October, 2007

Network Engineer Examination (Afternoon, Part 2)

Questions must be answered in accordance with the following:

Question Nos.	**Q1 – Q2**
Question Selection	**Choose 1 question from the 2 questions**
Examination Time	**14:10 - 16:10 (120 minutes)**

Instructions:

1. Choose 1 question from the 2 questions, and encircle the question number 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 both question numbers are encircled, the answers of the first question will be scored.

Encircle 3 question numbers below.
Q1
(Q2)

[An example when Q2 is chosen]

2. Use a pencil to write your answers on the answer sheet. If 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 security measures on a network, then answer Subquestions 1 through 5.

Company Y is an electronic equipment wholesale company with 300 employees and contracts the distributorship agreement with 200 dealers (hereinafter, “dealers”). Its head office is located in Tokyo. This company has one sales office in Osaka and one in Nagoya. Forty employees work in Company Y’s Osaka sales office and 20 employees work in its Nagoya sales office. The LANs in the head office and the sales offices (hereinafter, “in-house LANs”) are connected using a wide-area Ethernet service (hereinafter, “wide area Ether”). The in-house LANs are operated using a single network address. Various servers and personal computers (hereinafter, “PC[s]”) are connected to the in-house LANs, thereby constituting a network system. Figure 1 shows the network system configuration of Company Y.

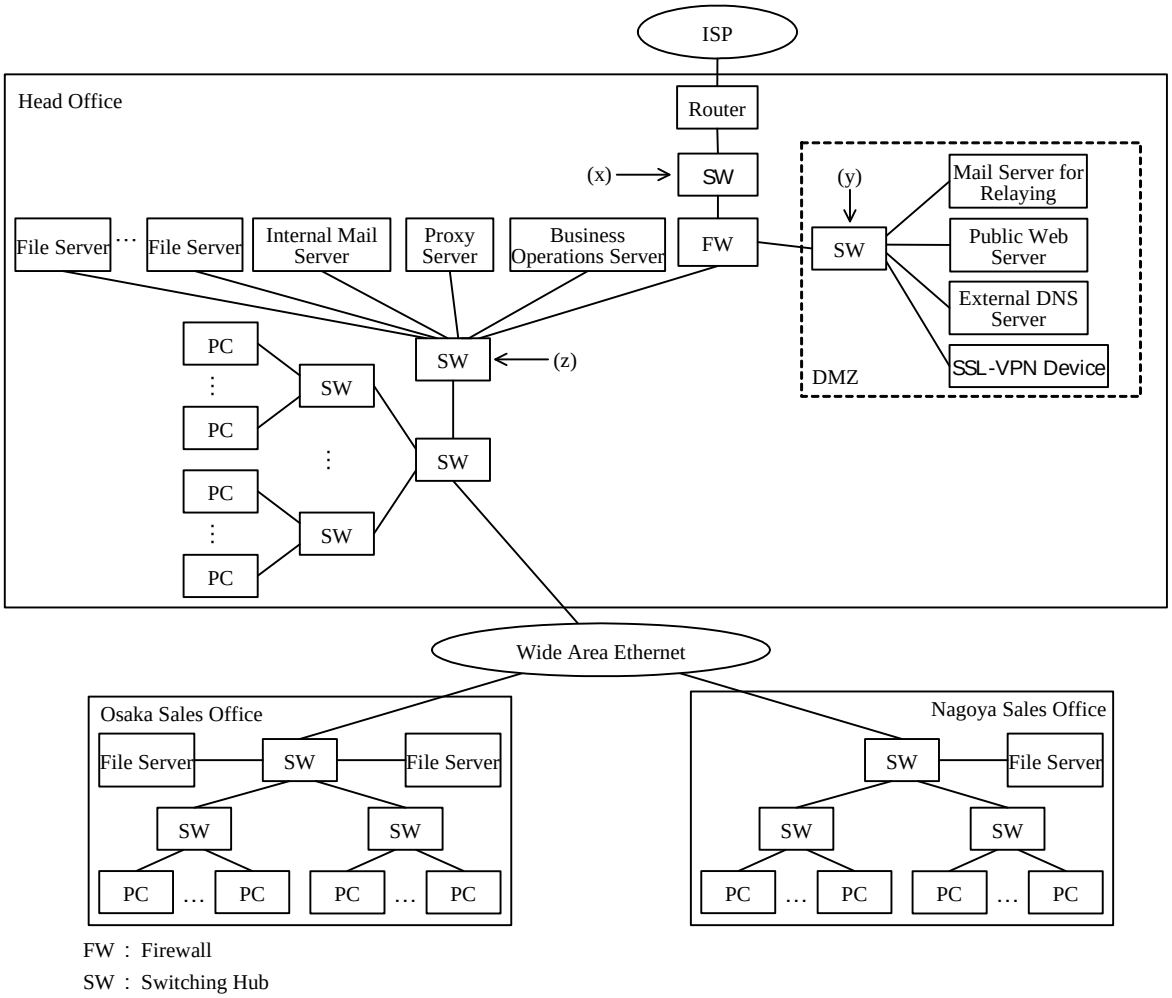


Fig. 1 Network System Configuration of Company Y

[Method of operating network system]

In Company Y, PCs have been introduced for the use of all employees and are being utilized for business purposes over in-house LANs. One hundred salespersons carry PCs with them to give presentations to customers and to use the business operations system to retrieve product information, confirm inventory, and process order fulfillment.

Furthermore, in Company Y a connection has been established from the head office to the Internet, which can also be used from the sales offices via the wide area Ether. An e-mail server for in-house use has been installed on the internal side of the FW, and employees in the head office and sales offices not only receive e-mail messages (hereinafter, "mail[s]") from the mail server for in-house use, but also transmit mails to destinations inside and outside the company via the mail server for in-house use. The following are installed in DMZs: a mail server that relays mail transmission/reception to and from locations outside the company; a Web server for open services; a DNS server for external destinations; and an SSL-VPN device. The SSL-VPN device is a device that enables the business operations system operating on the business operations server to be used via the Internet. From the in-house LANs, it is possible to transfer files via the Web or FTP in addition to transferring mail. Transferring files via the Web or FTP is performed via a proxy server.

