October, 2007

Network Engineer Examination (Afternoon, Part 1)

Questions must be answered in accordance with the following:

Question Nos.	**Q1 – Q4**
Question Selection	**Choose 3 questions from the 4 questions**
Examination Time	**12:10 - 13:40 (90 minutes)**

Instructions:

1. Choose 3 questions from the 4 questions, and encircle the question numbers you chose as seen in the example below. Please note that the answers are not scored if you don't encircle any of the question numbers. When all the 4 questions are encircled, the answers of the first 3 questions will be scored.

Encircle 3 question numbers below.
(Q1)
Q2
(Q3)
(Q4)

[An example when Q1, Q3, and Q4 are chosen]

2. Use a pencil to write your answers on the answer sheet. When you need to change an answer, erase your previous answer completely and neatly. Wipe away any eraser debris.
3. Mark your examinee information and test answers in accordance with the instructions below. Your test will not be graded if you do not mark properly. Do not mark or write on the answer sheet outside of the prescribed places.
   (1) **Examinee Number**
   Write your examinee number in the space provided, and mark the appropriate space below each digit.
   (2) **Date of Birth**
   Write your date of birth (in numbers) exactly as it is printed on your examination admission card, and mark the appropriate space below each digit.
   (3) **Answers**
   Write each answer in the space specified for that question.
   Write your answers clearly and neatly. Answers that are difficult to read will receive a lower score.

Do not open the exam booklet until instructed to do so.
Inquiries about the exam questions will not be answered.

Q1. Read the following description of the development of a videoconferencing system using the Internet, then answer Subquestions 1 through 4.

Company R, headquartered in Tokyo, is a systems development company that has five branch offices across the country.

Company R recently received an order for the development of an inventory management system from Company T, an apparel sales company. Company R determined that it would prepare the application requirements specifications and basic design specifications and conduct the acceptance inspection of the product to be delivered to Company T, and that the development of the program would be commissioned to a separate company. Company D was selected as the subcontractor because it has experience in the development of inventory control systems. Company D's office is located in Sapporo. Company R then decided to use a inter-company videoconferencing system using an Internet connection so that detailed discussions could be held with Company D whenever necessary, on matters such as explaining the basic design specifications during development and the coordination of the development schedule.

In its head office and branch offices Company R already has a videoconferencing system dedicated to in-house use. This system connects the head office to the branch offices via leased lines. To hold videoconferences with Company D, Company R decided to allocate two videoconferencing terminals (hereinafter, "terminal[s]") on a dedicated basis and to lend those two terminals and the necessary terminal software to Company D. The videoconferencing system consists of a videoconferencing server (hereinafter, "server") and terminals. The voices and images of conference participants are transmitted from each terminal to the server as voice data and image data, respectively. The collected voice data is mixed by the server, and the synthesized voices are delivered to each terminal. The image data of all conference participants obtained by a videoconferencing camera installed in each terminal is transferred to the server and synthesized by it. Synthesized image data is delivered to each terminal, thereby simultaneously displaying the images of all conference participants on every terminal.

Furthermore, the videoconferencing system not only displays on each terminal the images of all conference participants, but also has functions for displaying and editing the basic design specifications and the schedule table. It was decided to use these functions between Companies R and D.

Figure 1 shows the images displayed on a terminal at Company R.

