Copyright ⓒ 2021 KSII

Trade-off between Resource Efficiency and Fast Protection for Shared Mesh Protection

Choong-hee Cho[1]*
[1] Information & Electronics Research Institute, Korea Advanced Institute of Science and Technology
[e-mail: choonghee-cho@naver.com]
*Corresponding author: Choong-hee Cho

Received September 23, 2020; revised March 5, 2021; accepted June 23, 2021; published July 31, 2021

Abstract

Shared mesh protection (SMP) protects traffic against failures occurring in a working path, as with linear protection, and allows resource sharing of protection paths with different endpoints. The SMP mechanism coordinates multiple protection paths that require shared resources when failures occur on multiple working paths. When multiple failures occur in SMP networks sharing limited resources, activation can fail because some of the resources in the protection path are already in use. In this case, a node confirming that a resource is not available has the option to wait until the resource is available or to withdraw activation of the protection path. In this study, we recognize that the protection switching time and the number of protected services can be different, depending on which option is used for SMP networks. Moreover, we propose a detailed design for the implementation of SMP by considering options and algorithms that are commonly needed for network nodes. A simulation shows the performance of an SMP system implemented with the proposed design and utilizing two options. The results demonstrate that resource utilization can be increased or protection switching time can be shortened depending on the option selected by the network administrator.

Keywords: Availability, Protection, Protection Switching, Shared Mesh Protection, Transport Network

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2019R1A6A3A01093738).

http://doi.org/10.3837/tiis.2021.07.015 **ISSN : 1976-7277**

1. Introduction

A transport network transfers high volumes of traffic; thus, even a momentary pause caused by a failure leads to a tremendous loss of traffic. Therefore, it is important to ensure survivability of the transport network during network failure. Among the known fault recovery mechanisms, linear [1]-[4] and ring [5]-[7] protections are commonly used protection mechanisms that increase network survivability. However, these mechanisms involve a considerable network construction cost because the protection (backup) paths require a bandwidth equal to that reserved for the working path through which traffic normally flows. For this reason, private companies operating most transport networks need to effectively deal with network failures while minimizing their investment. Shared mesh protection (SMP) [8]-[10] is a mechanism that provides 1:1 linear protection for every pair of endpoints in a network in which protection paths share their protection resources. Sharing protection resources contributes to reducing network construction costs. However, SMP utilizes more control information transactions and may require more protection switching time than that required with other mechanisms because the sharing of resources causes contention when multiple end-to-end services fail. In other words, applying SMP to a network means adding overheads to reduce the initial network configuration costs. In a network environment where the probability of network failure is low, applying SMP to the network may prove to be a more financially suitable option. This paper compares and analyzes the options that can be selected when applying SMP to networks in terms of efficient use of resources and fast protection.

Fig. 1 shows a simple SMP network that includes three end-to-end services. C-D (working path 1), A-B (working path 2), and E-F (working path 3) are working paths protected by their corresponding protection paths C-A-G-D (protection path 1), A-G-H-B (protection path 2), and E-B-H-F (protection path 3). Links A-G and B-H correspond to segments 1 and 2, where a segment refers to a protection resource shared by multiple protection paths and can be a link or concatenated links. Suppose that a failure occurs on working path 2. In this situation, the traffic on working path 2 must be switched over to protection path 2. In the case of SMP for an optical transport network (OTN) [8], the switching of traffic proceeds via activation of the protection path. If node A detects a failure in working path 2, it checks for the availability of the link A-G. If link A-G is available because protection path 1 is idle, node A sends a message to node G to confirm the availability of link G-H. Node G then responds with a message to node A if G-H is available and simultaneously sends a message to node H to confirm the availability of link B-H. Currently, there are three options that service 2 can utilize at node H when the bandwidth of link B-H is not available due to the activation of protection path 3. With OTN SMP, if the resource is not available (due to failure or use by higher priority connections), the intermediate node may send a message to notify the end node or keep trying until the resource is available or the switching request is canceled. The third option, canceling