Information required for the use of the network, such as IP addresses, is set and fixed in each PC. Employees in the Osaka sales office and the Nagoya sales office make use of various servers installed at the head office in addition to the file server located in each sales office. Moreover, when these employees make business trips to the head office, the PCs they carry with them are connected to the LAN in the head office, and they are thereby able to perform business operations. When a salesperson needs to use the business operations system from outside the company, the following procedures must be followed. First, a connection is made to an SSL-VPN device and authentication is received. Then, not only does the business operations system become available, but also the communication data is encrypted.

Antivirus software runs in the mail server for in-house use, thus performing virus checks on mails transferred from inside and outside the company. In addition, antivirus software runs on the proxy server, thereby preventing virus intrusion through HTTP and FTP. Antivirus software is also installed on each PC. When virus definition files or security patches for the OS need to be updated, the person in charge in Company Y's Information Systems Department notifies all employees accordingly, urging them to perform the update. The Information Systems Department held meetings for all employees when the antivirus software was introduced to explain the necessity of performing this work and to instruct them in how to do it. Subsequently, relevant explanations have been given to new staff as part of employee training.

[Occurrence of security problems]

Company Y recently encountered two security problems and was compelled to devise countermeasures. The first problem was information leakage via mails. The company's confidential information on wholesale rates that the sales staff and some other employees are authorized to access was leaked; complaints were received from multiple dealers. The company was at a loss over how to cope with this matter. It was suspected that the information was leaked via mails, but the leakage path and the perpetrator were not identified. Therefore, it was impossible to take strong measures.

The second problem was damage to the in-house LANs caused by a virus. A virus infected the in-house LANs from a PC used by a certain salesperson, with the result that the network system stopped for a full day.

Reflecting on these problems, it was decided to devise measures to prevent both information leakage via mails and virus infections that may result in network system stoppage. Thus Mr. M, manager of the Information Systems Department, instructed Mr. N, supervisor of its network infrastructure section, to devise countermeasures.

[Estimation of the amount of damage]

Mr. N decided to estimate the amount of damage that resulted from the security problems that occurred recently. First, an estimation was made of the amount of damage resulting from the information leaked via mails. The persons concerned were interviewed, and the following information was discovered.

- Multiple salespersons, including the general manager of the Sales Department, spent the workload equivalent of about five person-days in total in order to resolve the problem.
- Multiple dealers requested a revision of the wholesale rates, and there was no choice but to reduce the wholesale rates for two dealers. The estimated result of this revision will be an income decrease of approximately three million yen per year.

Next, the amount of damage caused by the network system stoppage due to the virus was estimated on the basis of the damage calculation model shown in Figure 2.

[amount of primary damage by the virus]
= [tangible damage amount] + [intangible damage amount]

(1) [tangible damage amount]
= [lost profit] + [system recovery cost]
= (a1 × a2) + (a3 × a4 × a5 + a6)

(2) [intangible damage amount]
= [cost due to reduction in business operation efficiency during system stoppage]
+ [cost of general business operations that were devoted to recovery]
= (b1 × a2 × a7 × b3) + (b1 × b2 × a7)

Fig 2 Damage Calculation Model

The descriptions of items a1 through a7 and b1 through b3 in Figure 2 are as shown below.

a1: profit per hour (yen)
a2: system stoppage time (hours)
a3: labor cost per hour (in the information systems management section) (yen)
a4: time required for system recovery (hours)
a5: number of persons required for system recovery
a6: purchase cost of replacement hardware and software (yen)
a7: number of persons who suffered damage by the virus
b1: labor cost per hour (in business operations section) (yen)
b2: time required for business operations recovery (hours)
b3: operational efficiency reduction rate

Mr. N sorted the damage status as follows, and used this information as conditions for the estimation of the damage.

- A virus intrusion caused the whole network system to stop for eight hours. Forty PCs were infected with the virus. For an average of 12 hours, the users of the 40 infected PCs were unable to carry out operations using their PCs, because the virus removal process was performed only after the network system was recovered.
- Two people from the Information Systems Department took charge of the system recovery work, including restoration of the network system and removal of the virus from the PCs, which took 16 hours in total.
- Two hundred and fifty employees suffered damage due to the network system stoppage or the virus infection. After the network and PCs were restored, these employees spent an average of four hours in business-operations recovery work, such as inputting data to enable normal operations, checking consistency, and processing mails.

- The labor cost, which is the same for both sections, is 4,000 yen per hour. The operational efficiency reduction rate due to the network system stoppage is 0.3.
- There was no lost profit. Replacement hardware or software for recovery was not purchased.

The amount of the primary damage caused by the virus was calculated on the basis of these conditions. The tangible damage amount was calculated to be 128,000 yen, while the intangible damage amount was calculated to be 6,592,000 yen.

The damage amounts due to information leakage and the virus intrusion were larger than expected. Therefore, Mr. N judged that a certain level of investment would be necessary for measures to prevent such damages.

[Measures to prevent information leakage via mail]

First, Mr. N examined possible measures to prevent information leakage via mail. A mail filtering system was examined as a technical preventive measure. However, the workload required to increase the filtration accuracy to the point where it could prevent information leakage via mail was so high that it was judged impossible to introduce this system under the current company structure. An examination was made of prohibiting file attachments, and a number of employees were asked to give their opinions about this. Many answered that such prohibition would affect their business operations. Therefore, it was considered difficult to adopt this method.

After examining a number of preventive measures, it was deemed advisable to strengthen managerial measures and to implement them together with technical measures. For managerial measures, it was decided to clarify the information that should be protected by the enterprise, including trade secrets such as transaction records, confidential information such as investment plans, and [A] such as lists of seminar participants. In addition, it was decided that the employees allowed to use these categories of information should be kept to a minimum, and that access to this information should be strictly controlled. Moreover, it was decided that rules regarding the exchange of mail would be created and that mails would be audited. All employees will be notified of these rules. The introduction of mail auditing is expected to force the employees to only exchange mail on the basis of these rules. On the technical side, it was decided to introduce a mail collection system by which transmitted/received mails would be archived and the transmission/reception history could be securely stored for the purpose of mail auditing.

The mail collection system was equipped with auditing functions such as functions to search collected mails for multiple criteria, to display mail contents, and to conduct various analyses. Possible collection methods included the relay type and the traffic monitoring

type (hereinafter, “monitoring type”). The relay type is a method by which a mail is first received via SMTP, the received data is recorded in a memory device, and the data is transferred to a specified transfer destination. On the other hand, the monitoring type is a method whereby mail-related packets flowing on a LAN are extracted and these packets are recorded in a memory device. Both types have advantages and disadvantages. It was decided to adopt the monitoring type for the purpose of collecting all transmitted/received mails.

