3 Networks (LAN and WAN)

Chapter Objectives

Current network systems are mainly used as the LAN, which covers a limited local area, and are connected to the WAN, which covers a wide area.

In this chapter you will obtain knowledge required for using networks as you will learn about LAN and WAN, security technologies and various services that can be offered.

① Understanding the characteristics of LAN, connection methods, transmission media, access control methods, etc.

② Understanding the characteristics, mechanisms, and protocols of the Internet, and the services offered on the Internet, etc.

③ Understanding line capacities and traffic design related to network performance, and finding actual performance by calculations.

④ Understanding the types and contents of laws and regulations related to networks.

⑤ Understanding the meaning, types and technologies of network security.

⑥ Understanding the types and characteristics of a number of services provided over networks.

Introduction

The word "downsizing" had been the buzz word for a while in the computer industry. Since the birth of computers, their performance has shown continuous improvement thorough scientific and technological advancements. We have seen a transition from host computers to workstations to personal computers, with the size becoming smaller and smaller while the performance of the computers has improved dramatically. In concert with this transition, data processing has also moved from host-centric processing to distributed processing carried out on the local area network (LAN).

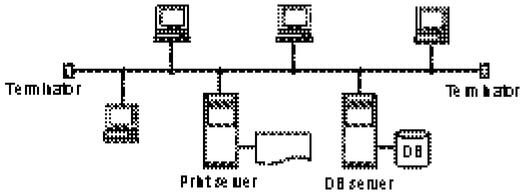
LAN covers a limited area such as within a corporation, and is designed to allow efficient use of system resources by sharing hardware connected by means of transmission media (cables). It is an area that is still accelerating advancements, with recent convergence of client/server systems and the Internet, and high-speed ATM-LAN, etc.

(1) LAN

LAN (Local Area Network) denotes network systems, which do not make use of the facilities (communication lines, etc.) of Type I telecommunications carriers, and cover a limited area (maximum range about 20 km) within factories, hospitals, schools, companies, etc. On a LAN, high-speed (transmission rate of 1 Mbps or higher) transmission media connect multiple computers and office automation equipment.

Figure 3-1-1

LAN example
(Bus-topology)



(2) WAN

WAN (Wide Area Network) denotes network systems that cover a wide area and use the facilities (high-speed digital lines, etc.) of Type I telecommunications carriers. The most significant difference from a LAN is the use of the communication lines of Type I telecommunications carriers (a LAN uses privately installed cables).

Conventionally, the most common WAN has been one in which a host computer is connected to terminals in remote locations. Recently, however, there has been an increase in systems in which a number of LANs connected to WAN to form a large network.

3.1 LAN

3.1.1 Features of LAN

Construction of a LAN has the following benefits.

- Resources, such as files, databases, printers, etc. can be shared.
- Management of otherwise individually managed information can be centralized.
- Highly reliable high-quality communication within a limited area, like on the same office floor, etc., is accomplished with cables (transmission media).
- Equipment expenses are involved but there is no charge for use of lines.
- Owing to the proliferation of groupware for LAN users, the trend toward a paperless office can be accelerated.
- Allows construction of open distributed systems.
- Users can access databases and other processing resources from where they are positioned.
- Using network connection equipment such as routers or gateways, LAN connects to other networks.
- There are few transmission errors compared with WAN that uses communication lines.

Despite the benefits mentioned above, however, LAN requires users to manage:

- The entire network.

3.1.2 Topology of LAN

LAN connection is made based on a topology (shape in which a network is configured). Three typical topologies include:

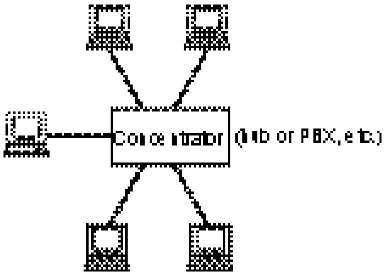
- Star type
- Bus type
- Tree type

(1) Star type

In the star type, multiple terminals are connected to a concentrator (hub or PBX, etc.) in a star-shaped configuration (Figure 3-1-2).

Concentrators are broadly divided into two types according to whether they perform switching or not. Equipment with switching capabilities is called PBX (Private Branch eXchange), and the one especially used with digital lines is called DPBX (Digital Private Branch eXchange). A device with no switching functions is called a hub.

Figure 3-1-2
Star type LAN



The features of star networks are:

- It is easy to add and move terminals connected to the network.
- Depending on the capabilities of the concentrator, there are restrictions on the number of connectible

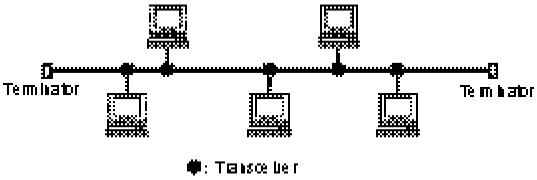
terminals and the transmission distance from the concentrator.

- Even if one terminal fails, this will have no effect on the overall system, but if the concentrator fails, the entire network will go down because data is exchanged by passing through the concentrator.

(2) Bus type

The bus type network is the most basic topology with all terminals connected to one trunk cable (bus).

Figure 3-1-3
Bus type LAN



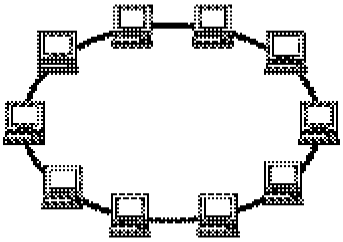
The features of bus networks are:

- This type of network features the simplest type of wiring but if a terminal is moved the bus wiring must be redone.
- There are certain restrictions on the length of the bus and the number of terminals that can be connected.
- Data sent from a terminal flows to all the other terminals enabling "multi-destination transmission" (broadcasting).
- The terminal seizes the received data if the destination address matches the terminal's.
- Unnecessary data may remain in the communication line but such data can be eliminated by "terminators" connected at both ends of the transmission cable.
- Collision may occur if data from multiple terminals is sent simultaneously.

(3) Ring type

The ring network is a configuration in which the terminals are connected in a closed loop.

Figure 3-1-4
Ring type LAN



The features of ring networks are:

- Data sent from a terminal passes around the ring in one direction.
- The terminal seizes received data if the destination address matches the terminal's. Otherwise, it passes the data along to the next terminal.
- Data transmission control (token passing) can be used to determine which terminal is allowed to transmit data to prevent collisions caused by simultaneous data transmission from two or more terminals.
- Establishment of bypass routes is necessary as the entire network goes down if just one terminal fails.

3.1.3 LAN Connection Architecture

LAN systems comprise many types of connection configuration, which can broadly be divided into:

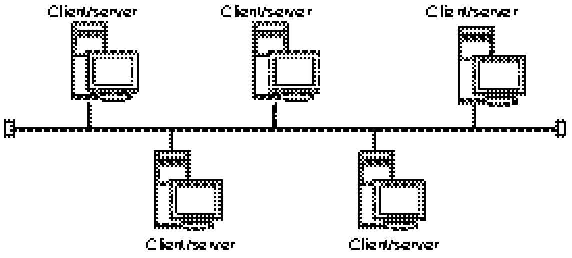
- Peer-to-peer
- Client/server

(1) Peer-to-peer LAN

Peer-to-peer is a simple LAN configuration that requires no dedicated server machine (Figure 3-1-5). Application programs running on personal computers or workstations manage all printers and other system resources, and each machine is considered equal and each acts as a server or client to the others in the network.

This configuration is frequently used in relatively small LAN because peer-to-peer networks are simple and cheap to construct. However, they are not suitable for large-scale systems where heavy data loads have to be processed or advanced computation is required.

Figure 3-1-5
Peer-to-peer LAN



Each machine is considered equal and acts both as a client and server.

(2) Client/server

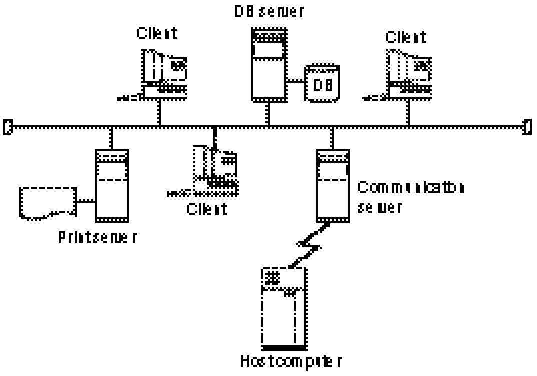
Client/server LAN is a typical computing processing system in which each computer is used for performing its dedicated role, and system resources in the network are allotted for specific roles.

For example, image processing may be performed on a workstation and the host computer may handle daily routine operations that generate a large volume of data. Business involving creation of normal documents or use of spreadsheet software may be done on personal computers.

In other words, this is system in which a number of different software programs running on different hardware and operating systems are linked to execute one application.

Client/server architecture is employed in relatively large-scale LAN systems.

Figure 3-1-6
Client/server LAN



3.1.4 LAN Components

The components that make up a LAN can be divided broadly into:

- Transmission media
- Peripheral equipment

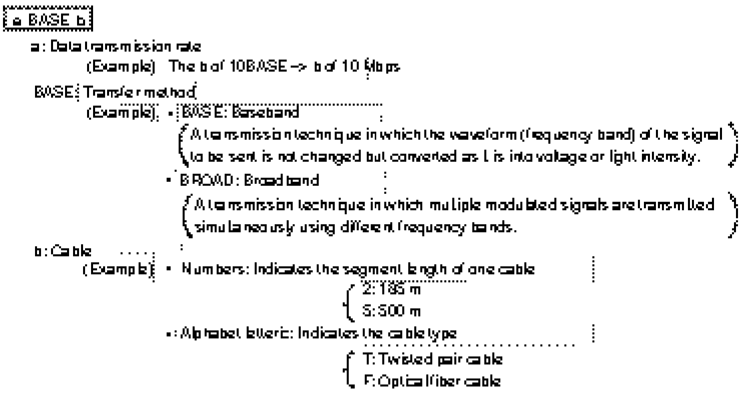
(1) LAN transmission media

The transmission media used in LAN are:

- Twisted pair cables
- Coaxial cables
- Optical fiber cables
- Wireless

The features of those cables are explained in the following, and access control of LAN is explained afterwards.
How to read Standard LAN Codes is laid down by the IEEE as shown in Figure 3-1-7.

Figure 3-1-7 How to read Standard LAN Codes



a BASE b

a : Data transmission rate
(Example) The b of 10BASE –> b of 10 Mbps

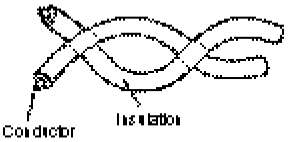
BASE: Transfer method
(Example) • BASE: Baseband
A transmission technique in which the waveform (frequency band) of the signal to be sent is not changed but converted as it is into voltage or light intensity.
• BROAD: Broadband
A transmission technique in which multiple modulated signals are transmitted simultaneously using different frequency bands.

b: Cable
(Example) • Numbers: Indicates the segment length of one cable
2: 185 m
5: 500 m
• : Alphabet letter: Indicates the cable type
T: Twisted pair cable
F: Optical fiber cable

① Twisted pair cable

Twisted pair is a cable widely used for telephone lines (Figure 3-1-8).

Figure 3-1-8
Twisted pair cable



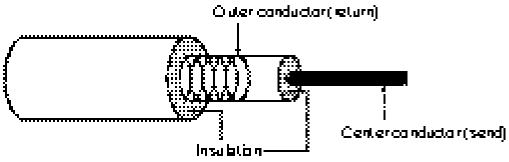
The characteristics of twisted pair cables are as follows:

- Maximum transmission rate: 100 Mbps
- Transmission distance: About several hundred meters
- Noise resistance: Easily affected.
- Price: Cheapest
- Cable installation: Easy
- Appropriate scale for application: Small-scale LAN on a same office floor.
- Access control method: CSMA/CD (10BASE-T is the standard), token-passing method.

② Coaxial cable

Currently, coaxial cable is the most popular cable for use as LAN cables. They are divided into the two types, baseband and broadband according to the different transmission modes.

Figure 3-1-9
Coaxial cable



The characteristics of coaxial cables are as follows:

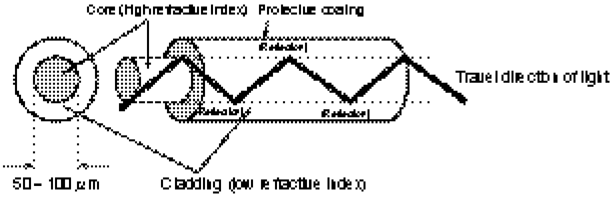
- Maximum transmission rate: Several Mbps to several hundred Mbps
- Transmission distance: 185 m to tens of kilometers (1 segment)
- Noise resistance: Relatively resistant
- Price: Somewhat expensive compared with twisted pair cable
- Cable installation: Requires time and effort compared with twisted pair cable
- LAN scale appropriate for application: Relatively large-scale LAN
- Access control method: CSMA/CD (10BASE5 or 10BASE2. 10BASE5 is the standard cable for Ethernet, cable length is 500 m. The 10BASE2 cable length is 185 m)

<Ethernet>
Ethernet is a LAN standard employing the CSMA/CD protocol that was invented by Dr. Robert Metcalf of Xerox Palo Alto Research Center in 1973 and later standardized by the IEEE. It enables transmission at a maximum speed of 10 Mbps.

③ Optical fiber cable

Optical fibers are cables constructed from materials of which quartz glass is the principal constituent that allow high-speed transmission. This transmission media will most likely become more and more used in the coming multimedia era as this type of cable enables transmission of large amounts of data.