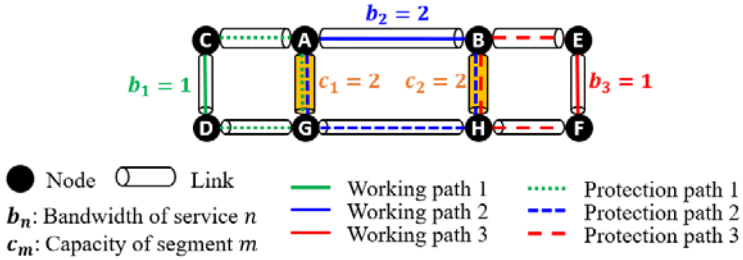

Fig. 1. Example of a shared mesh protection network

the switching request, does not meet the goals of SMP focused on resource efficiency. Therefore, herein, we consider only the first and second options for SMP. If the priority of protection path 3 in the activation process is higher than that of protection path 2, protection path 2 cannot use the link B-H because the link B-H is a segment in which the resource is shared and oversubscribed. In this situation, if the first option is used, node H sends a message to node A to release all resources used by protection path 2. Conversely, if the second option is used, node H waits until the resources of link B-H become available. When the resources become available, the activation of protection path 2 that had been suspended immediately resumes.

The motivation for this paper is that the brief description of the options in OTN SMP does not adequately reflect their impact. According to our study, the protection switching time and the number of protected services can be different, depending on which option is applied to the network with the SMP mechanism. The protection switching time and the number of protected services are important factors available for improving the survivability and ensuring efficient use of the construction costs expended for transport networks. This paper describes a study uncovering the differences and options that significantly affect these important factors.

The contributions of our work are listed as follows.

1) This paper details the design of the SMP mechanism, including aspects not covered by the standard OTN SMP. Behaviors depending on the position of a node placed on a protection path are described with flowcharts, and detailed actions are described with algorithms.
2) We reveal the relationships between options of SMP and important factors of SMP, such as protection switching time and the number of protected services. This helps a network manager configure networks that do not violate their policies when applying SMP to their network.
3) Finally, this paper serves as guide for network administrators on what options to use when applying SMP to a network.

The outline of our paper is as follows: Section 2 reviews prior related works in terms of how to find the path and the optimization problem. Section 3 describes the algorithms required according to the role of each node when the SMP mechanism is running. The problem formulation of protection switching time is described and then the available options are compared in terms of the number of transactions, protected services, and protection switching time in Section 4. Finally, conclusions are presented in Section 5.

2. Related Work

In a transport network, survivability is essential to prevent a significant loss of traffic in the event of failure. To improve survivability, fault recovery mechanisms have been developed and steadily improved. Fault recovery mechanisms can generally be classified using two aspects. The first aspect is the target of protected traffic, and the second aspect considers when backup resources are secured. Based on the first aspect, fault recovery mechanisms are classified into link-based (called span/local-based) scheme and path-based (called end-to-end) schemes. A link-based scheme reroutes the traffic of a working (active) link between adjacent nodes when the link suffers a failure. Multiprotocol label switching (MPLS), fast reroute [11], segment routing, and topology-independent loop-free alternate [12] are examples of link-based schemes. A path-based scheme reroutes the traffic between endpoints of a working (active) path to a disjoint (standby) path. Based on the second aspect, fault recovery mechanisms can be classified as protection-based [13] or restoration-based [14]. Protection-based fault

recovery mechanisms reserve backup resources in advance, while restoration-based fault recovery mechanisms find spare backup resources when needed. Protection-based fault recovery mechanisms can be further classified into linear protection [1]-[4], ring protection [5]-[7], and SMP [8]-[10]. Linear protection is used for coordinating the states of working and protection paths between two endpoints, and it has been standardized for transport network technologies such as OTN [1], transport Ethernet [2], and MPLS-TP [3]-[4]. In linear protection, the bandwidth of a protection path is dedicated. Therefore, protection resources equaling those of the working paths are required. Conversely, in SMP, bandwidths of protection paths are shared to increase the efficiency of protection resources. Therefore, the main task of SMP is to mediate the use of resources for the protection paths against failures of multiple working paths. SMP for OTN [8] has recently been standardized. In the case of SMP for MPLS-TP, only the requirements [9] and a generic version [10] have been standardized. The main focus of this study is on SMP, which is a path-based protection scheme.