In order to collect all mails transmitted/received with a monitoring-type mail collection system, it is necessary to nondisruptively extract mail-related packets. Moreover, the extraction process and the audit-related process should be carried out simultaneously. Therefore, thought was given to an arrangement whereby these two processes could operate separately on two different servers that would be mutually independent as a packet extraction device or a mail audit device. In order to configure this, it is necessary for the two servers to be capable of sharing a magnetic disk device that can store the collected mail (hereinafter, “disk”). This can be made possible by using a SAN (Storage Area Network) or a(n) [B]. A SAN is a network that consists of fiber channel switches and serves to share storage. A(n) [B] is a storage device that is connected to a LAN and uses a file-sharing protocol to enable file sharing. For disk sharing, it was decided from past experience to adopt a(n) [B], which is easier to operate. Figure 3 shows the configuration of a monitoring-type mail collection system.

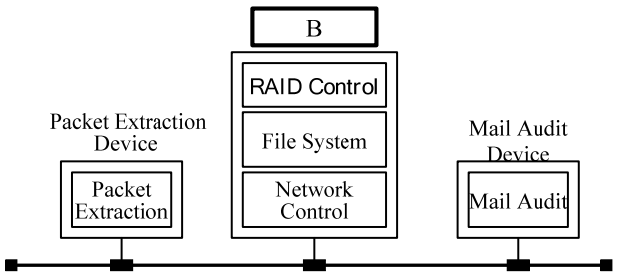


Fig. 3 Configuration of Monitoring-Type Mail Collection System

With this monitoring-type mail collection system, it became possible to prove that the stored data has not been [C] and that the data creation dates are valid, thus allowing the stored data to be considered as admissible evidence. These results were realized by adding electronic signatures and [D], each of which shows a data creation date.

[Measures to prevent network system stoppages caused by viruses]

The following were considered as possible measures to prevent virus infections leading to network system stoppages: imposing connection restrictions on PCs, conducting status

inspections, and performing remedy processing (hereinafter jointly referred to as "quarantine processing").

For connection restrictions, a method was adopted whereby a user is authenticated when using the network system with a PC connected to the in-house LANs. It was decided to use IEEE 802.1x for user authentication. Figure 4 shows an outline of the authentication procedure based on IEEE 802.1x.

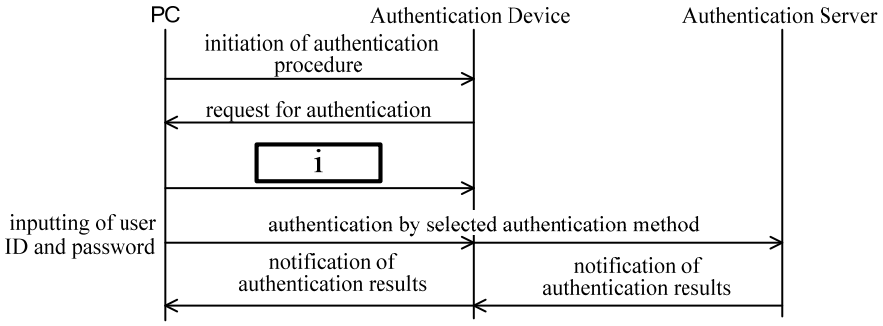


Fig. 4 Outline of Authentication Procedure Based on IEEE 802.1x

In the case of IEEE 802.1x, the following are used to make an authentication request using the EAP (Extensible Authentication Protocol): a(n) [E] implemented on a PC, an authentication device, and an authentication server. As regards IEEE 802.1x, multiple authentication methods can be used. After considering the ease of operation, it was decided to utilize not EAP-TLS, in which (I) digital certificates are used to authenticate users, but EAP-PEAP, in which user IDs and passwords are used.

After examining ways to impose connection restrictions on PCs, Mr. N requested that Mr. T at an SI company propose a quarantine system that uses authentication based on IEEE 802.1x and an authentication switching hub that has a dynamic VLAN function (hereinafter, "authentication SW"). Figure 5 shows the configuration of the quarantine system proposed by Mr. T.

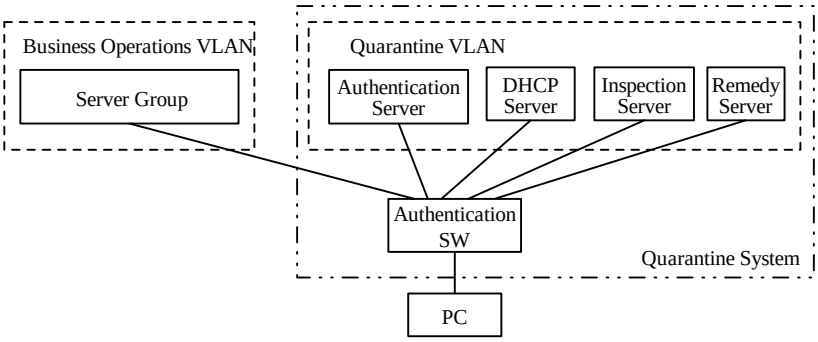


Fig 5　Configuration of Quarantine System Proposed by Mr. T

In Mr. T's proposal, an inspection server would inspect the status of the PCs' compliance with security standards, and a remedy server would implement measures to cause PCs that were not taking appropriate security measures to comply with the security standards.

The following is part of the procedures for user authentication, the distribution of network information, and the quarantine processing that Mr. T explained on the basis of Figure 5.

(1) After startup, the PC initiates the authentication procedure.
(2) The authentication screen is displayed on the PC.　The PC user enters his/her user ID and password following the prompts on the screen.
(3) The authentication SW makes an authentication request to the authentication server on the basis of the received data.　When the PC user is authenticated as an authorized user, the authentication server notifies the authentication SW of the authentication permission.
(4) The authentication SW notifies the PC of the authentication permission.
(5) The PC requests the DHCP server to provide necessary information such as the IP address.
(6) The DHCP server provides this necessary information to the PC.
(7) The inspection server checks the status of the PC regarding the application of [F] to the OS and [G] for the purpose of preventing virus infections, then displays the inspection results on the PC and notifies the authentication server accordingly.　If the inspection result meets security standards, the procedure continues at step (10) directly from this step.
(8) If security standards are not met, a security vulnerability warning is displayed on the PC.　The PC user then performs operations to receive the updates of [F] and [G] from the remedy server.
(9) After the update processing, the remedy server instructs the PC to check for viruses.