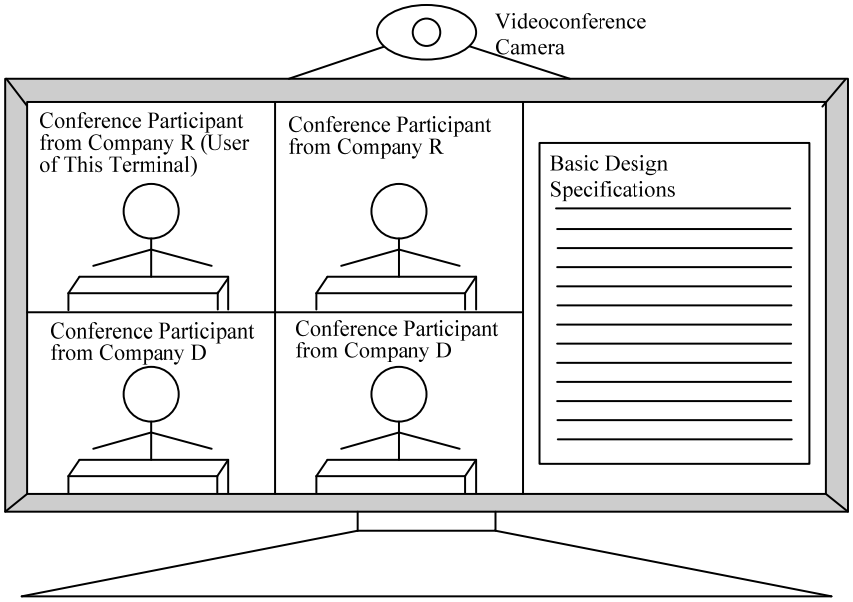


Fig. 1 Images Displayed on Terminal at Company R

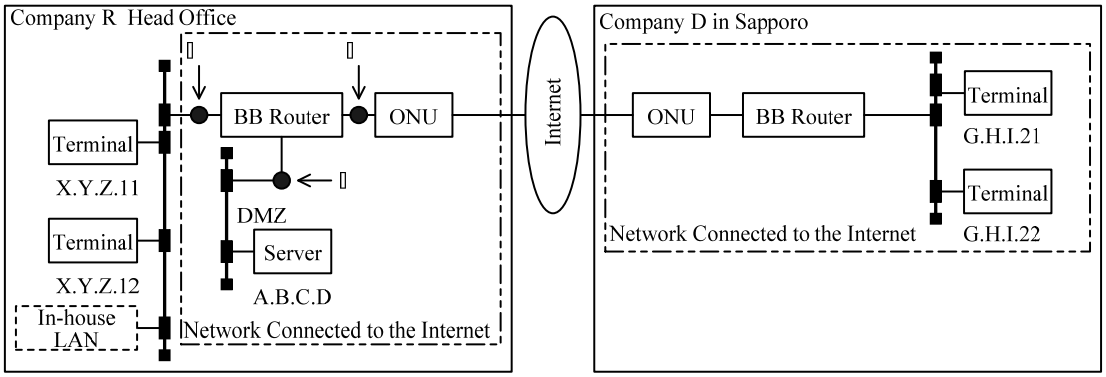
[Outline of the specifications for the videoconferencing system]

(1) Image data from each terminal is transmitted to the server at 0.8 M bits per second.
(2) Image data from the server is transmitted to each terminal at 1.5 M bits per second.
(3) Voice is encoded by G.711 (64 k bits per second).

[Network configuration of the inter-company videoconferencing system]

It was then decided that videoconferences with Company D would be conducted using the Internet in order to reduce communication costs. Mr. S at Company R, who was assigned the task of introducing the inter-company videoconferencing system, studied the configuration information and specifications of the videoconferencing system already installed in the head office. As a result, it was found that NAT could not be applied to the server for the videoconferencing system. Accordingly, Mr. S decided to build a new Internet connection network in Company R's head office, and to relocate the server to the DMZ. It was further decided that Company D's Sapporo office would install a network of terminals and connect them to the Internet.

Figure 2 shows the network configuration of the inter-company videoconferencing system.



BB Router : Broadband Router
ONU : Optical Network Unit
A.B.C.D : Global IP Address of Server
X.Y.Z.11, X.Y.Z.12 : Private IP Addresses of Terminals
G.H.I.21, G.H.I.22 : Global IP Addresses of Terminals

Fig. 2 Network Configuration of the Inter-Company Videoconferencing System

Mr. S then investigated the communication that occurs between the server and the terminals of the inter-company videoconferencing system when using Internet. Table 1 shows the protocols and port numbers for the inter-company videoconferencing system that were found as a result of his investigations.

Table 1 Protocols and Port Numbers for the Inter-Company Videoconferencing System (Partial)

Service between server and terminals	Protocol	Server Side		Terminal Side
		Port Number	Connection Initiation Direction	Port Number
file transfer	TCP	20, 21	←	1024～65535
conference control		6200		
conference image / voice data transfer control		6300		
conference image / voice data transfer	UDP	6000～6099	→ ←	6000, 6001

Furthermore, Mr. S decided that the setting for packet control, as shown in Table 2, would be added to the BB router in Company R's head office for the connection to the Internet.

Table 2 Description of Settings of the BB Router in Company R's Head Office (Partial)

Direction	Control	Protocol	Source IP Address	Source Port Number	Destination IP Address	Destination Port Number
IN	permission	A	G.H.I.21, G.H.I.22	6000, 6001	A.B.C.D	6000 ~ 6099
	permission	TCP	G.H.I.21, G.H.I.22	B	C	20, 21, 6200, 6300
OUT	permission	UDP	A.B.C.D	6000 ~ 6099	G.H.I.21, G.H.I.22	D

Note: The term "IN" denotes the flow of a packet from the Internet to the BB router, and the term "OUT" denotes the flow of a packet from the BB router to the Internet. The default packet control by the BB router is as follows: In the IN direction, all TCP and UDP packets are prohibited. In the OUT direction, all TCP packets are permitted and all UDP packets are prohibited.

[Consideration of security measures]

In developing the inter-company videoconferencing system, Mr. S followed Company R's internal procedures for obtaining an approval for the development plan, with the result that the following comment was submitted by its Systems Audit Department.

"Our conventional videoconferencing system has been developed on the assumption that it would be used over leased lines among entities such as the head office and branch offices, and therefore system security is not adequate when this system is used over the Internet. In establishing a connection with Company D, we must consider the measures that need to be taken for effective security management because we are entrusting Company D with the development of the inventory management system program."

Mr. S consulted a superior and decided to introduce a VPN to provide a secure network between Company R's head office and Company D's Sapporo office. It was decided that the VPN would be a remote-access type consisting of a VPN-dedicated device and VPN client software installed on the terminals. (a) Positions ① through ③ in Figure 2 were chosen as potential locations to connect a VPN-dedicated device. An investigation was performed and as a result of the investigation it was decided to connect this device to position ③.

VPN technologies include [i] at the network layer (Layer 3) as well as [ii] and [iii] at the data link layer (Layer 2). After investigation, [i] was adopted. Key management protocols for [i] include [iv]. Mr. S considered the possibility that the number of users of the terminals would increase in the future, and adopted [v] in which, by expanding [iv], it is possible to use

one-time passwords in the authentication portion, thereby authenticating individual users. [i] includes two modes: the transport mode and the tunnel mode. After comparison of the two, the tunnel mode was selected, and it was decided to encrypt [vi], the TCP header, and the data, thereby ensuring security.

