network and the typical services provided by a network. This section introduces the concept of the layering structure of the Open Systems Interconnect (OSI) model, and then of the Internet architecture. Layering structures and the corresponding functions of each layer are discussed to identify the differences between the OSI model and Internet architecture.

The OSI model

The **Open Systems Interconnection Basic Reference model** (**OSI reference model** or **OSI model** for short) is a layered, abstract description for communications and computer network protocol design. It was developed as part of the Open Systems Interconnection (OSI) initiative and is sometimes known as the **OSI 7-layer model**.

A layer is a collection of related functions that provides services to the layer above it and receives services from the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next-lower layer to send and receive packets that make up the contents of the path.

From top to bottom, the seven layers in the OSI model are: **Application** layer, **Presentation** layer, **Session** layer, **Transport** layer, **Network** layer, **Data Link** layer and **Physical** layer. The following table summarizes the functions of the OSI layers:

Table 1.1 The OSI layers and their functions

OSI model layer	Function
Application (Layer 7)	Provides interface between applications and network for interpreting application requests and requirements
Presentation (Layer 6)	Allows hosts and applications to use a common language to perform data formatting, encryption and compression
Session (Layer 5)	Establishes, maintains and terminates user connections
Transport (Layer 4)	Ensures accurate delivery of data through flow control, segmentation and reassembly, error correction and acknowledgment
Network (Layer 3)	Establishes network connections; translates network addresses into their physical counterparts and determines routing
Data Link (Layer 2)	Packages data in frames appropriate to the network transmission method
Physical (Layer 1)	Manages signalling to and from physical network connections

The following figures show how data flows through the layers in the OSI model:

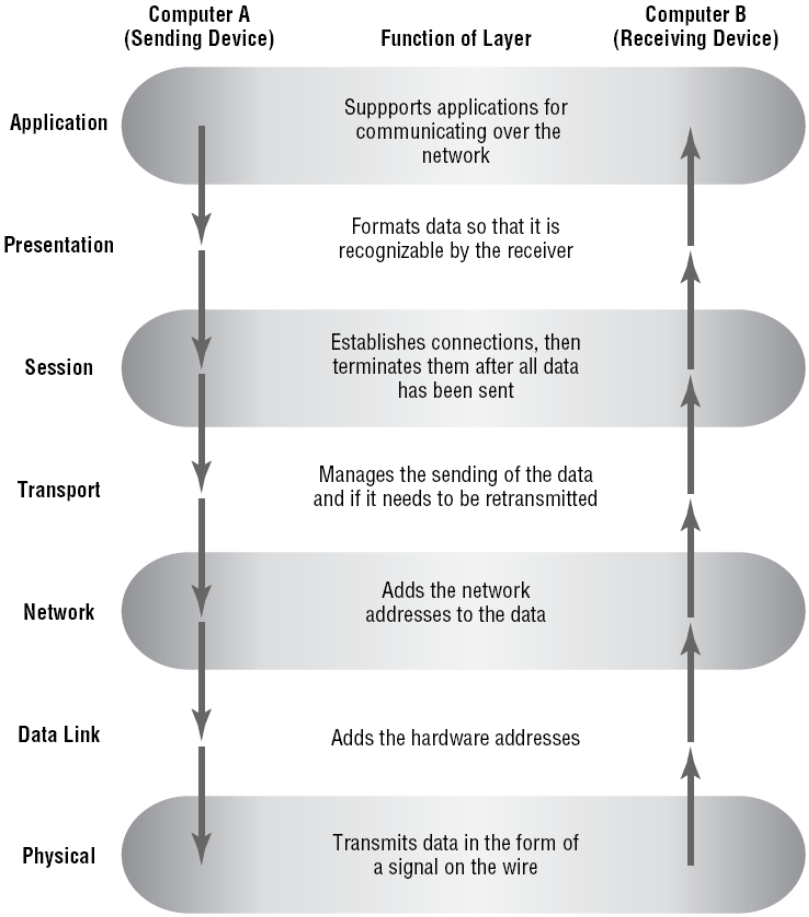

Figure 1.2 How data flows through the layers in the OSI model

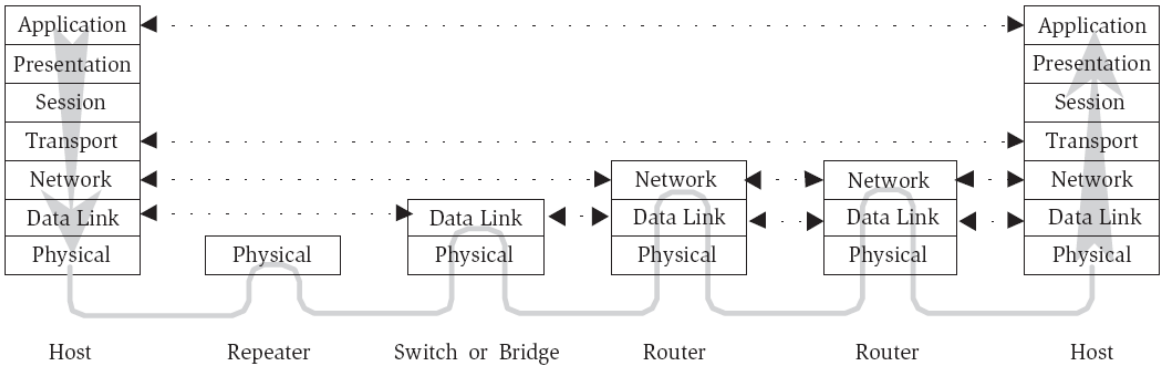

Figure 1.3 How data flows through the layers in the OSI model via the intermediate nodes

The following Wikipedia article gives you a very good and concise overview of the OSI model. After reading this article, read pages 44–59 of your Dean textbook to learn about the OSI layers in more detail. When you have finished these two readings, you should be able to identify and describe the functions of the OSI's seven layers.

Reading 1.1

http://en.wikipedia.org/wiki/Osi_model

Reading

Dean (2012) 42–59.

Activity 1.4

Search the Internet for a method to help you remember the names of the seven OSI layers. Give an example of how to apply this method.

Note that some of you may find it easier to remember the layers from top to bottom (i.e., from the Application layer down to the Physical layer), but others may find it easier the other way round (i.e. from the Physical layer up to the Application layer).

Self-test 1.3

If you use a password to log in to your email server program (e.g. Microsoft Exchange), which layer of the OSI model would decode your password?

The Internet reference (TCP/IP) model

Although the OSI model is more famous than any OSI protocol, just the opposite could be said about the **Internet suite of protocols model**. Also known as the TCP/IP protocol suite, or TCP/IP architecture, this communications architecture takes its name from Transmission Control Protocol/Internet Protocol (TCP/IP), the *de facto* standard protocol for open system internetworking. TCP/IP uses the original US Department of Defense (DoD) model which, like the OSI model, is a layered communications architecture in which the upper layers use the functionality offered by the protocols of the lower layers. Each layer's protocols are able to operate independently from the protocols of other layers.