After completion of the virus check, the remedy server instructs the PC to restart, and notifies the authentication server of the completion of quarantine processing. By restarting, the PC returns to step (1).

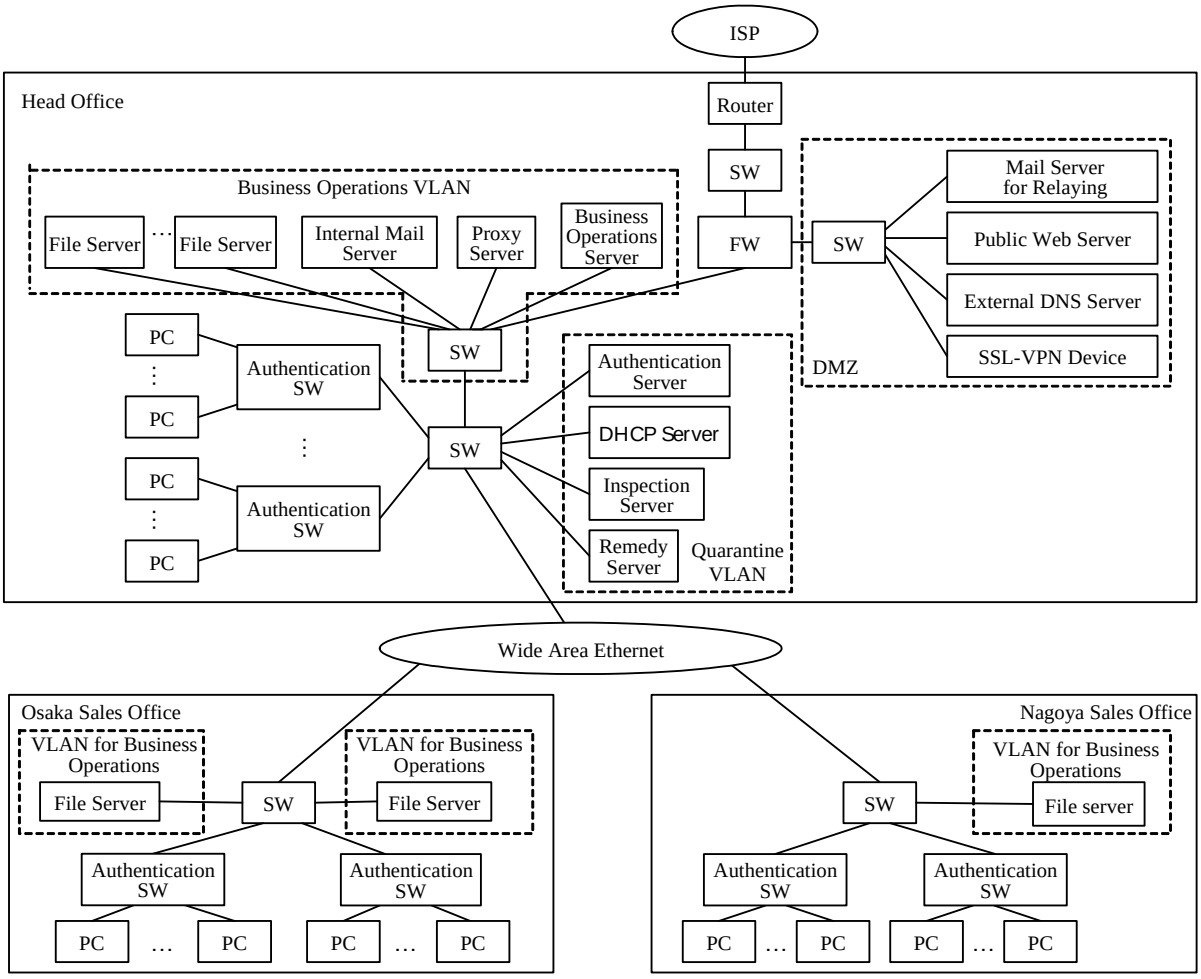
(10) The VLAN to which the PC belongs based on the configuration by the authentication SW is changed from a [ii] to a [iii] through (II) processing performed by the authentication server and the authentication SW.

(11) The PC is allowed to use the network system.

In the quarantine system shown in Figure 5, it is necessary to initialize the VLAN configured by the authentication SW as well as the authentication permission status retained by the authentication server in order to maintain the security status. If termination processing of the PC is normal, processing for VLAN resetting is executed on the PC, and the VLAN and the authentication permission status are initialized. However, if termination processing of the PC is abnormal, processing for VLAN resetting is not executed on the PC, and therefore, the authentication SW cannot initialize the VLAN and the authentication permission status. As a result, the problem arises that once a PC obtains authentication permission, the PC can use the network system even if quarantine processing is not performed. In order to solve this problem, (III) the authentication SW has the function of monitoring the statuses of the subordinate PCs.

[New network system configuration]

On the basis of the above examination, Mr. N planned measures for the introduction of a mail collection system and a quarantine system. By introducing these systems, it is possible to restrain and detect information leakage via mail as well as to prevent virus intrusion. (IV) In addition to these intended merits, it is also possible to obtain other positive effects on the operation of the network system. Figure 6 shows a new network system configuration into which the planned measures have been incorporated.



Note: The mail collection system is omitted here.

Fig 6　New Network System Configuration Incorporating the Planned Measures

In the configuration shown in Figure 6, if a PC infected with a virus is connected, there is a risk that the following two problems will occur: First, in the head office, the quarantine processing will be affected.　Second, in the sales offices, the use of the Internet as well as business processing and the quarantine processing that utilizes the servers in the head office will be affected.　However, it was decided to adopt the above configuration, because this configuration requires only a small investment amount and also because (V) the original goal can be achieved with regard to antivirus measures.

After the above conclusion was reached, Mr. N decided to report these planned measures to Manager Mr. M.

Subquestion 1

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

Subquestion 2

Answer the following questions, (1) through (3), regarding the mail collection system.

(1) From Figure 1, select two devices, other than the FW, for which it is necessary to change the contents of the settings when a relay-type mail collection system is installed.
(2) From positions (x) through (z) in Figure 1, select the location for installing a packet extraction device capable of collecting all mails transmitted/received in Company Y. In addition, give a summary of the contents of the SW setting that should be carried out when this device is installed.
(3) When the system in Figure 3 is installed, the LAN configuration must be considered carefully from the point of view of the traffic. Give the point to be considered briefly.