In the SMP network, several optimization problems verified as NP-complete have been studied. The routing and wavelength assignment (RWA) optimization problem is designed to find the optimal pair of working and protection paths by considering wavelengths, and has been studied mainly by minimizing the total number of wavelengths [15]-[17] or the total cost of the facility [18]. The path optimization problem excludes wavelength consideration in RWA and has been studied mainly for minimizing the total cost of working and protection paths [19]-[24]. The priority assignment optimization is used to find the optimal set of protection paths and has been mainly studied by maximizing the number of protected services [25]. The maximum segment elimination problem (MSEP) is used to find transparent segments that do not require coordination operations, even if they are shared for multiple protection paths. MSEP has been studied mainly by maximizing the number of transparent segments [26]. The centralized software-defined networking (SDN)-based approach, considered to be the most preferable option for network control and management tasks, can pre-calculate protection paths and apply them to switches [27]. In the author's opinion, there has been no study that has implemented OTN SMP and considered the various available options. This paper focuses on the implementation and correct use of existing SMP for fast protection while increasing resource efficiency. To the best of our knowledge, this is the first study to design SMP behavior in detail and compare the options available.

Table 1 compares the current study with previously published ones.

Table 1. Comparison of related papers

Ref.	Target					Basic Method	Remark
	#Wave-lengths	Link Capacity	#Protected Services	#Seg-ments	Protect-ion Time		
[15]	MIN	-	-	-	-	Integer linear programs (ILP)	Partitioned into routing and wavelength allocation sub-problems
[16]	MIN	-	-	-	-	Integer linear programs (ILP)	-
[17]	MIN	-	-	-	-	Heuristic algorithm	Uses a subpath protection scheme where the working path is partitioned
[18]	-	-	-	-	-	Integer programs (IP)	Minimizes the total facility cost
[19]	-	MIN	-	-	-	Heuristic algorithm	-
[20]	-	MIN	-	-	-	Integer linear programs (ILP)	Jointly collects the work path and the protection path
[21]	-	MIN	-	-	-	Integer programs (IP)	Jointly collects the work path and the protection path and fixes only the working path

[22]	-	MIN	-	-	-	Dijkstra's algorithm	Fixes only the working path
[23]	-	MIN	-	-	-	Dijkstra's algorithm	Fixes only the working path
[24]	-	MIN	-	-	-	Integer programs (IP) & Branch-and-bound	Fixes only the working path
[25]	-	-	MAX	-	-	Approximation algorithm	Expresses the ratio using the hypergraph theory
[26]	-	-	-	MAX	-	Branch-and-bound & Greedy algorithms	Reduces the number of branches in the number of all cases
[27]	-	MIN	-	-	-	Integer linear programs (ILP)	Fast ReRoute (FRR) model
This Paper	-	-	MAX	-	MIN	Heuristic algorithm	Comparison in terms of number of protected services and protection time

3. Shared Mesh Protection Mechanism

This section defines an SMP mechanism that meets the requirements of OTN SMP [8]. It also describes the specific implementations and considers the various available options.

