A Network-disaster Recovery System using Area-based Network Management

Toshiaki Suzuki, Hideki Endo, Isao Shimokawa,
and Kenichi Sakamoto
Central Research Laboratory
Hitachi, Ltd.
Yokohama, Kanagawa, Japan
{toshiaki.suzuki.cs, hideki.endo.es, isao.shimokawa.sd,
and kenichi.sakamoto.xj}@hitachi.com

Hidenori Inouchi, Taro Ogawa, Takanori Kato,
and Akihiko Takase
Telecommunications & Network Systems Division
Hitachi, Ltd.
Kawasaki, Kanagawa, Japan
{hidenori.inouchi.dw, taro.ogawa.tg, takanori.kato.bq,
and akihiko.takase.wa}@hitachi.com

***Abstract*—A "network-disaster recovery system" using area-based network management is proposed. In this system, a whole network is separated into multiple areas. A network-management server calculates recovery paths for every possible network-area failure and distributes them with a recovery identifier (ID) for each area-failure pattern before starting network operations. Network nodes receive and store the recovery IDs and recovery configurations. The network-management server determines after detecting the network-area failures and distributes the recovery ID to related network nodes. The network nodes that received the recovery ID start data transmission according to the path configurations specified by the recovery ID. After these procedures are completed, the network-area failures are swiftly recovered. A prototype system composed of a network-management server and 96 simulated packet-transport nodes was configured and evaluated. According to the evaluation results, the network-management server could transmit the recovery ID to the related network nodes within 100 milliseconds after it detected network-area failures. That is to say, the network could immediately start to recover from the network-area failures. On the other hand, the calculation time for 500 Pseudo Wires (PWs) is about 344 milliseconds, which is longer than the time taken to distribute the recovery ID (i.e., 100 milliseconds). In other words, if there are over 500 PWs, the proposed system can recover more swiftly than a conventional system (which re-calculates recovery PWs after detecting the network-area failures) under the same evaluation conditions used for the proposed system.**

Keywords-network management; disaster recovery; packet transport; reliable network

I. INTRODUCTION

Lately, as reflected in the rising number of Internet users [1] and the popularity of cloud services [2], applications and services provided by way of networks have become indispensable in daily life. Network services must, therefore, be highly reliable and "always available" [3]. When extensive disasters occur, network services could be out of service for a long time. Consequently, networks must be robust enough so that they can continue to provide network services even if network facilities are extensively damaged.

As recovery procedures for network failures, two major techniques are applied. One is "protection," by which recovery paths are physically prepared in advance of network failures by allocating extra network resources. The other approach is "restoration," by which recovery paths are "calculated" after network failures are detected.

Protection is easily applied to recovery procedures for multi-layer networks, and recovery is immediate because recovery paths are prepared in advance (that is, before network operations are started). However, if the prepared recovery paths are not available when network failures occur, network-connection services will become out of service. On the other hand, if restoration is applied, network connections can be recovered if recovery paths are recalculated after network failures are detected. However, a little more time is needed to recalculate the recovery path if the operated networks are huge and have many network nodes. Therefore, if huge quantities of paths are used to transmit data packets, much time is needed to recalculate all recovery paths, and the network will not recover from a disaster expeditiously. In addition, even if network connections are recovered, all network flows will try to use the same recovery path. As a result, the network will easily become congested, making it difficult to guarantee network-transmission quality.

In light of the above-described issues, a robust network-management scheme is required. Specifically, it controls multi-layer network resources so as to provide and maintain network-connection services at times of a network disaster. To achieve that control, a network-management system has to monitor and control the multi-layer network resources.

The overall aim of the present study is to develop a network-management scheme to provide robust networks that can swiftly recover from a network disaster by monitoring and controlling multi-layer network resources. To recovery swiftly from a network disaster, three steps should be taken. The first step is to find network failures in a short time. The second is to promptly determine how to recover the network. The third is to immediately configure recovery paths. In the present study, the second step is focused on, and a "network-disaster recovery system" using an area-based network-management scheme that controls networks composed of IP networks and packet-transport networks, such as the Multi Protocol Label Switching - Transport Profile (MPLS-TP) network, is proposed.

The rest of this paper is organized as follows. Section II explains the requirements concerning a network-disaster recovery system. Section III proposes the network-disaster recovery system. Section IV describes a prototype system and presents some results of evaluations of the system

 ISBN: 978-1-61208-373-5

performance. Related works are described in Section V, and Section VI concludes the paper.

II. REQUIREMENTS CONCERNING NETWORK-DISASTER RECOVER SYSTEM

The target network structure is shown conceptually in Figure 1. The target network is composed of an IP network layer and a Packet-Transport-Node (PTN) network layer such as an MPLS-TP network. The core network is composed of PTNs. On the other hand, the access network is composed of IP network nodes. In this study, recovery from multiple network failures on IP and PTN networks (for example, the two network failures shown in the figure), is focused on as follows.