Subquestion 3

Answer the following questions (1) and (2), regarding the damage by the virus and the measures.

(1) How much was the cost, in yen, of general business operations that were devoted to recover from the virus infection?
(2) Explain briefly the operational problems that enabled the virus damage to occur.

Subquestion 4

Answer the following questions (1) through (3), regarding user authentication.

(1) Describe necessary information for authentication transmitted as a reply in the blank [i] in Figure 4.
(2) Describe two task items briefly that impose high operation loads on the administrator, regarding underline (I) in the text.
(3) Give the name of the layer of the OSI basic reference model on which the user authentication protocol is contained. In addition, explain the grounds for the selection of the layer on the basis of the procedures explained by Mr. T.

Subquestion 5

Answer the following questions (1) through (5), regarding the new network system into which the planned measures were incorporated.

(1) Describe the content of the processing briefly that the authentication server performs for the authentication SW indicated in underline (ii) in the text.
(2) Fill in the blanks [ii] and [iii] in the text with the correct term or phrase.
(3) Describe two monitoring methods briefly regarding underline (iii) in the text.
(4) Describe two positive effects briefly, regarding underline (iv) in the text.
(5) Explain the original goal mentioned in underline (v) in the text, indicating the target devices.

Q2. Read the following description concerning network restructuring, and then answer the Subquestions 1 through 5.

Company F is a specialty firm that handles chemical products. Five years ago, the Systems Planning Department of Company F established a standard configuration of its servers which consists of disk units and tape units and constructed a DNS, a business system, and groupware as company-wide shared systems. It also constructed a company network and has been managing the operation of the shared systems and the company network.

Company F has ten departments, each of which has been operating its own departmental system. Each department constructed its departmental system using the standard server configuration established by the Systems Planning Department.

[Situation of the Company System]

Figure 1 shows the configuration of the company system.

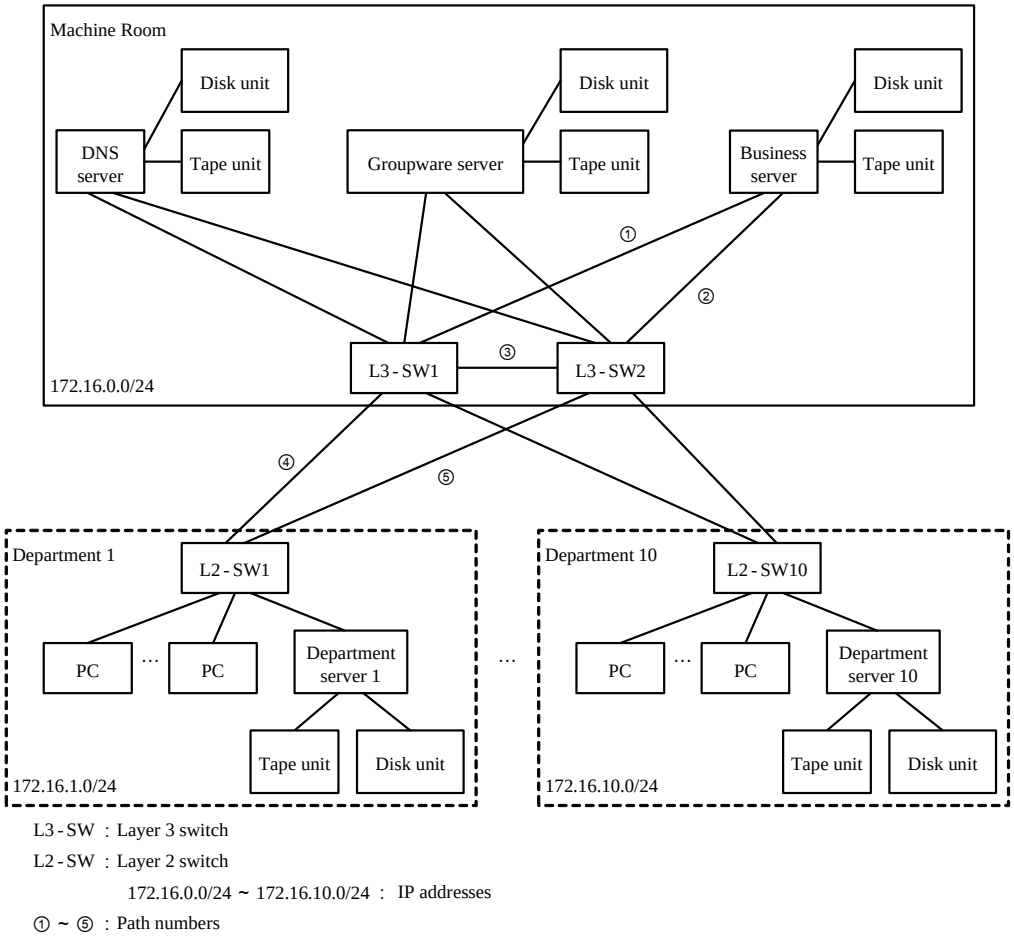


Fig 1 Configuration of the Company System (excerpt)

The company network consisted of two L3-SWs installed in the machine room and an L2-SW installed in each department. The L3-SWs and the L2-SWs were connected by

VLANs for each department, with double paths using the spanning-tree protocol. The L3-SWs were made redundant using the VRRP (Virtual Router Redundancy Protocol); normally L3-SW_1 was set as the master switch in the operation system. Due to the nature of the work, there was no need for a PC in one department to access the server of another department, so inter-departmental routing was disallowed by the definition of the L3-SW.

Each server in the shared systems was actually two LAN interfaces with an identical IP address, stored in one VLAN. The two LAN interfaces were controlled by the OS function of the server; normally, the L3-SW_1 side was the operation system whereas the L3-SW_2 side was the stand-by system. When the operation system encountered trouble, it would automatically be switched to the stand-by system (this function is referred to as the multi-path function hereafter).

Each departmental server was connected to an external disk unit and, for data backup, a tape unit as well. Partial backup was done on a daily basis, and full backup was done on a weekly basis.

Several years had passed since the beginning of this company system operation when various people started to complain about the processing performance of departmental servers and the insufficient capacities of disk units. Further, the servers are aging, getting worn out, and hardware failures and other problems are causing service interruptions more often. In one department, during data recovery following a disk failure, it was discovered that the data were not backed up properly, resulting in loss of data.