3.1 Definitions

We assume that there are *N* end-to-end services. A service represents traffic transported between two endpoints by either a working path or a protection path. Each service has only one working path and one protection path (1:1 protection). Assume that a pair of working and protection paths is given for each service. Thus, when failure is detected in the end node, the process related to SMP is immediately executed without path calculation. Each node on a protection path acts as a tail-end, intermediate, or head-end node, depending on its position. The tail-end node and head-end node are the end nodes of the working/protection path, and all nodes in the protection path except tail-end and head-end are intermediate nodes. For example, in the protection path 2 in **Fig. 1**, assuming that a failure has occurred from node B in the direction of node A, nodes A and B are tail-end and head-end nodes, respectively. The other nodes, G and H, are intermediate nodes. Protection paths for multiple end-to-end services can share their protection resources. When a failure occurs on the working path, it can be detected in both directions, but this paper focuses on unidirectional failure for the convenience of explanation. The network manager gives each service a priority value based on its importance, and if a need arises for multiple services to preempt shared resources, the service with the higher priority value preempts the other services. When contention occurs, the traffic of a lower priority service is degraded (soft preemption [9]) or completely blocked (hard preemption [9]). According to [28], traffic of a service must be 100% protected. Thus, we assume that the traffic of the service is not allowed to be partially protected in the protection path (that is, hard preemption). In a contention between services with the same priority, the choice is made on a first-come-first-served basis.

According to OTN SMP, nodes in an SMP network maintain the state values of the associated protection paths. The SMP operation we describe can be implemented using the following status values:

- No Request (NR): The transmitting endpoint has nothing to report. This means that traffic is being transmitted without any problems in the working path.

- Activation (ACT): The status of a service is in the process of activating the protection path because of the occurrence of a signal fail/signal degrade (SF/SD) on the working path. In this paper, SF and SD are represented as a single state called ACT.
- Lock Out (LO): This is the status requested to prevent switching data traffic to the protection path.

The automatic protection switching (APS) protocol is used for SMP according to [8], as shown in **Table 2**, but there are some additional messages introduced in this paper; these include NACK, NRA, and NRNA. These new messages are added to ensure that SMP is using resources efficiently. The NACK message is for disconnecting the established cross-connection at the adjacent (in the tail-end node direction) node. The NRA message is for restarting activation of the protection path at the tail-end node. The NRNA message is for disconnecting the established cross-connection at the tail-end node. Each APS message is transferred in a hop-by-hop manner.

Table 2. Events and APS messages that can be received at each node

Abbreviation	Description
WF	SF/SD is detected on a working path. The protection switching is required to protect the traffic of the working path.
WR	A working path is repaired from SF/SD.
APS(SF/SD)	A message sent to the adjacent (the head-end node direction) node to request setting up the corresponding protection transport entity.
APS(NR)	A message sent to the adjacent (the head-end node direction) node to notify that the working path is restored from SF/SD and returned to the NR state.
ACK(RR)	A positive message sent to the adjacent (the tail-end node direction) node for notifying the availability of the protection resource.
NACK	A negative message sent to the adjacent (the tail-end node direction) node for notifying the unavailability of the protection resource.
NRA	A positive message sent to the tail-end node for notifying the availability of the protection resource.
NRNA	A negative message sent to the tail-end node for notifying the unavailability of the protection resource.

3.2 Activation of the Protection Path

A series of tasks that send traffic to the protection path is enabled by the confirmations of resource availability in a hop-by-hop manner. If a failure of a path occurs, the tail-end node detects a WF event and then sends an APS(SF/SD) message to the adjacent intermediate node in the head-end node direction to determine the availability of protection resources. The tail-end node waits for the ACK(RR) message after sending the APS(SF/SD) message. The adjacent intermediate node receiving the APS(SF/SD) message can encounter one of two situations.

The first situation involves a case in which sufficient bandwidth exists to protect a service in the process of activating the protection path. In this case, the intermediate node sends an ACK(RR) message to the tail-end node, responding to the message and indicating that it allows the tail-end node to send traffic. In addition, this intermediate node sends an APS(SF/SD) message to the next adjacent intermediate node and waits for the ACK(RR) message as the tail-end node did. When the tail-end node receives the ACK(RR) message, it establishes the cross-connection to transmit traffic to the protection path. **Fig. 2** shows the process in which the protection path is activated by allocating protection resources from all nodes through

APS(SF/SD) messages.