Subsequently, smooth progress was made in the development of the inter-company videoconferencing system. The intention of Company R is that, as soon as the effectiveness of this system is confirmed, a wide range of future development projects will be commissioned to companies other than Company D. In delivering the system to Company R's Operations Department, Mr. S thought that it would be necessary to prevent increases in operational burdens in the event that the number of terminals is increased significantly in the future. Accordingly, he decided that, (b) in order to enable the users of the inter-company videoconferencing system to resolve system failures by themselves as much as possible, measures should be taken in parallel with the videoconferencing system development work.

Subquestion 1

Fill in the blanks [A] through [D] in Table 2 with the correct term or phrase.

Subquestion 2

From the answer group below, select the correct answers to be inserted into each of the blanks [i] through [vi] in the text.

Answer group:

a) ESP	b) GRE	c) IKE	d) IP header	e) IPsec
f) L2TP	g) NAPT	h) PKI	i) PPP header	j) PPTP
k) SSH	l) SSL	m) UDP header	n) X.24	o) XAUTH

Subquestion 3

For the case in which a conference is held by using all four of the terminals in the inter-company videoconferencing system as shown in Figure 2, give each transmission quantity per second for voice data and image data at position ③ in the BB router's IN and OUT directions. Here, control information such as packet headers of voice data and image data can be ignored. Answer in units of k bits for each quantity.

Subquestion 4

Answer the following questions (1) and (2), regarding the VPN environment.

(1) From the viewpoints of operation and security of the BB router, explain briefly why the VPN-dedicated device was connected to position ③ as stated in underline (a) of the text.

(2) Give two specific examples of measures that Mr. S decided to take as stated in underline (b) of the text.

Q2. Read the following description concerning improvement of a network system, and then answer the Subquestions 1 through 3.

Company A has 300 PCs installed in the company and uses them to share information via a file server and to access a Web server on the Internet. The PCs are connected to the company servers or the Internet via a wireless LAN with IEEE 802.11b standard (hereafter referred to as the wireless LAN). Mr. B and Mr. C are in charge of the network system. This is Mr. C's second year at the company, and he often works under Mr. B, who is more experienced.

Figure 1 shows the network system configuration of Company A.

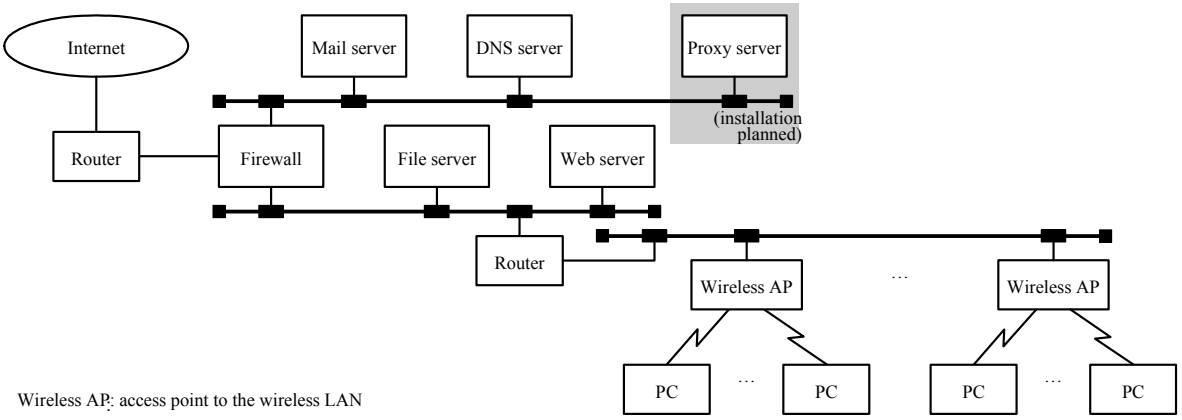


Fig 1 Network System Configuration of Company A

Recently, a department reported that the response of the file server is slow. When the file transfer time between the PCs of that department and the file server was measured, it was found that transfer time was different between normal hours and the peak hours. Mr. C thought that the wireless LAN, whose transmission speed is slower than a wired LAN, is causing the bottleneck and asked Mr. B about the throughput of a wireless LAN. The following is the explanation from Mr. B concerning the throughput of a wireless LAN.

[Throughput of a Wireless LAN]

The access control method of a wireless LAN is called [A], which corresponds to CSMA/CD for a LAN with IEEE 802.3 standard. The transmission speed of a wireless LAN fluctuates between 1 M and [B] M bps, depending on the communication condition. However, the transmission speed of physical headers including preambles is fixed.

Figure 2 shows the transmission frame format and transmission time for a wireless LAN.