Figure 3-1-10
Structure of optical fiber


Core (High refractive index)
Protective coating
Reflection
Reflection
Reflection
Travel direction of light
50 – 100 μm
Cladding (low refractive index)

An optical fiber cable consists of several of the above optical fibers bundled together.
The characteristics of optical fiber cables are as follows:

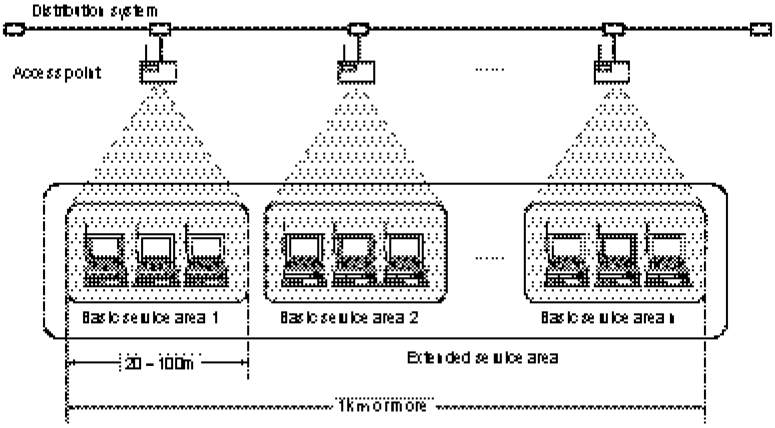
- Maximum transmission rate: Several hundred Mbps
- Transmission distance: Up to about 100 km (low-loss characteristic makes long-distance transmission possible)
- Noise resistance: Exceptionally resistant
- Price: About the same as coaxial cables
- Cable installation: Installation is easy but technicians must undergo technical training since this is a relatively recent invention.
- Appropriate scale for application: High-speed LAN systems such as FDDI (explained later) and ATM-LAN (explained later).
- The media itself is lightweight, compact and very easy to handle.
- Light (signal) can only be transmitted in one-way direction.
- The cost of peripheral equipment is high.

④ Wireless

Because cables must be installed for the construction of a LAN, the system layout must necessarily be decided in advance, and thus makes it difficult to change the layout later. In this respect, wireless systems have the advantage that wiring is not necessary as they use radio waves or infrared rays (Figure 3-1-11). This makes it easy to move the equipment and LAN systems can be designed more freely. However, it has to be taken into consideration that wireless systems are susceptible to noise compared with cable-based systems.

Low-speed wireless LAN (48 kbps/32 kbps) was standardized a while ago but the transmission speed was rather low compared to cable-connected LAN systems. Improvements were made afterwards, and medium-speed wireless LANs (1 Mbps/2 Mbps) and 10 Mbps or more high-speed wireless LANs have now been standardized.

Figure 3-1-11 Outline of wireless LAN



(2) Peripheral equipment for LAN

In addition to cables, various hardware (equipment) and connectors are necessary for construction of a LAN as shown below.

① Terminator

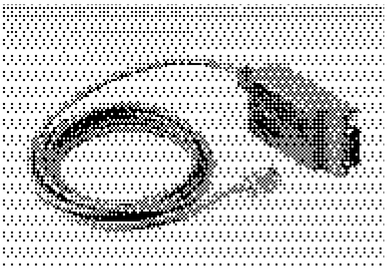
In a bus type LAN, unnecessary data not seized by terminals will remain in the transmission line and it is therefore necessary to connect a "terminator," which removes unnecessary data, at each end of the transmission cable.

② Transceiver

A "transceiver" is a device that connects the trunk cable and the node from the terminal and it also has the function of detecting data collisions (Figure 3-1-12).

- For construction of a 10BASE5 LAN
  Transceiver is attached to cable and connected.
- For construction with 10BASE-T and 10BASE2
  A transceiver is already incorporated in the LAN adapter port, and in 10BASE2 it is connected by means of a connector.

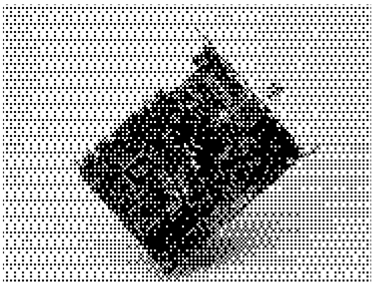
Figure 3-1-12
Transceiver and connector



③ LAN adapter

A LAN adapter is an interface device for connecting the computer to the LAN. It is also called a LAN card.

Figure 3-1-13
LAN adapter



3.1.5 LAN Access Control Methods

A LAN system connects multiple terminals on one cable, and if the terminals transmit data at their own discretion, data collisions and other problems will occur frequently and inhibit correct transmission of data. Consequently, access control is one of the most important basic LAN technologies.

In the OSI basic reference model, LAN access control methods are defined by the MAC (Media Access Control) layer in the lower half of the 2nd layer (data link layer).

LAN access control methods are broadly divided into the following two types.

- Deterministic access (TDMA)
  Deterministic access control is a method in which the transmission rights are allocated to terminals in advance. The terminals can send data in the allocated order, but a terminal will have to wait until it becomes its turn even if it wants to send something immediately.
- Nondeterministic access (CSMA/CD, token-passing)
  Nondeterministic access is a method in which transmission right control is carried out at the point of time when a transmission request is issued. This method works well when transmission rights can be obtained with good timing, but sometimes conflicts with other terminals occur, meaning that obtainment of transmission right is not always guaranteed.

The following three access controls are typically found in LAN systems, and are explained below.

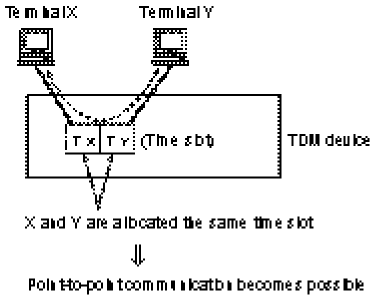
- TDMA
- CSMA/CD
- Token passing

(1) TDMA (Time Division Multiple Access)

TDMA (Time Division Multiple Access) controls access by dividing the data channel into specific time divisions and allocating units (called time slots) of these divisions to each terminal. It is a technique that applies the principles of time-division multiplexing (TDM).

Fundamentally, the technique allows point-to-point communication when data has to be transmitted from terminal X to terminal Y provided that these are given the same time slot.

Figure 3-1-14
TDMA


Terminal X
Terminal Y
T x
T y
(Time slot)
TDM device
X and Y are allocated the same time slot
⇓
Point-to-point communication becomes possible

The features of TDMA are:

- Data collision does not occur as in the CSAM/CD method, enabling reliable data transmission.
- Waste is large as time slots are also allocated to terminals that have no request for transmitting.

(2) CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

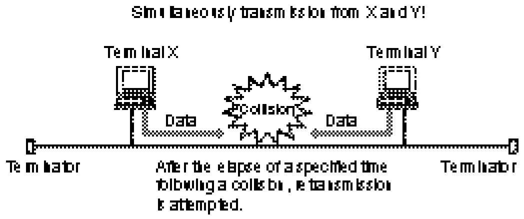
The CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is an access control method mainly used in bus topology LAN. 10BASE-T, which is designed around the CSMA/CD standard, physically looks like a star topology but logically it is bus topology.

The mechanisms of the CSMA/CD are as follows:

- All the terminals need to monitor whether data is passing on the cable.
- Transmission starts when no data is passed, and pauses for standby when data is passed.

- If several terminals transmit data simultaneously, data will collide on the bus. If a collision is detected, all terminals will have to wait a specified time (this time interval is calculated using backoff algorithms) before attempting retransmission.

Figure 3-1-15
CSMA/CD


Simultaneously transmission from X and Y!
Terminal X
Terminal Y
Collision
Data
Data
Terminator
Terminator
After the elapse of a specified time following a collision, retransmission is attempted.

A disadvantage in this method is that the frequency of data collisions will increase as the amounts of transmitted data increase, and thus can rapidly degrade the transmission efficiency.

The transmission speed of LAN (Ethernet, etc.) employing the CSMA/CD method is 10 Mbps. Recently, the so-called Fast Ethernet with a speed of 100 Mbps has been introduced.

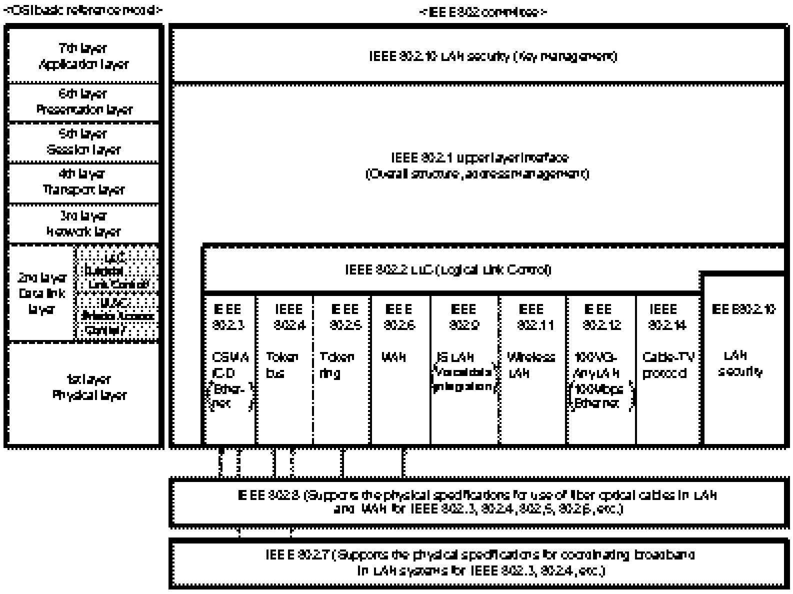
The CSMA/CD method is standardized as IEEE 802.3, and cable shapes, data transmission speed, transmission method, media access control (MAC), etc. have all been standardized. This standardization corresponds to the physical and data-link layers of the OSI basic reference model. However, the data-link layer of the OSI basic reference model has been divided into the following two sublayers, due to standardization factors.

- LLC (Logical Link Control): Controls the procedure for exchange of data.
- MAC (Media Access Control): Controls the access method of LAN.

<IEEE 802 Committee>

The IEEE 802 Committee was set up by the IEEE (Institute of Electrical and Electronics Engineers) in February 1980, and is an organ for promotion of standardization of LAN and MAN (Metropolitan Area Network) (Figure 3-1-16).

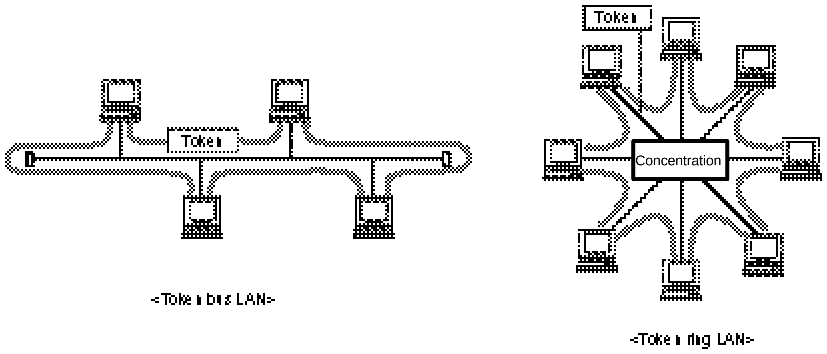
Figure 3-1-16 The relations between the IEEE 802 committee and the OSI basic reference model


<OSI basic reference model>
<IEEE 802 committee>
7th layer Application layer
6th layer Presentation layer
5th layer Session layer
4th layer Transport layer
3rd layer Network layer
2nd layer Data link layer
LLC (Logical Link Control)
MAC (Media Access Control)
1st layer Physical layer
IEEE 802.10 LAN security (Key management)
IEEE 802.1 upper layer interface (Overall structure, address management)
IEEE 802.2 LLC (Logical Link Control)
IEEE 802.3 CSMA /CD (Ethernet)
IEEE 802.4 Token bus
IEEE 802.5 Token ring
IEEE 802.6 MAN
IEEE 802.9 IS LAN (Voice/data integration)
IEEE 802.11 Wireless LAN
IEEE 802.12 100VG-AnyLAN (100Mbps Ethernet)
IEEE 802.14 Cable-TV protocol
IEEE 802.10 LAN security
IEEE 802.8 (Supports the physical specifications for use of fiber optical cables in LAN and MAN for IEEE 802.3, 802.4, 802.5, 802.6, etc.)
IEEE 802.7 (Supports the physical specifications for coordinating broadband in LAN systems for IEEE 802.3, 802.4, etc.)

(3) Token passing

Token passing method is an access control technique mainly used in ring topology LAN. Generally, the network is labeled token ring if it is of the ring-shape network, and if the same access control is used on a bus topology network, it is called "token bus."

Figure 3-1-17 Token bus LAN and token ring LAN

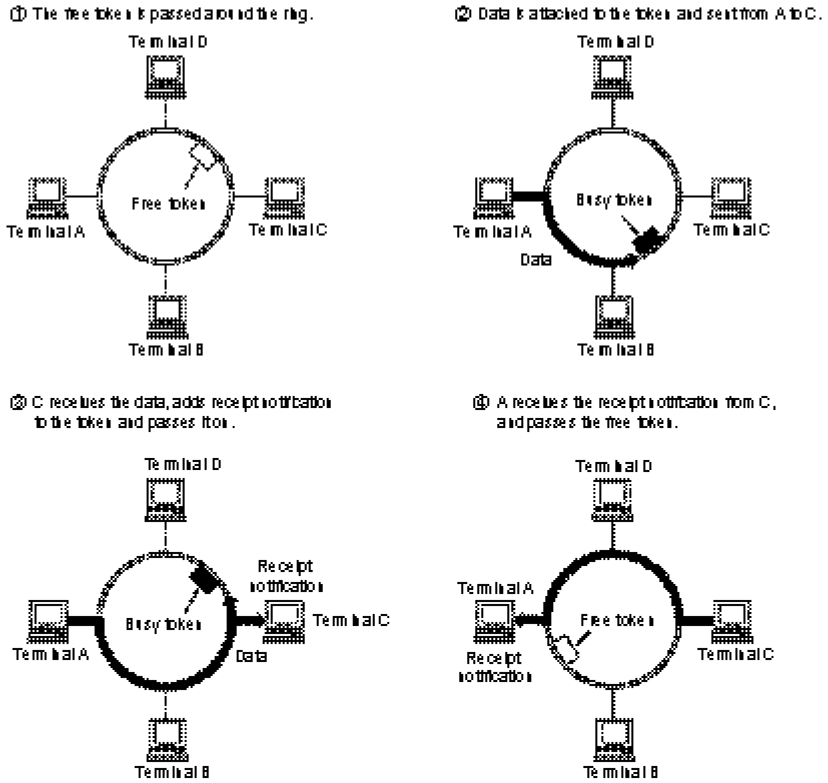


The mechanism of the token passing is as follows.