The second situation involves a case in which insufficient bandwidth exists to protect the service because other services are already using shared resources. In this case, the intermediate node compares the priorities of the service currently receiving the APS(SF/SD) message and those of the other services already under protection. If the priority of the current service is higher than those of the existing services, the current service can preempt protection resources allocated to the existing services. Conversely, if the priority of the current service is equal to or lower than those of the existing services, there are two options available to the intermediate node. The next section describes these two options and their features in detail.

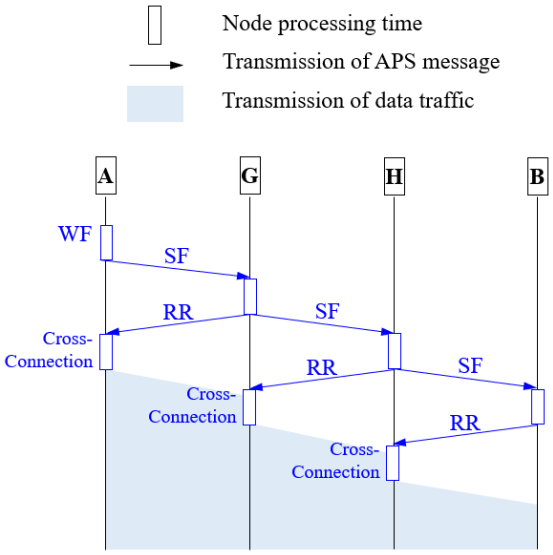

Fig. 2. Process by which the second service in **Fig. 1** activates the protection path when resources are available

3.3 Two Options for Situations in Which Protection Resources Are Unavailable

3.3.1 Introduction of Two Options

The SMP standard [1] presents two options for the case in which the protection resource is not available when the intermediate node receives the APS(SF/SD) message. **Fig. 3** describes the behavior and characteristics of each option in the SMP network presented in **Fig. 1**. **Fig. 3(a)** shows the situation where the first option, called NT, is used and **Fig. 3(b)** shows the situation where the second option, called KT, is used. In the example shown in **Fig. 3**, we assume that protection path 3 with a higher priority first uses the bandwidth of link B-H as a resource for the protection path. Protection path 2 then attempts to use the bandwidth of the link B-H, but this leads to failure because of bandwidth unavailability. Finally, protection path 3 eventually releases the resources of link B-H.

The first option, the NT option, is that the intermediate node sends an NRNA message to the tail-end node to indicate that the protection resource is unavailable. The tail-end node receiving the NRNA message stops sending traffic to the protection path and clears the established cross-connection. As shown in **Fig. 3(a)**, if the node H that sent the NRNA becomes capable of providing a protection resource because of the recovery of higher priority services, the intermediate node can send an NRA message to the tail-end node. When the tail-

end node receives the NRA message, it restarts the protection process.

The second option, the KT option, is to keep requesting resources until resources are available on the intermediate node. In other words, if no resources are available when an APS (SF/SD) message is received at an intermediate node, the service related to the APS(SF/SD) message waits for resources to become available after the service with the higher priority is restored. As shown in **Fig. 3(b)**, if the node H awaiting resource availability converts to a state capable of providing a protection resource because of the recovery of higher priority services, node H sends an RR message to the adjacent intermediate node G in the tail-end node direction. At the same time, an APS (SF/SD) message is sent to the next neighboring node, B, to resume protection. Node G, which received the RR message, establishes the cross-connection to transmit traffic to node H.

