1 Protocols and Transmission Control

Chapter Objectives

In network systems using computers, communication is conducted based on common protocols. Network architecture is necessary in order to define and regulate these protocols. When actual communication is performed, transmission controls containing various transmission procedures are used.
This chapter will provide the reader with an overview of network architecture and its significance for learning about transmission control procedures.

① Understanding the necessity of network architecture, standardization, types of architecture, and de facto standards, etc.
② Obtaining an overview and understanding of the representative network architectures, i.e. OSI and TCP/IP, their hierarchical structuring, the role played by each layer of the hierarchy, etc.
③ Learning about the mechanisms of transmission controls, and understanding the representative transmission control procedures such as "Basic Mode Link control" and "HDLC procedure."

Introduction

The open network connectivity has progressed in a great deal together with the spread of the Internet and Intranet. Constructing open network systems that allow communications with other organizations is not simply a matter of connecting different hardware from different manufacturers via transmission media.

When building network systems, it is indispensable to agree on communication protocols on which communications will be based. The communication protocols vary with the computer systems and communication lines, and many different protocols have been adopted both in Japan and abroad, ranging from vendor-specific types to types standardized by public organizations. Together with the increase in systems connected with other network systems, such as the Internet, network architecture is becoming of even more importance.

(1) Communication protocols

A communication protocol is a set of rules to enable communication. When you communicate by telephone or by letters, there are predetermined rules you follow to enable communication. Conversely, you can say that if both parties observe the rules, reliable communication becomes possible.
As data communication also involves communication with other parties (the destinations of the transmitted data) via communication lines, certain rules (communication protocols) for the communication are required, and when these rules are observed, reliable communication becomes possible.

(2) Network architecture

Network architecture is the underlying structure of a network, and it specifies system design logically not only for protocols, but also for message formats, codes, and hardware. However, earlier network architectures were of a closed nature in most cases. Since a number of vendor (hardware manufacturers) specific network architectures (like IBM's SNA, etc.) could form their proprietary networks, there were many networks unable to interoperate with networks based on different network architectures.

On this background, the International Organization for Standardization (ISO) proposed and standardized the so-called OSI (Open Systems Interconnection) network architecture as an internationally standardized network architecture, which is independent from vendor-specific factors. Even if it is not an international standard, the TCP/IP (Transmission Control Protocol/Internet Protocol), employed as the standard protocol for the Internet, is widely used and has become the de facto industry standard for data transmission.

Based on the situations outlined above, in this chapter you will learn about the significance, purpose and indispensability of network architecture through learning about communication protocols (mainly OSI and TCP/IP).

1.1 Network Architecture

According to the JIS (Japanese Industrial Standard) definition, "network architecture" is the "logical structure and operating principle of a network system." However, this is a very abstract definition. So let us first look at the birth of network architecture to gain an understanding of its significance. Then we will move from an overview to an explanation of the detailed components of network architecture.

1.1.1 The Background of the Birth of Network Architecture

Earlier network systems were "host-centric systems," i.e., the host computer determined what terminals and peripheral equipment should be used. The normal situation was that the host computer manufacturer was the pivotal point in the construction of systems. The systems themselves were also constructed to comply with the requirements of the each application.

However, the following issues have been raised.

- In the case of "host-centric systems," it is difficult to reconfigure or extend systems even with the same vendor systems environment.
- With the increasing complexity and increased number of systems, the development costs related to communications network have become greater and greater.
- As the structure of software increases its complexity, communication software faces scalability challenge in support of ever increasing number of terminal connections.
- The borders between hardware and communication control and application functions have become blurred.

The downsizing, movement has accelerated the transition from "host-centric systems" to "distributed systems," and the necessity for building multivendor systems environment using open systems became important factors for the birth of network architecture.

As a matter of fact, the trend toward open systems has been accelerated by the proliferation of the Internet on a worldwide scale, and this requires that computers can be connected regardless of the manufactures or the employed applications. Accordingly, it can be expected that the necessity of network architecture, which prescribes the logical structure and operating principles of network systems and defines the communication protocols required for real-world data exchange, will increase further in the future.

1.1.2 Outline and Standards of Network Architecture

(1) What is network architecture?

The meaning of network architecture was touched upon in abstract terms above, and we will now proceed to look at the contents in more specific terms.

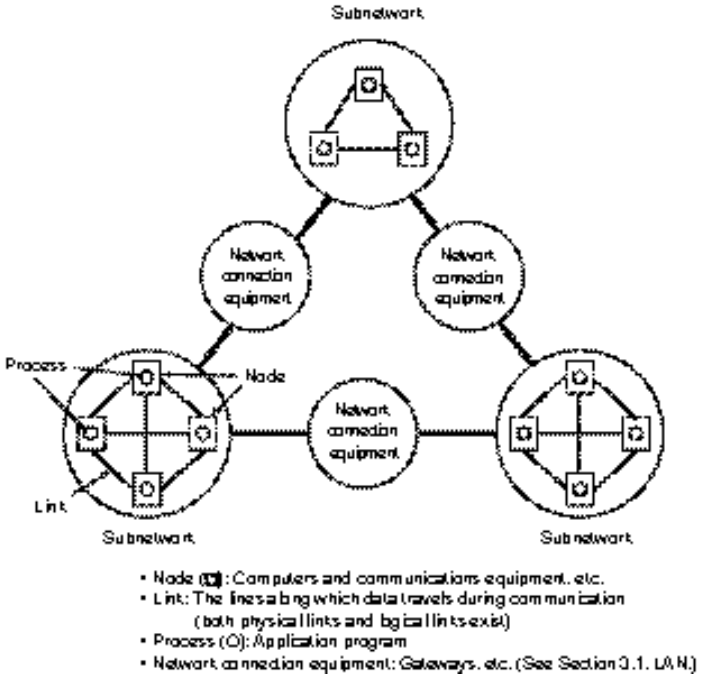
Network architecture defines and classifies all the functionalities (connector and access control methods, etc.) required for data transmission. Additionally, it determines "hierarchical structures" according to each classification and specifies protocols and interfaces between layers of the hierarchical structure. By establishing system structure using those determined interfaces and protocols, it enables effective operation of network systems.

(2) Logical network

Within the network architecture, all the network's physical elements (equipment and programs, etc.) are modeled and structured and treated as a logical network. More specifically, the main components of the logical network are:

- "node," i.e., hardware, such as computers and communication processing equipment,
- "link," i.e., communication lines,
- "process," i.e., application programs.

Figure 1-1-1
Logical network



In the logical network, the subnetworks linking the nodes (computers, etc.) are tied together by network connection equipment (gateways, etc.) as shown in Figure 1-1-1.

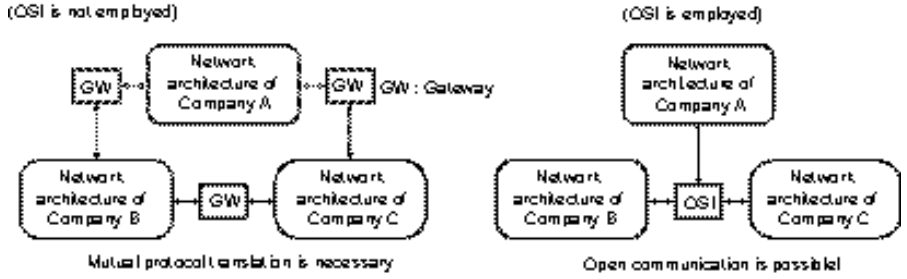
(3) Standardization of network architecture

Standardization of network architecture yields the following benefits.

- If the architecture is the same, a system can be built by adjusting the interfaces even when products from different manufacturers are combined. Earlier, system building was manufacturer-driven but the standardization of network architecture has made it possible for users to employ the products that best suit their purpose. (Multi-vendor system building)
- Employing a system compliant with standard interfaces makes it easy to develop, expand and maintain the system.
- Even independently developed systems can be easily integrated, which provides large effect especially on building distributed systems.
- The entire network can be treated logically (logical network); for example, no matter what type of the network system is, it will not affect the structure, etc.

Figure 1-1-2 compares the employment of a typical standard network architecture (OSI) versus a non-standard type.

Figure 1-1-2 OSI employed/not employed

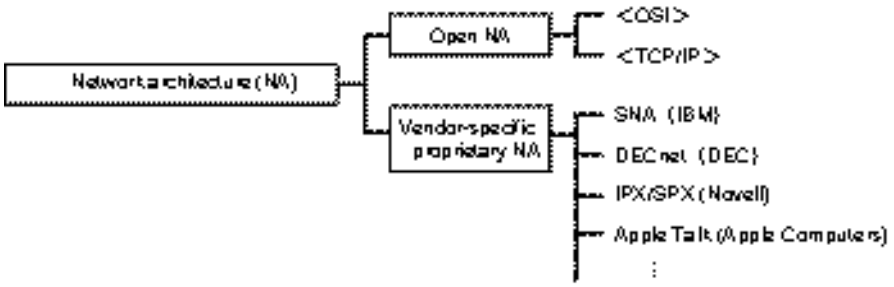


As shown in Figure 1-1-2, communication is not possible without the translation of protocols unless a standard architecture like OSI is employed.

1.1.3 The Types of Network Architecture

There are a number of network architectures, including vendor-specific architectures (IBM's SNA, etc.), internationally standardized architectures, as well as de facto standards. Among all these, the representative network architectures are OSI (Open Systems Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol).
Figure 1-1-3 shows various network architectures.

Figure 1-1-3 Types of network architectures



1.1.4 De Facto Standards

Network architectures include some typical architectures like TCP/IP and OSI. However, unlike OSI, TCP/IP is not an architecture established by ISO or similar standardization organization. TCP/IP is employed for the world's largest network, the Internet, and it is also a standard characteristic of UNIX, the main operating system for workstations and servers. In other words, it has become an industrial de facto standard.

The relations between TCP/IP and OSI are explained in Section 1.3 TCP/IP.

1.1.5 Network Topology and Connection Methods

(1) Network topology (the connection configurations of networks)

Connecting computers and terminals, etc. through communication lines makes it possible to create a variety of network configurations in accordance with the scale and purpose of use.
Typical network configurations are shown in Figure 1-1-4.

① Ring type

The ring type is a configuration in which the nodes (computers, etc.) are connected in a closed loop by communication lines. The transmission lines are short in this kind of network configuration and easily controlled. The drawback is that if just one node fails, it might affect the entire network.