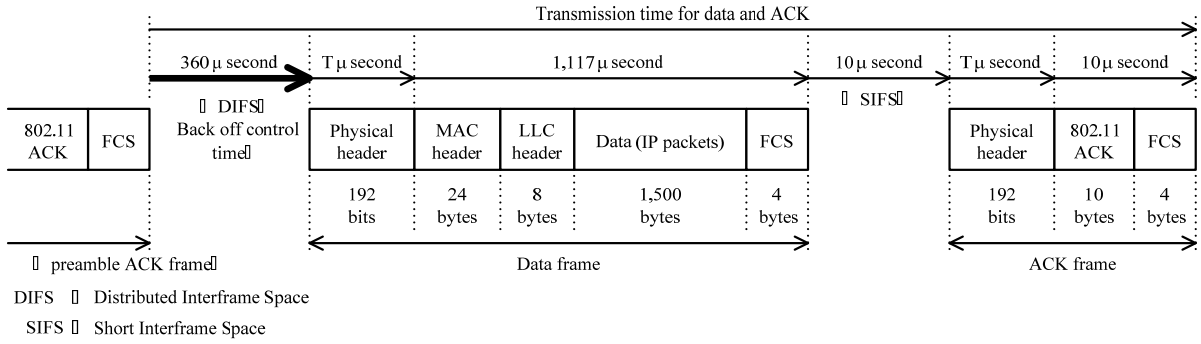


Fig. 2 Transmission Frame Format and Transmission Time

Time durations in Figure 2 represent the required amounts of time at the maximum transmission speed. However, since (i) the back off control time is random, for the queuing time (thick solid arrow in Figure 2) from the completion of the preamble ACK frame transmission to the start of the data frame transmission, the mean value is used.
Using these values, the upper bound of the throughput of the wireless LAN can be calculated by the following formula, and the value turns out to be at least 6 Mbps and less than 7 Mbps.

Upper limit of the throughput of the wireless LAN
= (data length) / (Transmission time of data and ACK)
= (1,500 × 8) bits / (360 + T + 1,117 + 10 + T + 10) μ second.

[Throughput of File Transfer]

When the data frame of Figure 2 is data transfer from the PC of Figure 1 to the file server, three MAC addresses are set up in the MAC header: the addressee is [C], the sender is [D], and the BSSID (Basic Service Set ID) is [E].

In communication between a PC and the file server, suppose that the IP header and the TCP header are both 20 bytes each and that the data frame is not split up. In order to maximize the throughput of this file transfer, one should make the TCP data [F] bytes long. At Company A, when installing wireless APs, the parameters of the file servers were adjusted, and the throughput of file transfer was measured. As a result, they found out that (ii) the rate was close to 5 Mbps, which is the upper bound obtained when the response time of devices such as PCs and the filer server is excluded.

At the department where the responses of the filer server are delayed, in order to keep up with the increase in traffic, one wireless AP was added last year, so the department now uses two wireless APs. Mr. B, suspecting that there may have been a problem with the work of adding the wireless AP, checked with Mr. C, who had carried out the work. Here is the explanation Mr. C gave:

- Out of the 60 PCs, 30 of them were chosen as the PCs to use the new wireless AP.

- In the added wireless AP, a new SSID and a WEP (Wired Equivalent Privacy) key were set up; for the frequency, the default value that had been set up in the wireless AP was used as is.
- On the 30 PCs selected, the SSID and the WEP key, identical to those in the added wireless AP, were set up.
- For each of the two wireless APs, file transfer was conducted between the file server and a PC designated for the AP. The throughput of file transfer was about 5 Mbps on each AP.

Having heard Mr. C give this explanation, Mr. B pointed out that the delay in file transfer may be due to an (iii) error in Mr. C's setup. The two wireless APs are identified by their SSIDs, and each wireless AP is able to communicate with a PC designated to the AP. However, according to Mr. C's setup, the two wireless APs cannot simultaneously communicate, so the throughput of the wireless LAN could decrease.

Mr. C corrected the setup based on what Mr. B had told him; the result is that, even during the peak hours, the system can achieve the same file transfer throughput as during normal hours.

[Installation of a Proxy Server]

Company A routinely checks the operation of its firewall. Web access on the Internet is increasing every year, and it was expected that the CPU usage rate of the firewall would reach its limit if nothing is done. Upon consulting the vendor, it was found that the load of the NAPT (Network Address Port Translation) used by Company A to access Websites on the Internet is high but that this could be improved by installing a new proxy server. Company A has decided to install a proxy server, and Mr. B was put in charge of the installation plan. The installation plan calls for a one-month period of parallel operation so that the work will not be interrupted.

In order to use a proxy server, it is necessary to set up the proxy server information on the Web browser of the PCs. This can be carried out either by directly setting the IP address of the proxy server or by registering, on the Web server, a file (hereafter referred to as the automatic setup file) where the proxy server usage information is defined and setting its registration location URL on the Web browser of the PCs. Mr. B compared these methods and has decided to go with the method using the automatic setup file. He also decided that the work of setting up the URL on the 300 PCs would be done sequentially when the users are not working on their PCs. Figure 3 shows the installation work schedule prepared by Mr. B.