One of the critical issues concerning network recovery is the time taken to recover numerous established paths of a packet network in the case of a network disaster. Here, each path is configured by a Label-Switched Path (LSP) and a Pseudo Wire (PW). Specifically, the issue is the time taken to recalculate numerous recovery paths one by one after disconnected paths are detected by monitoring network conditions.

In the case of a packet-transport network, the bandwidth of a network path is guaranteed. Guaranteeing the quality of a recovery path, such as bandwidth and/or end-to-end delays before (as well as after) a network failure, is therefore also an issue.

To tackle the above-mentioned issues, the proposed system should be managed in accordance with the following four requirements.

① Manage multi-layer networks
② Recover from multiple network failures
③ Rapidly establish recovery paths
④ Guarantee quality of recovery paths after network failures are recovered

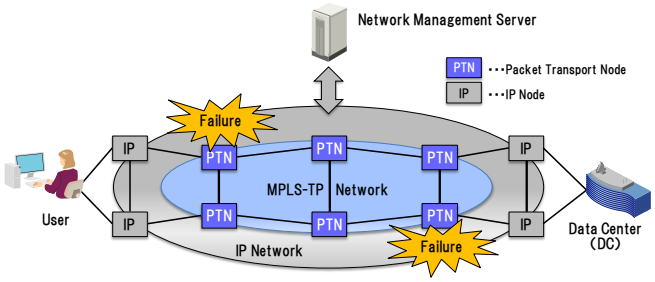

Figure 1. Target network structure

To meet these requirements, the network-disaster recovery system is designed on the basis of the following policy. If there are plenty of paths, recovery paths should not be recalculated after multiple network failures are detected (since it takes much time to recalculate them). On the other hand, recovery paths that guarantee bandwidths and delays for each possible network failure should be calculated preliminarily, and paths should be promptly recovered by using the prepared paths after the network failures are detected.

III. PROPOSED NETWORK DISASTER RECOVERY SYSTEM

In the proposed network-disaster recovery system, a network-management server centrally manages an entire network. In the target network, a core-network segment is composed of PTNs, and an access-network segment is composed of IP network nodes. In addition, the network-management server manages the entire network by dividing it into multiple network areas and controlling each of them by using an area-based network-management scheme.

A. Structure of proposed system

The structure of the proposed network-disaster recovery system is shown in Figure 2. As an example of an area-based management, the network-management server divides the whole PTN network into eight areas and manages them by using the area-based management scheme. The eight areas are shown as network areas (1) to (8) in the figure. In addition, the network-management server is connected to all PTNs, a user terminal, and servers in a datacenter (DC) by another management network (not shown in the figure). The network-management server monitors all PTNs and executes swift network-disaster recovery after detecting catastrophic network failures.

As for the proposed disaster-recovery system, the user terminal is connected to a server in a DC by way of IP networks and PTN networks, and it can get various application services from the server. To provide the user terminal with robust network access, the user terminal is connected to two "PTN network areas," at least. In addition, the DC is connected to two other "PTN network areas", at least.

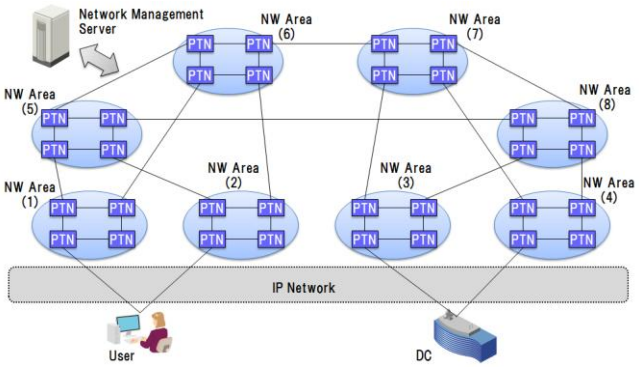

Figure 2. Proposed network-disaster recovery system

B. Overview of network-disaster recovery system

The procedures used by the proposed system for network-disaster recovery are overviewed in Figure 3. In the first procedure, the network-management server divides an entire PTN network into eight network areas, labelled (1) to (8) in the figure, and controls them by using the area-based network-management scheme. In addition, it configures the path shown as a solid line in the figure as the current path so that the user can access the server in the DC and use application services.

In the second procedure, the network-management sever calculates all recovery paths preliminarily by considering all

possible area-based failures. Specifically, the number of possible area-based failure patterns is 255 (since there are eight areas, and each area could be independently active or not active), namely, 256 (i.e., 2^8) patterns minus a "no area failure" pattern that is the current network operation. The network-management server assigns a recovery ID for each area-based network failure pattern and stores each recovery ID with information on the recovery paths. It then distributes all recovery IDs and the recovery-path information to all PTNs preliminarily. In Figure 3, it is assumed that network areas (1), (3), and (6), as stated in the figure, fail. In the case of these failures, a path depicted by a dashed line is prepared as a recovery path, and the recovery-path information is distributed to PTNs related to the recovery path before network operations are started.