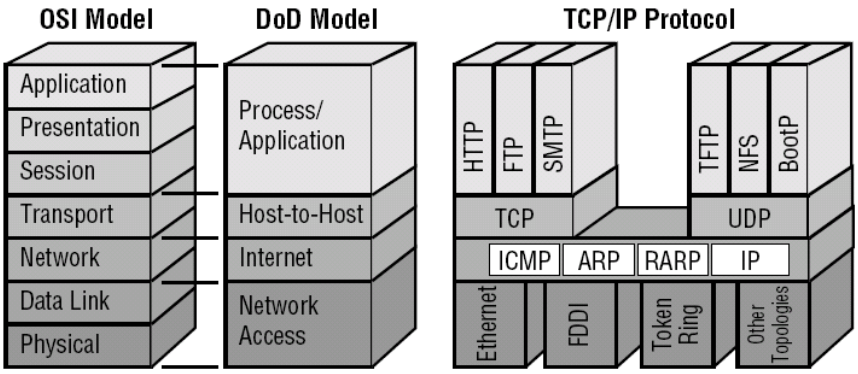

Figure 1.4 A comparison of the 7-layer OSI model, the 4-layer DoD model and TCP/IP

The original TCP/IP protocol suite was defined as having four layers, which were, from top to down: **Process/Application**, **Host-to-Host**, **Internet** and **Network Access**.

In the lowest Network Access layer, there are a wide variety of network access protocols. These protocols are implemented through a combination of hardware and software. To set up a TCP/IP network, one of the first things that you have to do is to choose the kind of network access protocols you will use. For example, one might find Ethernet or Fiber Distributed Data Interface (FDDI) protocols in this layer. The second Internet layer consists of a single protocol: the **Internet Protocol (IP)**. This protocol supports the interconnection of multiple networking technologies into a logical internetwork. The third Transport layer contains two main protocols: the **Transmission Control Protocol (TCP)** and the **User Datagram Protocol (UDP)**.

On top of the Transport layer is the Process/Application layer. Application protocols such as **File Transfer Protocol (FTP)**, **Telnet** and **Simple Mail Transfer Protocol** (i.e. **SMTP**, or electronic mail) are run in this layer.

The Internet architecture has the following features:

1 You may notice that the layering concept of the Internet architecture is different from that of the OSI model. As shown in Figure 1.4, the number of layers in the Internet architecture is reduced to four instead of the seven used in the OSI model.

2 The Internet Protocol (IP) working at the Internet layer is the most critical factor for the development of the Internet architecture: it defines a common method for exchanging packets among a wide collection of networks. Above the Internet layer, many transport protocols are available. The most commonly used ones are TCP or UDP. Below the Internet layer, the Internet architecture also supports a variety of network technologies. Different network technologies such as Ethernet, FDDI and **Asynchronous Transfer Mode** (**ATM**) can be applied in the Internet architecture.

Although the Internet architecture was not designed according to the OSI reference model (in fact, many fundamental TCP/IP protocols were designed prior to the OSI model), it is possible to arrange the functionality of the Internet protocols to fit into the OSI model, as seen in Figure 1.4. The Process/Application layer in the Internet model combines the functions of the top three layers in the OSI model. Both models consist of the Transport layers in the middle of the structures. The Network layer in the OSI model is similar to the Internet layer in the Internet model. Finally, the Network Access layer in the Internet model combines the functions of the Data Link layer and the Physical layer in the OSI model.

Self-test 1.4

1 What are the differences between the OSI model and the Internet model?

2 What are the advantages of using layering in modelling network systems?

The following Wikipedia article gives you a very good and concise overview of the TCP/IP model. After reading this article, you should be able to identify the layers in the TCP/IP model and describe some of the more important protocols in each of the layers.

Reading 1.2

http://en.wikipedia.org/wiki/TCP/IP_model

Many modern textbooks (including Forouzan 2006, Kurose and Ross 2008, and others) describe the TCP/IP as having five layers, which are, from top to bottom: **Application**, **Transport**, **Network**, **Data Link** and **Physical**. In these textbooks, the original Network Access layer is divided into the Data Link layer and the Physical layer.

The development of the Internet Protocol suite was included in the lists of request for comment (RFC). For more details of the Internet Protocol (IP) and Transmission Control Protocol (TCP), therefore, you can refer to RFC 791 and RFC 793 on the IETF website. These documents provide detailed explanations of the relationship between layer structure and the protocol data units in the OSI model. Depending on the running protocol in each layer, the corresponding header/trailer format may be varied. For now, it's enough just to take a quick look at these long documents' contents and introductions. You can refer to them later for more detail if you like. Don't worry if you do not fully understand these documents at

this point; they are intended to be read by experienced networking professionals or software engineers.

Reading 1.3

http://www.ietf.org/rfc.html

RFC 791 defines the IP and is the universal protocol of the Internet. This datagram protocol provides the universal addressing of hosts in the Internet. A few minor problems have been noted in this document. In addition, some changes are in the works for the security option. Note that Internet Control Message Protocol (ICMP) is considered an integral part of IP.

The Transmission Control Protocol is defined in RFC 793. It provides a reliable end-to-end data stream service. This document represents a specification of the behaviour required of any TCP implementation, both in its interactions with higher-level protocols and in its interactions with other TCPs.

You should now be ready to take on the following self-test.

Self-test 1.5

1 What is a protocol data unit (PDU)? What are the PDUs in each of the OSI layers?

2 Give the names of five protocols in the Application layer of the TCP/IP model and briefly describe their functions.

3 Give the names of three protocols in the Transport layer of the TCP/IP model and briefly describe their functions.

4 Give the names of two protocols in the Network layer of the TCP/IP model and briefly describe their functions.

5 Give the names of three protocols in the Network Access layer of the TCP/IP model and briefly describe their functions.

The Internet and Internet services

The Internet is a worldwide, publicly-accessible series of interconnected computer networks that transmit data via packet switching using the standard TCP/IP protocol suite. The Internet is a 'network of networks' that consists of millions of smaller domestic, academic, business and government networks. Together, they carry a variety of services, such as electronic mail, online chat, file transfer and the vast amounts of information contained in the interlinked webpages and other resources of the World Wide Web (WWW).