Given these circumstances, the Systems Planning Department has decided to review the current company system configuration and to construct a new company system. As a preparatory step, Manager H of the Systems Planning Department has instructed one of his subordinates, Mr. T, to investigate the current situation of the company system.

According to the results of Mr. T's investigation, a department which complained of insufficient disk unit capacity was already using at least 90% of the capacity. The disk was used not only to store the databases of the departmental system but also to store files created on PCs so that these files can be shared within the department. On the other hand, there were departments that were not using the disk as much. The total disk usage of the entire company was found to be about 60% of the total capacity.

In those departments with heavy disk usage, the backup processing time was increasing. The number of tapes used had grown so much that, during full backup, it was necessary for someone to actually change the tapes during the process.
Furthermore, the servers, the disk units, and the tape units were supposed to be stored on designated racks, but some departments had them on work room shelves or under a desk.

Based on these study results, the Systems Planning Department established the following basic policies for the construction of a new company system:

- Servers will be replaced with a new type for better server performance.
- For enhanced capacity management and effective use of the resources, the disk units connected to the servers will be aggregated to a large-capacity disk unit.
- To integrate the backup operation management, a large-capacity tape library unit will be installed.
- As a measure to improve information security, all servers, disk units, and the tape library unit will be placed in the machine room.

Manager H and Mr. T have begun discussing this new company system. First, they discussed the aggregated system for the disk units.

[Aggregated System for the Disk Units]

Disk units are aggregated by using SAN (Storage Area Network) or NAS (Network Attached Storage) instead of the DAS (Direct Attached Storage) directly connected to the server. There are two types of SAN: one type, FC-SAN, uses fiber channels, and the other, IP-SAN, uses an IP network.

In an FC-SAN, combinations of servers and the disk units to be connected to them can be defined using the [A] function. In an IP-SAN, often VLANs are used to do similar control.

In an IP-SAN, communication between a server and a disk unit is established by using [B], which is the extension of the input/output protocol used in the DAS for use in TCP/IP communication. With NAS, data on a disk unit are accessed from a PC or a server through a protocol for [C], such as NFS.

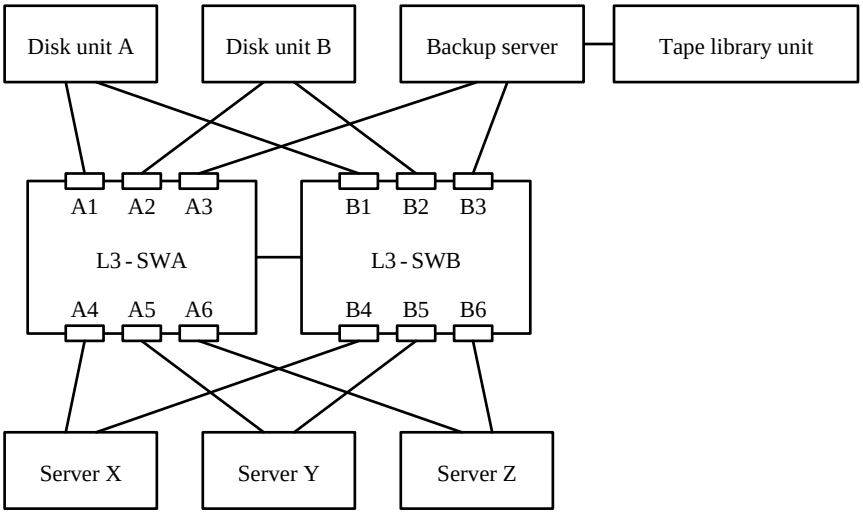
There are two usage modes for a disk unit. One is the mode where server databases are saved and are accessed from the server (hereafter referred to as server storage). The other is the mode where files used by PCs and servers are saved and shared (hereafter referred to as shared storage). Taking into account the current usage of the company system, Company F has decided to use both of these modes.

As for server storage, because DBMS is running on the business server and the departmental servers, it is necessary to have access to [D] devices instead of access through the file system. For this reason, for server storage, SAN will be used instead of NAS. Judging from the size of the company system and the technology the company has, it was decided that IP-SAN is the type of SAN that will be used by the company. On the other hand, it was decided that NAS will be used for shared storage since access from PCs will be central for this storage.

This is the first time SAN will be used at Company F, so Manager H has instructed Mr. T to consider a specific configuration of SAN and explain the details.

[Configuration of SAN]

Mr. T created a configuration (conceptual) of SAN as shown in Figure 2 and explained it to Manager H as follows:



Note: A1 through A6 and B1 through B6 inside the L3-SW indicate port numbers.

Fig 2 Configuration (conceptual) of SAN

Mr. T: Figure 2 is an excerpt of the configuration of the SAN we are going to install this time. The servers and the disk units are connected to both of the L3-SW units using the multi-path function, but all of these devices will have the LAN interface on the L3-SW_A side as the operation system. Each server uses only one of the two disk units. Here, let us assume that Server X uses Disk Unit A while Servers Y and Z use Disk Unit B.

Manager H: Explain to me why you will have two disk units in the SAN.

Mr. T: One disk unit is to store data from the business server and the departmental servers; the other disk unit is to store data from all other servers.

Manager H: According to this configuration, it seems that Server X can access Disk Unit B as well, doesn't it?

Mr. T: No, we disallow such access by defining VLANs properly.

Manager H: So then, how is backup done?

Mr. T: We use the backup server connected to a large-capacity tape library unit. Backup will be direct, without going through the individual servers from the disk units. The backup server collects data directly from the two disk units, so it accesses both disk units.

Manager H: But the two disk units belong to different VLANs, so the backup server cannot access both of them, can it?

Mr. T: The access is possible because we use the inter-VLAN routing function of

L3-SW. Let's summarize these. The definitions of the VLANs and routing to be set up in L3-SW_A and L3-SW_B are as shown in the table below:

Table Definitions of VLANs and Routing to Be Set Up at L3-SW_A and L3-SW_B

VLAN	Port number belonging to VLAN	VLAN that permits the routing
VLAN-1	A1, [i]	[iv]
VLAN-2	[ii], B6	[v]
VLAN-3	[iii]	VLAN-1, VLAN-2

Manager H: I understand the setting for L3-SW. But wasn't there any way to use L2-SW in the SAN?