- A signal (token) carrying the right to transmit on the cable is passed around the network. Only one token is passed around. And the token carrying no data is called "free token," and the token carrying data is called "busy token."
- If a terminal that wants to transmit is not capable of seizing the token, it will not be able to transmit. Only the station that seizes the "free" token can transmit.
- The terminal that seizes the "free" token turns this into the "busy" token, and sends this together with the data to the destination terminal.
- When the terminal receives the "busy" token, it returns the "busy" token together with data for receipt notification to the original sender.
- When the sender receives the "busy" token, it changes it into the "free" token and passes it back on the cable, and discard the data notifying completion of transfer.

Figure 3-1-18 shows the access control procedure of the token ring method.

Figure 3-1-18 Token ring



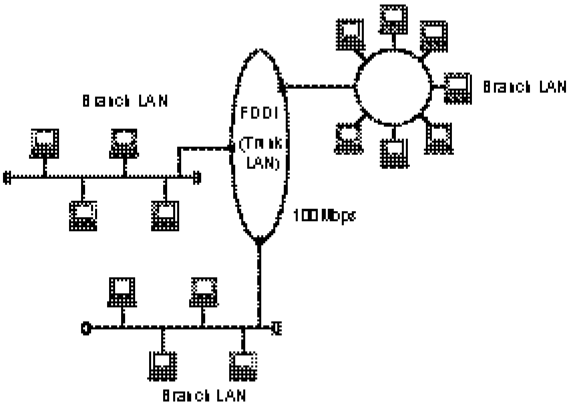
The token bus method is physically a bus topology, but logically it is a ring topology. Physically, a token ring LAN has a star topology but logically it performs a ring topology mechanism. In this way it is more appropriate to think of LAN topology in logical rather than physically terms.

The transmission speeds of LAN (such as token ring, etc.) employing the token passing method are 4 Mbps (priority token) and 16 Mbps (early token release).

The token bus is standardized by IEEE 802.4. The token ring is standardized by IEEE 802.5.

Token passing also used in the FDDI (Fiber Distributed Data Interface) that extends the access control of the token ring to the larger networks. FDDI is mainly employed in backbone LAN connecting other networks. It employs optical fiber cables and features a transmission speed of 100 Mbps. FDDI further includes the FDDI-I that corresponds to packet switching for data transmission and FDDI-II that also allows transmission of voice and video. However, due to the rapid progress made in ATM-LAN technology (explained later) there is not much interest in FDDI-II at the moment.

Figure 3-1-19
FDDI



3.1.6 Inter-LAN Connection Equipment

There is a limit to the size of one LAN and it cannot be unreasonably expanded. The need for connecting two or more LAN systems may therefore arise. By connecting multiple LAN, business operations' efficiency may be increased further and more system resources will be available for sharing.

The following explains four representative examples of LAN connection equipment for connecting multiple LANs:

- Repeater
- Bridge
- Router
- Gateway

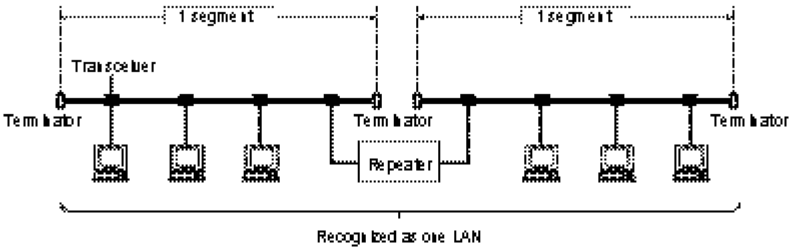
When studying LAN connection equipment, the OSI basic reference model will be referred to frequently, so please be sure to refer also to Section 1.2 OSI – Standardization of Communication Protocols.

(1) Repeater

A repeater is a device that performs relay functions on the physical layer, the first layer of the 7-layer OSI basic reference model. This is simply a piece of connection equipment that extends the transmission range of the LAN, and the same access control methods must be employed in both LAN systems. Accordingly, LAN systems connected by a repeater can logically be regarded as one LAN.

Recently, the favored transmission media for use in LAN has changed from conventional coaxial cables to twisted-pair cables that make LAN construction easier and also allow the use of cascade connections of hubs instead of using a repeater.

Figure 3-1-20 Repeater



(2) Bridge

A bridge is a device that performs relay functions on the data-link layer, the second layer of the 7-layer OSI basic reference model. When connecting, it is of no importance whether or not the physical layers (transmission media) differ. Some bridges can also perform the relay functions even if the LAN systems use different access control methods.

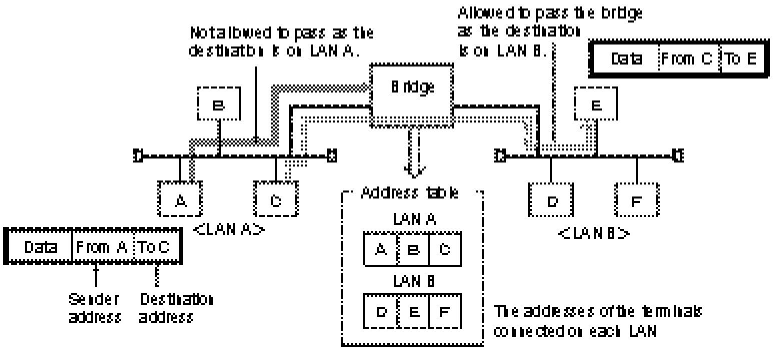
Bridge types comprise:

- Local bridges for direct connection of LAN systems
- Remote bridges for connection of LAN systems via communication lines (leased lines)

The decisive difference between a repeater and a bridge is that the repeater only recognizes coming data as electrical signals (bit strings) whereas the bridge recognizes it as one piece of data (packet).

As Figure 3-1-21 shows, the basic role of the bridge is to determine, by means of the addresses (MAC address) contained in the data traveling on the LAN, whether or not the data should be passed to another LAN system.

Figure 3-1-21 Basic bridge functionalities


Not allowed to pass as the destination is on LAN A.
Allowed to pass the bridge as the destination is on LAN B.
Data
From C
To E
Bridge
B
E
A
C
D
F
<LAN A>
<LAN B>
Address table
LAN A
A
B
C
LAN B
D
E
F
The addresses of the terminals connected on each LAN
Data
From A
To C
Sender address
Destination address

Note: The address is the MAC address (6 octets)

The bridge identifies the data flowing on the LAN and memorizes them in the address table inside the bridge. When data arrives at the bridge, it references the address table and the MAC address of the data. If the sender terminal and the receiver terminal of the data are located within the same LAN, the data is not allowed through the bridge but is passed directly to the destination terminal. If the sender terminal and the receiver terminal are located within different LAN systems, the terminal connects the two LAN systems and then let the data pass through.

Even if the transmission media is the same, in case the data loads are large, a bridge may be used instead of a repeater in order to reduce the traffic load on the LAN. Recently, so-called "switching hubs" that employ switching technology and have higher performance than bridges are frequently employed.

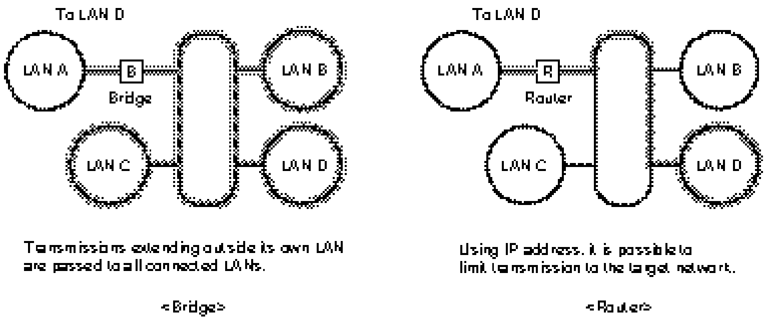
When several LAN systems are connected in parallel by means of multiple bridges, the network structure may become a loop. If broadcast address packets are sent under these circumstances, the packets will continue to circulate on the network. To prevent this situation, a representative bridge is selected to make the network a tree structure. The method to prevent packets traveling in loops and multiplying is called "spanning tree."

(3) Router

A router is a device that performs relay functions on the network layer, the third layer of the 7-layer OSI basic reference model. Interconnection between different networks becomes possible (even if transmission media and access control differ) because the linking function is performed on the network layer. Some routers (called "brouters") of bridges, and those complying with multiple protocols are called "multiprotocol routers."

When sending data from the sender terminal to a terminal on another LAN integrate the role connected by bridges, the data is passed to all the LANs connected, but a router only passes the data to the specified party (LAN). This is called "routing." When data has to be transmitted to a different LAN (network), the router identifies the address (IP address) of the data, and select the route along which the data will travel. This mechanism prevents the data to travel through other LANs (networks), because the data will arrive at the LAN (network) of the receiver along the route specified by the routing. Accordingly, employing routing can greatly reduce the traffic load on the network and also facilitates safeguarding of security.

Figure 3-1-22 Differences between bridges and routers

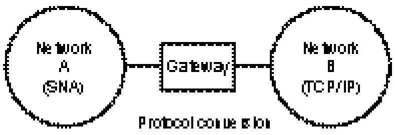

To LAN D
LAN A
B
Bridge
LAN B
LAN C
LAN D
Transmissions extending outside its own LAN are passed to all connected LANs.
<Bridge>
To LAN D
LAN A
R
Router
LAN B
LAN C
LAN D
Using IP address, it is possible to limit transmission to the target network.
<Router>

Many multiprotocol routers are normally equipped with PPP.

(4) Gateway

A gateway is a device for connecting networks in which the protocols of the 7-layer OSI basic reference model differ overall. Gateways are used, for example, to establish interconnection between an OSI network and a TCP/IP network. Gateways are also used to obtain interconnection between a network constructed with vendor-inherent protocols and a network constructed with the OSI system.

Figure 3-1-23
Gateway



3.1.7 LAN Speed-up Technology

These days, data is no longer limited to documents. Transmission and reception of data with large data sizes, in the form of images, video and audio, are becoming more and more frequent. To enable the user to send and receive data smoothly, speed-up of LANs and other network systems has become indispensable.

As representative LAN speed-up, the following technologies are introduced:

- 100BASE-T
- 100VG-AnyLAN
- Gigabit Ethernet
- Switching Hub
- ATM-LAN

(1) From 10BASE-T to 100BASE-T, 100VG-AnyLAN and Gigabit Ethernet

As the 100BASE-T label indicates, this is a LAN standard for transmission of data carrying 100 megabits per second. This standard represents an evolution of the 10BASE-T standard and standardization is promoted by the IEEE 802.3 standard. 100BASE-T is also called "Fast Ethernet" with reference to the conventional 10 megabits Ethernet. The 100BASE-T standard comprises the following types:

- 100BASE-T4 } (both using twisted-pair cable)
- 100BASE-TX }
- 100BASE-FX (using optical fiber cable)

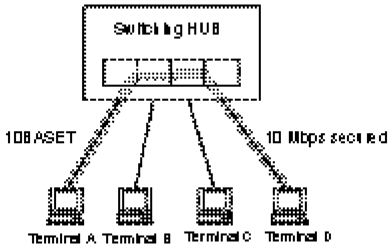
100VG-AnyLAN is another LAN standard that is also attracting attention as a media that allows transmission at the speed of 100 Mbps as the 100BASE-T standard. Standardization of the Gigabit Ethernet that should enable high-speed transmission at 1 Gbps is also progressing.

(2) Switching Hub

A switching hub is a communication device that employs switching technology to accomplish high-speed transmission on LAN (see Figure 3-1-24). There are two types, Ethernet switch and Token ring switch.

Figure 3-1-24

Switching hub



In the Ethernet standard, all the terminals share one cable (media sharing), and if terminals send data at the same time, data collision will occur, meaning that the physical performance will decrease considerably even if the logical transmission speed is 10 Mbps.

However, by using Ethernet switching, the data is switched to the destination terminal as the MAC address of the data is identified inside the switching hub, and this means that use of the cable can be monopolized (media possession). In other words, higher speeds than those obtainable with the conventional Ethernet standard become attainable because the entire 10 Mbps is secured by the switching hub.

(3) ATM-LAN (Asynchronous Transfer Mode-LAN)

ATM-LAN (Asynchronous Transfer Mode-LAN) is attracting much attention as it is seen as a full-fledged multimedia LAN solution.

ATM-LAN uses the ATM technology (see Section 2.3.3 Switching Systems) and enables data transmission at ultra-high speeds. Theoretically, transmission speeds in the class ranging from Mbps to Gbps are possible.

Differing from currently existing LAN, ATM-LAN offers variable transmission speeds and this allows the construction of more flexible network. Since this LAN is extremely fast, there will only be very little time lag when data is transmitted, making it ideal for multimedia communications such as transfer of video.