During network operations, the network-management server monitors area-based network failures. When it detects area-based network failures, it determines a failure pattern and a recovery ID, and it then distributes the recovery ID to related PTNs, a user terminal, and a server in the DC. The PTNs that receive the recovery ID start to promptly recover and transmit packet data according to the recovery-path information specified by the ID. In addition, the network-management server configures IP networks to transmit packet data from the user terminal to network area (2). Alternately, it transmits a request that asks the user terminal to change an output port so as to transmit packet data to another active network area, if necessary. Besides, the network-management server configures IP networks to transmit packet data from network area (4) to the server in the DC.

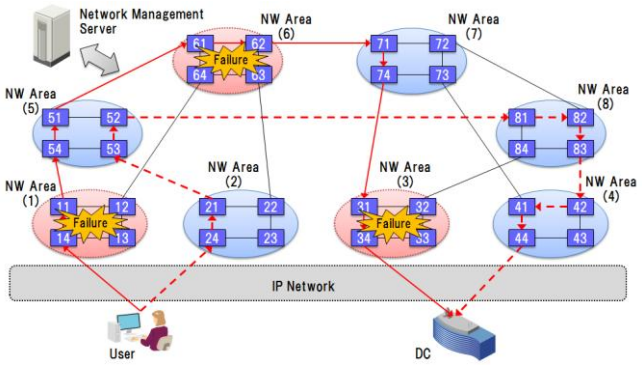

Figure 3. Proposed procedures for network-disaster recovery

C. Sequence of network-disaster recovery

The proposed network-disaster recovery follows the sequence shown in Figure 4. First, the network-management server divides the entire PTN network into multiple network areas and manages each area by using the area-based network-management scheme, labeled "area mgmt" in Figure 4. Specifically, the PTN networks are divided into eight areas and managed as shown in Figure 3. Subsequently, the network-management server calculates the current path (which is composed of the LSP and PW) for transmitting packet data from the user terminal to the server in the DC, shown as "current path" in Figure 4. It starts network operations by configuring the calculated path to related PTNs.

As for the calculation of a path, a route that can provide required bandwidths and transmit packet data within allowed delays is selected as the current path. In addition, the network-management server configures the current path to PTNs, shown as "current-path configuration" in the figure.

The network-management server then calculates all recovery paths by considering all possible area-based network failures, shown as "recovery path". Specifically, it calculates a recovery path for each possible area-based network failure, as shown in Table I. Each recovery path (labelled "P1" in the table) is identified by a recovery ID from "0" to "255." The top row of the table, containing recovery ID "0", indicates current-recovery-path configurations for no area-based network failure. The next row in the table, containing recovery ID "1", indicates recovery-path configurations for a failure of network area (1). In this case, the network failure in the area (1) is assumed. The recovery path for "P1" is calculated on the basis of available network resources. In other words, network resources in area (1) are excluded from the available resources, and the recovery path is calculated. The next row in the table, containing recovery ID "2", indicates the recovery-path configurations for a failure of network area (2). The row of the table containing recovery ID "38" indicates the recovery-path configurations in the case of failures of network areas (1), (3), and (6). As an example recovery path, the dashed line in Figure 3 is that for the current path depicted by the solid line. In Figure 3 and Table I, the recovery-path information for only path "P1" is shown as an example. However, the proposed system is able to manage multiple paths.

As the next step of the recovery sequence, the network-management server calculates recovery-path configurations for each node in case of each area-based network-failure pattern according to the recovery-path information shown in Table I. In addition, the recovery-path tables for PTN 53 and 54 are shown in Table II. The top row of the table, containing recovery ID "0" on PTN 53, shows the current configuration (i.e., "Connection 1" and "Connection 2"). With regard to PTN 53, path P1 (composed of an LSP and a PW) is not configured, since it does not transmit the related packet data. The next row of the table, containing recovery ID "1", indicates the configuration for recovery path P1 in case of a failure of network area (1). Specifically, it is shown that PTN 53 transmits packet data of P1 from PTN 21 to PTN 54 and from PTN 54 to PTN 21. In addition, the row of the table containing recovery ID "2" indicates the recovery-path configurations in the case of a failure of network area (2). However, P1 is not configured. Besides, the row of the table containing recovery ID "38" indicates the configurations of recovery path P1 in the case of failures of network areas (1), (3), and (6). Specifically, it is shown that PTN 53 transmits packet data of path P1 from PTN 21 to PTN 52 and from PTN 52 to PTN 21.

In the lower half of the table, recovery-path configurations on PTN 54 are indicated. The row of the table containing recovery ID "0" shows the current configuration. As shown in the table, PTN 54 transmits packet data of path P1 from PTN 11 to PTN 51 and from PTN 51 to PTN 11.

 ISBN: 978-1-61208-373-5

The row of the table containing recovery ID "2" indicates the recovery-path configurations in case of a failure of network area (2). PTN 54 transmits packet data of path 1 from PTN 11 to PTN 51 and from PTN 51 to PTN 11. In addition, the row of the table containing recovery ID "38" indicates the recovery-path configuration in the case of failures of network areas (1), (3), and (6). However, recovery path 1 is not configured, since PTN 54 does not transmit path-1-related packet data. After the network-management server calculates all recovery-path tables shown in Table II, it distributes them to all PTNs. When each PTN receives the configurations, it stores them with each recovery ID.