Mr. T: Actually, (i) there is a way to use L2-SW. But if you do, the access control between the servers and the disk units would depend on the hardware, so the maintenance would be very hard. That's why I thought we should use L3-SW this time.

Manager H: I see. Go ahead and consider a configuration plan for the new company system then.

[Configuration Idea for a New Company System]

Under the direction of Manager H, Mr. T came up with a configuration idea for a new company system.

In this new company system, three networks are defined: SAN, server LAN, and client LAN. The SAN is an IP-SAN-only network, and all of its component devices will be newly installed. The server LAN is a network to cover the servers, where two new L2-SWs and each server will be installed anew, and two existing L3-SWs will also be used. The client LAN is a network to cover the PCs, and existing devices will be used.

Figure 3 shows the configuration idea for this new company system considered by Mr. T.

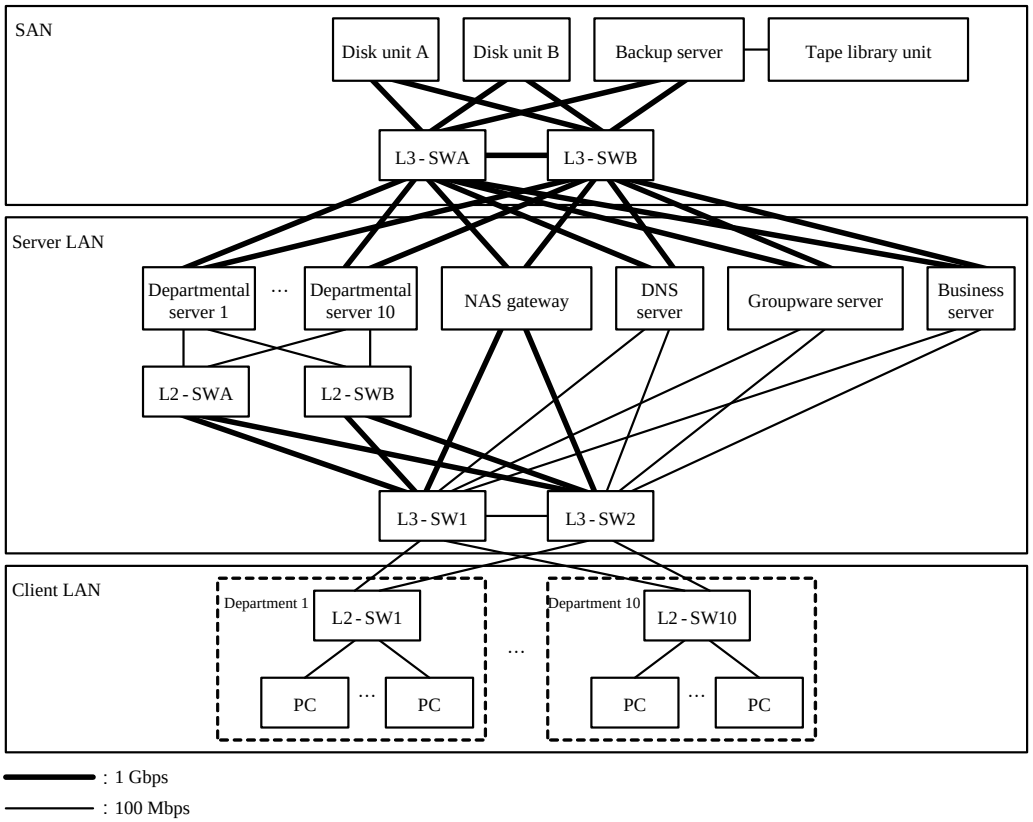


Fig. 3 Configuration Idea for a New Company System (excerpt)

The following is a conversation between Manager H and Mr. T concerning the configuration idea for the new company system:

Manager H: Let's begin with the server LAN. Can you explain it?

Mr. T: Sure. The current L3-SW does not have unused ports, so L2-SW_A and L2-SW_B will be newly installed, and we will connect the departmental servers to them. In the current company network, PCs in one department cannot access servers of other departments, so we need to disallow the access in the same way in the new company network, also. Since VLAN data travel back and forth between the L2-SWs and L3-SWs on one port and cable, we need to set up [E] VLANs; at the L3-SWs, we will disable unnecessary routing between VLANs.

Manager H: Are you going to change the IP address of each server?

Mr. T: The IP address of each departmental server will be changed. Access from PCs to departmental servers use the host names, so during the transition, the definition information on the DNS server will also be changed. On the other hand, for the DNS server, the groupware server, and the business server, the same ports of the L3-SW will still be used, so I am not going to change their IP addresses.

Manager H: Isn't there a way so that you won't have to change the IP addresses of the departmental servers?

Mr. T: Yes, there is. For instance, we can define the VLANs so that the VLAN to which a departmental server belongs will be the same VLAN to which the L2-SW of that department belongs. But then the network setting gets complicated. That's why I thought about changing the IP addresses of the departmental servers instead.

Manager H: I see. By the way, what kind of devices are in the configuration of the NAS?

Mr. T: The NAS consists of an NAS gateway installed in the server LAN and the disk unit B installed in the SAN.

Manager H: Okay. Next, I see that the paths with 1Gbps and 100Mbps are mixed together. Can you explain why?

Mr. T: Yes. First, for the SAN, to maintain the server response, I set the speed at 1Gbps everywhere. Our studies of the current company system suggest that there are no significant problems with connection between the servers on the server LAN and the L2-SW or L3-SW, so I left the speed at 100Mbps for now. Between the L2-SWs and the L3-SWs on the server LAN, access from multiple departments share the same path, so I set the speed at 1Gbps. Also, between the L3-SWs and the NAS gateway on the server LAN, I set the speed at 1Gbps because the NAS gateway gets accessed by PCs from multiple departments.

Manager H: The path between L3-SW1 and L3-SW2 still has a speed of 100Mbps, but does this not cause a problem when the path is changed due to a failure?

Mr. T: This path is used as a detour route when there is a problem with the path between the L3-SWs of the server LAN and the L2-SWs of the client LAN. It is rare that multiple path failures occur at the same time, so as a detour route, the rate of 100Mbps should be sufficient.

Manager H: But this detour route is also used when the path [vi] fails, too, right? Wouldn't it cause a bottleneck?

Mr. T: You are right. I overlooked that. I will change it to 1Gbps.