Furthermore, once the B-ISDN service employing ATM begins, ATM-WAN using both ATM-LAN and B-ISDN will make ultrafast data transmission possible over very wide areas.

3.2 The Internet

Up until only several years ago the Internet was only something used by a limited number of experts, but these days its is used by the young and old regardless of gender to exchange information in the form of e-mail or people surf the Net for searching and gathering information from around the world. Individuals also have homepages and the Net has become a base for transmitting information aimed at the entire world. In these ways, the use of the Internet has grown explosively.

One of the factors behind this is that together with the proliferation of WWW (World Wide Web) and the WWW browsers, it has become possible and easy to search for information without the need for special knowledge. Other factors include the higher performance of computers, not least personal computers, and the increased speeds offered by the lines connecting the Internet.

However, as information technology engineers we will have to turn our eyes from the usefulness of the Internet, and face the many problems that have followed on the heels of the spread of the Internet, such as serious security problems, ethical problems, scarcity of IP addresses, etc.

And it is still indispensable to understand the history of the Internet and the supporting technologies behind it.

The following explains the development of the Internet, security problems and other aspects. Based on this knowledge, the aim is to bring you to a level where you are able to discuss the Internet from the standpoint of an engineer.

3.2.1 The Historical Background of the Development of the Internet

This section traces back the historical developments from the birth of the Internet until today.

(1) The birth of the Internet

The Internet was born as a network developed for military purposes. A network called ARPANET (Advanced Research Projects Agency Network) developed for experiments and research by the US Department of Defense Advance Research Projects Agency (DARPA) in 1969 was the genesis of the Internet. At the time, computer systems were mainly host-centric systems and thought to be vulnerable to missile attacks, as all information could be destroyed by a single attack. ARPANET was therefore constructed as a research project into distributed computer systems.

In the beginning, the transmission speed was slow (56 kbps), and the system was made up of research institutes and universities inside the US connected by a packet network. Later technological progresses enabled the ARPANET to play a central role as a communications network in the following nearly 20 years.

(2) Development of the basic technology

The communications protocol TCP/IP is one of the fundamental technologies that cannot be neglected when you are talking about the development of the Internet. Because DARPA employed TCP/IP as the standard protocol for the ARPANET, TCP/IP since then developed into the standard protocol on the Internet.

LAN technologies, into which much research and development investments were made since the middle of the 1970s, have also contributed greatly to the development of the Internet.

(3) Development of networks (1980s)

In 1983, the part of the ARPANET that was focusing on military purposes was cut away (this was named MILNET (MILitary NETwork), and the remaining was changed into a network for science and research. TCP/IP was adopted as the transmission protocol at the same time.

The US National Science Foundation (NSF) developed and started operating its independent network called NSFNET in 1986.

Later, NSFNET and ARPANET were interconnected to form the prototype of the world's first Internet (NSFNET absorbed the ARPANET in 1990).

In Japan, the three universities University of Tokyo, Tokyo Institute of Technology and Keio University constructed the UUCP (UNIX to UNIX Copy: explained later) connected JUNET (Japanese University NETwork) for academic research. In 1988 this developed into the WIDE project (Widely Integrated Distributed Environment: WIDE) and further research was carried out. Following the JUNET, other networks for academic research and development were constructed, such as the Ministry of Education's academic network SINET (Science Information Network). In this way, the Japanese part of the Internet also has its roots in a variety of prototypes.

(4) The proliferation of the Internet (1990s)

① The birth of commercial networks

As the trend towards distributed networks continued, interest in the Internet further increased, and calls for commercial networks in order for the Internet to break out of the shell of academic and research oriented networks increased. This was the genesis of the concept of "providers" (Internet provider: explained later) that led to the explosive growth of the Internet.

In 1994 the operation of NSFNET was transferred to a private company, further reducing the official streak of the Internet and increasing public influence.

② NII plan

An indispensable element in the development of the Internet is the establishment of an information transmission infrastructure. One of the first to realize the importance of this was the then Vice-president of the United States, Al Gore, who proposed the NII (National Information Infrastructure) plan in 1993. This plan centered on research and development of an ultrafast (Gpbs class) network, and worldwide it was to become the trigger for construction of information transmission infrastructures.

③ Increasingly powerful computers

So far most of the computers connected to the Internet had been UNIX workstations with the TCP/IP protocol as the standard. The reason was that the Internet from the beginning was developed for academic and research purposes, and these institutions tended to select workstations as the computers connected to the Internet because these offered higher performance and capabilities than personal computers.

In recent years, however, personal computers have also supported TCP/IP and have more processing power and become less expensive, leading to today's situation where the general public can easily connect to the Internet using an ordinary personal computer. This has contributed to making the use of the Internet even more common among the general public.

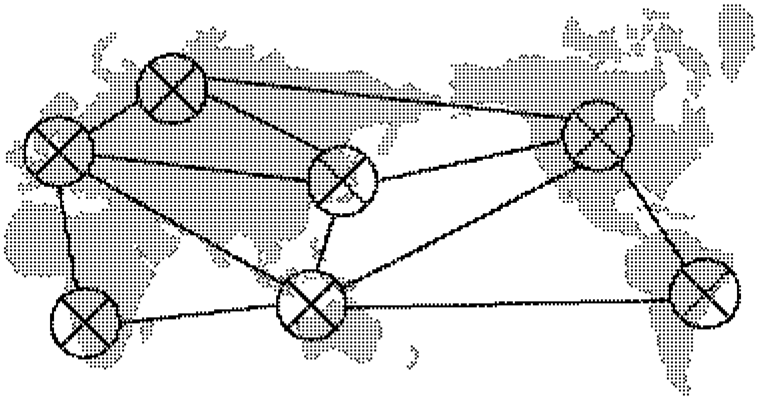
3.2.2 The Structure of the Internet

This section explains the basic structure of the Internet.

(1) A network of networks

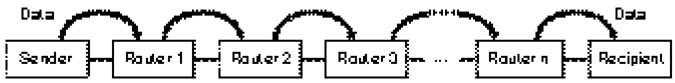
The Internet can be said to be "a network of networks." The Internet is a network on a worldwide scale that is made up of large and small interconnected networks (Figure 3-2-1).

Figure 3-2-1 The Internet = a network of networks



As Figure 3-2-2 shows, the Internet uses the bucket-relay like transmission to transfer data sent from a terminal connected to the Internet to the terminal at the destination via countless routers (relay devices).

Figure 3-2-2 Data transmission on the Internet (bucket relay)



Traveling through routers, data is sent from the sender to the recipient, just like the bucket relay method.

(2) The difference between the Internet and personal computer communication

Network services labeled "personal computer communication" have existed from before the Internet became popular. Personal computer communication networks are run by companies (organizations) that have a host computer and offer various services founded on databases to members (Figure 3-2-3).
Both personal computer communication and the Internet use networks to provided services but basically differ in the following ways.

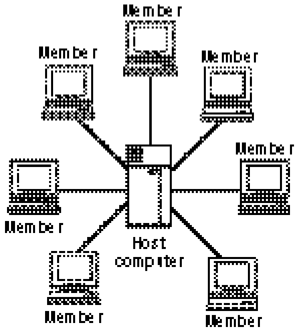
<Internet>

There is no mother organization running the Internet, and anybody can receive services provided that they are connected to the net.

<Personal computer communication>

The company (organization) that owns the host computer manages everything, and service is only available to its members.

Figure 3-2-3
Personal computer communication



In recent years, however, personal computer communication providers have also been providing connection to the Internet making it possible to exchange E-mail between personal computer communication networks and the Internet.

(3) The Internet and TCP/IP

The Internet is interspersed with countless computers of different types and performances, and their manufacturers are also different. In order for any manufacturer's computer to be able to connect to the Internet and receive services, all the computers must employ the same protocol. In other words, anybody can receive services by connecting his/her computer to the Internet provided that the TCP/IP protocol is employed as the communication protocol.

TCP/IP was developed for the ARPANET in 1974 and began being used as a superior network protocol for LAN in the later part of the 1970s. The beginning of the 1980s saw a jump in its proliferation as it was implemented as the protocol in the BSD UNIX (Berkeley Software Distribution UNIX). When the military purpose network was separated from ARPANET in 1983, DARPA replaced the communication protocol with the TCP/IP. The origin of the TCP/IP being the standard protocol of the Internet goes back to these factors.

However, it must be kept in mind that while the TCP/IP is not a protocol that is swayed by particular vendor interests it is not managed by any international organization like the ISO. It is a de facto standard protocol.

3.2.3 Internet Technology

As mentioned earlier, the Internet is a "network of networks." To put it differently, the Internet is a giant network in which all the computers connected to the network can exchange information. It is thanks to the realization of this idea that it has become easy to exchange information among all computers all over the world.

The technologies that have made this possible are:

- IP routing
- DNS

(1) IP routing

On the Internet, each computer connected to the network is given and managed by an IP address. IP addresses are unique addresses that are used all over the world. IP routing is the technique that determines the transmission route from the sender to the destination.

(2) DNS (Domain Name System)

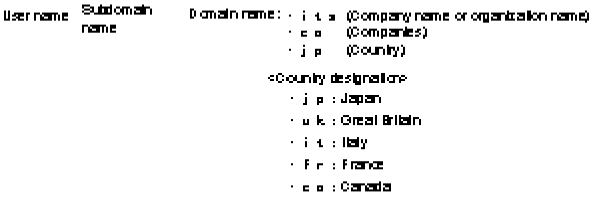
Each computer connected to the Internet is given an IP address but the format of this is very difficult to understand by humans. The "domain name" was therefore invented as a name that should be readily understandable.

There is a one-to-one coordination between a domain name and the IP address, and the DNS (Domain Name System) manages this coordination. In practice, name servers (DNS server) all over the world are working in unison to carry out the DNS function.

Figure 3-2-4 shows an example of a possible domain name.

Figure 3-2-4

Domain name example

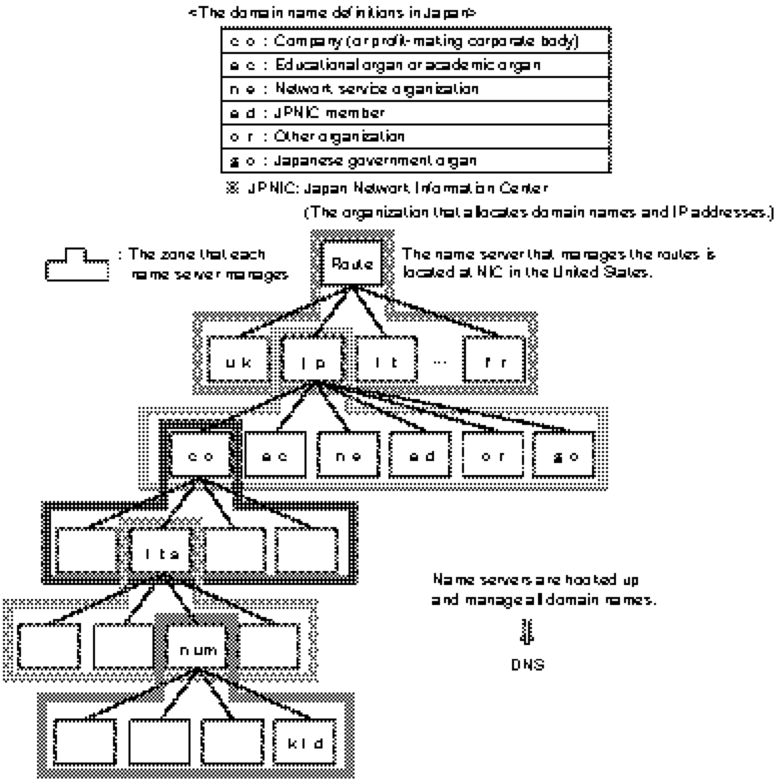


The meaning of the identifiers comprising the domain name is indicated in Figure 3-2-5. As the birthplace of the Internet, the United States is the only country where domain names do not contain the country identifier.

A domain name is very easy to handle as it is understandable at a glace since it tells you "which country," "what kind of organization," "who." An increasing number of the name servers that make DNS possible are clustered o be fault-tolerant against any possible failures.

Figure 3-2-5

The hierarchical structure of domain names and name server zones


<The domain name definitions in Japan>
co : Company (or profit-making corporate body)
ac : Educational organ or academic organ
ne : Network service organization
ad : JPNIC member
or : Other organization
go : Japanese government organ
※ JPNIC: Japan Network Information Center
(The organization that allocates domain names and IP addresses.)
: The zone that each name server manages
Route
The name server that manages the routes is located at NIC in the United States.
uk
jp
it
...
fr
co
ac
ne
ad
or
go
its
num
kid
Name servers are hooked up and manage all domain names.
⇓
DNS

3.2.4 Types of Servers

There are a number of servers performing different roles on the Internet. Simple explanations of the representative servers are as follows.

(1) Mail servers

Mail servers are servers that transmit the E-mail sent from the mailer (mail software) installed in the user's machine to the mail server of the destination (Figure 3-2-6).

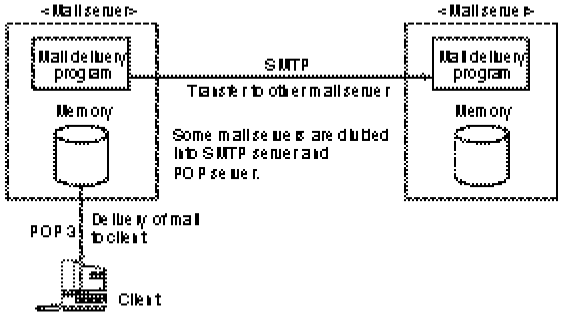
Mail servers controls the e-mail in accordance with the following two protocols:

- SMTP (Simple Mail Transfer Protocol)
- POP 3 (Post Office Protocol Version 3)

For details on E-mail, see Section 3.2.5 (1) E-mail.