The following two figures together illustrate the infrastructure of the Internet, using a connection to an overseas Web server as an example:

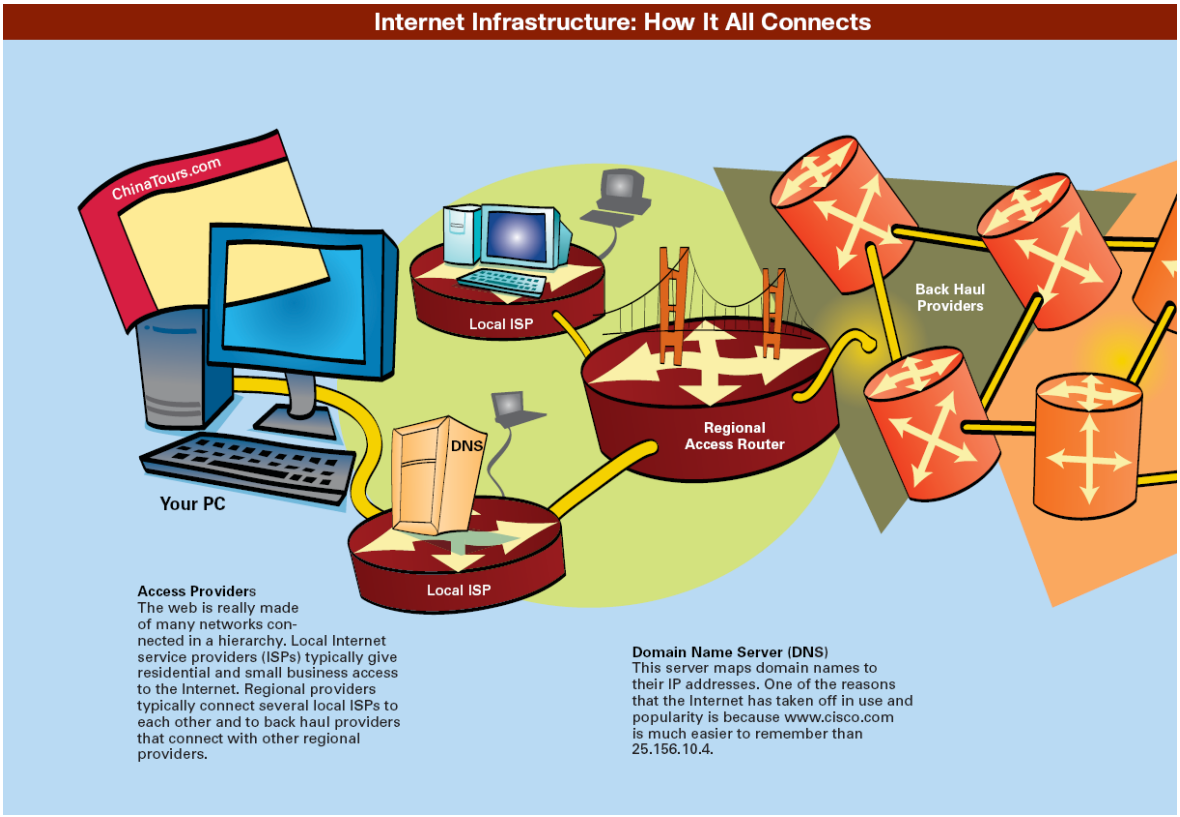

Figure 1.5a How the Internet connects clients and services

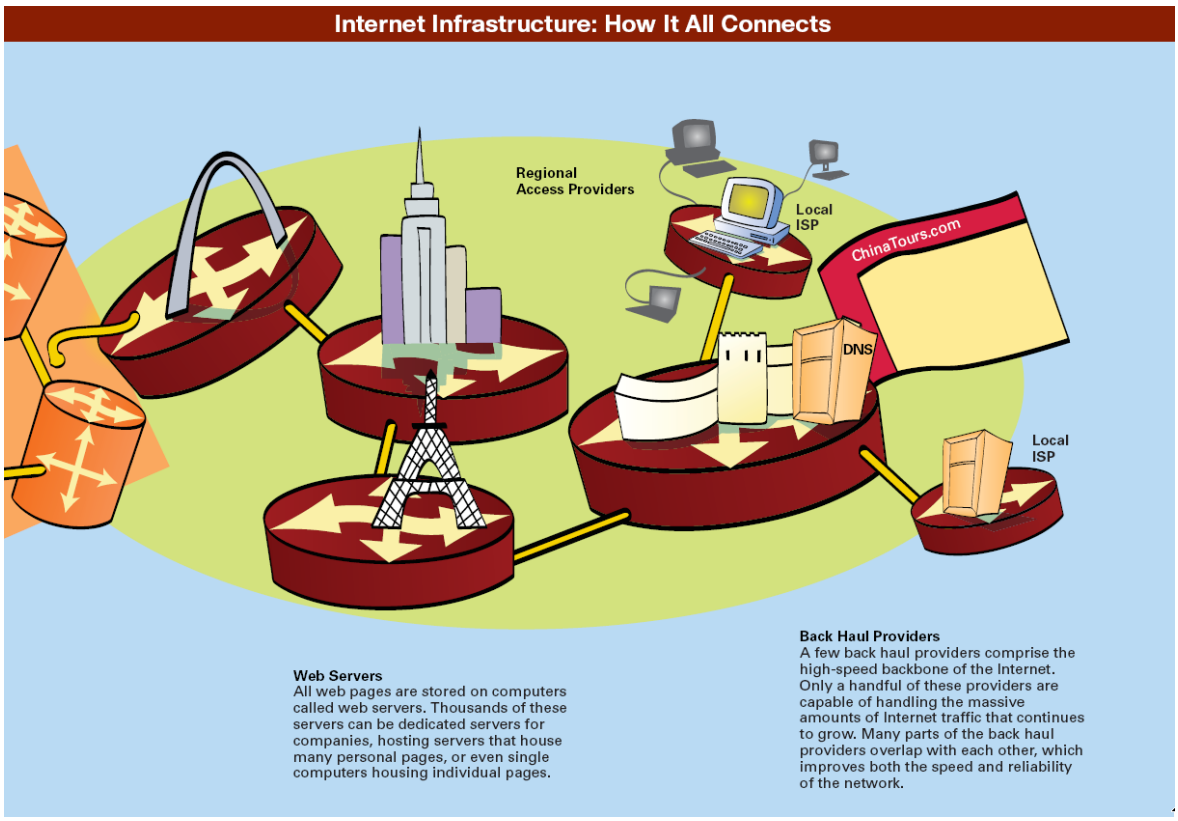

Figure 1.5b How the Internet connects clients and services

A brief history of the Internet

> The Internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a worldwide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location. (http://www.isoc.org/internet/history/brief.shtml)

In fact, the Internet has almost become indispensible to our daily lives today. But how did the Internet grow into its ubiquitous existence? For those of you who are not afraid of historical material, you are highly encouraged to read the following interesting online article.

> ***Reading 1.4 (optional)***
>
> http://www.isoc.org/internet/history/brief.shtml

Introduction to Internet services and applications

To the average user, what makes the Internet useful and interesting is not the network, but rather the applications that run on it. The two most common Internet applications in use today are email and Web browsers. However, peer-to-peer sharing and media streaming applications have also become increasingly popular in recent years.

In the following pages, we briefly discuss some of the most important Internet services from an end user's perspective.