② Mesh type

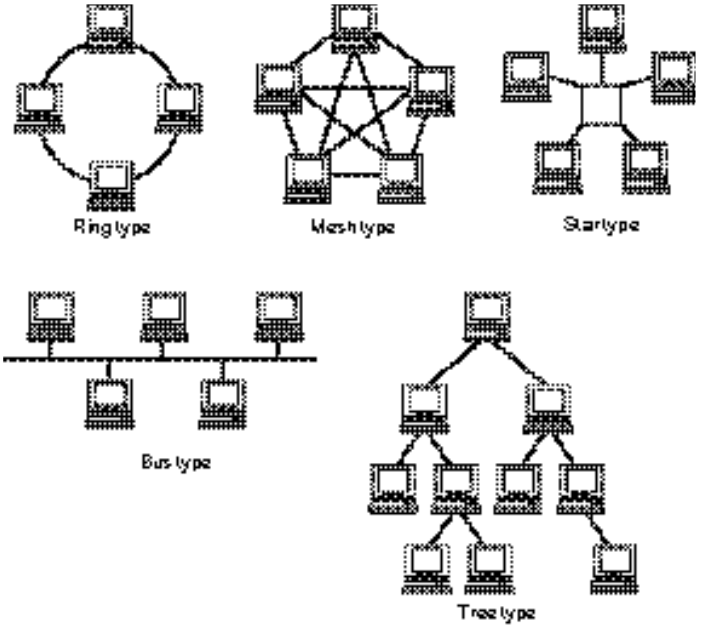
In the mesh type, two or more paths lead to each node so that the overall structure becomes that of a mesh. This means that even if a node fails, that node can be bypassed by routing (selection of communication path), meaning that the reliability of this type of network is very high.

③ Star type

In the star type, each node is connected to a central node (line concentrator, etc.) in a star-shaped configuration.

Even if one node fails, this will have no effect on the overall system, but if the central node fails, the entire network will no longer be functional.

Figure 1-1-4
Network topology



④ Bus type

In the bus type, all nodes are connected to a common communication line.
The bus configuration makes it easy to add or remove nodes without affecting the overall system and at the same it is economical. However, when there are many nodes and the traffic load (the information load carried in a specific interval) increases, data collisions may occur on the common communication line and the transmission efficiency (throughput) may deteriorate suddenly.

⑤ Tree type

In the tree type, several child nodes are connected to a parent node. This configuration is also called a cascade connection.
Recently, this configuration has become more widely adopted, but if the parent node is malfunctioning it will affect all the subordinate nodes.

(2) Line connection methods (methods for connecting networks)

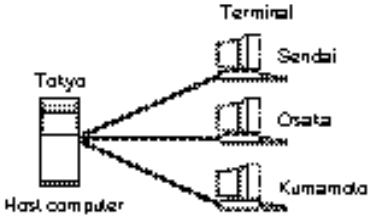
To ease understanding, we will use a simple network with one central computer connected by several terminals through communication lines as an example for explaining the methods for connecting networks. There are three typical connection methods that are used in accordance with what best suits the communication distance and data load, etc. These are:

- Point-to-point connection
- Multipoint connection
- Switched connection

① Point-to-point connection

In the point-to-point connection, the computer is connected one-to-one to each terminal through leased communication lines.
This configuration is appropriate if the heavy data traffic between two points is required but it is uneconomical if the data traffic is not heavy enough. As the number of terminals are increased, the same number of communication lines will also have to be added.

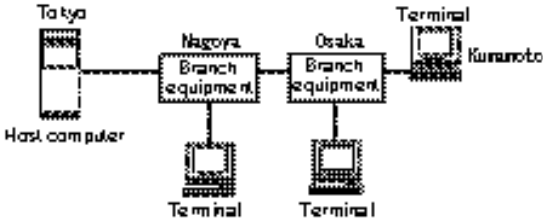
Figure 1-1-5
Point-to-point connection



② Multipoint connection (multi-drop system)

In the multipoint connection, multiple branching devices are connected sequentially to the same communication line. Terminals are then connected to the branching equipment.
This configuration allows construction of a network that is cheaper than using the point-to-point configuration when the communication distance is long and the data traffic is light. However, since the main communication line is shared, other terminals have to wait while one terminal is transmitting data.

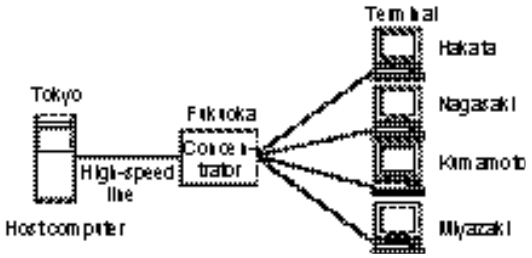
Figure 1-1-6
Multipoint configuration



③ Concentration connection

In the concentration connection, the lines from several terminals are connected to a concentrator, which is connected to the host computer through a high-speed line. (Figure 1-1-7).
This can be the same communication method as that employed by the point-to-point configuration in which each terminal is separately connected to the host computer. However, the cost of leased lines is smaller than in the case of the point-to-point configuration allowing for economical network construction but attention has to be paid to the capacity of the line between the host computer and the concentrator. In other words, the data load from each terminal connected to the concentrator must be taken into consideration to design network.

Figure 1-1-7
Concentration configuration



1.2 OSI – Standardization of Communication Protocols

This section gives an overview of the internationally standardized network architecture OSI (Open Systems Interconnection) established by the ISO (International Organization for Standardization) and explains the roles of the layers of this model and relations with headers, etc.

1.2.1 Overview of OSI

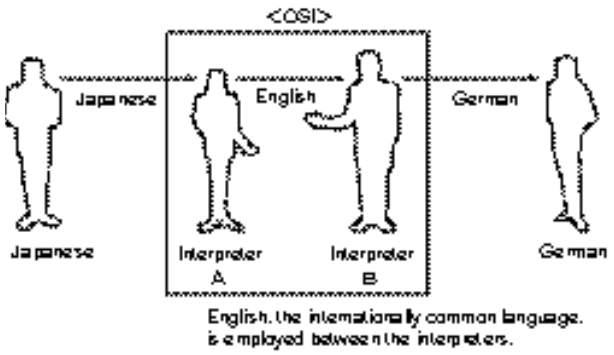
(1) OSI as an international standard

OSI is an international standard established primarily by the ISO and ITU-TS (International Telecommunication Union-Telecommunication Standardization Sector). In other words, OSI is manufacturer-independent, international standard network architecture.

(2) The role played by OSI

The role that OSI plays is outlined in Figure 1-2-1.
Let us assume that the Japanese person only can speak Japanese, and that the German can only speak German. If these two persons have to work together, how can communication and conversation be carried out between the two?

Figure 1-2-1 Communication between a Japanese and a German



Interpretation has to be done to act as a bridge and allow communication between the two. English or another internationally common language is employed for the interpretation. The role played by the common language is the role that OSI plays in network architectures.
In other words, no matter what kind of software is running on a network, and regardless of what kind of data is transmitted, problem-free data communication will be possible on the OSI compliant network.

(3) Hierarchical structuring

When several different networks have to be connected, communication functionalities become complex, manifold and intertwined. Gaining an overview is facilitated by grouping the functionalities in a hierarchical structuring. OSI came up with this idea, and the OSI model comprises 7 layers. The actual contents of the 7 layers (protocol hierarchy) are explained in detail in Section 1.2.2.
When summing up the merits of layering, we get the following:

- Even if the protocol of one layer is modified, it has not effect upon the other protocols meaning that development can be done easily.
- Lower order layers can be treated as black boxes meaning that complicated communication functionalities can be simplified.

Layering is extremely important in network architecture, because considerations must always be given to ensure:

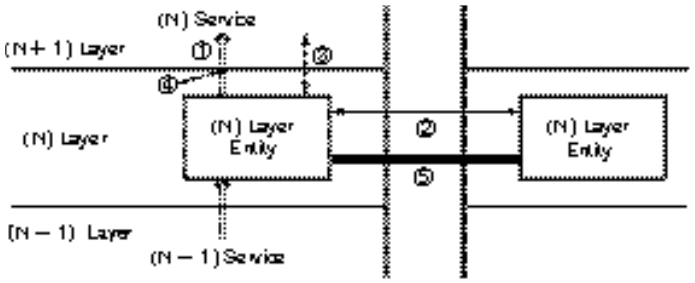
- Horizontalness: Protocols are determined between the same layers.
- Independence: Even if one layer is modified, this does not affect other layers.

In the basic OSI reference model and other open models, each layer is abstracted as "(N) layer," and all its concepts and relations to each of the other layers are grasped logically.

(4) Relations between higher layers and lower layers

To perform communication between open systems, functional modules, such as communication programs called "entities," are required, and two or more entities exist in each (N) layer. The relations between the (N) layer and the higher and lower layers are shown in Figure 1-2-2.

Figure 1-2-2 Relations between (N) layer and higher and lower layers



Using Figure 1-2-2, the relations between the different layers are briefly explained in the following.

① The service, which the (N) layer provides for the layer above (N + 1), is called (N) Service. Normally, the (N) layer integrates the services it receives from the (N-1) layer with its own functionalities and provides this in the form of (N) Service.

② The protocol used between (N) entities is called the (N) Protocol.

③ The action (service) performing the function of exchanging information between the (N) layer and the higher and lower layers, i.e., acting as interface between layers, is called (N) Service Primitive. (There are four primitives, such as "request.")

④ The access point between the layer receiving the (N) Service and the (N) layer is called (N) Service Access Point (SAP).

⑤ The logical communication channel used for the exchange of data between (N) Entities is called (N) Connection.

1.2.2 OSI Basic Reference Model

(1) Structure

Figure 1-2-3 shows the structure of the OSI basic reference model.

Figure 1-2-3 OSI basic reference model

Application layer	7th layer	Provides communication services required for applications
Presentation layer	6th layer	Data representation, format translation and mapping
Session layer	5th layer	Dialog management, synchronization point control, etc.
Transport layer	4th layer	Guarantees data transmission between end-to-end, etc.
Network layer	3rd layer	Routing functions, etc.
Data-link layer	2nd layer	Guarantees data transmission between adjacent systems, error control, etc.
Physical layer	1st layer	Connector and pin shapes, transmission media, etc.

These seven layers can be divided into upper and lower layers as shown in the following.

- Upper layers from the Application layer to the Session layer provides communication service functionalities
- Lower layers from the Transport layer to the Physical layer: Data transmission functionalities

The lower layers mainly ensure high-quality transfer of data, and the upper layers utilize the functions of the lower layers to provide communication services for applications.