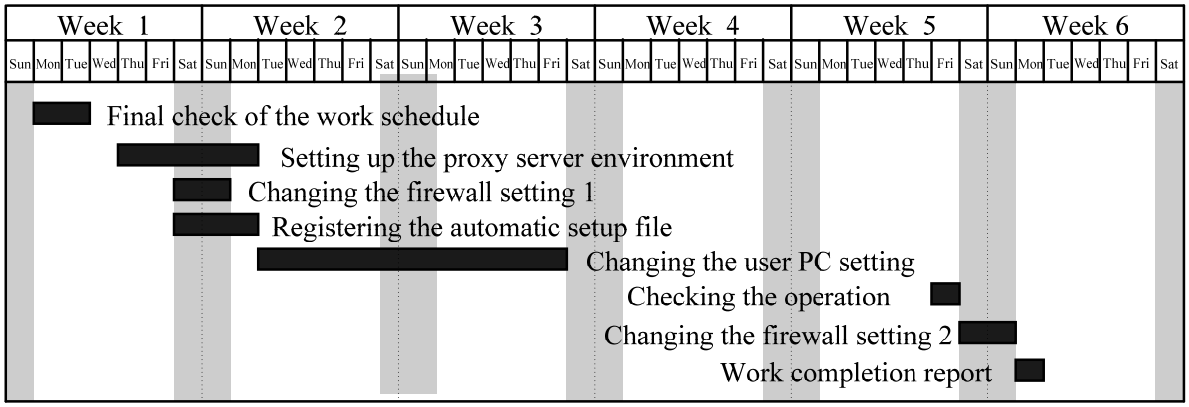


Fig. 3 Installation Work Schedule for a Proxy Server

Mr. B and Mr. C completed all the work as planned according to the installation work schedule. They were able to prevent the firewall bottleneck.

Subquestion 1

Answer (1) through (3) below concerning the [Throughput of a Wireless LAN].

(1) Fill in the blanks [A] and [B] in the text with the correct term or phrase.

(2) Concerning underline (i) in the text, state the reason briefly that the back off control time is random under the IEEE 802.11b standard.

(3) Find "T" in Figure 2.

Subquestion 2

Answer (1) through (4) concerning the [Throughput of File Transfer].

(1) From the device names shown in Figure 1, select the correct name to be inserted in each of the blanks [C] through [E] in the text.

(2) Give the correct numerical value to be inserted in the blank [F] in the text.

(3) Concerning underline (ii) in the text, state the reason briefly that the maximum throughput of file transfer does not reach the maximum throughput of the wireless LAN.

(4) Concerning underline (iii) in the text, describe the error in Mr. C's setting briefly.

Subquestion 3

Answer (1) and (2) below concerning the [Installation of a Proxy Server].

(1) Give a summary of what advantage(s) the method of using an automatic setup file has in the installation work.

(2) Describe briefly what is involved in the steps "Changing the firewall setting" 1 and 2 in Figure 3.

Q3. Read the following description concerning a review of remote connection, and then answer the Subquestions 1 through 4.

Company Y is a 300-employee company that sells information machines, with its headquarters in Tokyo and four branch offices across the country. A LAN is set up for the headquarters as well as at each office. These LANs are mutually connected with IP-VPN to constitute the network for Company Y. A total of 120 employees, equipped with mobile notebook PCs (hereafter referred to mobile PCs), use the company network from the outside via PIAFS-type remote connection with the remote access server (hereafter referred to as the RAS) installed inside the headquarters firewall (hereafter referred to as the FW). Once on the company network via the RAS, the user can do everything a person inside the company can.

Figure 1 shows the network configuration of Company Y.

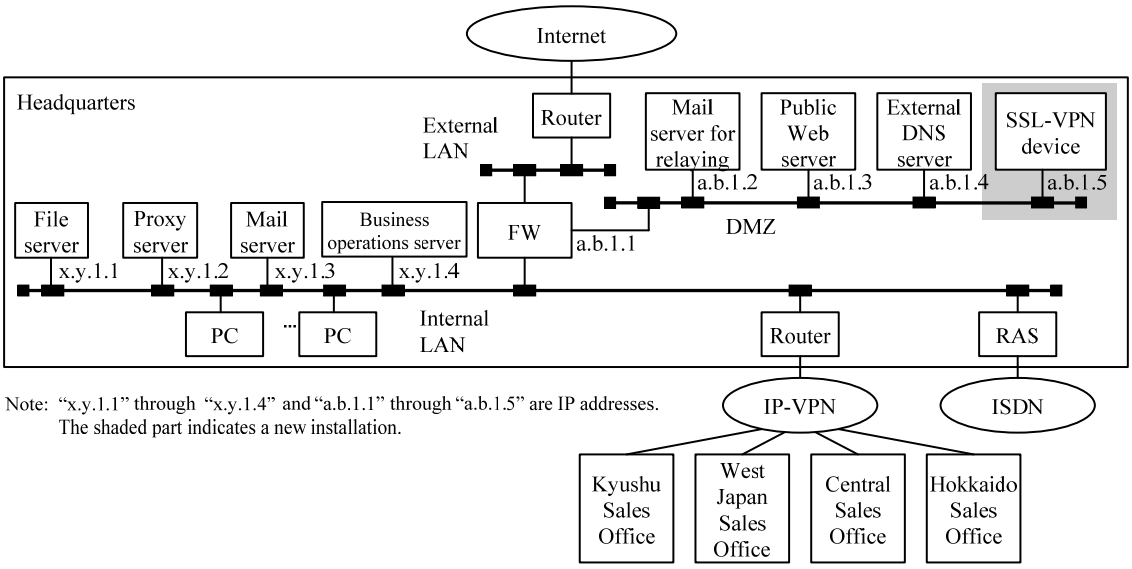


Fig. 1 Network Configuration of Company Y

Recently, with progress in mobile PC usage, the frequency of the company network usage from the outside is increasing. As a result, some have begun to complain that they cannot make the connection and that it is affecting their work. There are also requests to reduce the communications-related expenses for remote connection and to take security measures that would limit the work that can be performed from the outside. To solve these problems, Mr. K, a sectional supervisor of the Information Systems Department, asked Mr. F, the network manager, to consider improvement strategies for the remote connection system.