Email

Email has been around since the beginning of the Internet and it is still one of the most common Internet services in use today. In fact, email is so widespread that ISPs just assume that you want an email address and automatically assign you one when you begin your service agreement. Traditionally, you run an email client application on your desktop PC to send and receive email messages via your ISP's email server. Increasingly, however, people are using Web-based email (or simply webmail) services such as Gmail, Hotmail, and Yahoo! Mail. By using such services, you can access your email on any PC that has a Web browser installed.

The application protocols that are related to email include **Simple Mail Transfer Protocol** (**SMTP**), **Post Office Protocol version 3** (**POP3**) and **Internet Message Access Protocol version 4 revision 1** (**IMAP4**).

Read the following Wikipedia article for an overview of email.

> ***Reading 1.5***
>
> http://en.wikipedia.org/wiki/E-mail

The World Wide Web

The World Wide Web is a huge collection of interlinked documents, images and other resources, linked by hyperlinks and URLs. These hyperlinks and URLs allow the Web servers that store originals, and cached copies of these resources to deliver them as required using the **HyperText Transfer Protocol** (**HTTP**). Web services also use HTTP to allow software systems to communicate in order to share and exchange business logic and data.

Read the following Wikipedia article for an overview of the World Wide Web.

Reading 1.6

http://en.wikipedia.org/wiki/World_wide_web

Remote access

The Internet allows computers to connect to other computers and retrieve information easily. Through the Internet, applications based on TELNET, Secure Shell (SSH) and Remote Desktop (RDP) allow a computer user to connect to another computer on the other side of the globe in a very cost-effective way. In addition, virtual private networks (VPNs) can be used to set up secure and protected connections for data transmission across the public Internet. We discuss VPNs in more detail in *Unit 8*.

Instant messaging and Internet telephony

Instant messaging applications such as ICQ, MSN Messenger, and AOL Messenger have become extremely popular in recent years. You have probably used one of them yourself — in fact, you probably use one daily! In many situations, instant messaging has replaced long distance telephone calls as a cost-effective means for communication between people in geographically-remote locations. In addition to voice communication, instant messaging applications also support video calls for PCs equipped with webcams.

In situations in which one of the communicating parties must use a telephone, Internet telephony applications such as Skype can be used. A computer user can use a PC equipped with a microphone to call any telephone in the world; the cost is minimal compared with traditional long distance telephone calls.

Streaming media

Many existing radio and television broadcasters provide Internet versions of their live and on-demand audio and video streams. In addition, there are a range of pure Internet broadcasters who don't have traditional broadcast licenses. Any Internet-connected device, such as a computer, a personal digital assistant (PDA) or a smart telephone can be used to access online media in much the same way as was previously possible only with a television or radio receiver.

YouTube, a free video sharing and streaming service provider, streams video content in the Flash format. As such, users are able to watch YouTube videos on any PC equipped with a Flash-enabled web browser. As of January 2008, YouTube hosted over 65,000,000 videos.

Collaboration and social software

A wiki is software application that allows users to create, edit and link webpages easily. Wikis are often used to create collaborative websites and to power community websites. They are also sometimes installed by businesses to provide affordable and effective Intranets and to encourage Knowledge Management. One of the best known wikis is Wikipedia, which we have referred to already in this course material.

A blog, short for 'Web log', is a website where entries are commonly displayed in reverse chronological order. Many blogs provide commentary or news on a particular subject, while others are used as personal online diaries. The most well-known blogs include Slashdot, BlogSpot and LiveJournal. In January 2008, the blog search engine Technorati was tracking over 112 million blogs.

File sharing

Traditionally, file sharing is the sharing of files on a website or an FTP (i.e. file transfer protocol) server for easy download by others. In the recent years, however, file sharing has moved over swiftly to the peer-to-peer (P2P) model, in which shared files are both stored on and served by users' own computers. Most people who engage in file sharing on the Internet therefore both provide (upload) and receive (download) files.

The first P2P file sharing system used on a large scale was Napster, which used a centralized file list. Newer P2P file sharing systems such as BitTorrent and eMule use decentralized file indices.

Reading 1.7 (optional)

http://en.wikipedia.org/wiki/BitTorrent_%28protocol%29

You should now work through your first Lab activity. These opportunities for practical work are included in your Lab Book, which you should have received with your course materials. You should complete the first two sections.

Activity 1.5

Perform *Lab 1.1 Making the most of the Internet I: Webmail, Online Storage and Online Photo Sharing* and *Lab 1.2 Making the most of the Internet II: Blogs, Wikis and Web Hosting* in the Lab Book.

Protocols and standards

Protocols

In computer networks, a protocol is a standard method or format for communication between network devices. Protocols ensure that data are transferred whole, in sequence, and without error from one node on the network to another. The key elements of a protocol are syntax, semantics and synchronization:

- **Syntax** — the structure or format of the data.
- **Semantics** — the meaning of each section of the data.
- **Synchronization** — when data should be sent and how fast they can be sent.

Standards and standards organizations

Standards are documented agreements containing technical specifications or other precise criteria that stipulate how a particular product or service should be designed or performed. Many different industries use standards to ensure that products, processes, and services suit their purposes. Because of the wide variety of hardware and software in use today, standards are especially important in the world of networking. Without standards, it would be very difficult to design a network because you could not be certain that software or hardware from different manufacturers would work together.

The major standards organizations include ISO, IEEE, ANSI and others. The following reading introduces you to some of the more important ones.

> ***Reading***
>
> Dean (2012) 39–42.

IEEE 802: standards for local and metropolitan area networks

IEEE 802 refers to a family of IEEE standards dealing with local area networks and metropolitan area networks. These standards define the Physical and Data Link layers of the OSI model. The most widely used standards are for the Ethernet family, Token Rings and Wireless LANs.

Reading

Dean (2012) 59.

Internet standards

An **Internet standard** is a specification for an innovative internetworking technology or methodology, which the **Internet Engineering Task Force** (**IETF**) ratified as an open standard after the innovation underwent peer review. An Internet standard is a formalized regulation that must be followed.

An Internet standard begins as an **Internet draft**, which is a working document with no official status. After several revisions and upon recommendation from the Internet authorities, a draft may be published as a **Request for Comment** (**RFC**). RFCs that are intended to become Internet standards evolve through three maturation stages: **proposed standard**, **draft standard** and **standard**. Collectively, these stages of evolution are known as the **standards track**.

The following table sets out the RFCs that are related to some of the more important protocols that are of interest to us in this course.

Table 1.2 Networking protocols and related RFCs

Protocol	**Related RFCs**
Domain Name System	1034, 1035
Dynamic Host Configuration Protocol	2131, 3315 (IPv6)
File Transfer Protocol	114, 265, 354, 959, 2228, 4217
HyperText Transfer Protocol	1945 (v1.0), 2616 (v1.1)
Internet Control Message Protocol	792
IPv4	790, 791
IPv6	2460, 3513
Post Office Protocol version 3	1939
Simple Mail Transfer Protocol	2821, 2822
Transmission Control Protocol	793
User Datagram Protocol	768

Summary

In this unit, you studied basic computer networking concepts. This is intended as an introduction to network programming and design and will help you understand various concepts related to networking to be presented in the later units.