(2) The role of each layer

① Application layer (7th layer)

The application layer is the 7th layer and the highest level and deals primarily with providing services such as:

- FTAM (File Transfer Access and Management)
- RDA (Remote Database Access)
- VT (Virtual Terminal)

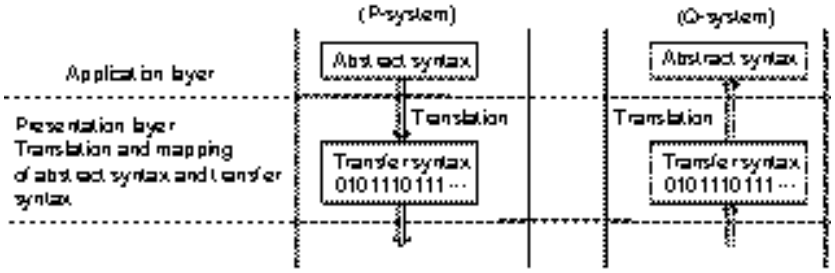
Figure 1-2-4 Primary functions of the application layer

FTAM	File transfer access and management
RDA	Remote database access
VT	Virtual terminal
TP	Transaction processing
MHS	Message handling system

② Presentation layer (6th layer)

The presentation layer is one level below the application layer and performs translation of data formats, etc. to ensure efficient transmission of various types of information. In the upper application layer, description is normally done using the representation system called "abstract syntax" but in order to enable efficient exchange of information between network systems, abstract syntax is translated to a data format (called "transfer syntax") in the presentation layer in which mappings of abstract syntax and transfer syntax, etc. is also taking place. These presentation layer functions allow the application layer to provide services without being conscious of the data encoding and physical representation of the other party's computer.

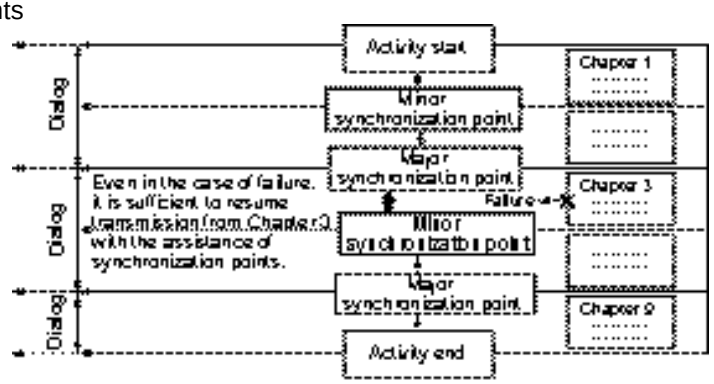
Figure 1-2-5 Translation between abstract syntax and transfer syntax



③ Session layer (5th layer)

The session layer is one level below the presentation layer and primarily performs "dialog management." Dialog management controls and manages the data flow between applications and systems by employing the end-to-end data transfer capabilities provided by the transport layer.
The communication mode can be set freely. In the case of normal communications (E-mail transmission, etc.), for instance, half-duplex transmission (one direction at a time) is employed. In the case of simultaneous two-way communication (as in video conference systems, etc.), full-duplex transmission (both directions simultaneously) is used. By establishing synchronization points, transmission can be restored from a synchronization point in case transmission fails due to one reason or another during the data transmission. Time loss can thus be minimized.

Figure 1-2-6
Synchronization points



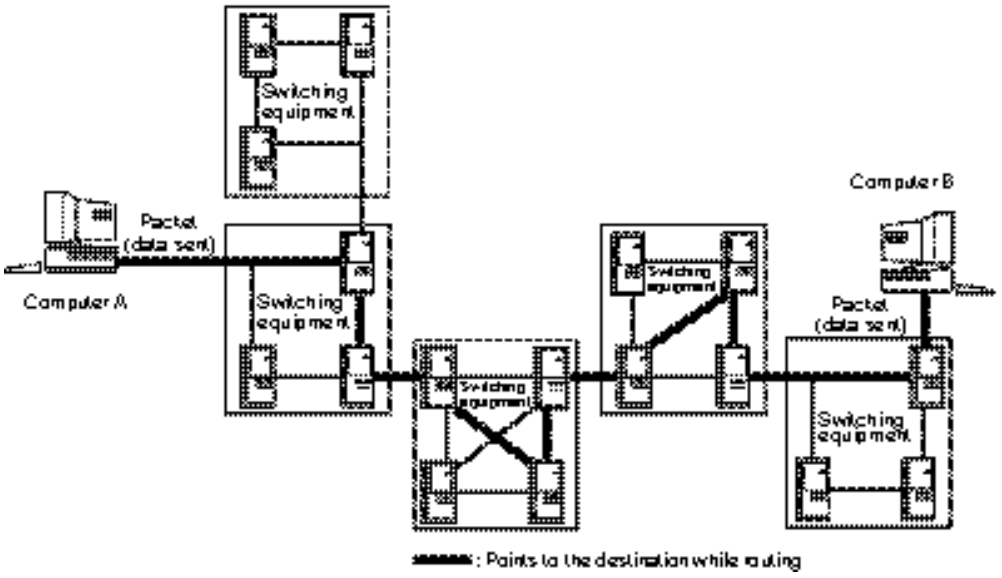
④ Transport layer (4th layer)

The transport layer is one level below the session layer and its function is to guarantee the quality of data transfer between system ends (from end-to-end). Accordingly, if the quality of the services provided by the layers below is insufficient, the transport layer compensates for the lower quality by additional error detection and recovery.

⑤ Network layer (3rd layer)

The network layer is one level below the transport layer and is concerned primarily with path selection (routing) and relays. The ITU-T recommendation X.25 (see Section 1.5.2 X-series) packet level protocol is well known.

Figure 1-2-7
Routing function



While the transport layer one level above guarantees the data transmission between system ends, this layer is concerned with selecting the most appropriate paths and ensures "transparent" data transmission.

⑥ Data-link layer (2nd layer)

The data-link layer is one level below the transport layer and ensures transparent and error-free data transmission.
In general, the roles of the data-link layer comprise transmission controls, such as HDLC (High-level Data Link Control), establishment of data-link connection, error control (CRC (Cyclic Redundancy Check), coding, etc. (For details on transmission control procedures, see Section 1.6 Transmission control.)
In LAN (Local Area Network), this layer is also concerned with access controls, such as CSMA/CD (Carrier Sense Multiple Access/Collision Detection) and token passing, and logical link controls, such as LLC (Logical Link Control), etc.

⑦ Physical layer (1st layer)

The physical layer is one level below the data-link layer and transmits electric signals ("0" and "1") using transmission media (twisted pair cables or coaxial cables, optical fiber cables, etc.)
Some of the actual DCE (Data Circuit terminating Equipment) and DTE (Data Terminal Equipment) interfaces are:

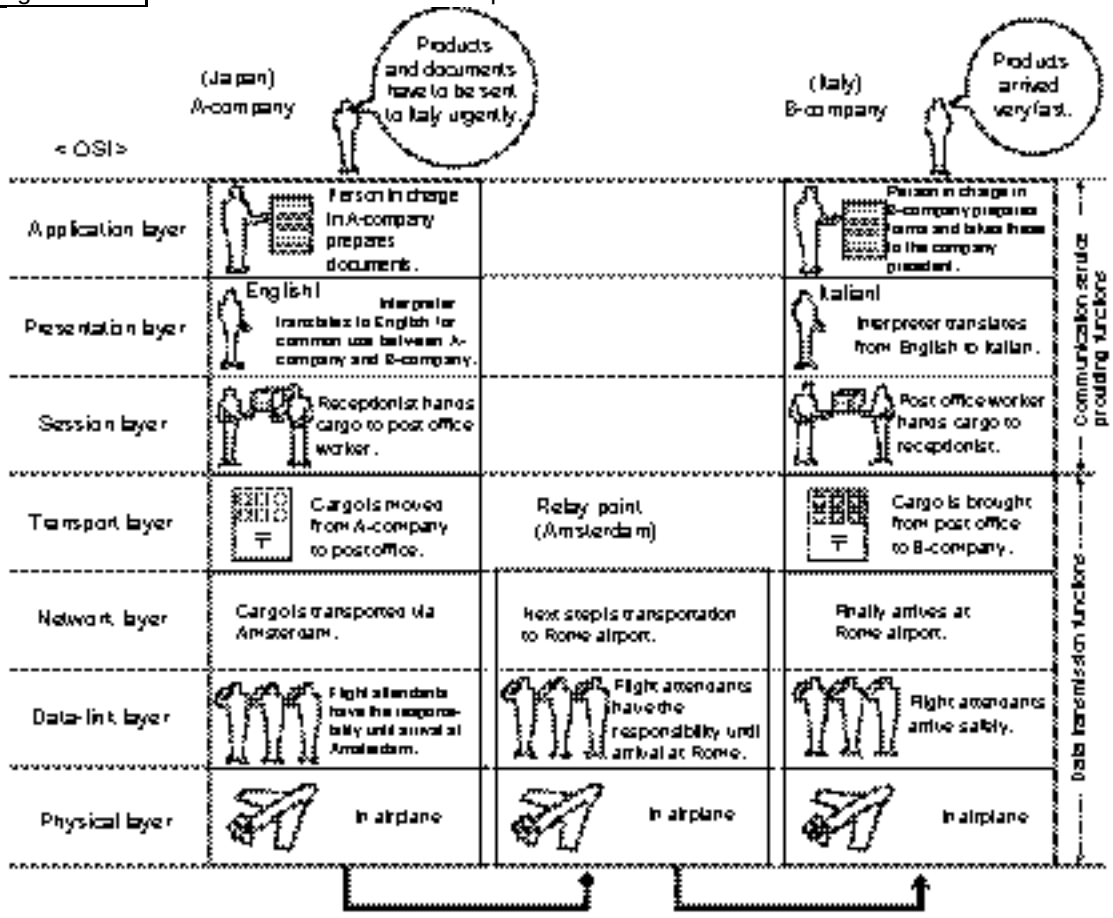
- ITU-T recommendation X-series: X.21 and others; defines the shape of connectors and pin array, etc.
- V-series: V.24 and others, defines modems, etc. for use with analog lines
- ISDN (Integrated Services Digital Network) terminal interface I-series: defines TA (Terminal Adapter), etc.

For details on the interfaces, see Section 1.5 Terminal Interfaces.

1.2.3 Communication Procedures in OSI

Figure 1-2-8 likens OSI with the steps involved in transactions between a Japanese and an overseas company.