[Consideration for the Remote Connection System]

First, Mr. F considered and looked into the remote connection system. He discovered as a result that, by changing the system to an Internet-connected system, not only can he reduce

the communications-related expenses but also solve the difficulty in establishing the connection. In this system, it is necessary to take measures to maintain security, so he checked into an SSL-VPN unit, which constitutes VPN via SSL.

The initial SSL-VPN unit was made up only of the SSL server function and the [A] proxy function; hence, only the applications that use a Web browser (hereafter referred to as a "browser") could be used. As an improvement strategy, he considered a (a) system whereby mobile PCs are used to control Java applets, equipped with the local proxy function, which a re SSL clients. Using this system, many applications not previously compatible with SSL became compatible with SSL without changing the programs. The Java applets wait for and receive packets that contain TCP port numbers used by applications; once they are received, communication using SSL (hereafter referred to as SSL communication) is established with the SSL-VPN unit. The SSL-VPN unit enables communication between a mobile PC and the servers by transferring the packets received from the mobile PC to the servers corresponding to the port numbers. Such transfers are called [B] forwarding. The Java applets controlled by a mobile PC are (b) downloaded from the SSL – VPN unit. In addition, the work that can be performed from the outside can be limited by the SSL-VPN unit and FW.
Mr. F has determined that the remote connection system can be improved by using this SSL-VPN unit.

[Consideration of How to Use the SSL – VPN Unit]

Next, Mr. F considered how to use the SSL-VPN unit. Applications that go through the SSL-VPN unit are used in the following steps.

(1) The browser is started on a mobile PC, and HTTPS is used to establish connection with the SSL-VPN unit.
(2) On the authentication screen displayed on the mobile PC, authentication information is entered.
(3) The mobile PC displays all applications that can be used. The user chooses one, and the application is started.

By Step (1), SSL communication is started. Steps (2) and (3) are carried out after the mutual authentication is completed between the SSL-VPN unit and the mobile PC. Figure 2 shows the SSL communication sequence.

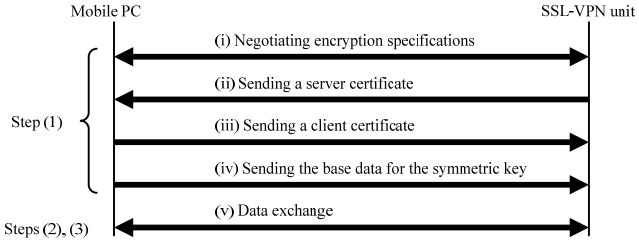


Fig 2　SSL Communication Sequence (simplified)

In procedure (ii) in Figure 2, the SSL-VPN unit sends a server certificate in order to be authenticated. Because [C] has a certificate of the CA authority that issued the server certificate, it verifies the validity of the server certificate using the (c) key contained in this certificate. Procedure (iii) is an optional step and is implemented when authentication by client certificate is requested. By procedure (iv), a symmetric key is generated on both the mobile PC and the SSL-VPN unit.

At the RAS, unauthorized use of the company network is prevented, not only by user authentication by password, but also by [D], whereby the connection is re-established from the RAS based on the information of the authenticated user. Hence, it was decided that the SSL-VPN unit would also carry out two-element authentication, not just by step (2) but by using procedure (iii) as well. There are several ways in which to use a client certificate, but here, we assume that (d) the manager would install it on the mobile PCs and use it.

[Consideration of Installing the SSL-VPN Unit]

Finally, Mr. F considered the installation of the SSL-VPN unit. The use of the internal LAN from the outside is through the SSL-VPN unit. For safety, the SSL-VPN unit is to be installed in the location shown in Figure 1. In order for the communication between mobile PCs and the servers to go through the SSL-VPN unit, the sender's IP address and the (e) addressee's IP address in the packets received from mobile PCs are converted by the SSL-VPN unit before the packets are transferred.

Currently, communication with the servers of Company Y through the Internet is limited to the servers installed in the DMZ. Hence, the installation of the SSL-VPN unit would require the setting of the FW to be changed. The table below indicates the additional communication contents to be permitted at the FW.

Table　Additional Communication Contents to Be Permitted at the FW

Communication direction	Sender's IP address	Addressee's IP address	Addressee's port number
Direction 1	arbitrary	a.b.1.5	E
F	G	H	15000
Direction 2	a.b.1.5	I	25
Direction 2	a.b.1.5	x.y.1.3	110

Note 1: The port numbers for main applications used at Company Y are as follows: SMTP: 25, POP3: 110, HTTP: 80, HTTPS: 443, DOMAIN: 53
Work application protocol: 15000
Note 2: The communication directions in the table are defined as follows:
Direction 1: from the external LAN to the DMZ
Direction 2: From the DMZ to the internal LAN
Note 3: The table omits communication contents concerning returned packets.

Mr. F has summarized his improvement strategies for the remote connection system based on the above results and reported it to Supervisor K. Mr. K in turn agreed that the problems can be solved by implementing this improvement strategy and thus decided to go forward with the restructuring.

Subquestion 1

Fill in the blanks [A] and [D] in the text with the correct term or phrase.

Subquestion 2

Answer (1) and (2) below concerning the SSL-VPN unit.

(1) Even with the system described by underline (a) in the text, there are some applications that are not compatible with SSL. Give a summary of what characteristics of IP communication these applications have.

(2) Describe briefly what is made easy by underline (b) in the text.

Subquestion 3

Answer (1) and (2) below concerning the operation of SSL.