In the next step of the recovery sequence, the network-management server monitors operations of all PTNs and area-based network failures, shown as "monitoring" in Figure 4. For example, the network-management server detects failures of network areas (1), (3), and (6) shown in Figure 3. In this case, the network-management server selects recovery ID 38 to recover the configured path, shown as "recovery decision". The PTNs receive recovery ID 38 and configure a data-transmission function to transmit packet data according to the recovery-path information specified by the recovery ID 38.

In the next step, the network-management server configures IP networks to transmit packet data from the user terminal to PTN 24. In addition, it configures IP networks to transmit packet data from PTN 44 to the server in the DC. By executing the above-described recovery procedures, failures of network areas (1), (3), and (6) are recovered.

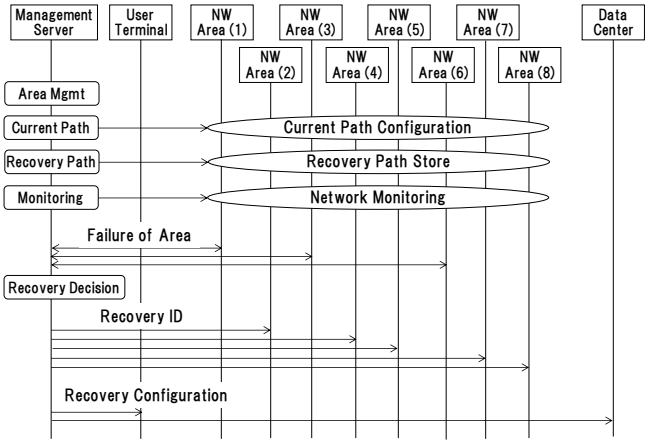

Figure 4. Sequence of network-disaster recovery

TABLE I. RECOVERY-PATH CONFIGURATION

Failure Pattern	Recovery ID	Path	Recovery Path Configuration
No failure	0	P1	14, 11, 54, 51, 61, 62, 71, 74, 31, 34
Area (1) failure	1	P1	24, 21, 53, 54, 51, 61, 62, 71, 74, 31, 34
Area (2) failure	2	P1	14, 11, 54, 51, 61, 62, 71, 74, 31, 34
- - -	- - -	- - -	- - -
Area (1), (3), (6) failures	38	P1	24, 21, 53, 52, 81, 82, 83, 42, 41, 44
- - -	- - -	- - -	- - -
All area failures	255	P1	No Recovery

TABLE II. RECOVERY-PATH TABLE FOR EACH PTN

PTN	Recovery ID	Path(LSP/PW)	Connection 1	Connection 2
53	0	- - -	- - -	- - -
	1	P1	21	54
	2	- - -	- - -	- - -
	- - -	- - -	- - -	- - -
	38	P1	21	52
	- - -	- - -	- - -	- - -
54	0	P1	11	51
	1	- - -	- - -	- - -
	2	P1	11	51
	- - -	- - -	- - -	- - -
	38	- - -	- - -	- - -
	- - -	- - -	- - -	- - -

D. Calculation of recovery paths for possible failure patterns

The flow for calculating a recovery path for an area-based network failure is shown in Figure 5. After the recovery-path calculation starts, delays and available bandwidths between PTNs are calculated from a database that includes topology information and available resources such as link bandwidths. Next, one of the possible area-based network failures, for example, failure of network area (1), is assumed. After that, the PTNs belonging to the assumed area failure are excluded from the available resources to calculate recovery paths. After available resources such as PTNs and bandwidth are fixed, one of the established PWs is selected as the recovery path. Then, the minimum delay path that has the same starting and ending points is selected as the recovery path. If the recovery path is not found because of link disconnection, etc., a message indicating "lack of resources" to find the recovery path is displayed, and the recovery-path calculation process moves on to the next step, namely, selection of another PW. If the recovery path is found, whether it meets the allowed delay time or not is checked. If the path does not meet the allowed delay time, a "lack of available resources" message is displayed, and the process moves on to the next step to find a recovery path for another PW. If the path meets the allowed delay time, it is determined as the recovery path. After the recovery path is confirmed, available bandwidth is decreased by the amount of bandwidth consumed by the recovery path itself. Subsequently, if the route of the LSP path is not the same as the previously calculated route, it is stored as a new LSP route. Then, whether all recovery paths for a selected area-based network-failure pattern have been calculated or not is checked. If all the recovery paths are not calculated, the process moves on to the next step, that is, selection of another PW. If all recovery paths for one area-based network-failure pattern are calculated, whether all recovery paths for all possible area-based network-failure patterns are calculated or not is checked. When all recovery paths for all possible area-based network failure patterns are calculated, the recovery-path calculation process stops.