Figure1-2-8 Transactions between companies

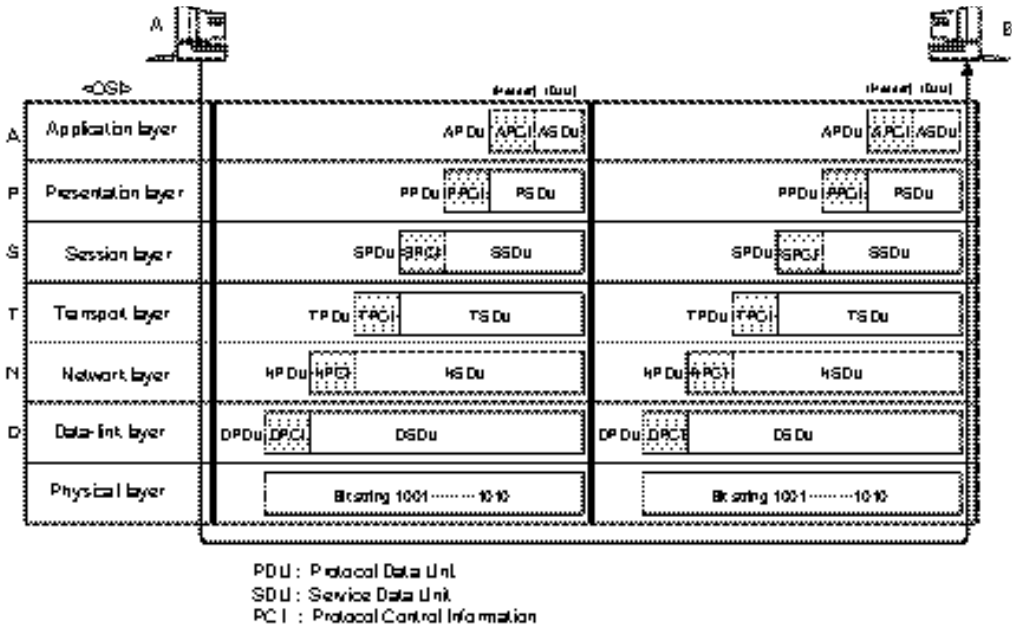


When communication is carried out using OSI in reality, the following procedures are carried out.

1. When a request for communication is issued, the communication channel is secured first of all (establishment of connection).
2. When the data passes through each layer at the sender side, headers (control information) are attached to the user data before the data is sent onward.
3. When the data passes through each layer at the receiver side, headers are removed sequentially.
4. When data transmission is completed, the communication channel is closed (connection is disconnected).
5. Communication resources are released and the process is completed.

The headers attached by the (N) layer are called (N)-PCI (Protocol Control Information), and (N) layer user-data is called (N)-SDU (Service Data Unit). The data combined by both of them is called (N)-PDU (Protocol Data Unit). I.e., (N)-PDU is supported by (N-1)-SDU (Figure 1-2-9).

Figure 1-2-9 Relations between headers and layers



1.3 TCP/IP – The De Facto Standard of Communication Protocols

TCP/IP has become the de facto standard protocol for the world's largest network, i.e., the Internet. This section gives an overview of and explains the hierarchical structure and roles played by each layer of the protocol while comparing it with the OSI model.

1.3.1 Overview of TCP/IP

(1) What is a TCP/IP?

TCP/IP (Transmission Control Protocol/Internet Protocol) has become the standard protocol for the Internet. Due to the worldwide spread of the Internet, TCP/IP has become the de facto standard network protocol. There is a close relationship between the TCP/IP and the Internet, and the historical background for this is explained in details in Section 3.2.1 The Historical Background of the Development of the Internet.
TCP/IP was developed as part of ARPANET (explained later) in the 1970s, and it is a stack of flexible protocols that ensure high reliability and high speed transmission. This stack of protocols is comprised of the "TCP protocols" and the "IP protocols") but normally the TCP/IP protocol is taken to refer to the protocols that define the communication mode used on the Internet. (Sometimes it is also referred to as the "TCP/IP protocol architecture" or the "TCP/IP protocol suite.")

(2) Hierarchical structure

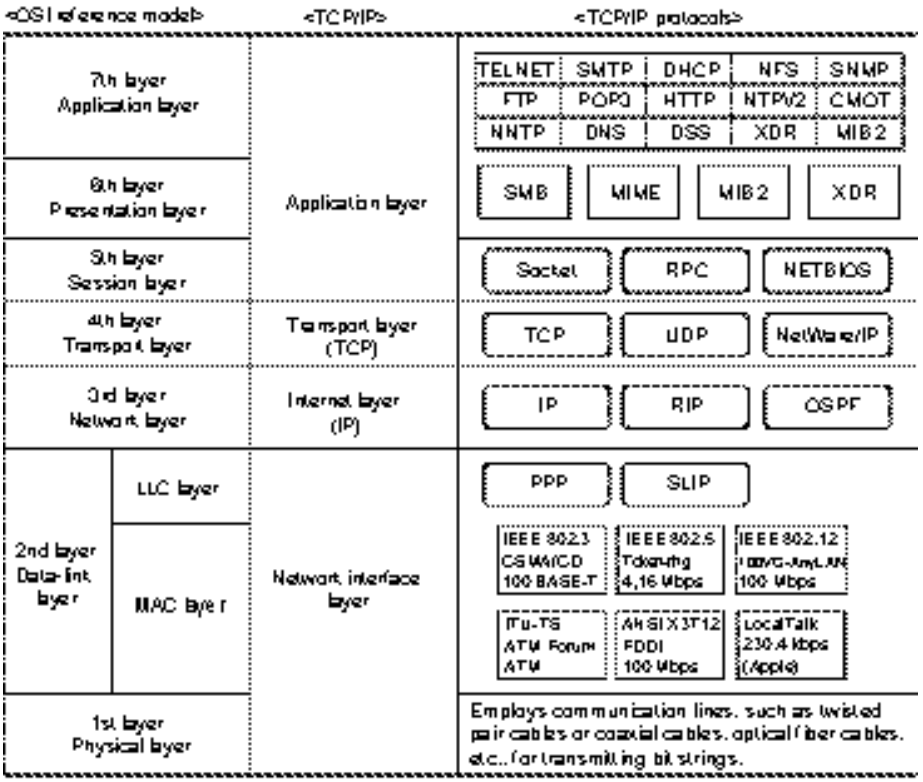
As the OSI model, the TCP/IP also has a hierarchical structure. Basically, it is constructed from the four layers shown below, with each layer containing several protocols (hierarchical protocol).

- Application layer
- Transport layer
- Internet layer

- Network interface layer

Comparison between OSI and TCP/IP is show is Figure 1-3-1.

Figure 1-3-1 Comparison of the hierarchical structures of TCP/IP and OSI



TCP and IP are both important protocols, each having the following functions.

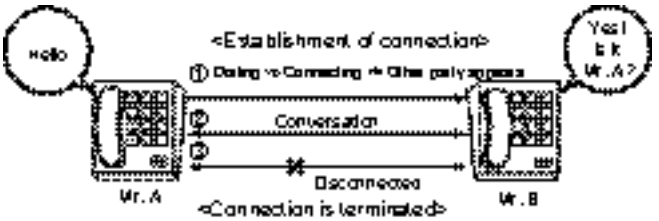
- TCP (transport protocol; connection-oriented mode) = ensures high reliability
- IP (Internet protocol; connectionless mode) = ensures high-speed data transmission.

The connection-oriented and connectionless modes are explained briefly in the following.

① Connection-oriented mode (TCP)

The connection-oriented mode requires a direct connection (logical channel) to be established between the sender and the recipient before data is transmitted. Data is transmitted through this channel to arrive at the target terminal. When the transmission is completed, the connection is disconnected. The establishment of the connection results in communication with high reliability.
The workings are shown in Figure 1-3-2, using telephones as examples.

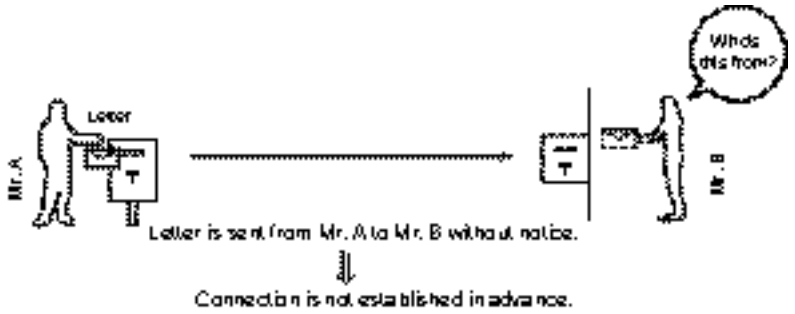
Figure 1-3-2 Connection-oriented image (telephone)



② Connectionless mode (IP)

The connectionless mode skips the establishment of a direct connection and reservation of a communication channel before data is transmitted, meaning that there is no guarantee that the data will reach the other party. On the other hand, it enables high-speed data transmission. Accordingly, it is a precondition for use of the connectionless mode that communication takes place on a highly reliable communication line in order to raise the probability that the data reaches the other party.
The workings are shown in Figure 1-3-3, using postal mail as an example.

Figure 1-3-3 Connectionless image (postal mail)



As shown above, a role is allotted to each of TCP and IP in the TCP/IP model to enable highly reliable and high-speed transmission on the Internet. I.e., TCP ensures highly reliable data transmission, so that this function can be omitted by IP, which results in high-speed data transmission.

(3) The roles of each layer

① Application layer

The application layer is the highest level and is concerned with services related to user applications. Services on the Internet are made possible by the protocols of this layer.
The key protocols are indicated below. (For details, see Section 3.2, The Internet.)

- DNS (Domain Name System): A protocol matches domain names and IP addresses.
- HTTP (Hyper Text Transfer Protocol): A protocol for transmitting files in the HTML markup language.
- FTP (File Transfer Protocol): A protocol for transmitting files.
- SMTP (Simple Mail Transfer Protocol): A protocol for transmitting simple mail.
- POP3 (Post Office Protocol Version 3): A protocol for receiving mail from mail servers.
- NNTP (Network News Transfer Protocol): A protocol for transmitting network news.
- TELNET (TELecommunication NETwork): A protocol that enables log on to a remote terminal.
- SNMP (Simple Network Management Protocol): A protocol for management of simple networks.
- DHCP (Dynamic Host Configuration Protocol): A protocol for automatic setting of IP addresses.

② Transport layer

The transport layer is one level below the application layer and its function is to provide the service for data transfer between system ends (end-to-end).
The following two protocols ensure reliability and high speed.

- TCP: Ensures high reliability.
- UDP: (User Datagram Protocol): Instead of ensuring high reliability this protocol ensures high speed.

As mentioned earlier, the mode of the TPC protocol is the connection-oriented but the UDP protocol is connection-less. Which of the two protocol should be used is determined by the higher level application layer. TCP is appropriate when a large amount of data should be transmitted sequentially, and UDP is appropriate when small size data (packet) is transmitted intermittently.