3.3.2 Two Options in Terms of Resource Efficiency and Protection Switching

As described above, SMP is a mechanism for increasing resource efficiency by sharing protection resources. Therefore, SMP is expected to protect as many services as possible. At another point, since SMP is one of the mechanisms for protecting traffic, there is a basic requirement to reduce traffic loss through protection switching as quickly as possible. In these two aspects, the two options described above have different effects.

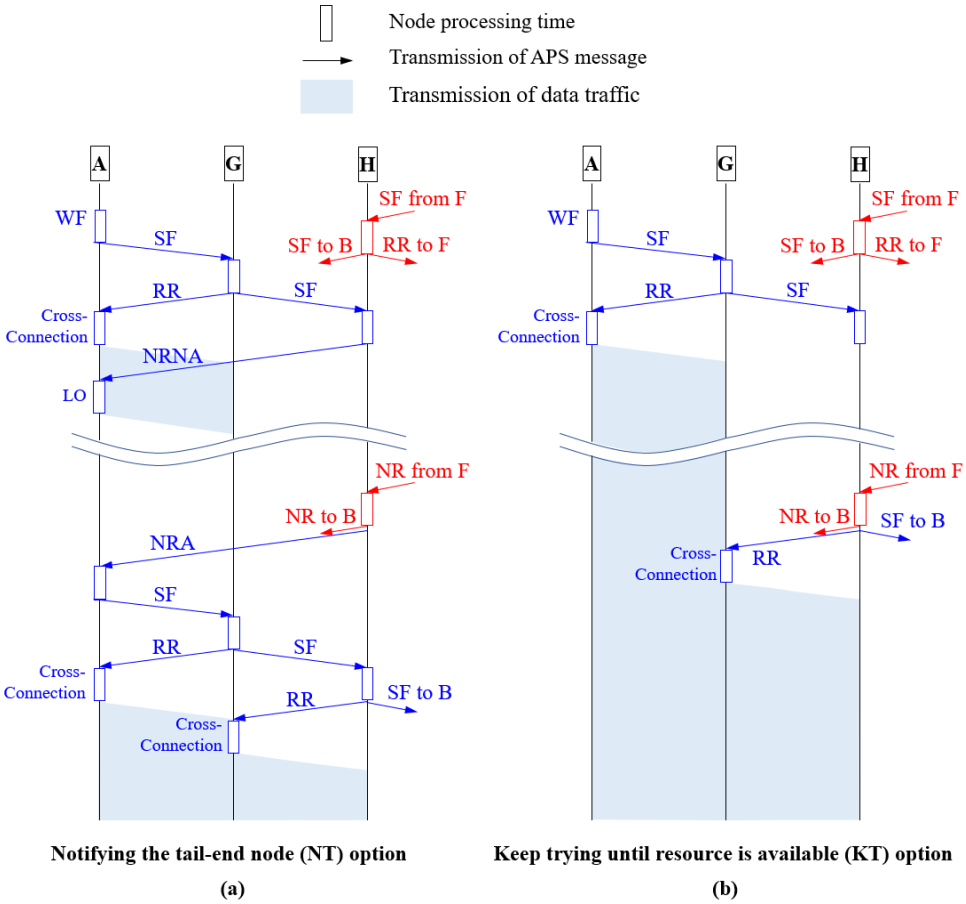

Fig. 3. Two options available when resources become unavailable

In terms of resource efficiency, the NT option is more efficient than the KT option. The NT option blocks the service traffic by sending an NRNA message to the tail-end node when the intermediate node recognizes that the resource is unavailable. This means that the resources in the protection path are not partially allocated so that other services sharing the same resources with lower priority can perform the protection process. As shown in **Fig. 3(a)**, protection path 1 can use the link A-G as a protection resource from the moment when the traffic of protection path 2 is blocked at node A. However, in the same situation in which the KT option is used, protection path 1 cannot use the resources of link A-G because node A continues to send traffic to protection path 2, even though resources are not available at node H.