 ISBN: 978-1-61208-373-5

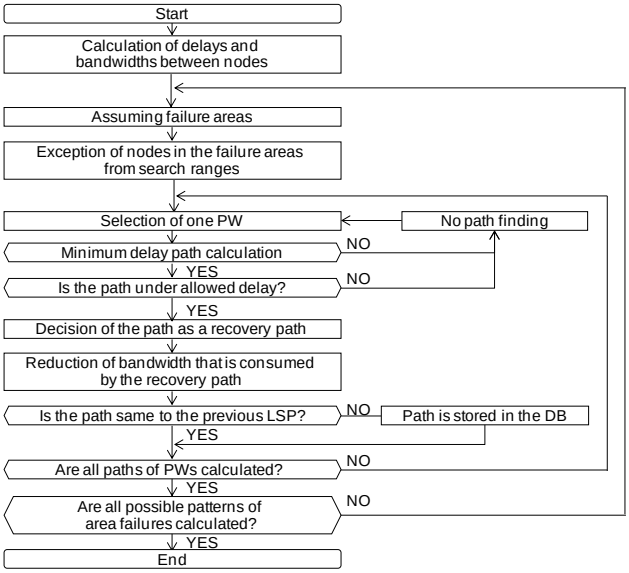

Figure 5. Calculation of recovery paths

All recovery paths are calculated, and the recovery- path information is distributed to all network nodes before network operations are started. The nodes can therefore select an appropriate recovery path swiftly when a network fails.

IV. EVALUATION AND RESULTS

The above-described recovery procedures were evaluated in the case of multiple area-based network failures. The evaluations were intended for networks composed of IP and PTN networks. First, current paths composed of LSPs and PWs were configured to allow users to access application servers in the DC and use applications provided by the server. In the evaluation, the recovery procedure to recover from multiple area-based network failures by using recovery paths was evaluated in terms of whether users can access the application servers or not. In addition, time for calculating the current recovery paths and distributing the information concerning the calculated paths to all PTNs was evaluated by changing the numbers of LSPs and PWs used to construct the current paths.

A. Evaluation system

The system used for the evaluation is depicted in Figure 6. It is composed of a network-management server, PTNs, a user terminal, and an application server in a DC. An entire PTN network is divided into eight network areas. Each network area is composed of 12 PTNs, as shown in area 7, which is an example network composing of about 100 network nodes. These PTNs are connected in a reticular pattern of 96 PTNs in total. In addition, the user terminal is directly connected to PTN-network areas (1) and (2) by IP networks. In addition, the application server is connected to PTN-network areas (3) and (4) directly by IP networks.

Note that the PTN networks (composed of 96 PTNs) are simulated by a physical server. In addition, the user terminal and application server in the DC are also simulated by the same physical server. The specification of the physical server that simulates the PTN networks, user terminal, and application server is listed in Table III. In addition, another physical server that executes the network-management function has the same specifications as the simulator server.

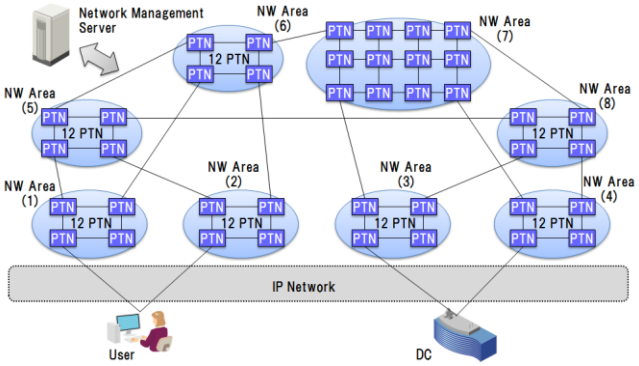

Figure 6. Evaluation system

TABLE III. SPECIFICATIONS OF SERVER

#	Item	Specifications
1	CPU	1.8 GHz, 4 cores
2	Memory	16 GB
3	Storage	600 GB

B. Evaluation conditions

The time taken to calculate PWs by using one route between the user and the application server in the DC was evaluated. As an evaluation condition, one LSP between the user and the application server was established. The LSP houses 10 PWs since it usually houses multiple PWs. The evaluations were executed according to the patterns listed in Table IV. Specifically, time to calculate current paths and recovery paths for 255 area-based network failure patterns was evaluated by changing the number of PWs (namely, 100, 500, and 1000). In addition, the time to distribute all calculated recovery-path configurations and recovery IDs was also evaluated.

TABLE IV. EVALUATION ITEMS

#	Item	Specifications
1	Current path calculation time	Time to calculate 100, 500, and 1000 PWs
2	Recovery path calculation time	Time to calculate recovery 100, 500, and 1000 PWs for 255 possible area failure patterns
3	Distribution time	Time to distribute all calculated recovery PWs and LSPs for 255 possible area failure patterns
4	Recovery ID distribution time	Time to distribute a recovery ID after detecting a first area failure

C. Evaluation result

1) Current-path calculation time

The times taken to calculate current PWs using one route are plotted in Figure 7. The evaluation condition is that 10 PWs are housed in one LSP. As shown in the figure, the times taken to calculate 100 current PWs, 500 current PWs, and 1000 current PWs were about 64, 344, and 769 milliseconds, respectively.