③ Internet layer

The Internet layer is one level below the transport layer and its function is to provide routing (selection of communication path) and relaying capabilities for data transmitted via networks, such as the Internet.
The IP protocol plays an extremely important role in this layer, as it affixes IP headers (control information) and sends IP datagrams (data information unit used in TCP/IP) from sender to recipient. At this point, the other party is recognized through the IP address (described later) contained in the IP header, and the optimal routing is carried out to send the data to the recipient.
The following protocols are employed for routing.

- RIP (Routing Information Protocol): Protocol containing information for selection of the communication route.

- OSPF (Open Shortest Path First): Protocol that offsets the defects of RIP.

④ Network interface layer

The network interface layer is one level below the Internet layer and performs error-free transparent transmission of any kind of data.
The TCP/IP network interface layer is a layer that combines the functionalities performed by the physical layer and data-link layer of OSI. For convenience' sake, OSI Reference Model's data-link layer is divided into the LLC layer (Logical Link Control) and the MAC layer (Media Access Control) groups of protocols.
Three protocols are described in the following.

- SLIP (Serial Line Internet Protocol)
  SLIP is a protocol for point-to-point connection using public lines (telephone lines, etc.) and measures against failures and error control are handled by higher-level layers.
- PPP (Point to Point Protocol)
  PPP is a protocol that basically performs the same functions as SLIP but is designed to provide improved functions in terms of management, etc.
- ARP (Address Resolution Protocol)
  ARP is a protocol for mapping IP addresses to MAC addresses (MAC layer addresses are described later).

1.3.2 Communication Procedures in TCP/IP

The communication procedures in TCP/IP are the same as those taking place in OSI.

1. When a request for communication is issued, connection is established.
2. On the sender side, headers (control information) are affixed to the user data when it passes through each layer before the data is sent out.
3. On the receiver side, headers are sequentially removed as the data passes through each layer.
4. When transmission of the data is completed, the connection is disconnected.
5. The communication resources are released and the session is completed.

1.4 Addresses Used for TCP/IP

Addresses are used to specify the destination node, etc. when transmission is conducted.
TCP/IP uses the following two types of addresses to specify the transmission destination.

- IP address (logical address)
- MAC address (physical address)

1.4.1 IP Address

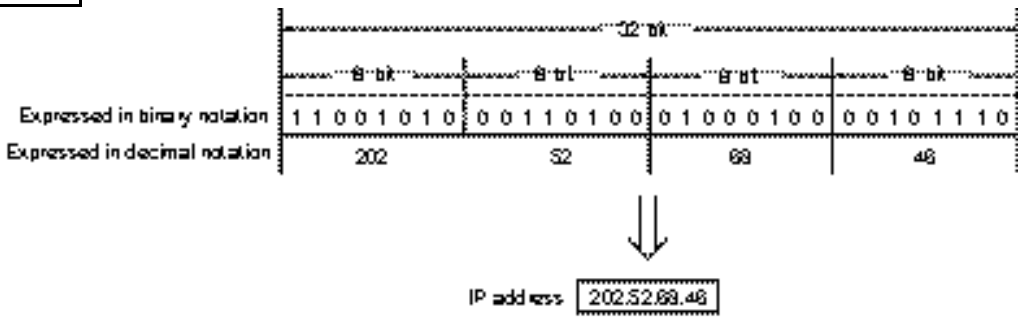
(1) What is an IP address?

Computers connected on the Internet are assigned a 32-bit IP (Internet Protocol) address. Because IP address under no circumstances must be duplicated, the Network Information Center (NIC) has been put in charge of worldwide, centralized management and allocation of IP addresses. In Japan, Japan Network Information Center (JPNIC) is in charge of domestic allocation of IP addresses. This means that an IP address must be obtained from JPNIC when you plan to construct a network for which it is a prerequisite to be connected to the Internet.
IP addresses are allocated after consideration of the scale of a network, etc.

(2) IP address classes

Figure 1-4-1 shows the structure of IP addresses.

Figure 1-4-1 Structure of IP addresses



The two parts of an IP address show the following:

- Network address part: Which network the IP address belongs to
- Host address part: The address of the computer

IP addresses are grouped into the following four classes A to D in accordance with contents and size of the network address parts and host address parts.

Figure 1-4-2 IP addresses (Class A to Class D)

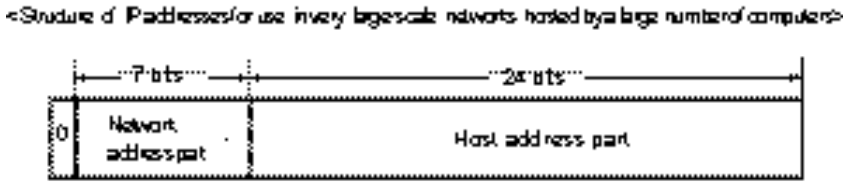
	Adaptive network scale	No. of networks applicable to	No. of host addresses allocable per network
Class A	Large	Few	Many
Class B	↓	↓	↓
Class C	Small	Many	Few
Class D	(Only used for special communication modes)		

IP addresses in which the 32 bits are all "0" or "1," and the network part is "127" are only used in special cases and is not normally used.

① Class A

Class A is for use in very large-scale networks. Figure 1-4-3 shows the structure of Class A.

Figure 1-4-3 Class A structure

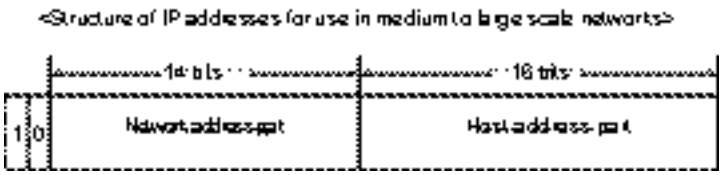


- Leading bit: "0"
- Network address part: 7 bits
- Host address part: 24 bits
- No. of networks for which allocable addresses are available: 126
- No. of host addresses available for allocation to one network: 16,777,214

② Class B

Class B is used for large and medium sized networks, in which the shortage of available addresses is becoming a serious issue. Figure 1-4-4 shows the structure of Class B.

Figure 1-4-4 Class B structure

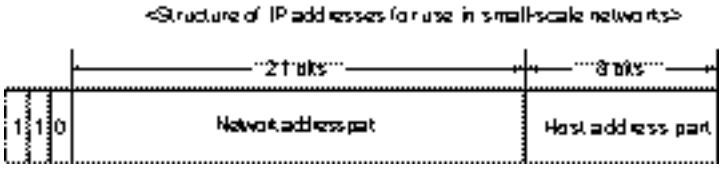


- Leading bit: "10"
- Network address part: 14 bits
- Host address part: 16 bits
- No. of networks for which allocable addresses are available: 16,382
- No. of host addresses available for allocation to one network: 65,534

③ Class C

Class C is used for comparatively small-scale networks in which the number of hosts are smaller than in Class A and B.
Figure 1-4-5 shows the structure of Class C.

Figure 1-4-5 Class C structure

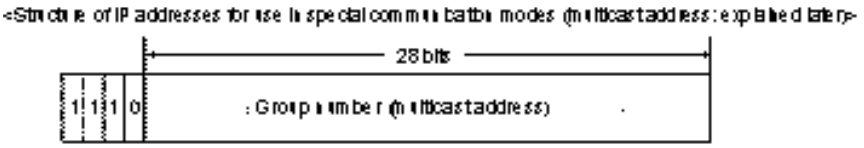


- Leading bit: "110"
- Network address part: 21 bits
- Host address part: 8 bits
- No. of networks for which allocable addresses are available: 2,097,150
- No. of host addresses available for allocation to one network: 254

④ Class D

Class D addresses do not contain the host address part and are only used for special communication modes.
Figure 1-4-6 shows the structure of Class D.

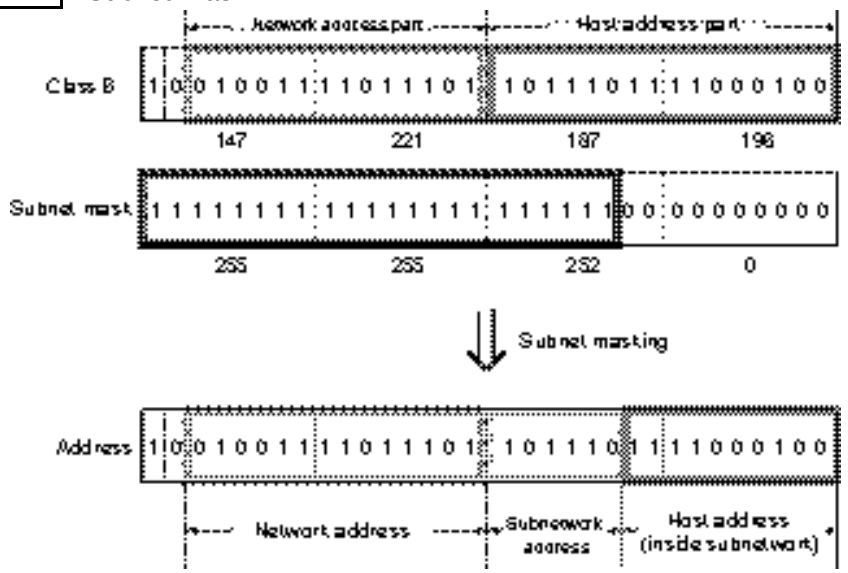
Figure 1-4-6 Class D structure



(3) Subnet mask

Subnet mask is a technique born out of the necessity for effective use of IP addresses as the number of available addresses are becoming scarce.
In the case of a Class B address, for example, the maximum number of host addresses that can be allocated to one network is 65,534. However, currently it is difficult to imagine a network comprising such a large number of computers. The subnetwork address is therefore used to increase the number of network addresses by only using a part of the host address. The method used for this is called "subnet mask." In other words, the subnet mask indicates the range of the network address and subnetwork address. To be more specific, the subnet mask indicates the network address part as "1" and the host address part as "0," as shown in Figure 1-4-7.

Figure 1-4-7 Subnet mask



In this way, even if the network address is the same, the subnetwork addresses will be different and form a completely separate network and IP addresses can thus be allocable to extended number of users.

(4) Special IP addresses

Some IP addresses have special meanings. These are:

- Network addresses
- Broadcast addresses
- Multicast addresses

① Network addresses

Network addresses are addresses in which the host address part of the IP address consists entirely of 0, and it is appropriate to think of these as network nameplates.