In the next unit, you will study the network infrastructure and the elements involved in the actual implementation of a computer network. Topics like transmission basics, transmission media, network topology, network access technologies and networking equipment will be presented in great detail.

Suggested answers to self-tests and activities

Self-test 1.1

1 A computer network is a group of computers, equipment (such as printers) and other communication devices (such as personal digital assistants) that are connected by and can exchange data via some type of transmission media such as a cable, a wire or the atmosphere.

2 The major advantages that networks bring are they:

- enable resource sharing
- enhance communication and collaboration between people
- allow remote and central management of resources and computers
- enable distributed systems.

3 The major network services include:

- file and print services
- communication services
- mail services
- Internet services
- management services.

Self-test 1.2

1 A comparison of peer-to-peer networks and client/server networks:

Peer-to-peer networks	**Client/server networks**
Decentralized management	Centralized management
Not scalable: support only up to 10 or 20 computers	Scalable: support up to thousands of computers
No dedicated servers	Dedicated (and often more powerful) servers
No single point of failure	Single point of failure
Easy to configure and use	Complicated to set up and maintain
Do not require an administrator	Require an administrator
Poor security	High level of security
Lower setup cost	Higher setup cost

2 A comparison of LANs and WANs:

LAN	**WAN**
Usually confined to a relatively small area such as a building	Spans city, regional, national or continental boundaries
High transfer speeds: typically 100 Mbps–1000 Mbps	Low transfer speeds in inexpensive WANs: typically 56 kbps to 1.5 Mbps
Typically uses a WAN connection to access the Internet	Interconnects LANs to form a large network
Ethernet is the prevalent technology	Multiple technologies in use, including PPP, Ethernet, ATM, ISDN, DSL and Frame Relay
Inexpensive and abundant equipment	Expensive equipment

Self-test 1.3

The Presentation layer, because it is responsible for encoding and decoding data.

Self-test 1.4

1 Some differences between the OSI model and the Internet model are:

- The OSI is a seven layer model. The seven layers are the Application layer, Presentation layer, Session layer, Transport layer, Network layer, Data Link layer and Physical layer. The Internet model is simplified into a four-layer model. It comprises a Process/Application layer, Transport layer, Internet layer and Network Access layer.
- The layering structure of the Internet model is not as restrictive as the structure of the OSI model. Applications can access the IP layer directly.
- The Transport layer in the Internet model is dominated by TCP/UDP. However, the Transport layer in the OSI model can use different protocols, e.g. SPX for NetWare systems.

2 The advantages of using the layering models include:

- They clearly structure the functional specifications of each protocol.
- They are able to provide control and error checking on different layers.
- They are suitable for heterogeneous systems' internetworking.

Self-test 1.5

1 The PDU is a unit of data that is specified in a protocol of a given OSI layer and that consists of protocol-control information of the given layer and possibly user data of that layer:

- Layer 1 — bit
- Layer 2 — frame
- Layer 3 — packet
- Layer 4 — segment
- Layer 5 and above — data.

2 Some of the protocols in the Application layer of the TCP/IP model include:

- Dynamic Host Configuration Protocol (DHCP) — A protocol that manages the dynamic distribution of IP addresses on a network. Using DHCP to assign IP addresses can nearly eliminate duplicate-addressing problems.
- Domain Name System (DNS) — A hierarchical way of tracking domain names and their databases. The DNS database is distributed over several key computers (the root servers) across the Internet to prevent catastrophic failure if one or a few computers go down.
- File Transfer Protocol (FTP) — A protocol that sends and receives files via TCP/IP.
- HyperText Transfer Protocol (HTTP) — A protocol that formulates and interprets requests between web clients and servers.
- Post Office Protocol version 3 (POP3) — A protocol that retrieves email from a remote server over a TCP/IP connection. When a client retrieves mail via POP3, messages previously stored on the mail server are downloaded to the client's workstation, and then deleted from the mail server.
- Simple Mail Transfer Protocol (SMTP) — A relatively simple, text-based protocol that moves messages from one email server to another.
- Secure Shell (SSH) — A protocol that allows data to be exchanged over a secure channel between two computers. SSH encrypts data exchanged throughout the communication session.
- Telecommunication Network (TELNET) — A protocol used to connect to network hosts across the Internet or a local area network.

3 Some of the protocols in the Transport layer of the TCP/IP model include:

- Transmission Control Protocol (TCP) — A core protocol of the TCP/IP protocol suite that provides reliable and connection-oriented data delivery services.
- User Datagram Protocol (UDP) — A core protocol of the TCP/IP protocol that provides connectionless transport services.
- Stream Control Transmission Protocol (SCTP) — A new transport layer protocol defined in 2000 that provides reliable, message-connected data delivery services.

4 Some of the protocols in the Network layer of the TCP/IP model include:

- Internet Protocol (IP) — A core protocol of the TCP/IP protocol suite that provides information about how and where data should be delivered. It enables TCP/IP to internetwork.
- Address Resolution Protocol (ARP) — A core protocol of the TCP/IP protocol suite that obtains the MAC (physical) address of a host, and then creates a local database that maps the MAC address to the host's IP (logical) address.

5 Some of the protocols in the Data Link layer of the TCP/IP model include:

- Ethernet — A family of frame-based computer networking technologies for LANs developed by Xerox in the 1970s and improved by Digital Equipment Corporation (DEC), Intel and Xerox. Ethernet is the most common form of network transmission technology in use today. It is standardized as IEEE 802.3.
- IEEE 802.11 — A set of standards for wireless LANs. Popular standards inside the 802.11 family include 802.11b, 802.11g and 802.11n.
- Token Ring — A LAN technology developed by IBM in the 1980s. It relies upon direct links between nodes and a ring topology, using tokens to allow nodes to transmit data. It is standardized as IEEE 802.5.
- Fiber Distributed Data Interface (FDDI) — A networking standard originally specified by ANSI in the mid-1980s and later refined by ISO. FDDI uses a dual fibre-optic ring to transmit data at speeds of 100 Mbps. It was commonly used as a backbone technology in the 1980s and early 1990s, but lost favour as Fast Ethernet technologies emerged in the mid-1990s. FDDI provides excellent reliability and security.