Figure 3-2-6

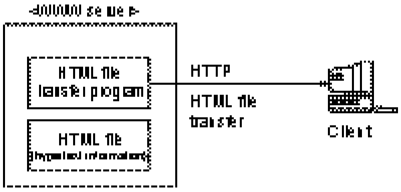
Mail server


<Mail server>
<Mail server>
Mail delivery program
Mail delivery program
SMTP
Transfer to other mail server
Memory
Memory
Some mail servers are divided into SMTP server and POP server.
POP 3
Delivery of mail to client
Client

(2) WWW server

WWW servers are also called HTTP (Hyper Text Transfer Protocol) servers or web servers. These servers consist of programs used to transfer hyperlinked text, video, audio, etc. (also called hypertext information) and HTML (Hyper Text Markup Language) files.
For details on WWW, see Section 3.2.5 (2) WWW.

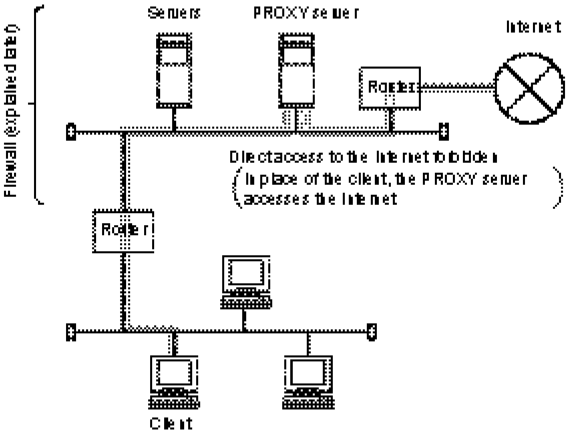
Figure 3-2-7
WWW server



(3) PROXY server

A PROXY server is a server that allows access to the Internet for computers that are forbidden to access the Internet directly (Figure 3-2-8). A PROXY server also has the functionality to temporarily store (caching) accessed information, designed to reduce the traffic load and faster access.

Figure 3-2-8
PROXY server

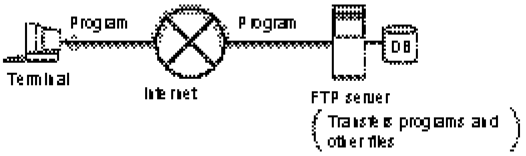


Firewall (explained later)
Servers
PROXY server
Internet
Router
Direct access to the Internet forbidden
(In place of the client, the PROXY server accesses the Internet)
Router
Client

(4) FTP (File Transfer Protocol) server

FTP (File Transfer Protocol) servers deliver files, programs, etc, to the user over the Internet.
For details on FTP, see Section 3.2.5 (3) FTP.

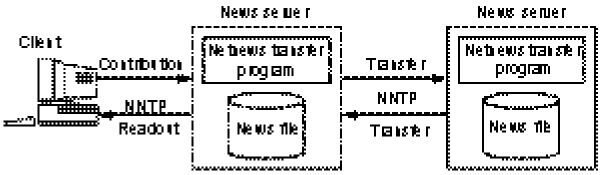
Figure 3-2-9
FTP server



(5) News server

News servers, also called NNTP (Network News Transfer Protocol) servers, transfer news from other news servers and control the readout of news and news contributions from users.

Figure 3-2-10
News server



NNTP: Network News Transfer Protocol

(6) Name server

Name servers, also called DNS (Domain Name System) servers, are servers that can answer domain name inquiries from users with IP addresses. This function is one of those that have facilitated use of the Internet. To ensure high reliability, name servers usually have the following redundant configuration.

- Primary name server: A server that has the management rights for a specified zone.
- Secondary name server: Server that holds the information of the primary server.

3.2.5 Internet Services

Various services are provided via the Internet. The following representative services are explained in this section:

- E-mail
- WWW
- FTP

(1) E-mail

E-mail is one of the communication methods over the Internet or other networks (personal computer communications, LAN, etc.). It has become a widely used communication means in place of telephones and fax.

The features of E-mail are:

- Allows all sorts of data to be sent in large amounts and at high speed.
  Due to improvements in compression technologies and bandwidth expansion, large amounts of data can be transmitted at high speed. In addition to text (characters), video and audio can also be transmitted.
- Regardless of whether or not the recipient is at home, the mail arrives in the mailbox inside the mail server.
- Running costs are low.
  Apart from the fee to be paid to the provider, the cost of sending or receiving E-mail only amounts to the telephone charge for the connection between the user and the provider (in the case of a dial-up IP connection), and this applies both to domestic E-mail and E-mail sent to other countries.

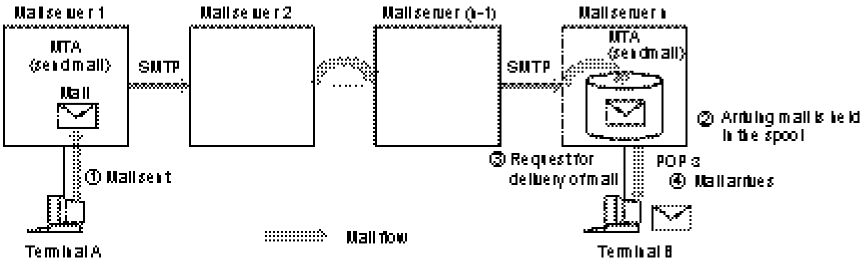
The mechanisms behind E-mail are shown in Figure 3-2-11.

The mail server exchanges and transfers mail using a program called MTA (Mail Transfer Agent) (the far most common software is called "sendmail").

The mail server sends and receives mail according to the following two protocols:

- SMTP (Simple Mail Transfer Protocol)
- POP 3 (Post Office Protocol Version 3)

Figure 3-2-11 The mechanisms behind E-mail



· SMTP (Simple Mail Transfer Protocol)
· POP 3 (Post Office Protocol Version 3)

<Order of procedure>

① Mail sent from Terminal A is relayed consecutively through mail servers using the SMTP protocol until it arrives at the destination mail server.
② Arrived mail is temporarily stored in the spool.
③ Terminal B requests delivery of mail from mail server "n."
④ Mail is delivered from the server to Terminal B using the POP3 protocol.

The SMTP protocol is used for transferring mail between mail servers, and POP 3 is the protocol used for transferring mail from the mail server to the user's terminal. Sometimes mail servers are thought of as being divided into a SMPT server and a POP 3 server in accordance with these protocols.

When sending other items than text as E-mail, such as video or audio, these data is compressed and converted into character information and transferred using a method called MIME (Multipurpose Internet Mail Extensions).

Mailing lists can be mentioned as an example of how E-mail can be utilized. Originally, this was a function for sending mail to the members of a specific group using the broadcasting method. However, these days it is often taken to refer to the activities of a group (groups of friends sharing the same interests, etc.) on the Internet that uses this distribution function.

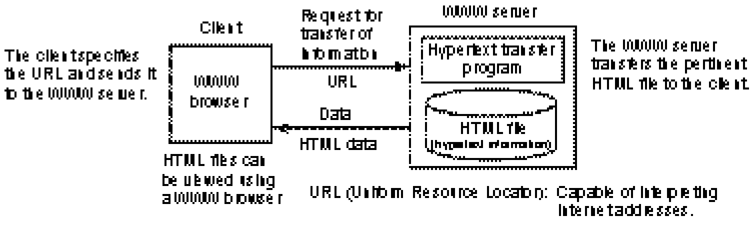
(2) WWW (World Wide Web)

The most important reason for the explosive growth in Internet users was the development of the WWW. The WWW interlinks all the WWW servers all over the world to allow search for information by surfing through the links. This is referred to as "net surfing."

The World Wide Web was developed at the European Laboratory for Particle Physics (CERN) in 1989. The number of WWW users increased rapidly after the National Center for Super-computing Applications (NCSA) at the University of Illinois developed and released the first popular WWW browser, called Mosaic, which could handle not only text but also images and audio.

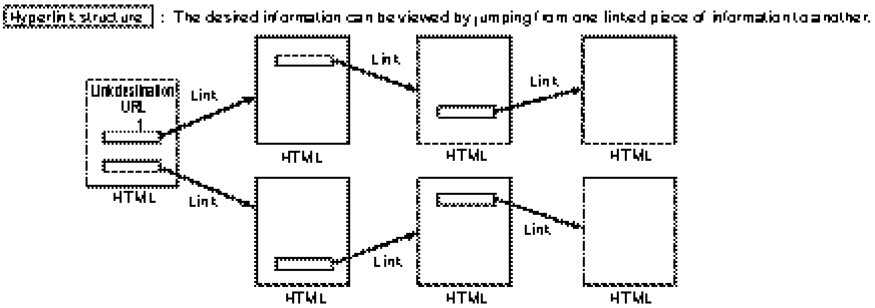
Figure 3-2-12 illustrates the structure of the WWW.

Figure 3-2-12 The structure of the WWW


Client
The client specifies the URL and sends it to the WWW server.
WWW browser
HTML files can be viewed using a WWW browser
Request for transfer of information
URL
Data
HTML data
WWW server
Hypertext transfer program
HTML file (hyperlinked information)
The WWW server transfers the pertinent HTML file to the client.
URL (Uniform Resource Locator): Capable of interpreting Internet addresses.

Most of the data housed in WWW servers is in the HTML format. Recently, Java (object-oriented language suitable for use on networks), VRML (Virtual Reality Modeling Language; language that can express 3-D), XML (eXtensible Markup Language; language that extends HTML and can be used on the Web), etc. have also become widely used, promoting more visual and advanced use of the Internet.

Figure 3-2-13 Hyperlink structure and HTML


Hyperlink structure : The desired information can be viewed by jumping from one linked piece of information to another.
Link destination URL
Link
Link
Link
Link
Link
Link
HTML
HTML
HTML
HTML
HTML
HTML
HTML

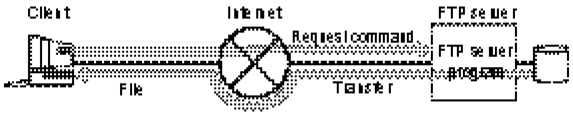
```
<HTML example>
<IMG SRC=" img/smallblueball.gif "><font size=+0><a href=" html/syuppan/press01.html ">press release
</a><BR>
<IMG SRC=" img/smallblueball.gif "><font size=+0><a href=" html/tenshu/shiken.html ">Information on examination
for information technology engineers</a><BR>
<font size=+0><a href=" html/tenshu/shiken.html ">(Central Academy of Information Technology for Japan Information
Processing Development Corporation Japan Information-Technology Engineers Examination Center)</a><BR>
<IMG SRC=" img/smallblueball.gif "><a href=" html/nintei/index.html ">List of schools with authorized curriculum
for education of IT personnel (Authorized by the Minister of Economy, Trade and Industry) </a><BR></font></ul>
<hr size=5>
<center>
```

Underlined parts: Linked information
(From CAIT's homepage)

(3) FTP (File Transfer Protocol)

Figure 3-2-14 shows the structure of FTP (File Transfer Protocol).

Figure 3-2-14
FTP structure



The file transfer sequence of FTP is as follows:

1. As the FTP delivery request command differ with the user's OS, the command is converted to a standard command by the FTP client program, and then sent to the FTP server.
2. The FTP server converts the standard command by the FTP server program into a command conforming to the server's OS and interprets the command and transfers the file. For the transfer, the FTP server program also converts the object file into a standardized form before it is transferred.

Some FTP servers require an "account" (authorization for use) to enable use and others can be used as "anonymous" FTP.

3.2.6 Search Engines

There is countless data (homepages) registered in countless WWW servers on the Internet. In principle, users can freely get their hands on all these data. However, finding the data you are searching for among all these many data is very cumbersome. Therefore search engines are used for this purpose. A search engine is an information retrieval tool (system) found on the Internet. It can be thought of as site specialized for information search.

Search engines are divided into the following groups:

- Search engine type: Directory type, robot type
- Search method: Keyword search, directory search

(1) Search engine types

① Directory type search engines

Directory type search engines search indices in which homepage titles and contents (comments) are registered to find the target homepage. Humans perform the indexing. These engines yield good search results and are highly reliable but they do not necessarily support the latest information. Another shortcoming is that the total amount of data to be searched is somewhat small. "Yahoo!" is one of the representative search engines belonging to the directory type.

② Robot type search engine

Robot type search engines employ search robots (programs) that automatically search WWW servers and collect information for indexing. These search engines regularly search all the WWW servers throughout the world and can thus gather large amounts of the newest information. However, since automatic judgments are left to programs, the search results and reliability are somewhat low (homepages that are almost irrelevant will often be shown).

Among the representative robot type search engines is "goo."

(2) Search methods

① Keyword search

Keyword search is a method in which search is performed based on keywords specified by the user. There are many inconvenient points in connection with the keyword search method as it can be very difficult to find the desired information. The method is probably most useful to advanced users.

② Directory search

Directory search is a method in which you find the desired information by gradually narrowing the search object to fields or genres, etc. Since the search is performed in stages, it can be bothersome but it is a search method that is easy to use by beginners.

There are also full-text retrieval systems that work in ways similar to search engines. While search engines search through indexes with registered information, full-text retrieval systems search the entire text of homepages. Because the full text is searched, the application area is wide but there are many technological challenges involved, as a large amount of data has to be searched.