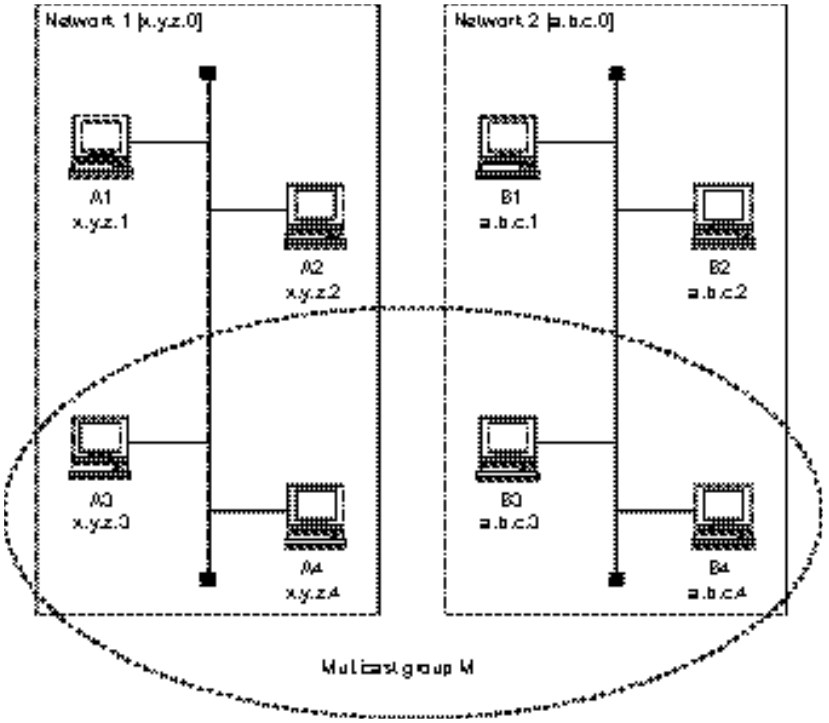
② Broadcast addresses

Broadcast addresses are addresses in which the host address part of the IP address consists entirely of 1. These addresses are used for broadcasting data to all the nodes belonging to a network, etc. In contrast to what a broadcast address is used for, an address used to send to a specified node only is called a "unicast address."

③ Multicast addresses

Multicast addresses are used for sending data to all the nodes belonging to a specific group. A Class D IP address is used for identifying the specific group (multicast group).
In Figure 1-4-8, a Class C IP addresses are used in Network 1 and 2.
Consequently, the host address parts (lower-order 8 bits) consist entirely of 0, i.e., "x.y.z.0" and "a.b.c.0," but these are the network addresses of the respective networks.
Conversely, when a host address part consists entirely of 1, i.e., "x.y.z.255" and "a.b.c.255," this is the broadcast address. When data is addressed to this address (tentatively "x.y.z.255,") the data is transmitted to all the nodes (A1 to A4) belonging to this network (Network 1 in this example).
Conversely, if you only want to send data to B2, for example, a unicast address such as "a.b.c.2" is used.
A multicast address is used to send data to all the nodes (A3, A4, B3, B4) belonging to the multicast group M.

Figure 1-4-8
Special IP addresses



1.4.2 MAC Addresses

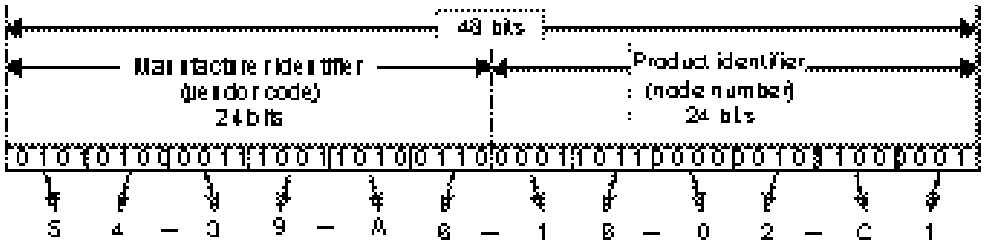
(1) What is a MAC address?

IP addresses are used to distinguish the nodes connected to a network. However, the IP address identification takes place on the Internet layer of the TCP/IP protocol. Consequently, an address that is capable of performing identification on the network interface layer (one level below the Internet layer) is required to carry out physical communication. This is the MAC (Media Access Control) address.

(2) The structure of the MAC address

The MAC address is a 48-bit address allocated to each piece of hardware (LAN port: Device used for connecting to the network).
Figure 1-4-9 shows an example of a MAC address structure.

Figure 1-4-9 Example of MAC address structure



The MAC address consists of:

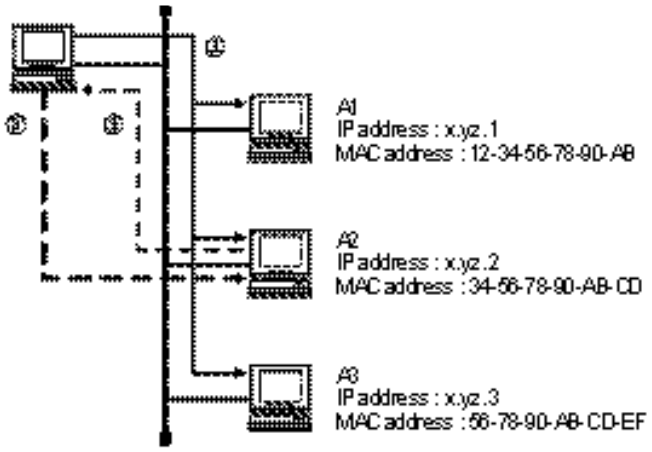
- Manufacturer identifier: ID number specific to the manufacturer
- Product identifier: ID number specific to the hardware and attached by the manufacturer

The MAC address is expressed in hexadecimal notation with each byte separated by "–" or ":." For example, the address in Figure 1-4-9 can be expressed as "54 – 39 – A6 – 1B – 02 – C1" or "54 : 39 : A6 : 1B : 02 : C1."

(3) ARP (Address Resolution Protocol)

In the TCP/IP model, the IP address is used as the address for the recipient of the transmission. However, in order to actually deliver data to the recipient within the network, the recipient's MAC address must be specified. It is therefore necessary to map the IP address to the MAC address. ARP plays the role of this mapping.
ARP is a protocol for converting the IP address into the MAC address, and the actual arrangement is shown in Figure 1-4-10.

Figure 1-4-10 ARP mechanism



① The ARP packet including the recipient IP address (x.y.z.2) is sent to all the nodes by broadcasting.
② The node (A2) having the recipient IP address included in the ARP packet returns its unique MAC address (34-56-78-90-AB-CD) to the sender.
③ Based on the obtained MAC address, data is transmitted.

It takes time and lowers efficiency if this procedure is used to convert the IP address into the MAC address every time. Consequently, the mapping of once investigated IP addresses and MAC addresses are preserved in lists, and mapping can thus be performed by using these lists as indices.

1.5 Terminal Interfaces

Terminal interfaces refer to arranged conditions and transmission control methods to ensure that transmission is performed between terminals. More specifically, this concerns connector types and standards for signal levels, and standards for operation conditions. The following three types are typical terminal interfaces, and each of these was define upon ITU-T recommendation.

- V-series: Interface between DTE and DCE with analog lines
- X-series: Interface between DTE and DCE with digital lines
- I-series: Interface for connecting to ISDN lines

The following outlines and explains the special characteristics of each series. Further details and explanation of the equipment and lines mentioned in the tables are given from Chapter 2.

1.5.1 V-series

The V-series documents the interfaces between DTE-DCE (MODEM) used for data transmission with analog lines.

Figure 1-5-1 V-series interfaces

Interface name	Definitions
V.10 (X.26)	Electrical characteristics of general-purpose unbalanced double-current interchange circuits used in IC devices in the field of data transmission
V.11 (X.27)	Electrical characteristics of general-purpose balanced double-current interchange circuits used in IC devices in the field of data transmission
V.21	300-bps modems for use on public switched telephone networks; full-duplex transmission
V.22	1,200-bps modems for use on public switched telephone networks and leased lines; full-duplex transmission
V.23	600/1,200-bps synchronous or asynchronous modems for use on public switched telephone networks
V.24	Definition of interchange circuits between data terminal equipment and data circuit-terminating equipment
V.26	2,400-bps modems for use on four-wire leased lines
V.26bis	1,200/2,400-bps modems for use on public switched telephone networks; half-duplex transmission
V.26ter	2,400-bps modems for use on two-wire lines; full-duplex transmission
V.27	4,800-bps modems with manual equalizer for use on four-wire (full-duplex) or the wire (half-duplex) leased lines
V.27bis	2,400/4,800-bps modems with manual equalizer for use on four-wire (full-duplex) or the wire (half-duplex) leased lines
V.27ter	2,400/4,800-bps modems for use on public switched telephone circuits; half-duplex transmission
V.28	Electrical characteristics of unbalanced double-current interchange circuits
V.29	9,600-bps modems for use on point-to-point four-wire leased circuits; full-duplex (4-wire) half-duplex (2-wire)
V.32	9,600-bps modems for use on two-wire lines; full-duplex transmission
V.33	14.4-kbps modems for use on four-wire leased lines
V.35	48-kbps data rate trunk interface using 60 - 108 kHz bandwidth lines

1.5.2 X-series

The X-series documents the interfaces between DTE-DCE (Digital Service Unit; DSU) used for transmission with digital lines. X.20, X.21 and X.25 (packet switching) are widely used.

Figure 1-5-2 X-series interfaces

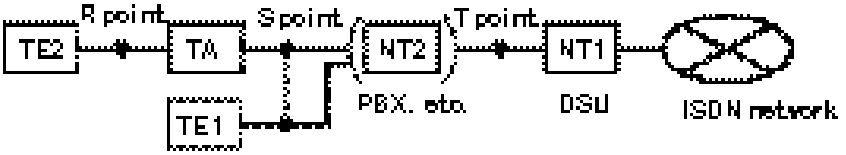
Interface name	Definitions
X.20	DTE-DCE (asynchronous communication) interface between data terminal equipment (DTE) and data circuit terminating equipment (DCE) for start-stop transmission on public switched telephone networks.
X.20bis	Specification for data terminal equipment (DTE) designed for interfacing to asynchronous two-wire V-series modems for use on public-access networks.
X.21	Interfaces between data circuit-terminating equipment (DCE) and data terminal equipment (DTE) for synchronous operation on public switched telephone networks.
X.21bis	Specifications for DTE designed for interfacing to synchronous V-series modes in public switched telephone networks.
X.24	Lists the definitions for interchange circuits between data circuit-terminating equipment (DCE) and data terminal equipment (DTE) for use in public switched telephone networks.
X.25	Interfaces between data circuit-terminating equipment (DCE) and data terminal equipment (DTE) for devices with direct connection to packet switched public telephone networks.