Activity 1.1

Below are some definitions of a computer network from the Internet and from some well-known textbooks on computer networking:

> A computer network is multiple computers connected together using a telecommunication system for the purpose of communicating and sharing resources. (http://en.wikipedia.org/wiki/Computer_network)

> 電腦網路是利用通信設備和線路將地理位置不同的、功能獨立的多個電腦系統連接起來，以功能完善的網路軟體實現網路的資源共享和信息傳遞的系統。簡單的說即連接兩台或多台電腦進行通信的系統。 — Wikipedia (Chinese) — 電腦網路 (retrieved 27 April 2007)

> A computer network is 'a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire; fibre optics, microwaves, infrared, and communication satellites can also be used'. (Tanenbaum 2003, 11)

> A network is a set of devices (often referred to a nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. (Forouzan 2006, 7)

The key characteristics of a computer network therefore include the following points:

- A network comprises multiple devices that are interconnected by some communication media.
- The network devices are capable of communicating with each other in some way.
- The network devices communicate with each other to exchange data or facilitate resource sharing.
- There is no theoretical limit to the physical size of a network.

Activity 1.2

There are many potential uses of the WCG effort. One of these is the long-term weather simulations and forecasts to prevent the worsening of the global warming effect.

A user may not wish to participate in the WCG effort due to the following concerns:

- The client software may negatively affect the performance of the user's computer.
- The client software may itself be some kind of malware.

- The user may not be interested in the particular problems to be solved by the WCG effort.

Activity 1.3

PPTV (http://www.pptv.com) is a peer-to-peer streaming video network created in Huazhong University of Science and Technology, People's Republic of China. It is part of a new generation of P2P applications that combine P2P and Internet TV called 'P2PTV'. Some similar applications include Icecast (http://www.icecast.org), PeerCast, and PPStream (http://www.ppstream.com).

Activity 1.4

If you do a Google search for the words 'how to remember OSI seven layers', you will easily find the most common approach: using *mnemonics*. A very good description of this approach is given at http://www.osi7layer.com:

A mnemonic is a memory aid, designed to make it easier to remember lists of data. A typical technique involves taking the first letter of each word in the list, and creating a sentence based on those letters. This technique is often used to help people remember the order of each layer in the OSI 7-layer model. Sometimes the mnemonic is created from the bottom up, and sometimes from the top down.

The mnemonic traditionally suggested by many IT trainers is:

All People Seem To Need Data Processing (top-down)

Other interesting mnemonics include:

Please Do Not Take Sales People's Advice (bottom-up)

Please Do Not Throw Sausage Pizza Away (bottom-up)

People Design Network To Send Packets Accurately (bottom-up)

You may have found others on the Internet — or have made up one of your own!

Glossary

Address Resolution Protocol — A core protocol in the TCP/IP suite that belongs in the Network layer of the OSI model. ARP obtains the MAC (physical) address of a host, or node, and then creates a local database that maps the MAC address to the host's IP (logical) address.

addressing — The scheme for assigning a unique identifying number to every workstation and device on the network. The type of addressing used on a network depends on its protocols and network operating system.

Application layer — The seventh layer of the OSI model. Application layer protocols enable software programs to negotiate formatting, procedural, security, synchronization and other requirements with the network.

ARP — See *Address Resolution Protocol*.

Asynchronous Transfer Mode — A Data Link layer technology originally conceived in 1983 at Bell Labs, and standardized by the ITU in the mid-1990s. It relies on fixed packets, called cells, that each consist of 48 bytes of data plus a 5-byte header. ATM relies on virtual circuits and establishes a connection before sending data. Having a reliable connection therefore allows network managers to specify QoS levels for certain types of traffic.

ATM — See *Asynchronous Transfer Mode*.

backbone — The part of a network to which segments and significant shared devices (such as routers, switches and servers) connect. A backbone is sometimes referred to as 'a network of networks', because of its role in interconnecting smaller parts of a LAN or WAN.

bus topology — A topology in which a single cable connects all nodes on a network without intervening connectivity devices.

CAN — See *campus area network*.

campus area network — A network made up of an interconnection of local area networks (LANs) within a limited geographical area. A CAN can be considered a form of a metropolitan area network that is specific to an academic setting.

Carrier Sense Multiple Access with Collision Detect (CSMA/CD) — A network access method in which devices that are ready to transmit data first check the channel for a carrier. If no carrier is sensed, a device can transmit. If two devices transmit at once, a collision occurs and each computer backs off and waits a random amount of time before attempting to retransmit. This is the access control method used by Ethernet.

circuit switching — A type of switching in which a connection is established between two network nodes before they begin transmitting

data. Bandwidth is dedicated to this connection and remains available until users terminate the communication between the two nodes.

client — A computer on the network that requests resources or services from another computer on a network. In some cases, a client can also act as a server. The term 'client' can also refer to the user of a client workstation or a client software application installed on the workstation.

client/server network — A networking system in which one or more servers (the server) provide services, such as network management, application and centralized data storage for workstations (the clients).

connection-oriented — A protocol for exchanging data in which a logical connection is established between the end points. After the connection is established, the transmission of data will follow the logical path. The receiving host will send an acknowledgement to the sender to guarantee the correctness of the transmission.

connectionless-oriented — A protocol for exchanging data in an unplanned way and without prior coordination. Data can be transmitted to the receiving end via different paths. The completeness of the data arriving at the receiving end is not guaranteed, however, and upper layer services have to handle the lost data in transmission.

connectivity device — One of several types of specialized devices that allows two or more networks or multiple parts of one network to connect and exchange data.

Data Link layer — The second layer in the OSI model. The Data Link layer bridges the networking media with the Network layer. Its primary function is to divide the data it receives from the Network layer into frames that can then be transmitted by the Physical layer.

data packet — A discrete unit of information sent from one node on a network to another. Breaking a large stream of data into many packets allows a network to deliver that data more efficiently and reliably.

DHCP — See *Dynamic Host Configuration Protocol*.

DNS — See *Domain Name System*.

domain name — The symbolic name that identifies a domain. Usually, a domain name is associated with a company or other type of organization, such as a university or military unit.

Domain Name System (or Domain Name Service) — A hierarchical way of tracking domain names and their addresses, devised in the mid-1980s. The DNS database does not rely on one file or even one server, but rather is distributed over several key computers across the Internet to prevent catastrophic failure if one or a few computers go down. DNS is a TCP/IP service that belongs to the Application layer of the OSI model.

Dynamic Host Configuration Protocol — An Application layer protocol in the TCP/IP suite that manages the dynamic distribution of IP addresses on a network. Using DHCP to assign IP addresses can nearly eliminate duplicate-addressing problems.

Ethernet — A network protocol invented by the Xerox Corporation and developed jointly by Xerox, Intel and the Digital Equipment Corporation. Ethernet networks use **CSMA/CD** and run over a variety of cable types at 10 Mbps up to 1000 Mbps.

FDDI — See *Fiber Distributed Data Interface*.

Fiber Distributed Data Interface — A networking standard originally specified by ANSI in the mid-1980s and later refined by ISO. FDDI uses a dual fibre-optic ring to transmit data at speeds of 100 Mbps. It was commonly used as a backbone technology in the 1980s and early 1990s, but lost favour as Fast Ethernet technologies emerged in the mid-1990s. FDDI provides excellent reliability and security.

file server — A specialized server that enables clients to share applications and data across the network.

file service — The functions of a file server that allow users to share data files, applications and storage areas.