3.2.7 Internet Related Knowledge

(1) QoS (Quality of Service)

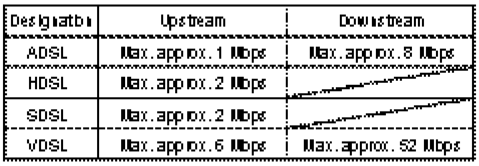
Based on transmission delay and lowest guaranteed speed, etc., QoS is used as an indicator to show the quality of the service provided by the network layer of the OSI basic reference model. Recently, QoS standards for offering Internet services have been laid down by the IETF (Internet Engineering Task Force).

(2) xDSL (x Digital Subscriber Line)

xDSL is the general term for technologies for high-speed transmission using telephone lines. The x is substituted to indicate the various types, e.g., ADSL (Asymmetric DSL), HDSL (High-speed DSL), SDSL (Symmetric DSL), VDSL (Very-high-speed DSL). Figure 3-2-15 shows various methods and the limitations in terms of transmission distance and transmission speed.

Figure 3-2-15

xDSL transmission speeds



Designation	Upstream	Downstream
ADSL	Max. approx. 1 Mbps	Max. approx. 8 Mbps
HDSL	Max. approx. 2 Mbps	
SDSL	Max. approx. 2 Mbps	
VDSL	Max. approx. 6 Mbps	Max. approx. 52 Mbps

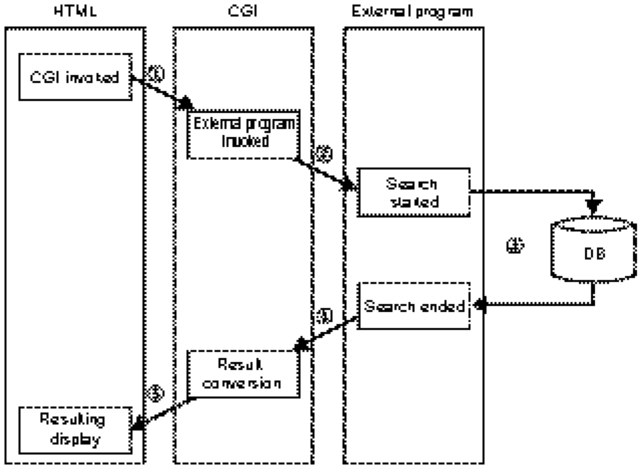
(3) Best Effort Service

Best effort services are services that give no guarantee for the transmission bandwidth that can be used on the network at times of congestion. In lieu of guarantees, charges are normally lower. In contrast to best effort services, services that offer guarantees even in times of congestion are called "guaranteed services."

(4) CGI (Common Gateway Interface)

CGI is an interface between a WWW server and programs. The CGI is invoked by commands included in HTML documents held in the WWW server and it can issue commands to external programs. Employing CGI makes it possible to create conversational homepages in which processing is carried out in accordance with the inputs made by the user.

Figure 3-2-16
The workings of CGI

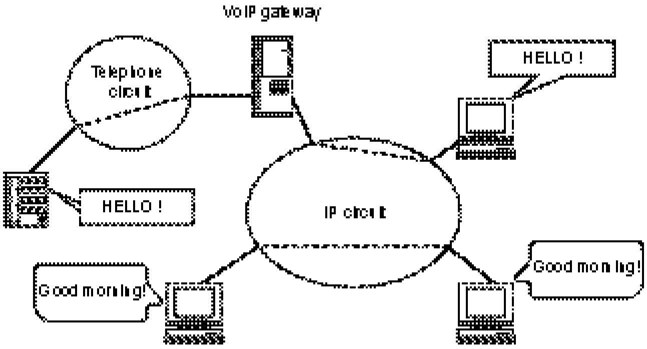


① CGI is invoked by commands contained in the HTML document.
② CGI organizes the search conditions and invokes the external program used for DB retrieval.
③ The external program organizes the search conditions passed to it and retrieves the database(s).
④ The search result is transferred to the CGI program used for converting the results of the DB retrieval.
⑤ The CGI program integrates the search results into the HTML document for display.

(5) VoIP (Voice over IP)

VoIP is a voice data transmission technology employing the IP protocol. VoIP is used to carry out voice communication over the Internet by using a personal computer as an Internet phone (Figure 3-2-17).
By using VoIP gateways it is possible to connect public switched telephone network and IP networks. For this purpose the MGCP (Media Gateway Control Protocol) is used to control the VoIP gateway. Standardization is under way by the IETF.

Figure 3-2-17
Voice network using VoIP



Currently, the quality of Internet telephones is lower than that of public switched telephone networks. However, research into how to prevent delays or fallout of the sound is progressing, and it can be envisioned that Internet telephones will make up a high-quality and low-cost telephone network in the future.

3.3 Network Security

The development of networks has expanded the areas of computer applications and networks have become the foundation of today's information society. Together with the spread of networks these have also been exposed to the various threats.
Some of the threats facing networks are:

- Eavesdropping of the contents of communications by third parties.
- Falsification with the contents of communications by third parties.
- Illegitimate intrusion into networks by persons without authorization.

Network security refers to the overall term to embrace the ideas and efforts trying to counter these threats and make networks safe to use.

3.3.1 Confidentiality Protection and Falsification Prevention

The first aspect that must be considered in terms of network security is the protection of information (data). Eavesdropping and falsification with information is a serious problem to both companies and individuals.
The following are some of the methods available to prevent eavesdropping or falsification of information:

- Encryption of information
- Authentication of user identities
- Control of access rights

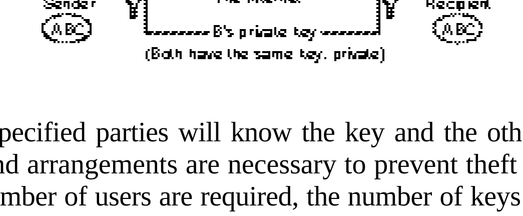
(1) Cryptography technology

With the spread of the Internet, the social structures (distribution structures and pricing structures) are likely to undergo major changes. One of the representative themes is EC (Electronic Commerce). Simply expressed, EC is the conduct of various commercial transactions on the Internet. This involves important data flowing on the communications lines. However, there is a risk that the data may be bugged or falsified, since these are not private lines. Technology to counter these threats is required and technology to carry out "data encryption" preventing the contents of any stolen data from being read is indispensable.
Private key cryptography and public key cryptography are the two representative encryption technologies.

① Private key cryptosystem

In private key cryptosystem a set of symmetric keys is used by the sender for encryption and by the recipient for decryption. A representative example of this method is the DES (Data Encryption Standard), created by the U.S. National Bureau of Standards.

Figure 3-3-1
Private key cryptosystem

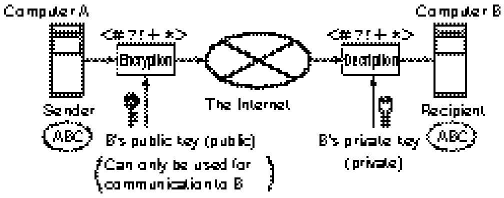


As the key is private, only specified parties will know the key and the other party can thus be identified but thorough management and arrangements are necessary to prevent theft of the key. Since a number of keys corresponding to the number of users are required, the number of keys can swell dramatically.

② Public key cryptosystem

In public key cryptosystem the sender uses a public key to encrypt data, and the recipient uses a dedicated private key to decrypt it. A representative example of this method is RSA (Rivest, Shamir, Adleman, the names of the three inventors).

Figure 3-3-2
Public key cryptosystem



Public key cryptosystem differs from private key cryptosystem in the way that there is no need for management of the public key. The private key cannot be found from the public key. However, since the key for encryption is public it is impossible to confirm the identity of the sender, which means that there is a risk of "impersonation."

Recently, PGP (Pretty Good Privacy) has become widely used in email encryption software. This software was developed by Philip Zimmermann of the PGP Corporation in the United States and it combines both the functions of encryption and authentication (explained later).

③ Encryption algorithms

Representative encryption algorithms are: Substitution ciphers, transposition ciphers, insertion ciphers, etc.

a. Substitution ciphers

The substitution cipher is an encoding technique that replaces the original characters with other characters or symbols according to a rule. A representative substitution cipher is the Caesar cipher. In the Caesar cipher a character is replaced with another character placed at a specified interval from the original character. This method was used by Julius Caesar and is said to be the world's oldest encryption method.

Example Caesar cipher (shift interval: 2 characters)
Text to be sent: "Tomorrow" → Encrypted text: "Vqoqttqy"

b. Transposition ciphers

The transposition cipher is an encoding technique in which the order of the original characters is changed to create a separate character string. This technique enables more complicated ciphertext as the order can be changed not only in the direction of the line but also vertically.

Example Order changed for every 4 characters (ABCD → BDAC)
Text to be sent: "tomorrow" → Encrypted text: "ootmrwro"

c. Insertion ciphers

The insertion cipher method is an encryption technique in which an extra character is inserted after a specified interval. Because the original order of the characters is not jumbled, this encryption method is somewhat weak.

Example Extra character inserted for every two characters.
Text to be sent: "Tomorrow" → Encrypted text: "Toqmosrrgowa"

The DES private key encryption is a combination of the substitution cipher and transposition cipher methods. This method divides the message into fixed lengths and repeats substitution and transposition cipher encryption several times for each block.

The RSA public key encryption is a substitution cipher that relies on second power residue calculation. The security of this encryption is guaranteed by the fact that huge calculations are necessary to solve the prime factorization.

Other methods, such as the ECC (Elliptic Curve Cryptography), which is a public key encryption method that relies on calculations of curves, are also attracting attention.

(2) Authentication

Following the countermeasures to eavesdropping, prevention of falsification of data and impersonation has to be considered.

Commercial transactions cannot be conducted on the network if it is easy to falsify the data. If, for example, the number of ordered items can be rewritten, the transaction cannot be concluded as it should be. If impersonation is possible, it will be possible for third parties to pretend that they are ordering for others.

The following are some of the technologies employed to prevent this:

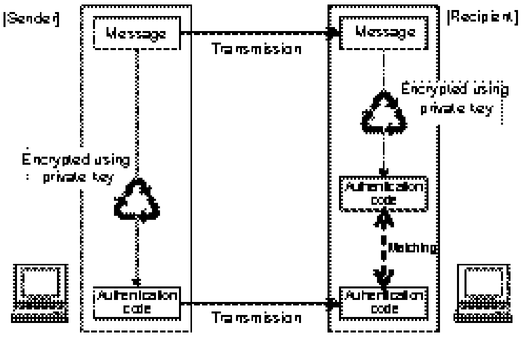
- Message authentication
- Digital signature

① Message authentication

Message authentication is a technology for checking whether the sent data has been altered during the transmission. Error detection methods (parity check, CRC, etc.) that detect whether or not errors are generated and executed when the message is transmitted, can also be said to be a type of message authentication.

However, more than this, attention has to be paid to whether or not the message has been falsified. To prevent falsification of the message, private key encryption, etc. can be used. When this technique is used, the sender sends the message together with an authentication code encrypted using a private key. Based on the received message, the recipient uses the same private key as that used for the encryption to create an authentication code, and by matching this with the received authentication code it can be checked whether or not the message has been falsified.

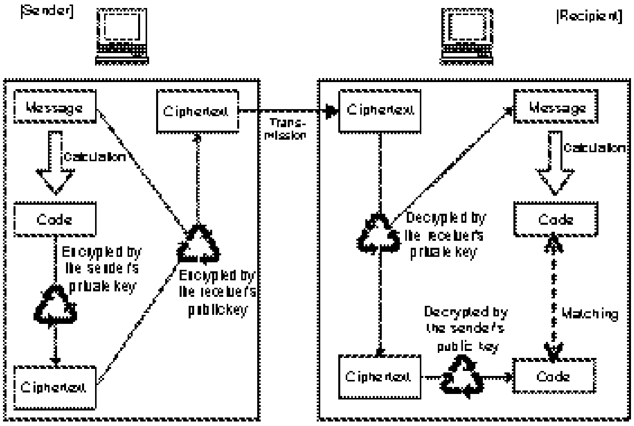
Figure 3-3-3 Message authentication mechanism



② Digital signature

Digital signature is a user authentication method to prevent impersonations. Using the public key, this authentication method identifies the sender's authenticity as well as certifies that the data has not been falsified.

Figure 3-3-4 Digital signature mechanism


[Sender]
[Recipient]
Message
Ciphertext
Trans-
mission
Ciphertext
Message
Calculation
Calculation
Code
Encrypted by the sender's private key
Encrypted by the receiver's publickey
Decrypted by the receiver's private key
Code
Ciphertext
Decrypted by the sender's public key
Matching
Ciphertext
Code

The digital signature is a technique in which the data "encrypted" by the sender's private key is "decrypted" by the sender's public key on the receiver side. The public key and private key correspond one-to-one, meaning that the message "decrypted" correctly using the public key is made a person who possesses the private key corresponding to the public key. In this context, the Certification Authority (CA) certifies the authenticity of the public key itself.

Whether the contents of the message have been altered can be detected by the code embedded into the transmitted message. In the digital signature, this embedded code is the "encrypted" data by the sender's private key. Also, by encrypting the message and code with the recipient's public key before transmission, eavesdropping of the data can be prevented.

In general public key encryption, it is called "encrypting" when the public key is used and "decrypting" when the private key is used. Accordingly, it can be said that digital signature is "a method in which the data "decrypted" by the sender's private key is "encrypted" by the sender's public key on the receiver side."

(3) Security protocols

Security protocols are protocols providing security measure to prevent interception of information, etc. SLL is one of the representative security protocols.

① SSL (Secure Sockets Layer)

SSL provides security measure for the upper level protocols like HTTP, SMTP, FTP, etc. It is a protocol located midway between the application layer and the transport layer, and it performs the role of encrypting the information received from the upper level protocols and passing it to the lower level protocol (TCP).

By employing the SSL eavesdropping of information can be prevented, as encrypted data will be transmitted on the communication channel. However, the safety of SSL is somewhat low because it offers common security measure for all the upper level protocols. Consequently, several separate methods have been proposed for use according to purpose. Representative of these are SHTTP and SET.