 ISBN: 978-1-61208-373-5

2) Recovery-path calculation time

The times taken to calculate all recovery PWs for 255 possible area-based network-failure patterns by using one route are plotted in Figure 8. The evaluation condition is that 10 PWs are housed in one LSP. As shown in the figure, the time taken to calculate all recovery PWs for 255 area-based network-failure patterns and 100 current PWs, 500 current PWs, and 1000 current PWs are about 5.2, 35.9, and 114.2 seconds, respectively.

3) Distribution time for recovery paths

The times taken to distribute all configurations of calculated recovery PWs to all PTNs are plotted in Figure 9. The evaluation condition is that 10 PWs are housed in one LSP. As shown in the figure, times taken to distribute all configurations of recovery PWs for 255 area-based network-failure patterns and the 100 current PWs, 500 current PWs, and 1000 current PWs are about 245, 282, and 455 milliseconds, respectively.

4) Recovery ID distribution time

The evaluated times taken to distribute the recovery ID to related PTNs after the first area-based network failures are detected are shown in Figure 10. The evaluation condition is that 10 PWs are housed in one LSP. The evaluations were executed for 100 current PWs, 500 current PWs, and 1000 current PWs. In the case of three area-based network-failure patterns, namely, a failure of network area (5), failures of network areas (1), (5), and (8), and failures of network areas (1) and (2) are evaluated. As shown in the figure, the time taken to distribute the recovery ID depends on the number of area-based network failures. According the figure the time taken to distribute the recovery ID ("recovery-ID distribution time" hereafter) in case of one area failure is the shortest for the three area-based network-failure patterns. This tendency is the same for each current PW number. In addition, the recovery-ID distribution time in the case of three area failures is the longest. In particular, the recovery-ID distribution time for 1000 PWs in the case of failures of network areas (1), (5), and (8) is about 3.4 seconds. However, the recovery-ID distribution time includes finding multiple network failures. Therefore, the recovery-ID distribution time depends on the number of area-based network failures. If the time taken to find network failures is excluded, the recovery-ID distribution time itself is independent of the number of the area-based network failures and is always less than 100 milliseconds, as shown in the case of the failure of network area (5). In this sense, the proposed system is useful for not only single area failure but also multiple area failures.