File Transfer Protocol — An Application layer protocol used to send and receive files via TCP/IP.

FTP — See *File Transfer Protocol*.

host — A computer that enables resource sharing by other computers on the same network.

host name — A symbolic name that describes a TCP/IP device.

HTTP — See *HyperText Transfer Protocol*.

hybrid topology — A physical topology that combines characteristics of more than one simple physical topology.

HyperText Transfer Protocol — An Application layer protocol that formulates and interprets requests between Web clients and servers.

ICANN — See *Internet Corporation for Assigned Names and Numbers*.

IEEE — See *Institute of Electrical and Electronics Engineers*.

IEEE 802.11 — The family of IEEE standards dealing with local area networks and metropolitan area networks.

IEEE 802.11 — The IEEE standard for wireless networking.

IEEE 802.11b — The IEEE standard for a wireless networking technique that uses DSSS (direct sequence spread spectrum) signalling in the 2.4–2.4835-GHz frequency range (also called the 2.4-GHz band). 802.11b separates the 2.4-GHz band into 14 overlapping 22-MHz channels and provides a theoretical maximum of 11-Mbps throughput. 802.11b is also known as 'Wi-Fi'.

IEEE 802.11g — The IEEE standard for a wireless networking technique designed to be compatible with 802.11b, while using different encoding techniques that allow it to reach a theoretical maximum capacity of 54 Mbps. 802.11g, like 802.11b, uses the 2.4-GHz frequency band.

IEEE 802.3 — The IEEE standard for Ethernet networking devices and data handling.

IEEE 802.5 — The IEEE standard for Token Ring networking devices and data handling.

IETF — See *Internet Engineering Task Force*.

IMAP/IMAP4 — See *Internet Message Access Protocol*.

Institute of Electrical and Electronics Engineers — An international society composed of engineering professionals. Its goals are to promote development and education in the electrical engineering and computer science fields.

International Organization for Standardization — A collection of standards organizations representing 146 countries with headquarters located in Geneva, Switzerland. Its goal is to establish international technological standards to facilitate the global exchange of information and barrier-free trade.

International Telecommunication Union — A United Nations agency that regulates international telecommunications and provides developing countries with technical expertise and equipment to advance their technological bases.

Internet — A global 'network of networks' used to exchange information using the Transmission Control Protocol over Internet Protocol (TCP/IP) protocol. It allows for electronic mail and the accessing and retrieval of information from remote sources.

Internet Corporation for Assigned Names and Numbers — The non-profit corporation currently designated by the US government to maintain and assign IP addresses.

Internet Engineering Task Force — An organization that sets standards for how systems communicate over the Internet (for example, how protocols operate and interact).

Internet Message Access Protocol — A mail retrieval protocol that improves on the shortcomings of POP. The single biggest advantage IMAP4 has relative to POP is that it allows users to store messages on a mail server, rather than always having to download them to a local machine. The most current version of IMAP is version 4 (IMAP4).

Internet Protocol — A core protocol in the TCP/IP suite that operates in the Network layer of the OSI model and that provides information about how and where data should be delivered. IP is the subprotocol that enables TCP/IP to internetwork.

Internet service provider — A business that provides organizations and individuals with Internet access and often other services such as email and Web hosting.

Internet services — The services that enable a network to communicate with the Internet, including World Wide Web servers and browsers, file transfer capabilities, Internet addressing schemes, security filters, and a means for directly logging on to other computers.

IP — See *Internet Protocol*.

IPv4 — The current standard for IP addressing that specifies 32-bit addresses composed of four octets.

IPv6 — A newer standard for IP addressing that will replace the current IPv4 (IP version 4). Most notably, IPv6 uses a newer, more efficient header in its packets and allows for 128-bit source and destination IP addresses. The use of longer addresses will allow for many more IP addresses to be in circulation.

ISO — See *International Organization for Standardization*.

ISP — See *Internet Service Provider*.

ITU — See *International Telecommunication Union*.

LAN — See *local area network*.

Linux — A freely-distributable implementation of a UNIX-type of system. Originally developed by Finnish computer scientist Linus Torvalds.

local area network — A network of computers and other devices that is confined to a relatively small space, such as one building or even one office.

logical topology — A characteristic of network transmission that reflects the way in which data is transmitted between nodes (which may differ from the physical layout of the paths that data takes). The most common logical topologies are bus and ring.

MAC address — A 12-character string that uniquely identifies a network node. The manufacturer hardcodes the MAC address into the NIC. This address is composed of the Block ID and Device ID.

Mac OS X Server — A proprietary network operating system from Apple Computer that is based on a version of UNIX.

mail server — A server that manages the storage and transfer of email messages.

mail service — The network services that manage the storage and transfer of email between users on a network. In addition to sending, receiving, and storing mail, mail services can include filtering, routing, notification, scheduling and data exchange with other mail servers.

MAN — See *metropolitan area network*.

management service — The network services that centrally administer and simplify complicated management tasks on a network. Examples of management services include license tracking, security auditing, asset management, address management, software distribution, traffic monitoring, load balancing and hardware diagnosis.

message switching — A type of switching in which a connection is established between two devices in the connection path; one device transfers data to the second device, then breaks the connection. The information is stored and forwarded from the second device after a connection between that device and a third device on the path is established.

mesh topology — A network layout in which each node is connected to the two nearest nodes so that the entire network forms a circle. Data is transmitted unidirectionally around the ring. Each workstation accepts and responds to packets addressed to it, then forwards the other packets to the next workstation in the ring.

metropolitan area network — A network that is larger than a LAN, typically connecting clients and servers from multiple buildings, but within a limited geographic area. For example, a MAN could connect multiple city government buildings around a city's centre.

network — A group of computers and other devices (such as printers) that are connected by and can exchange data via some type of transmission media, such as a cable, a wire or the atmosphere.

network adapters — See *network interface card*.

network interface card (NIC) — The device that enables a workstation to connect to the network and communicate with other computers. NICs are manufactured by several different companies and come with a variety of specifications that are tailored to the workstation's and the network's requirements. NICs are also called 'network adapters'.

Network layer — The third layer in the OSI model. Protocols in the Network layer translate network addresses into their physical counterparts and decide how to route data from the sender to the receiver.

network operating system (NOS) — An operating system designed to pass information and communicate between more than one computer. Examples include Windows Server 2003, Linux, Solaris and Novell NetWare/OES.

network services — The functions provided by a network.

node — A computer or other device connected to a network, which has a unique address and is capable of sending or receiving data.

OSI (Open Systems Interconnection) model — A model for understanding and developing computer-to-computer communication developed in the 1980s by ISO. It divides networking functions among seven layers: Physical, Data Link, Network, Transport, Session, Presentation and Application.

packet switching — A type of switching in which data is broken into packets before it is transported. In packet switching, packets can travel any path on the network to their destination, because each packet contains a destination address and sequencing information.