Manager H: I think this configuration of the new company system is pretty good now. Let's go ahead and talk about the transition. Consider a plan of the transition method and procedures for the transition.

[Transition to the New Company System]

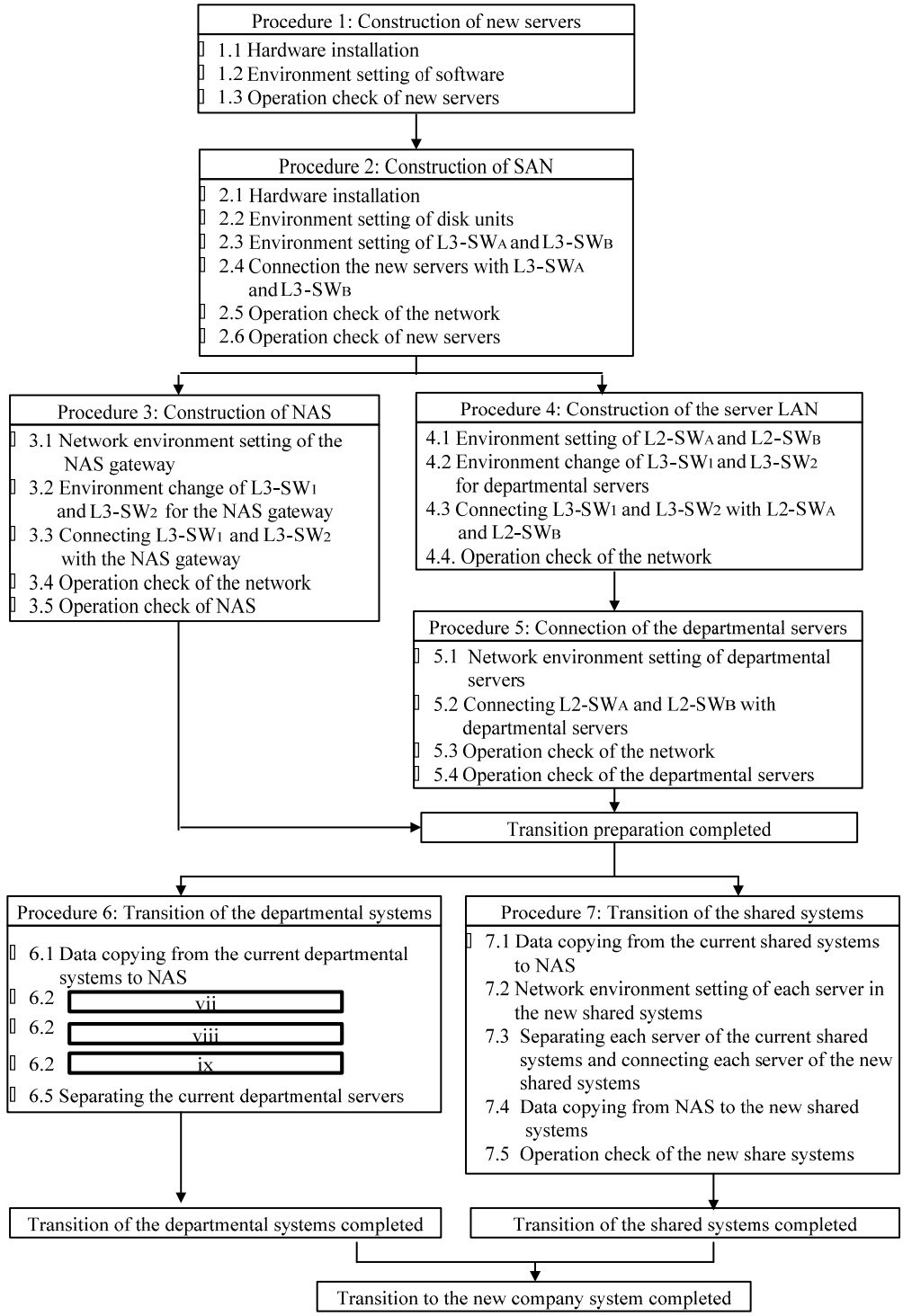
Mr. T then considered a method of transition into the new company system.

The key is how to transfer the data that are in the 10 departmental servers and 3 servers in the shared system. Ideas include using the backup tape and using the NAS. Mr. T compared these methods, and he has decided to carry out the transition using the NAS.

In addition, (ii) changes in the environment in the existing network devices could affect the work of the users, so the transition work will be carried out on holidays in general.

Having considered these issues, Mr. T has prepared his idea for the transition procedures

as shown in Figure 4, and he explained it to Manager H.



Note: New servers include the NAS gateway and the backup server, both of which are installed as new equipment. They also include the departmental servers, DNS servers, business server, and groupware server, all of which are going to be replace d by new models.

Fig. 4 Idea for Transition Procedures

Manager H and Mr. T continued these discussions even after this, and they finalized the construction plan for the new company system. Half a year later, Company F completed its transition to the new company system without incident.

Subquestion 1

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

Subquestion 2

Answer (1) and (2) below concerning Figure 1 in [Situation of the Company System].

(1) Describe the default gateway to which the PCs in Department 1 are to be set.

(2) Suppose that a PC installed in Department 1 accesses the business server in such a way that the path from L2-SW1 to the business server is ④①. Describe briefly how the path changes, when a failure occurs on path ④, using the path numbers in Figure 1.

Subquestion 3

Answer (1) and (2) below concerning the [Configuration of SAN].

(1) Fill in the blanks [i] through [v] in the table with the correct term or phrase.

(2) Describe briefly how to implement underline (i) in the text.

Subquestion 4

Answer (1) and (2) concerning the [Configuration Idea for a New Company System].

(1) Describe briefly what kind of process the NAS gateway in Figure 3 performs?

(2) Describe the path to be inserted in the blank [vi] in the text briefly.

Subquestion 5

Answer (1) through (4) concerning the [Transition to the New Company System].

(1) Using the device names in Figure 3, identify the path of data flow when the data on the current business server are copied onto NAS in Procedure 7 of Figure 4.

(2) Describe briefly the task item to be inserted in each of the blanks [vii] through [ix] in Figure 4.

(3) Concerning Procedure 4 in Figure 4, describe briefly two tasks that are referenced/implied by underline (ii) in the text.

(4) In regard to the construction of the new company system, the four basic policies established by the Systems Planning Department have been accomplished. From the standpoint of further system extension, list two more effects (positive results) of the new system.