In terms of protection switching time, the KT option is faster than the NT option. Unlike NT, the KT option does not take any action when the intermediate node recognizes that the resource is unavailable. This means that the activation of the protection path can resume from the intermediate node where it was suspended. As shown in **Fig. 3(b)**, when the availability of link B-H is confirmed at node H, activation of protection path 2 is resumed by sending an RR message from node H to node G. However, in the same situation in which the NT option is used, more protection switching time is required because the activation of protection path 2 has to be restarted from node A, which is a tail-end node.

Therefore, resource efficiency and protection switching times vary according to which option is used. The following section describes the node behavior of the SMP mechanism by considering these two options.

3.4 Node Behavior for Switching

As mentioned above, each node plays the role of a tail-end, intermediate, or head-end node for each service. In this section, we detail the behavior of each node, and **Table 3** summarizes the notations used. There are three algorithms commonly used; these are PREEMPTABLE_SERVICES, AVAILABLE_SERVICES, and SEND_APS_MSGS. These algorithms are covered in detail in Section 3.5.

Table 3. Notations for the shared mesh protection mechanism

Symbol	Description
e	Event detected by tail-end, head-end, or intermediate nodes. An event is a software notification reprocessed from a physically detected APS message signal or SF/SD signal. All event types are indicated in **Table 1**.
S	Service that should act on event e. Each service has its own *state* value expressed as "$S.state$."
$\mathfrak{S}$	A set of all services belonging to the SMP network, $\forall S \in \mathfrak{S}$
P_T	Port number in the direction of the tail-end node of S. If the current node is a tail-end node, it does not exist.
P_H	Port number in the head-end node direction of S. If the current node is a head-end node, it does not exist.
$B(S)$	Service S requires bandwidth $B(S)$ to protect the traffic of S.
$B(P)$	Available bandwidth in the direction of port P at the current time.
X_{list}	Services that have lower priority than service S and are using the resources needed for S to be protected at the current time. These services are selected by the PREEMPTABLE_SERVICES algorithm.
Y_{list}	Services that have lower priority than service S and can be protected by consuming the currently released bandwidth. These services are

	selected by the AVAILABLE_SERVICES algorithm.
SWITCHING	A function that determines whether to send the traffic of the service corresponding to the current event to the working path or the protection path.
SET_CROSS_CONNECTION	A function for setting a cross-connection.
UNSET_CROSS_CONNECTION	A function for unsetting a cross-connection.
SEND_APS	A function that sends a given message to a given port direction.
SEND_APS_MSGS	An algorithm that sends an NRNA message or NACK message so that the given services stop the protection process, or sends an NRA message or ACK (RR) message so that given services can resume protection.

3.4.1 Tail-end Node Behavior

Fig. 4 shows the behavior of a tail-end node using a flowchart. The tail-node handles events such as WF, WR, NRA, ACK, NRNA, and NACK.

When a tail-end node receives WF and NRA messages, it starts activating the protection path of *S*. If the port in the head-end node direction does not have enough free bandwidth to protect *S*, services that can be preempted are sought. If there are no services that can be preempted, activation of the protection path is stopped after setting the state value of *S* to LO. If the bandwidth required by *S* is sufficient, or there are services that can be preempted, the activation of the protection path proceeds as follows: first, the traffic path is changed from the working path to the protection path after changing the state value of *S* to ACT. Then, the services selected to be preempted are deactivated, and services that can be protected with the newly created free bandwidth are activated. Finally, the node sends an APS (SF/SD) message to a neighboring intermediate node to ask the availability of the next-hop resource.