② SHTTP (Secure HyperText Transfer Protocol)

SHTTP is a protocol that adds function for encryption of HTML documents to the HTTP protocol and is used when data should be encrypted for transmission between a WWW browser and a WWW server.

③ SET (Secure Electronic Transaction)

SET is used for conducting secure electronic commerce transactions on networks, and it provides a series of security measures such as encryption of transaction data, issue of digital certificate from a Certification Authority.

(4) Access control

Encryption of data can reduce the risk of data flowing on the communications lines from being bugged (eavesdropping or falsification of information). However, eavesdropping or falsification of information can also be done directly from databases or files if an intruder gains illegal access to the network.

To prevent this kind of threat, it is of utmost importance to prevent illegal access to the network. Nevertheless, it is also possible to envision that a user who has legal access to the network could steal or falsify files belonging to other people or confidential company information. To prevent this, access control to prevent unauthorized access to data on the network is required.

Access control is implemented by the use of such measures as:

- Access right
- Password

① Access right

This is one of the aspects of access control that sets access right for each user in relation to files and databases. Access rights comprise the right to read, write, delete and execute, etc. It is not possible for a user to perform other processing than he/she has the right to. For example, a user that only has the right to read can view the contents but cannot change the contents.

Often access rights are not defined for each individual user in practical access control. Instead users are divided into several layers, and access rights are defined for each layer. The three common user divisions are:

- Network system administrator
- The group to which the creator (owner) of the file belongs, such as department or project.
- Other users that are legitimate network users.

For a file created by A, for example, A himself/herself and the administrator may have full access rights. Members of the department to which A belongs may be granted the right to read the file together with the right to execute it. Other users may only be given the right to read the file.

Setting access rights in this way can help prevent theft and unauthorized alteration of information. However, the access right is not enough to prevent illegal access if a third party impersonalizes as a user who has legitimate access right. To minimize this risk, it is desirable to limit access right to the minimum required.

② Password

A password is a predetermined keyword that the user types in. The password is used to confirm that the person knows the keyword and is a legitimate user.

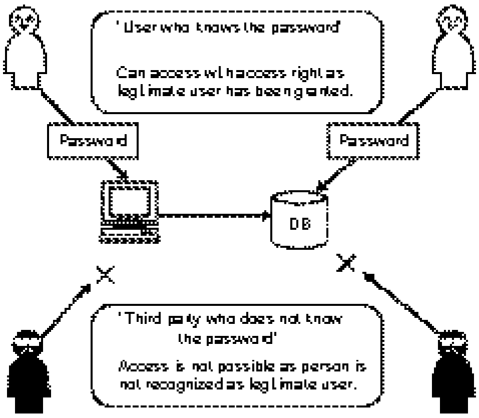
In access management, the password is used in two ways (Figure 3-3-5).

In one method, it is used on the level where the user is required to prove that he/she is a legitimate user who has been granted access right. As a means to control access, this will be ineffective if an illegitimate person impersonalizes as a legitimate user with access right. To prevent impostors from gaining access to the network, it is necessary to have persons enter a password when using the network in order to confirm that they are legitimate users.

Another way to use passwords is to set a password for files and databases. In other words, the user must enter a password in order to gain access to files and databases. By ensuring that only persons with legitimate access right know the password, illegitimate access can be prevented.

Figure 3-3-5

Use of passwords


'User who knows the password'
Can access with access right as legitimate user has been granted.
Password
Password
DB
'Third party who does not know the password'
Access is not possible as person is not recognized as legitimate user.

The most important thing to ensure when using passwords is that the password itself is not disclosed to third parties.

Full attention must be paid to the following in association with the use of passwords:

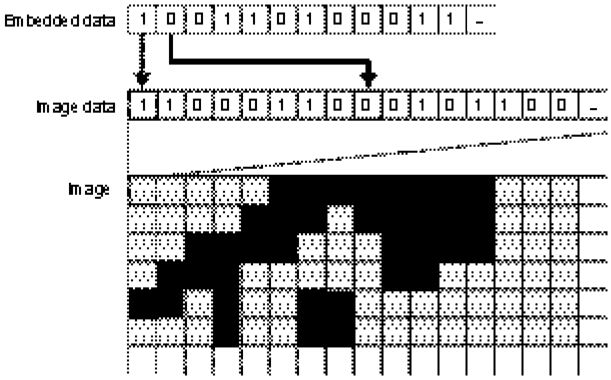
- Other people must not be told the password.
- Passwords must be difficult to guess (birthdays, etc. must not be used).
- Passwords must be changed periodically.
- Password files must be encrypted.

(5) Electronic watermarking

Electronic watermarking is a technology for embedding special information, which is not discernable to the human eye, in image information, etc. It is often used to prevent piracy of image data, etc. by embedding information on copyrights. Electronic watermarks cannot be erased by normal operations (copy, compression/decompression, enlargement/reduction, etc.). Unless special software is used, the watermarks cannot be removed or modified which makes this technology highly efficient for countering illegitimate use of image information.

There are several methods for implementing electronic watermarking. An easily understandable example is the method that embeds special information bits in the bit strings that express image information (Figure 3-3-6). For example, when each of the colors red, blue and green for one image dot are saved as 8 bits, an information bit is included as the most significant bit for each of the colors. In this case, the gradation of each color falls from 256 colors to 128 colors but this degree of difference in color is very difficult to detect by the human eye.

Figure 3-3-6 Mechanism of electronic watermarking



Another method disassembles the data into frequency bands and only embeds a special signal in specified frequency bands. While this electronic watermarking demands work and efforts, safety is higher than in the case of the simple embedding method and currently this method is the most widely used.

(6) Confidentiality management

Confidentiality management aims to prevent disclosure of confidential company information, etc. Disclosure of confidential information is often associated with illegitimate behavior of third parties while in fact it is often leaked by people inside the company.

To prevent employees from disclosing information, it is necessary to arrange things so that it is not easy to get close to valuable and sensible information – even for people working inside the company. There is no sense in enhancing network security if it remains easy to enter and leave the computer room. Consequently, entrance control of people is required in association with computer rooms where sensible information is kept.

Some of the conceivable techniques for entrance control are:

- Identification by means of ID card with photo.
- Identification by PIN (personal identification number) and password.
- Identification by means of IC card.
- Identification by special physical features (fingerprints, voiceprint, etc.).

By implementing strict entrance control, illegitimate entry and exit can be prevented. However, this does not prevent people entering legitimately from disclosing information. That is the reason why laws and regulations related to prevention of disclosure of information have become necessary.

Fundamentally, the Japanese Civil Code and criminal law protect confidential company information. The Civil Code stipulates that by exchanging confidentiality agreement with an employee at the time of employment, an employee can be dismissed if found guilty in disclosing information. Furthermore, if the company suffers unnecessary damage due to the disclosure of the information it can demand compensation from the employee and from any company that may have used the information. In the context of criminal law, embezzlement and breach of trust may apply. The Unfair Competition Prevention Law can also be applied to halt illegitimate use of trade secrets.

As the information society is developing, one bill after another is being enacted to curb illegal disclosure of information. However, the real way to prevent leakage of information is not by punishment by means of bills and laws, but by enacting intra-company education and creating an environment inside the company so as to raise the consciousness of each employee.

3.3.2 Illegal Intrusion and Protection against Computer Viruses

Connecting a network inside a company (LAN) to an external network (WAN) accelerates exchange of information, and brings great benefit to the company. However, this requires the company to deal with risk of attacks on the company's intranet (in the form of illegal intrusion, computer viruses, etc.).

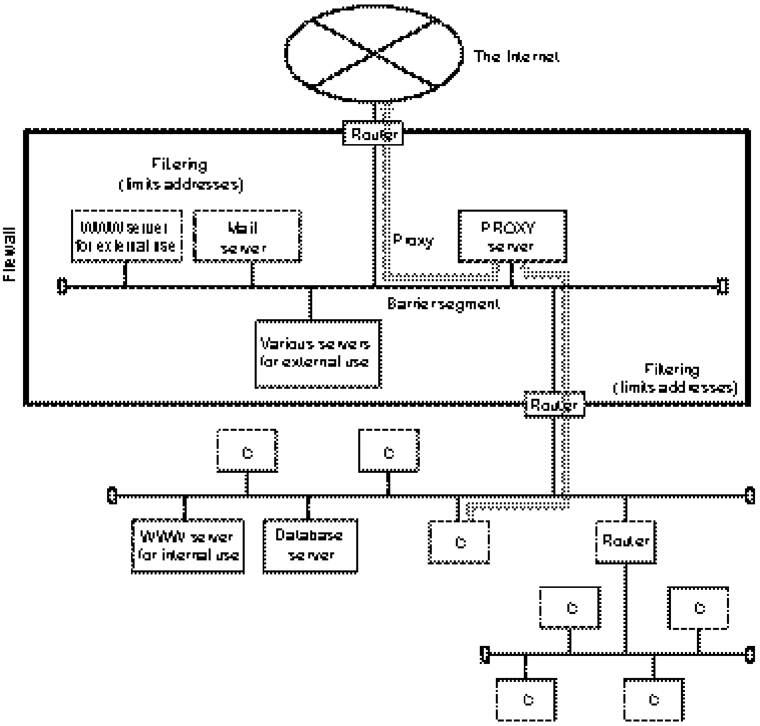
This section explains firewalls enacted to prevent illegal intrusion into intranets, RAS, and precautions against computer viruses, etc.

(1) Firewall

A firewall is a security system set up between the Internet and the intranet and it is comprised of a network (called "barrier segment") of connected servers (WWW servers, mail servers, etc.) (Figure 3-3-7).

The fundamental role of the firewall is to control the passage of data (packets) and allow or deny the passage of data by means of the filtering performed by a router. Also, transactions between the intranet and the Internet are relayed through a PROXY server to prevent computers inside the company from accessing the Internet directly.

Figure 3-3-7
Firewall

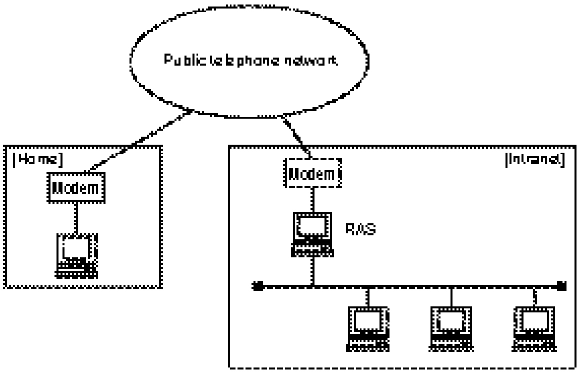


(2) RAS

A RAS (Remote Access Server) is a server that enables users to access the intranet over telephone lines. Installing such a server makes it easy to connect to the intranet from a remote location so that a user can obtain the same kind of service when he/she is at home or on a business trip as when in the office (Figure 3-3-8).

When a RAS is used, a "callback" is performed to prevent illegal intrusion. The callback works in the way that when a request for connection to the RAS is received from the remote location, the line is disconnected once before the RAS server dials the remote location and connects the line. This process prevents illegal intrusion even if user IDs or passwords have been stolen because only telephone numbers registered in advance are allowed to be connected to the intranet.

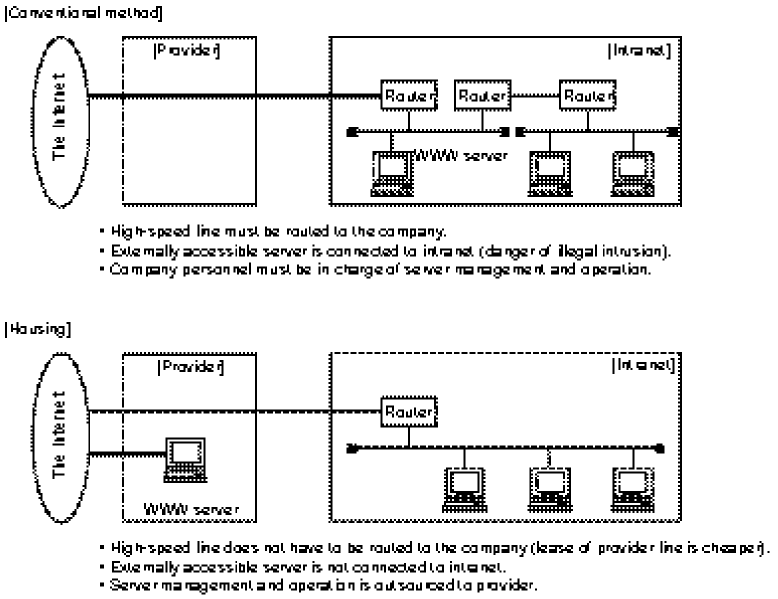
Figure 3-3-8
RAS



(3) Housing

Housing is method where the user places servers on the premises of the provider and leaves management to the provider.

Figure 3-3-9
Housing



- High-speed line must be routed to the company.
- Externally accessible server is connected to intranet (danger of illegal intrusion).
- Company personnel must be in charge of server management and operation.

- High-speed line does not have to be routed to the company (lease of provider line is cheaper).
- Externally accessible server is not connected to intranet.
- Server management and operation is outsourced to provider.

When you use a server supplied by the provider, you call it "hosting." In this case, a user can borrow one server, or several users may share one server.
The benefits of housing and hosting are:

- Direct use of the provider's high-speed line.
- Separation between intranet and externally accessible server.
- Security service is provided.

(4) Computer virus

Computer viruses are programs that intrude into computers and can destroy the contents of the computer's hard disk or memory or alter programs. Often the infection route or the time of infection cannot be determined, and the virus may lay dormant for a while following intrusion before it starts working after a certain period of time has elapsed. Representative effects of viruses are:

- Destruction of programs.
- Destruction of data in files.
- Images or characters may suddenly appear on the monitor screen.