1.5.3 I-series

The I-series defines the interfaces used for connecting terminals to ISDN lines. It is also referred to as user/network interface. It also defines the logical connection points between DTE-DCE for use with ISDN.

Figure 1-5-3 I-series interfaces and ISDN

Interface name	Definitions	
I. 430	ISDN basic rate physical layer user/network interface	Layer 1 specifications
I. 431	ISDN primary rate physical layer group user/network interface	Layer 1 specifications
Q. 921	ISDN frame format at the data-link layer	Layer 2 specifications
Q. 922	ISDN frame mode bearer service (Frame Relay)	Data-link layer specifications
Q. 931	ISDN user/network interface for message type and content	Layer 3 specifications



- TE1: ISDN standard terminal equipment
- TE2: ISDN non-terminal equipment
- TA: Terminal adapter
- NT1: Digital service unit (DSU)
- NT2: PBX, etc.
- R, S, T points: Each interface point (defined by the I. 400-series)

ISDN comprises logical interface reference points like R, S and T in Figure 1-5-3. Separate points are found between R to T.
However, when TE1 is directly connected to the DSU, S and T becomes the same point. Also, if the DSU and TA functionalities are integrated in the same equipment, the three points become the same point.
The user/network interface comprises basic interfaces and primary group interfaces, and these details are mainly defined in the I. 400-series.

1.5.4 RS-232C

RS-232C (Recommended Standard 232C) is a standard adopted by the EIA (Electronic Industries Association, USA) that has become the ITU-T recommendation V.24. RS-232C defines various characteristics used for asynchronous transmission between DTE-DCE (MQdd Modulator/DEModulator; MODEM) for data transmission with analog lines. Because MODEM only handles serial data, RS-232C also is defined for serial data.

1.6 Transmission Control

Transmission control is the control capabilities used to ensure high-quality, efficient and reliable transmission of data. The steps involved in this are codified in a series of rules called "transmission control procedures."

1.6.1 Overview and Flow of Transmission Control

(1) Overview of transmission control

A number of controls and procedures are required to ensure efficient and reliable data transmission. Collectively, these controls and procedures are labeled "transmission control," which comprises the following four controls.

① Line control

A control exercised in the case of circuit switching that controls the switching between connection and disconnection of data transmission lines. In the case of leased lines, since the relationship between sender and recipient are fixed, line control is not necessary.

② Synchronous control

Synchronous control coordinates the timing for data exchange as well as data flow "flow control."
Synchronous control comprises modes like start-stop synchronization, SYN synchronization, and frame synchronization, etc. Flow control regulates the data transfer rate.
(For details on synchronization, see Section 2.2.2 Synchronous Control.)

③ Error control

Error control detects, corrects and retransmits erroneous data.
(For error detection methods, see Section 2.2.1 Error Control.)

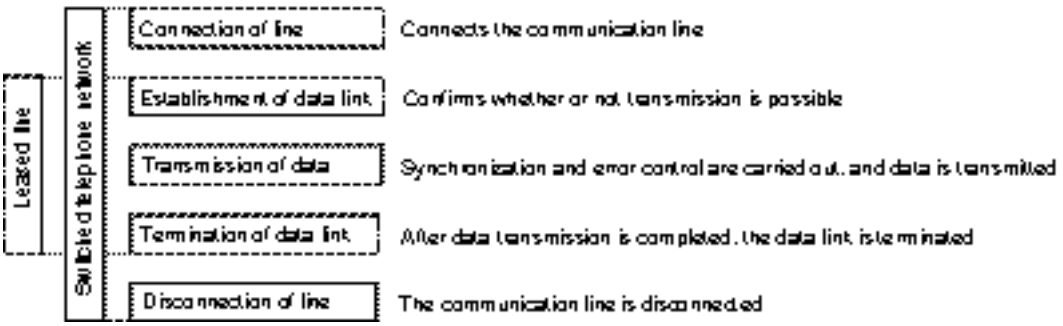
④ Data link control

Data link is the path that physically enables communication between the sender and the recipient. Data link control establishes the data link and performs data transmission according to a specified procedure and then terminates the data link.

(2) The flow of transmission control

The general flow of transmission control in switched telephone networks and leased lines is shown in Figure 1-6-1.

Figure 1-6-1 Data link establishment and lines



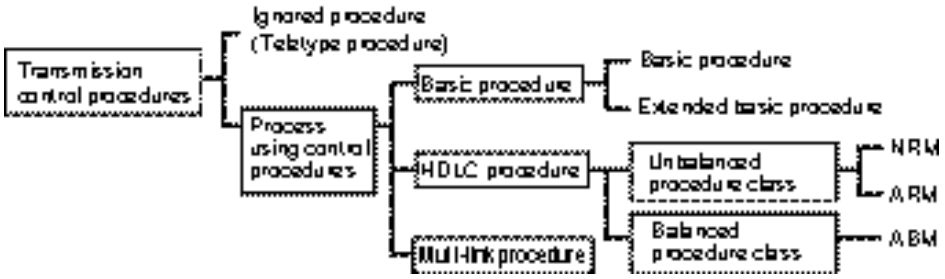
1. Phase 1 (line connection) (not necessary on a leased line)
   Simultaneously with dialing the other party and connecting the line, the necessary communication equipment (MODEM, etc.) is set to the functional state.
2. Phase 2 (establishment of data link)
   The other party is called, and it is inquired whether communication with the party is possible and the answer is confirmed. If the answer is "communication enabled," the first data link is established at this point.
3. Phase 3 (transmission of data)
   By establishing the data link, data transmission is performed while various controls (synchronous control and error control, etc.) are carried out.

4. Phase 4 (termination of data link)
   After data transmission is completed, it is checked that communication between the two parties has ended, and then the data link is terminated.
5. Phase 5 (disconnection of line) (not necessary on a leased line)
   The line is disconnected.

1.6.2 Transmission Control Procedures

Figure 1-6-2 shows typical transmission control procedures used to ensure efficient, reliable transmission of data.

Figure 1-6-2 Transmission control procedures



(1) Teletype procedure (TTY mode)

In the TTY (TeleTYpewriter) mode, the operator performs the control with regards to the data transmission. Since the transmission control procedures are ignored, it is called ignored procedure. This is widely used for personal computer communications using low-speed lines (300-bps class).
TTY is a mode in which a character flows along the communication line the moment that it is typed with a key. Since only the lowest level of control required for data transmission is in effect, the operator is required to take remedial actions if troubles occur (transmission errors, etc.).
In TTY mode, the sender transmits the data upon the issue of a request for data transmission. No controls are exercised, such as confirming the state of the other party, etc.
Basically, only the following three controls are used in TTY mode, and therefore reliability is low.

- The recipient confirms the delimitation of the data by delimiters, such as CR (Carriage Return).
- Flow control codes are used to start and stop data transmission to accommodate differences in processing speed on the sender and recipient side, respectively.

(2) Basic procedure (basic mode data link control)

Historically, the basic procedure is the oldest as it was established as the JIS X 5002 standard in 1975.

Figure 1-6-3 Characteristics of the basic procedure

Link code	JIS 7-unit code
Link control	Link control performed by 10 transmission control characters
Transmission unit	Block unit
Data length	Character (8-bit) times an integer
Synchronization	SYN synchronization
Error control	Parity check
Adaptive line speed	Appropriate for lines with a speed of up to 9,600 bps
Transmission efficiency	Normal (better than the ignored procedure mode)
Communication mode	Half-duplex (Extended mode uses full-duplex)

① Transmission control characters

In the basic procedure, the 10 transmission control characters shown in Figure 1-6-4 are used for transmission control.

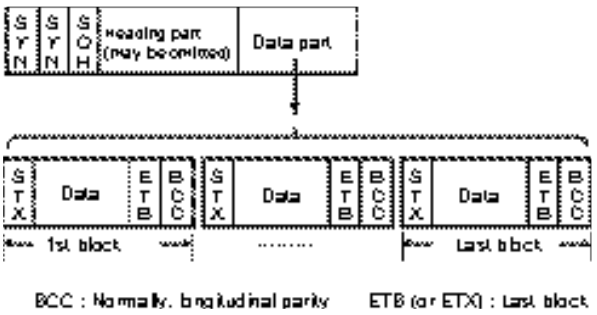
Figure 1-6-4 Transmission control characters

Code	Name	Definition
SOH	Start of Heading	Character for starting the basic mode.
STX	Start of Text	Transmission control character to indicate start of text. When heading is present, it is used for ending.
ETX	End of Text	Ends one text.
EOT	End of Transmission	Indicates the end of transmission of one or more texts.
ETB	End of Transmission Block	Indicates the end of a block split due to transmission considerations.
SYN	Synchronous idle	Ensures synchronization in the state in which other characters are not sent and maintains synchronization.
ENQ	Enquiry	Used for requesting an acknowledgement from the other party.
ACK	Acknowledge	Transmission control character sent from the recipient as an acknowledgement to the sender.
NAK	Negative Acknowledge	Transmission control character sent from the recipient as a negative acknowledgement to the sender.
DLE	Data Link Escape	Transmission control character used when adding transmission control to change the meanings of the following finite number of characters.

② Message format

The message in the basic procedure consists of the heading part and the data part.

Figure 1-6-5 The message format of the basic procedure



- Heading part: Contains control information for transmission (may be omitted).
- Data part: Data is divided into a number of blocks for transmission, and the BCC (Block Check Character) is added at the end of each block (normally attached as longitudinal parity bit, and the type is odd parity).

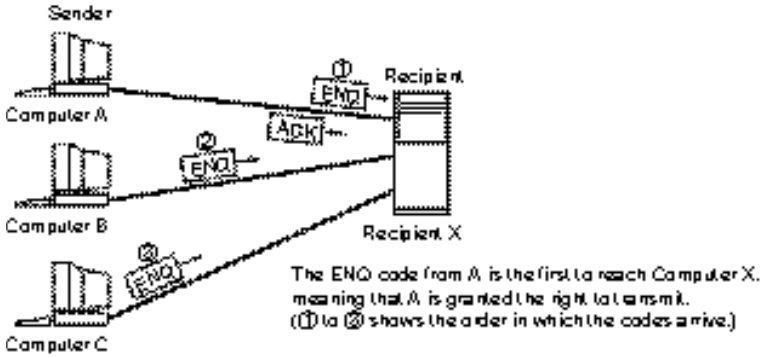
③ Establishment of data link

The basic procedure characteristics two methods for establishment of data link: Contention and polling/selecting.

a. Contention

Contention is the method used in the case of point-to-point connection. The sender (master station) sends the ENQ code, and after receiving the ACK code from recipient, transmission of data is commenced. I.e., in order to obtain the right to transmit, the ENQ code must be sent first, and therefore this method is sometimes referred to as the "first-come, first-served" method.