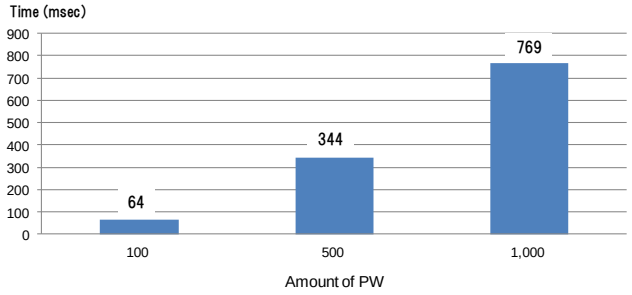

Figure 7. Time for calculating current paths

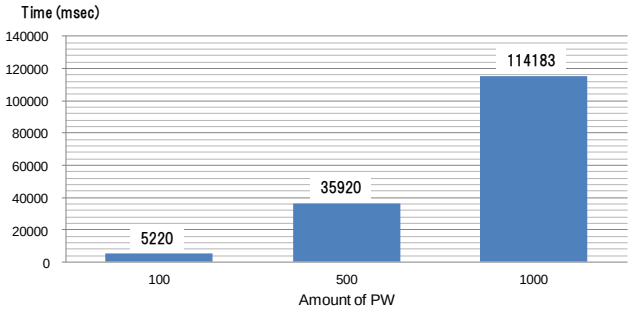

Figure 8. Time for calculating recovery paths

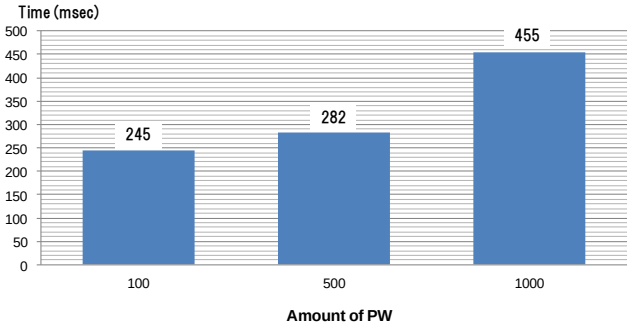

Figure 9. Time for distributing recovery paths

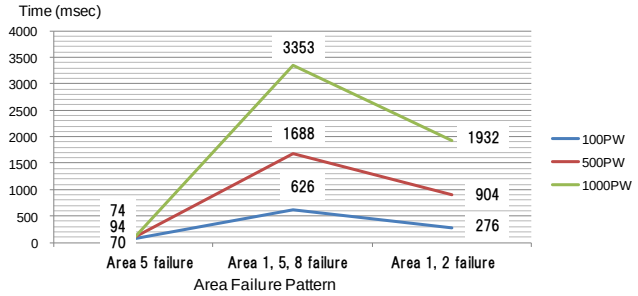

Figure 10. Time for distributing recovery ID

D. Discussion

As shown in Figure 10, the time taken to distribute the recovery ID after the first area-based network failure is detected was evaluated. If two or three area-based network failures occur, the time taken to distribute the recovery ID includes the time taken to detect the second and third area-based network failures after the first area-based network failure is detected. Consequently, the more area-based network failures occur, the longer the time taken to distribute the recovery ID. On the other hand, "pure" recovery-ID distribution time (namely, recovery-ID distribution time excluding the time taken to detect network failures) is shown as the time in Figure 10 in the case of only one area-based network failure. Namely, recovery-ID distribution time in the case that network area (5) fails is equivalent to the pure recovery-ID distribution time. The recovery-ID distribution time is under 100 milliseconds for any number of PWs (i.e., 100, 500, and 1000).

 ISBN: 978-1-61208-373-5

The time taken to calculate 100 current PWs is about 64 milliseconds, which is shorter than the time taken to distribute the recovery ID (i.e., 100 milliseconds). However, the time to calculate 500 current PWs is about 344 milliseconds, which is longer than the time taken to distribute the recovery ID. As a result, if there are over 500 PWs, the proposed network-disaster recovery system can start to recover faster by using preliminarily calculated configurations of recovery PWs and distributing the recovery ID than by recalculating the recovery PWs after an area failure is detected under the evaluation conditions described above.

E. Comparison of proposed system and conventional system

In case of a conventional network system, a restoration scheme is basically used when catastrophic network failures occur. In other words, a large number of setup paths are recalculated after finding the network failures. According to Figure 7, it takes 769 milliseconds to calculate paths for 1000 PWs. If there are 100,000 PWs, it may take over 10 minutes to calculate the paths. That is, over 10 minutes are needed to calculate recovery paths for the 100,000 PWs setup after the network failures were found. On the other hand, in the case of the proposed system, information to recover all the setup paths is distributed to all the network nodes (such as PTNs). The recovery-ID distribution time after finding the network failures is less than 100 milliseconds. Therefore, even if there are 100,000 PWs, the proposed system can start recovery within 100 milliseconds after finding network failures.

With regard to cost, compared to conventional systems (which use a restoration scheme), the proposed system needs more memory (storage) capacity to keep the recovery paths. However, memory and/or storage costs have been gradually decreasing, so the proposed system is promising for the near future.

V. RELATED WORK

Regarding highly available and reliable network management, several standardization activities have been ongoing. For example, MPLS-TP-related Operation, Administration, and Maintenance (OAM) has been standardized. In the first stage, in the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T)[4], specifications such as Transport – Multi Protocol Label Switching (T-MPLS) were discussed. In the next stage, the ITU-T jointly standardized MPLS-TP [6][7][8][9] specifications with the Internet Engineering Task Force (IETF)[5]. Using MPLS-TP OAM functions makes it easy to detect network failures in transport networks. In relation to the proposed system, it is useful to detect network failures promptly to determine areas that are out-of-service.

With regards to failure recoveries, two major techniques have been proposed: “protection” [10][11][12][13][14] and “restoration” [15][16][17][18][19]. With the protection technique, a standby path is preliminarily calculated and established by using extra physical resources. When network failures are detected, an active path is promptly changed from a current path to the standby path. With this technique, when a large number of standby paths are prepared in the case of multiple network failures, physical resources might be voluminously needed. It is therefore useful for limited network failures such as failures of a few link only. On the other hand, with the restoration technique, recovery paths are calculated one by one after network failures are detected. This scheme is useful for catastrophic network failures since all reroutes are calculated after the failures are detected. However, if there are a large number of current paths, much time might be needed to calculate all recovery paths to the current paths.

VI. CONCLUSION

A “network-disaster recovery system” using area-based network management is proposed. As for this system, a whole network is separated into multiple areas. Each area is composed of multiple network nodes, such as MPLS-TP nodes. The system is managed by a network-management server that monitors the condition of every network node. The network-management server manages the network by detecting area-based failures. It calculates recovery paths for every possible area failure and distributes them with a recovery ID for each area-failure pattern before starting network operations. The network nodes receive and store the recovery-path configuration and recovery ID. The network-management server detects the network-area failures during network operations and determines a pattern of area failures. Specifically, it determines numbers and positions of area failures. After determining the pattern of area failures, the network-management server selects a recovery ID to recover the area failures and distributes the ID to recovery-related network nodes. The network nodes receive the recovery ID and start data transmission based on the path configuration specified by the distributed ID. After these procedures are completed, the area failures are swiftly recovered.