PAN — See *personal area network*.

PDU — See *protocol data unit*.

peer-to-peer network — A network in which resources and files are shared without a centralized management source.

personal area network — A small (usually home) network composed of personal communications devices.

Physical layer — The lowest, or first, layer of the OSI model. Protocols in the Physical layer generate and detect voltage so as to transmit and receive signals carrying data over a network medium. These protocols also set the data transmission rate and monitor data error rates, but do not provide error correction.

physical topology — The physical layout of a network. A physical topology depicts a network in broad scope; it does not specify devices, connectivity methods, or addresses on the network. Physical topologies are categorized into three fundamental geometric shapes, i.e. bus, ring and star. These shapes can be mixed to create hybrid topologies.

POP/POP3 — See *Post Office Protocol*.

Post Office Protocol — An Application layer protocol used to retrieve messages from a mail server. When a client retrieves mail via POP, messages previously stored on the mail server are downloaded to the client's workstation, and then deleted from the mail server. The latest and most common version is version 3 (POP3).

Presentation layer — The sixth layer of the OSI model. Protocols in the Presentation layer translate between the application and the network. Here, data are formatted in a schema that the network can understand, with the format varying according to the type of network used. The Presentation layer also manages data encryption and decryption, such as the scrambling of system passwords.

print server — A server that manages printers and print jobs.

print services — The network service that allows printers to be shared by several users on a network.

protocol — A standard method or format for communication between network devices. Protocols ensure that data are transferred whole, in sequence, and without error from one node on the network to another.

protocol data unit — A unit of data at any layer of the OSI model.

remote access — A method for connecting and logging on to a LAN from a workstation that is remote, or not physically connected, to the LAN itself. Remote access can be accomplished by one of many ways, including dial-up connections, terminal services, remote control or Web portals.

remote access server — A server that runs communications services that enable remote users to log on to a network. Also known as a communications server or access server.

remote control — A remote access method in which the remote user dials into a workstation that is directly attached to a LAN. Software running on both the remote user's computer and the LAN computer allows the remote user to 'take over' the LAN workstation. Only keystrokes, mouse clicks, and screen updates are exchanged between the two computers.

resources — The devices, data, and data storage space provided by a computer, whether standalone or shared.

ring topology — A network layout in which each node is connected to the two nearest nodes so that the entire network forms a circle. Data is transmitted unidirectionally around the ring. Each workstation accepts and responds to packets addressed to it, then forwards the other packets to the next workstation in the ring.

Secure Shell — A connection utility that provides authentication and encryption. With SSH, you can securely log on to a host, execute commands on that host and copy files to or from that host. SSH encrypts data exchanged throughout the session.

Session layer — The fifth layer in the OSI model. The Session layer establishes and maintains communication between two nodes on the network. It can be considered the 'traffic cop' for network communications.

segment — A part of a network. Usually, a segment is composed of a group of nodes that share the same communications channel for all their traffic.

server — A computer on the network that manages shared resources and provides services. Servers usually have more processing power, memory and hard disk space than clients. They run network operating software that can manage not only data, but also users, groups, security and applications on the network.

Simple Mail Transfer Protocol — The Application layer TCP/IP subprotocol responsible for moving messages from one email server to another.

SMTP — See *Simple Mail Transfer Protocol*.

Simple Network Management Protocol — An Application layer protocol in the TCP/IP suite used to convey data regarding the status of managed devices on a network.

SNMP — See *Simple Network Management Protocol*.

Solaris — A proprietary implementation of the UNIX operating system by Sun Microsystems.

SSH — See *Secure Shell*.

standalone computer — A computer that uses applications and data only from its local disks, and that is not connected to a network.

standard — A documented agreement containing technical specifications or other precise criteria that are used as guidelines to ensure that materials, products, processes and services suit their intended purpose.

star topology — A physical topology in which every node on the network is connected through a central device, such as a hub. Any single physical wire on a star network connects only two devices, so a cabling problem will affect only two nodes. Nodes transmit data to the hub, which then retransmits the data to the rest of the network segment where the destination node can pick it up.

switching — A component of a network's logical topology that manages how packets are filtered and forwarded between nodes on the network.

TCP (Transmission Control Protocol) — A core protocol of the TCP/IP suite. TCP belongs to the Transport layer and provides reliable data delivery services.

TCP/IP (Transmission Control Protocol/Internet Protocol) — A suite of networking protocols that includes TCP, IP, UDP and many others. TCP/IP provides the foundation for data exchange across the Internet.

TCP/IP core protocols — The major subprotocols of the TCP/IP suite, including IP, TCP and UDP.

Telnet — A terminal emulation protocol used to log on to remote hosts using the TCP/IP protocol. Telnet resides in the Application layer of the OSI model.

Token Ring — A networking technology developed by IBM in the 1980s. It relies upon direct links between nodes and a ring topology, using tokens to allow nodes to transmit data.

topology — The physical layout of computers on a network.

Transmission Control Protocol — See *TCP*.

Transmission Control Protocol/Internet Protocol — See *TCP/IP*.

transmission media — The means through which data are transmitted and received. Transmission media may be physical, such as wire or cable, or atmospheric (wireless), such as radio waves.

Transport layer — The fourth layer of the OSI model. In the Transport layer, protocols ensure that data are transferred from point A to point B reliably and without errors. Transport layer services include flow control, acknowledgment, error correction, segmentation, reassembly and sequencing.

UDP (User Datagram Protocol) — A core protocol in the TCP/IP suite that sits in the Transport layer of the OSI model. UDP is a connectionless transport service.

user — A person who uses a computer.

User Datagram Protocol — See *UDP*.

virtual private network — A logically constructed WAN that uses existing public transmission systems. VPNs can be created through the use of software or combined software and hardware solutions. This type of network allows an organization to carve out a private WAN through the Internet that serves only its offices, while keeping the data secure and isolated from other (public) traffic.

VPN — See *virtual private network*.

WAN — See *wide area network*.

Web server — A computer that manages website services, such as supplying a webpage to multiple users on demand.

wide area network — A network that spans a long distance (typically across metropolitan, regional or national boundaries) and that connects two or more LANs. The largest and most well-known example of a WAN is the Internet.

Wi-Fi — See *IEEE 802.11b*.

wireless LAN — A LAN that uses wireless connections for some or all of its transmissions.

wireless personal area network — A small office or home network in which devices such as mobile telephones, PDAs, laptops and computers are connected via wireless transmission.

WLAN — See *wireless LAN*.

WPAN — See *wireless personal area network*.

workstation — A computer that runs a desktop operating system and connects to a network.

References

Forouzan, B A (2006) *Data Communications and Networking*, 4th edn, McGraw-Hill.

Kurose, J and Ross, K W (2008) *Computer Networking, A Top-Down Approach*, 4th edn, Addison Wesley.

Tanenbaum, A S (2003) *Computer Networks*, 4th edn, Prentice Hall.