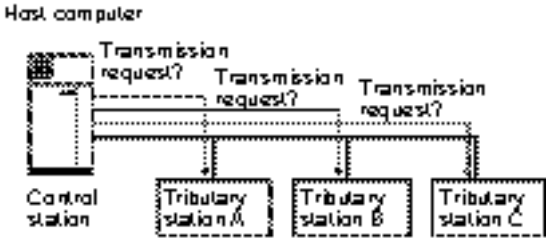
Figure 1-6-6
Contention



b. Polling/selecting

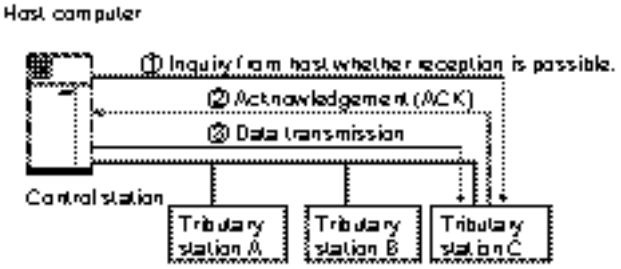
The polling/selecting method is used when several tributary stations are connected to a primary station (control station). The host computer, called the "control station," controls all the sending and reception of data within the network system.
This method consists of the following two operations.
<Polling>
In a specified order, the control station inquires all the tributary stations (stations other than the control station) whether or not they have transmission requests.

Figure 1-6-7
Polling



<Selecting>
In a specified order, the control station inquires a tributary station for which it has a request for transmission whether this tributary station is able to receive.

Figure 1-6-8
Selecting



(3) HDLC procedure (High-level Data Link Control)

The HDLC (High-level Data Link Control) procedure is a transmission control procedure for advanced, high-speed data communication.

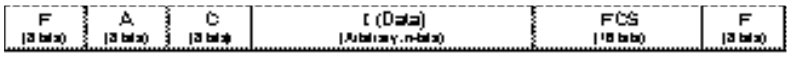
Figure 1-6-9
Characteristics of HDLC

Link code	-
Link control	By command/response
Transmission unit	Frame (up to 8 frames can be sent consecutively)
Data length	No restrictions
Synchronization	Frame synchronization
Error control	CRC (Cyclic Redundancy Check)
Adaptive line speed	2,400-bps or higher medium- or high-speed lines
Transmission efficiency	Good
Communication mode	Full-duplex

① Frame structure

In the HDLC procedure, information is transmitted in frames.

Figure 1-6-10 Frame structure



a. Flag sequence (F; 8-bits)

In the flag sequence, codes are inserted for synchronization to indicate the separation between frames, and these codes have the "01111110" bit pattern. In order that this bit pattern does not appear in other areas, the sender must insert 0 after 1 has appeared consecutively 5 times, and the sender must remove the 0 after 1 has appeared consecutively 5 times. Implementing this enables transmission of any bit pattern.

b. Address field (A; 8-bits)

The address field contains the address of the frame's sender and recipient.

c. Control field (C; 8-bits)

The control field contains information on the frame type, frame serial number, etc.
There are three frame types:

- Information (I) frame: For transmitting information
- Supervisory (S) frame: Used for confirming reception of I-frames and request for retransmission
- Unnumbered (U) frame: For control, such as mode setting, etc.

Frame serial numbers are attached in consecutive order to frames to be sent consecutively to enable check of whether frames are missing. The numbers 0 to 7 are available, allowing up to 7 frames to be sent consecutively.

d. Information field (I; n-bits)

Transmission data of an arbitrary bit length can be entered in the information field.

e. Frame check sequence (FCS; 16-bits)

CRC codes (16-bits) for error detection are entered in the frame check sequence.

② Establishment of data link

The data link establishment methods of the HDLC procedure comprise two classes; unbalanced procedure class and balanced procedure class.

Figure 1-6-11 The HDLC procedure methods for data link establishment

a. Unbalanced procedure class

In the same manner as the polling/selection of the basic procedure, the unbalanced procedure class is made up of one primary station and several secondary stations with the primary station controlling transmission. The frames sent from the primary station are called "commands," and those going the other way are called "responses."
In the unbalanced procedure class data is exchanged using the following two modes:

- Normal Response Mode (NRM)
  When the transmission permission is issued from the primary station, the response can be sent from the secondary station, but other than this, only commands from the primary station are allowed.
- Asynchronous Response Mode (ARM)
  Even if the transmission permission is not issued from the primary station, the response can be sent from a secondary station.

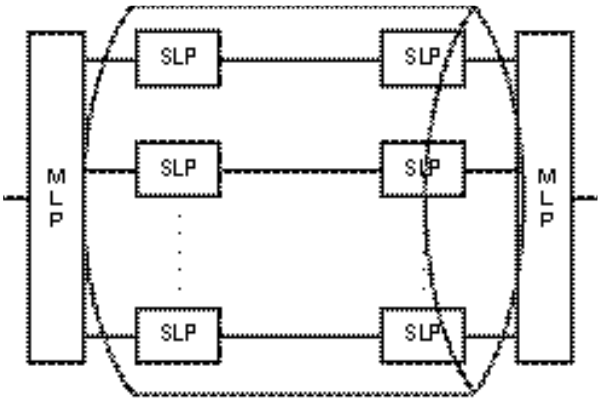
b. Balanced procedure class

In the balanced procedure class, combined stations, which possess the functionalities of both a primary station and a secondary station, are in charge of all transmission control. In the same manner as the contention mode used in the basic procedure each station can send command and response. In the balanced procedure class, data is exchanged using the Asynchronous Balanced Mode (ABM) in which both command and response can be sent even without obtaining the transmission permission from the combined station that is the other party in the communication.

(4) Multi-link procedure

The multi-link procedure combines multiple data links (single links), and is used for providing one data link offering various transmission capacities. Representative examples of this use are INS Net-64 and INS Net-1500 using ISDN lines. ISDN lines are provided with multiple channels (data links) for transmission of information, and the transmission capability of one channel is 64 kbps, but by using the multi-link procedure it becomes possible to provide data links having multiple transmission capabilities.
MLP (Multi Link Procedures), which executes the multi-link procedure, simultaneously controls parallel SLP (Single Link Procedures) that execute single-link procedures. Difference of transmission capability, etc. of the SLPs working in parallel operation does not matter. Figure 1-6-12 shows a diagram indicating the relations between MLP and SLP.

Figure 1-6-12
Relations between MLP and SLP



- Bundles several data links together to treat them as one data link.

The single-link procedure uses a single data line and is a data link protocol for establishing the data link, data transmission and disconnection of the data link. The multi-link procedure combines the data units for sending into a multi-link frame and hands it over to the SLPs. The SLPs transmit the received multi-link frame and notifies the MLP of the result. Based on this notification, MLP performs post-processing (recovery of transmission irregularities, etc.,) and closes the chain of control.

Exercises

Q1 **The figure shows the hierarchical structure of the OSI basic reference model. Please enter the correct terminology instead of a, b and c.**

Application layer
a
Session layer
b
c
Data-link layer
Physical layer

	a	b	c
A.	Transport layer	Network layer	Presentation layer
B.	Transport layer	Presentation layer	Network layer
C.	Network layer	Transport layer	Presentation layer
D.	Presentation layer	Transport layer	Network layer
E.	Presentation layer	Network layer	Transport layer

Q2 **Which of the following is the correct explanation of the "Network Layer" of the OSI basic reference model?**

A. Performs setting and release of routing and connections in order to create a transparent data transmission between end systems.
B. This is the layer closest to the user, and allows the use of file transfer, e-mail and many different applications.
C. Absorbs the differences in characteristics of physical communication media, and secures a transparent transmission channel for upper level layers.
D. Provides transmission control procedures (error detection, retransmission control, etc.) between adjacent nodes.

Q3 **Which of the following protocols has become a worldwide de facto standard? The protocol is used by the ARPANET in the USA, and is built into the UNIX system.**

A. CSMA/CD B. FTAM C. ISDN
D. MOTIS E. TCP/IP

Q4 **Which of the following illustrations appropriately shows the relationship between the 7 layers of the OSI basic reference model and the TCP and IP protocols used on the Internet?**

	A	B	C	D
Transport layer	IP		TCP	
Network layer	TCP	IP	IP	TCP
Data-link layer		TCP		IP

Q5 **Which protocol is used for file transfer on the Internet?**

A. FTP B. POP C. PPP D. SMTP

Q6 **What is the maximum number of host address that can be set within the one and same subnet when the 255.255.255.0 subnet mask is used with the Class B IP address?**

A. 126 B. 254 C. 65,534 D. 16,777,214

Q7 Which is the most appropriate description of the ARP of the TCP/IP protocol?

A. A protocol for getting the MAC address from the IP address.
B. A protocol that controls the path by the number of hops between the gateways.
C. A protocol that controls the path by the network delay information based on a time stamp.
D. A protocol for getting the IP address from a server at the time of system startup in the case of systems having no disc drive.

Q8 Which ITU-T recommendation specifies the communication sequence between data terminal equipment (DTE) in data communication systems and packet switched networks?

A. V.24 B. V.35 C. X.21 D. X.25

Q9 In transmission control, what performs the following processing?

- Supervises data circuit-terminating equipment (Modems, etc.).
- When used with telephone networks, it issues the dial tone and connects to the recipient, and disconnects the line after communication is completed.

A. Error control
B. Line control
C. Data-link control
D. Synchronous control

Q10 There is a data communication system in which multiple terminals are connected on one line coming from the center. After the center control station inquires the tributary stations on the terminal side whether or not they have data to send, or after inquiring the state of readiness for signal reception, data transmission is carried out. What is this method called?

A. Contention
B. Synchronous transmission
C. Asynchronous transmission
D. Polling/selecting

Q11 Among the transmission control characters used in the basic mode data link control (basic procedure), which is the one that indicates acknowledgement of the received information message?

A. ACK B. ENQ C. ETX D. NAK E. SOH

Q12 In the information unit (frame) transmitted in the High-level Data Link Control procedure (HDLC procedure), which is the field employed for error detection?

A. A B. C C. FCS D. I

Q13 Which description most appropriately describes the multi-link procedure?

A. A protocol for enhancing the reliability of each of the data links when multiple lines are multi-step connected in series.
B. A protocol that relays multiple parallel data links.
C. A protocol that treats multiple parallel data links as one logical data link.
D. A line-multiplexing protocol that divides one physical line logically into multiple data links.