(1) What type of key is described in underline (c) in the text?

(2) Identify where a symmetric key is used from (i) through (v) in Figure 2. Then, describe briefly an advantage in using a symmetric key.

Subquestion 4

Answer (1) through (4) below concerning the installation of the SSL-VPN unit.

(1) Fill in the blanks [E] through [I] in the text with the correct term or phrase.

(2) Describe briefly the content the connection control that is made possible by underline (d) in the text.

(3) Give a summary of what underline (e) in the text gets converted to.

(4) Describe briefly a security measure implemented by the installation of an SSL-VPN unit, besides authentication and encryption.

Q4. Read the following description of connection between networks, then answer Subquestions 1 through 4.

Companies A and B are telecommunications companies providing communications services in Prefecture C. Companies A and B are using the networks ISP-A and ISP-B, respectively, for their Internet connection services. ISP-1 through ISP-3 are nationwide networks for Internet connection services. ISP-A is connected to ISP-1, and ISP-B is connected to ISP-2. Furthermore, both ISP-1 and ISP-2 are connected to ISP-3.

It has recently been decided to integrate the ISP business of Companies A and B and to connect ISP-A and ISP-B. After ISP-A and ISP-B are connected together, the connection between ISP-B and ISP-2 will be removed for the purpose of cost reduction. However, a transition period for the connection work will be provided, and during this period ISP-B and ISP-2 will continue to be connected together. Figure 1 below shows the configuration of the network during the transition period.

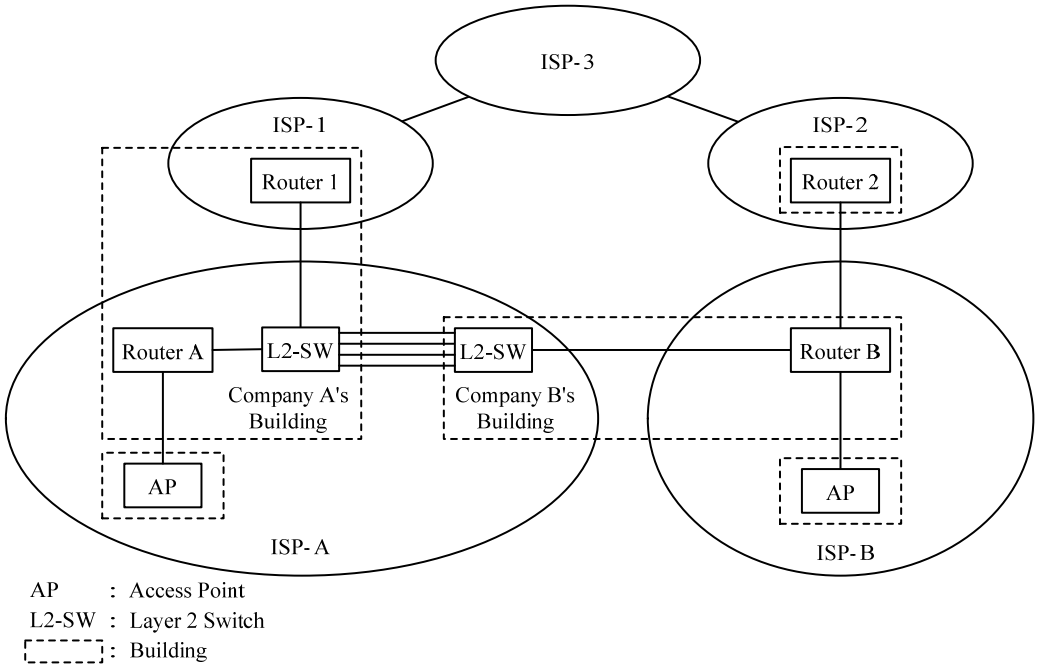


Fig. 1 Configuration of Networks during the Transition Period

[Connection between ISP networks]

Eight optical fiber cables will be rented from a telecommunications company, thereby opening an optical transmission line between Company A's building and Company B's. The optical fiber cables to be rented are [A] mode fiber cables suited to high-speed and long-distance transmission. With this type of optical fiber cable, the central portion

called a(n) [B] is as small as 10 μm or less in diameter, and the number of routes transmitting light (modes) is one, thus permitting high-speed and long-distance transmission. There are several types of gigabit Ethernet ports (hereinafter, "GE ports") suited to such an optical fiber cable, but they have different optical level specifications. Therefore, confirmation will be made as to whether the GE ports on the L2-SWs can be used for the optical transmission line. Table 1 below shows the optical level specifications for the L2-SWs.

Table 1 Optical Level Specifications for the GE Ports on the L2-SWs

Unit: dBm

Item	Maximum Value	Minimum Value
transmission level	5	1
reception level	- 3	- 23

In order for communication to be guaranteed at the GE ports on the L2-SWs, the attenuation value (in dB) on the optical transmission line cannot be more than the difference between the minimum value of the transmission level and the minimum value of the reception level. From Table 1 above, this difference can be obtained as [i] dB. The telecommunications company from which the cables were rented said that the attenuation value on the optical transmission line is 17 dB. The L2-SW manufacturer advised that a margin of 3 dB should be allowed. Therefore, no problems should develop if the GE ports on the L2-SWs are used for the optical transmission line because the sum of the attenuation value and the margin is 20 dB.