A prototype system composed of a network-management server and 96 simulated packet-transport nodes was constructed and evaluated. The system could calculate 500 PWs as current paths that are accommodated in 50 LSPs in about 344 milliseconds. That is, it takes about 344 milliseconds to calculate recovery paths in the case of a network-area failure. Recovery paths of all the current PWs for 255 network-area failure patterns were calculated in about 36 seconds. With the proposed system, however, this calculation is done before network operations start. The network-management server could transmit the recovery ID to the related network nodes within 100 milliseconds after a network-area failure is detected, and the system could immediately start to recover from the failure. The recovery-ID distribution time is shorter than the time required for calculating recovery paths for 500 PWs. In other words, if there are over 500 PWs, the proposed system can start to recover faster than a conventional system (which recalculates the recovery paths after detecting the network failures) under the same conditions as those in the present evaluation.

 ISBN: 978-1-61208-373-5

As for the prototype system, the whole network is divided into eight areas as one of examples to divide the whole network into multiple area networks. However, scalability of this approach is an issue. For example, a recovery scheme is needed when only one link or node failure occurs. The prototype system will therefore be further developed so it can manage a larger range of failures (from small ones to large ones).

ACKNOWLEDGMENT

Part of this research was included in Research Project 0_3 (Open, Organic, Optima) and was supported by the MIC (Japanese Ministry of Internal Affairs and Communications) program, "Research and Development on Virtualized Network Integration Technology".

REFERENCES

[1] Internet World Stats, http://www.internetworldstats.com/stats.htm [retrieved: August, 2014].

[2] C. L. Belady, Microsoft Corporation, "Projecting annual new datacenter construction market size," Mar. 2011 http://cdn.globalfoundationservices.com/documents/Projecting_Annual_New_Data_Center_Construction_PDF.pdf[retrieved: August, 2014].

[3] A. Bianco, J. Finochietto, L. Giraudo, M. Modesti, and F. Neri, "Network planning for disaster recovery," 16th IEEE Workshop on Local and Metropolitan Area Networks, LAMAN 2008, PP. 43-48, Sept. 2008.

[4] International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) http://www.itu.int/en/ITU-T/Pages/default.aspx [retrieved: August, 2014].

[5] The Internet Engineering Task Force (IETF), http://www.ietf.org/ [retrieved: August, 2014].

[6] B. Niven-Jenkins, D. Brungard, M. Betts, N. Sprecher, and S. Ueno, "Requirements of an MPLS transport profile," RFC 5654, Sept. 2009.

[7] M. Bocci, S. Bryant, D. Frost, L. Levrau, and L. Berger, "A Framework for MPLS in transport networks," RFC 5921, July 2010.

[8] T. Busi and D. Allan, "Operations, administration, and maintenance framework for MPLS-based transport neworks," RFC 6371, Sept. 2011.

[9] N. Sprecher and A. Farrel, "MPLS transport profile (MPLS-TP) survivability framework," RFC 6372, Sept. 2011.

[10] M. Pickavet, P. Demeester, and D. Colle, "Recovery in multilayer optical networks," Journal of Lightwave Technology, Vol. 24, no. 1, pp. 122-134, Jan. 2006.

[11] J. Zhang, J. Zhou, J. Ren, and B. Wang, "A LDP fast protection switching scheme for concurrent multiple failures in MPLS network," 2009 MINES '09. International Conference on Multimedia Information Networking and Security, pp. 259-262, Nov. 2009.

[12] Z. Jia and G. Yunfei, "Multiple mode protection switching failure recovery mechanism under MPLS network," 2010 Second International Conference on Modeling, Simulation and Visualization Methods (WMSVM), pp. 289-292, May 2010.

[13] G. Kuperman and E. Modiano, "Network protection with guaranteed recovery times using recovery domains," INFOCOM, 2013 Proceedings IEEE, pp. 692-700, April 2013.

[14] J. Rack, "Fast service recovery under shared protection in WDM networks," Journal of Lightwave Technology, Vol. 30, no. 1, pp. 84-95, Jan. 2012.

[15] A. Valenti, P. Bolleta, S. Pompei, and F. Matera, "Experimental investigations on restoration techniques in a wide area gigabit Etherneti optical test bed based on virtual private LAN service," 11th International Conference on Transparent Optical Networks, ICTON '09, We.B3.4, June 2009.

[16] M. Lucci, A. Valenti, F. Matera, and D. Del Buono, "Investigation on fast MPLS restoration technique for a GbE wide area transport network: A disaster recovery case," 12th International Conference on Transparent Optical Networks (ICTON), Tu.C3.4, June 2010.

[17] D. Sheela, M. Smitha Krishnan, and C. Chellamuthu, "Combined link weight based restration Strategy in optical networks," 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 687-690, March 2012.

[18] T. S. Pham. J. Lattmann, J. Lutton, L. Valeyre, J. Carlier, and D. Nace, "A restoration scheme for virtual networks using switches," 2012 4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 800-805, Oct. 2012.

[19] X. Wang, X. Jiang, C. Nguyen, X. Zhang, and S. Lu, "Fast connection recovery against region failures with landmark-based source routing," 2013 9th International Conference on the Design of Reliable Communication Networks (DRCN), pp. 11-19, Mar. 2013.

[i] Ethernet is a registered trademark of Xerox Corporation.

 ISBN: 978-1-61208-373-5