- Damage occurs on specific dates (for example Friday the 13th).

In many instances it is too late to do anything after the computer has become infected. Accordingly, it is a wise police to always inspect floppy diskettes, etc., brought in from the outside by running them through a virus check program (vaccine program) before inserting them into computers, and refrain from using media whose origin is unknown, etc. The Ministry of Economy, Trade and Industry has published guidelines on this in the form of the notice "Standards for Countering Computer Viruses."

3.3.3 Availability Measures

When considering network security, safety in terms of hardware must also be considered. It is necessary to make arrangements so that databases, etc. can be quickly restored if affected by computer viruses, and it must be ensured that the network does not go down if a line malfunctions, etc.

Security measures concerning hardware are referred to as "availability measures" or "hardware security."

(1) File backup

File backup is the most fundamental availability measures, and it refers to the act of taking copies of important data for backup. Representative methods comprise:

- Full backup
- Incremental backup
- Difference backup

① Full backup

Full backup is a method for backing up all the files, including OS and software. In case of failure, the system can quickly be restored. However, long time is required for the backup.

② Incremental backup

Incremental backup is a method that only makes a backup of the items that have changed since the last backup. Backup can be accomplished in relatively short time but recovery in case of failure takes a little longer time.

③ Difference backup

Difference backup is a method that backs up the items that have been newly added since the last full backup was performed. It takes longer to perform than the incremental backup but the time required for restoring is shorter.

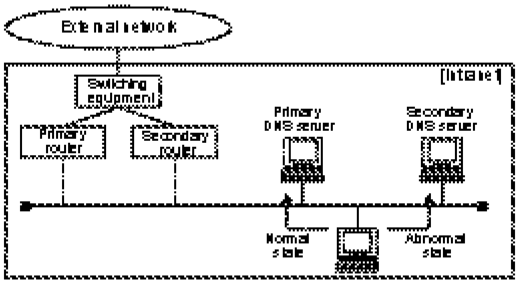
Data recovery service is another file recovery method. This is a service provided by certain vendors where data is extracted from a damaged file and then recovered as a file. Using a special technique, data is extracted from data that the user cannot read. This allows 60 to 80% of the old data to be restored. However, currently this is a very expensive service and 100% recovery is not achievable, meaning that some data has to be inputted again.

(2) Redundant system configuration

It must be ensured that all the functionalities of an intranet do not come to a stop in case of failure of any of the devices that make up the network. Consequently, it is necessary to arrange redundant system configuration for the most important equipment and devices, such as the communications lines and transmission control devices.

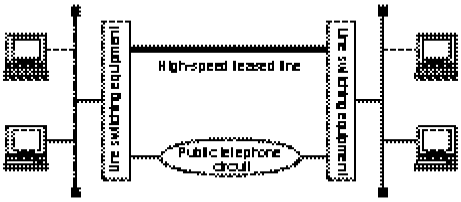
By preparing two or more of the same devices, it is possible to switch from the primary device to the secondary device if failures occur in the primary device so that the functionalities of the network can be retained. This redundant configuration is also applied to servers such as DNS and database servers.

Figure 3-3-10
Redundant system configuration



In the case of a network that connects two locations, a backup route, such as a public telephone line, should be prepared in advance for emergency situations, in addition to the high-speed leased line used under normal circumstances.

Figure 3-3-11
Duplication of communications lines

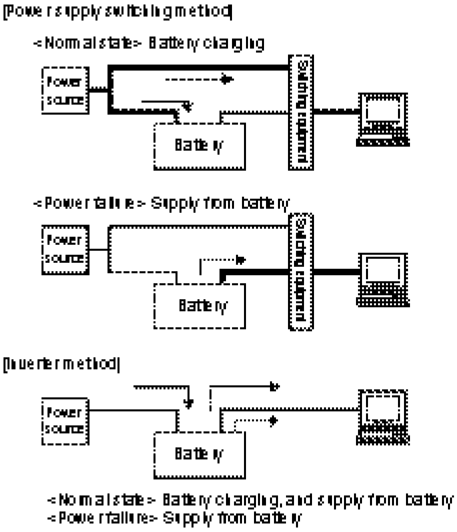


(3) Countermeasures against natural calamities

In the context of network security it is not sufficient to take precautions against human threats such as leakage of information or illegal intrusion. Preparations must also be made for natural calamities such as typhoons or earthquakes.

Most damage to networks stemming from natural calamities comes from the interruption of power. Countermeasures against power interruption include installation of UPS (Uninterruptible Power Supply). A UPS is a system that switches to operate on battery in case of a power interruption and supplies power for a certain period of time. One type of UPS only switches to battery in cases of abnormalities, and another inverter type supplies power via the battery under normal circumstances. In the case of the power supply switching method, the power supply might possibly be momentarily interrupted (short break), and thus the inverter type is more reliable even though it is more expensive.

Figure 3-3-12
UPS methods


[Power supply switching method]
<Normal state> Battery charging
Power source
Battery
Switching equipment
<Power failure> Supply from battery
Power source
Battery
Switching equipment
[Inverter method]
Power source
Battery
<Normal state> Battery charging, and supply from battery
<Power failure> Supply from battery

CVCF (Constant Voltage Constant Frequency) equipment that combines a home generator with an uninterruptible power supply is used for large-scale computers.

Some of the countermeasures required for earthquakes are:

- Network equipment must be fixed in place so that it cannot fall down
- Backup media should be stored in a room away from the computer room.

3.3.4 Privacy Protection

Through sales activities, private enterprises amass a variety of personal information from the order slips and application forms received from consumers. In many cases the obtained information is entered into databases to support the company's sales activities. A great amount of information ranging from address and gender, date of birth, family structure to states of financial and property, can thus be collected. Much personal information, such as resident registration, taxpayer register, drivers license, social insurance, etc., is also registered by many public organizations.

This personal information involves the right to privacy, and the security of the information ought to be guaranteed. However, if this information is made public by some kind of mistake, the right to privacy may be violated. Free access to information and the right to privacy are often mutually contradictory, and organizations that possess personal information must consider safety precautions to ensure that information is not improperly disclosed.

(1) Personal information management

As a guideline on personal information, the OECD (Organization for Economic Cooperation and Development) proposed "Committee Recommendation on Guidelines for Protection of Privacy and International Circulation of Personal Information" in 1980. This recommendation provided the following 8 basic rules concerning personal information.

① Restrictions on collection
Unrestricted collection of personal information must not take place.

② Clarified purpose
The purpose must be clearly stated when data is collected.

③ Contents of data
Only information conforming to the purpose of the information gathering must be collected.

④ Restrictions on use
The information must not be used for other purposes than those for which it was collected.

⑤ Safety guarantee
Measures must be taken to guarantee the safety of the collected data.

⑥ Announcement of the purpose of use
How the data is used must be made public.

⑦ Participation by individuals
Individuals can confirm the existence of data. Furthermore, correction, deletion, etc. of data must take place upon request by an individual.

⑧ The collector's responsibility
The collector of the data must be responsible for the items described above.

Based on this guideline, most countries have enacted laws to protect personal information. In Japan, the "Bill on the protection of personal information in connection with computer processing in possession of administrative bodies" was enacted in 1988. However, this bill aimed at administrative organs. A bill covering private enterprises is under discussion. Until this bill is enacted, management of personal information by private enterprises is conducted in accordance with the principles of the voluntary guideline "Guidelines on the protection of personal information in connection with computer processing in the private sector."

(2) Anonymity

On the Internet, it is possible to release information anonymously (under a pen name). This means that the Internet is a network that does not allow tracking and prevents identification of the source of the information.

Among the benefits of anonymity are:

- Personal information can be kept secret.
- Ensures freedom of expression.

Some of the demerits, on the other hand, are:

- Irresponsible release of information.
- Can promote illegal behavior (criminal acts, etc.).

When used in the normal way, an IP address is known even if the transaction is conducted anonymously. However, by using a certain type of mail forwarding service the mail can be sent from a completely different IP address.

In this case, the IP address can be investigated if a crime has been committed. If, for example, a mail forwarding service has been used to send a threatening letter, the IP address can be investigated by viewing the log of the provider offering the service. However, it is possible that a false name and address were used when the IP address was obtained.

To prevent this and similar kinds of crimes, some are in favor of eliminating anonymity from the Internet. This is a very complicated problem, and some hold the opinion that eliminating the right to anonymity will also remove the right to free speech. There is also a way of thinking that says that because private information is leaked, the right to anonymity must be protected.

As this is an ongoing discussion and problem, no conclusion can be drawn, but considerations of actual laws to prevent crimes committed under the cover of anonymity are under way.

Ultimately, whether or not to use anonymity and under what circumstances are questions that are probably best left to the moral of the user.

Exercises

Q1 Which of the following classifies the LAN according to the configuration (topology) of the communication network?

A. 10BASE 5, 10BASE 2, 10BASE-T
B. CSMA/CD, token passing
C. Twisted-pair, coaxial, optical fiber
D. Bus, star, ring/loop
E. Router, bridge, repeater

Q2 Which is the correct description of the special features of peer-to-peer LAN systems?

A. Discs can be shared between computers but printers cannot be shared.
B. Suitable for large-scale LAN systems because this type is superior in terms of capabilities for scalability and reliability.
C. Suitable for construction of transaction processing systems with much traffic.
D. Each computer is equal in the connection.
E. LAN systems cannot be interconnected using bridge or router.

Q3 Which of the LAN communication line standards possesses the following characteristics?

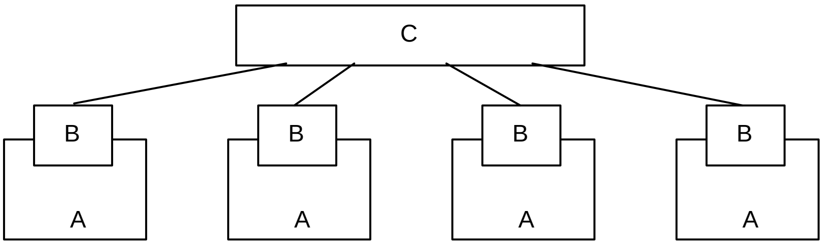
Transmission media	Coaxial cable
Topology	Bus
Transmission speed	10M bit/sec
Max. length of one segment	500 m
Max. number of stations for each segment	100

A. 10BASE 2　B. 10BASE 5　C. 10BASE-T　D. 100BASE-T

Q4 Which is the most appropriate description of the LAN access control method CSMA/CD?

A. When collision of sent data is detected, retransmission is attempted following the elapse of a random time interval.
B. The node that has seized the message (free token) granting the right to transmit can send data.
C. Transmits after converting (by modulation) the digital signal into an analog signal.
D. Divides the information to be sent into blocks (called cells) of a fixed length before transmission.

Q5 The figure shows an outline of a network with computers connected by means of 10BASE-T. If A in the figure is a computer and B is a network interface card, what is the appropriate device name for C?



A. Terminator　B. Transceiver　C. Hub　D. Modem

Q6 **What is the appropriate description of a router?**

A. Connects at the data-link layer and has traffic separating function.
B. Converts protocols, including protocols of levels higher than the transport layer, and allows interconnection of networks having different network architectures.
C. Connects at the network layer and is used for interconnecting LAN systems to wide area network.
D. Connects at the physical layer and is used to extend the connection distance.

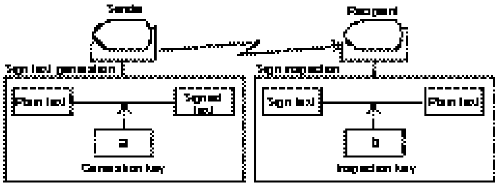
Q7 **Which is the correct explanation of the role played by a DNS server?**

A. Dynamically allocates the IP address to the client.
B. Relates the IP address to the domain name and host name.
C. Carries out communication processing on behalf of the client.
D. Enables remote access to intranets.

Q8 **To use E-mail on the Internet, the two protocols SMTP and POP3 are used on mail servers. Which is the appropriate explanation of this?**

A. The SMTP is a protocol used when one side is client, and POP 3 is a protocol used when both sides to transmit are mail servers.
B. SMTP is the protocol for the Internet, and POP3 is the protocol for LAN.
C. SMTP is the protocol used under normal circumstances when reception is possible, and POP3 is the protocol for fetching mail from the mailbox when connected.
D. SMTP is a protocol for receiving, and POP3 is a protocol for sending.

Q9 **The illustration shows the structure of an electronic signature made by public key encryption. Which is the appropriate combination for "a" and "b"?**



	a	b
A	Recipient's public key	Recipient's private key
B	Sender's public key	Sender's private key
C	Sender's private key	Recipient's public key
D	Sender's private key	Sender's public key

Q10 **The Caesar cipher system is an encryption method in which an alphabetic letter is substituted by a letter located "N" places away. If "abcd" is encrypted with N=2, we get "cdef." What is the value of N, if we receive the Caesar encrypted "gewl" and decode it as "cash"?**

A. 2 B. 3 C. 4 D. 5

Q11 **Which of the following <u>operation methods is NOT appropriate</u> for use with a computer system used with public telephone network?**

A. If a password is not modified within a previously specified period of time, it will no longer be possible to connect using this password.

B. When there is a request for connection, a callback will be made to a specific telephone number to establish the connection.

C. To ensure that the user does not forget the password, it is displayed on the terminal at the time of log on.

D. If the password is entered wrongly for a number of times determined in advanced, the line will be disconnected.

Q12 **What is the item used for detection and extermination of virus infections in connection with already-known computer viruses?**

A. Hidden file B. Screen saver C. Trojan horse
D. Michelangelo E. Vaccine