The connection between the L2-SWs is to be established by means of the four GE ports, thereby securing a total communication capacity of 4 G bits per second. For this purpose, these GE ports will be divided into groups and will be configured in such a way as to enable the load-balancing function. The load-balancing function uses two fields in a transmission frame as keys and has frames that contain different keys transmitted from different GE ports. In order for the communication capacity between the L2-SWs to be brought as close to 4 G bits per second as possible, the fields to be used as keys must be selected in such a way that the frames will be transmitted evenly from each of the grouped GE ports. For the default key setting for the L2-SWs, (I) the source MAC address and the destination MAC address fields are selected as keys. Here, however, the keys will be set in such a way that the source IP address and the destination IP address will be selected as keys, thereby ensuring that the load balancing will be more efficient.

Because the connection between the L2-SWs will be established by means of the four GE ports, the risk of communication disconnection is considered to be low. However, the link-fault signaling function of the L2-SWs will be used to further increase the reliability.

(II) The link-fault signaling function is installed in such a way that when any fault is detected on the reception side of a GE port on an L2-SW, then the fault signaling will be sent from the transmission side of the same GE port to its counterpart L2-SW, thereby bringing the transmission side of the latter GE port into a suspended state.

[Routing between ISP networks]

The address spaces allocated to ISP-A and ISP-B are represented in prefix lengths of 17 bits and 18 bits, respectively. Multiple, consecutive network addresses that belong to Class [C] are used in these address spaces.

ISP-A and ISP-B use RIPv2 as a routing protocol, and it was decided to use RIPv2 in the connection between ISP-A and ISP-B as well. RIPv2, which is an extended version of RIPv1, has the following features in common with RIPv1: the [D], the number of routers that a message passes through to reach the destination network, is used as a metric for route selection; and the route information held by each router is transmitted among routers every [ii] seconds by default.

RIPv2 has a route aggregation function, and the prefix lengths at which route aggregation is performed can be configured by a router. When a prefix length of 24 bits is configured for route aggregation by the routing of routers A and B, then the sum of the numbers of entries of route information transmitted from routers A and B to the respective counterpart routers turns out to be [iii]. Furthermore, if the prefix length at which route aggregation is performed is configured at 17 bits in router A and at 18 bits in router B, then the number of entries of route information transmitted from each router to the counterpart router turns out to be 1.

[Adjustment of the communication route between ISP-B and ISP-3]

The connection of ISP-A in Company A's building and ISP-B in Company B's building was completed, and operations were initiated in the network configuration shown in Figure 1 above. Before and after the connection, the administrator of ISP-B transferred files from an open server in ISP-3 to a personal computer in ISP-B in order to check the performance of the communications. The transfer speed after the connection was found to be lower than it was prior to the connection. With cooperation from an employee who was a subscriber to ISP-3, the [E] command was used to investigate the communication path. It was found that the outgoing communication path from ISP-B to ISP-3 prior to the connection was ISP-B → ISP-2 → ISP-3 and that the incoming communication path was in reverse order. After the connection, the outgoing path was the same but the incoming path became ISP-3 → ISP-1 → ISP-A → ISP-B. Congestion of the line between ISP-3 and ISP-1 probably had some effect. The fact that ISP-1 started to transmit route information

to ISP-3 on the ISP-B network partly explains the change in the incoming path. It was impossible, by performing ISP-B control, to return the incoming path to its former state. Therefore, Company B asked the telecommunications company handling ISP-1 to resolve this problem.

BGP is used as the routing protocol between ISP-1 and ISP-3. The route selection metric to which the highest priority in operation is given is the number of ASs (Autonomous Systems) that traffic passes through to reach the destination network. The communication path on which the number of ASs is the smallest is selected as the optimum communication path. ISP-1, ISP-2, and ISP-3 each constitute an AS. ISP-1 statically sets route information on ISP-A and ISP-B by means of router 1, and transmits this information to ISP-3 as route information on the ISP-1's AS. ISP-2 statically sets route information on ISP-B by means of router 2, and similarly transmits this information to ISP-3.

The telecommunications company handling ISP-1 (III) altered the metric values for the route information to be transmitted to ISP-3, thereby providing the communication path requested by Company B. In this regard, the communication line between ISP-1 and ISP-3 is owned by the company providing ISP-1. It was planned to replace this communication line with a high-speed line. This plan was implemented ahead of schedule.

Subsequently, the route information metric value changed by ISP-1 was returned to the original value, and it was confirmed that there was no problem with communication. Thereafter, the connection between ISP-B and ISP-2 was removed.

Subquestion 1

Fill in the blanks [A] through [E] in the text with the correct term or phrase.

Subquestion 2

Answer the following questions, (I) through (III), regarding [Connection between ISP networks].

(1) Fill in the blank [i] in the text with the correct numerical value.

(2) Explain briefly why load balancing has not been not efficiently performed in the case of the default key setting described in underline (i) of the text.

(3) Describe two faults that can be detected by the link-fault signaling function described in underline (ii) of the text. Give a summary of each fault.

Subquestion 3

Answer the following questions, (1) and (2), regarding [Routing between ISP networks].

(1) Fill in the blanks [ii] and [iii] in the text with the correct numerical values.

(2) Describe two problems caused by not performing route aggregation when the number of communication paths increases. Give a summary of each problem.

Subquestion 4

Regarding underline (III) in the text on [Adjustment of the communication route between ISP-B and ISP-3], answer the destination network whose routing information was changed. Also describe how the metric values were changed using the term “AS.”