When a tail-end node receives WR and the current state value of *S* is ACT, the traffic path

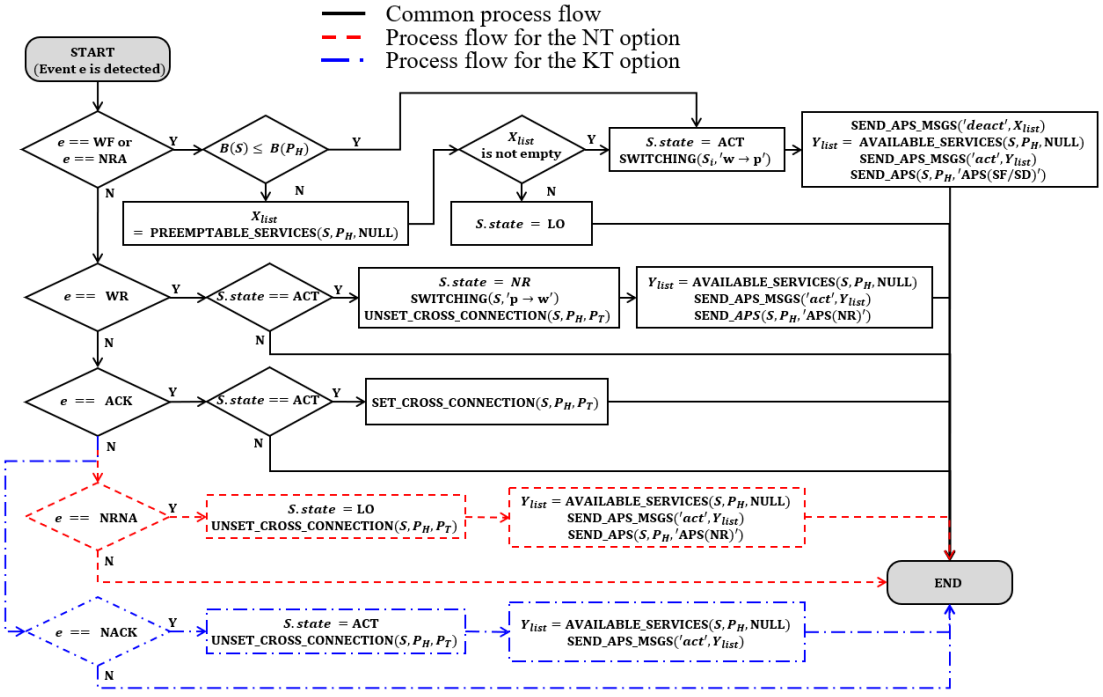

Fig. 4. Tail-end node behavior

is changed from the protection path to the working path after changing the state value of *S* to NR. Services that can be protected with the free bandwidth created by the restoration of *S* are then activated. Finally, the node sends an APS (NR) message to a neighboring intermediate node to release resources preempted by *S*.

When a tail-end node receives an ACK message and the current state value of *S* is ACT, a cross-connection is established to transmit traffic to the protection path.

The tail-end node receives an NRNA message only when the NT option is used. Since receipt of an NRNA message means the activation of the protection path has failed, the state of *S* is changed to LO, and the establishment of the cross-connection is canceled to stop sending traffic. The services that can be protected with the free bandwidth created by releasing the resources of *S* are then activated. Finally, the node sends an APS (NR) message to a neighboring intermediate node to release resources preempted by *S*.

The tail-end node receives a NACK message only when the KT option is used. Since receipt of a NACK message means resuming the wait to receive an APS(RR) message, the state of *S* is changed to ACT, and the establishment of the cross-connection is canceled to stop sending traffic. Services that can be protected with the free bandwidth created by the releasing resources of *S* are then activated.

3.4.2 Intermediate Node Behavior

Fig. 5 shows the behavior of an intermediate node using a flowchart. The intermediate node handles events such as APS(SF/SD), APS(NR), ACK, and NACK.

When an intermediate node receives an APS(SF/SD) message, it begins activating the protection path of *S* and acts as the tail-node does when it receives WF and NRA messages. One difference is that the bandwidths of ports in both directions must be considered. This is because the protection path cannot be activated unless either port is available, the services to be preempted or to be protected may belong to either one port direction, or both. Another difference is that an NRNA message is sent to the port in the tail-end node direction when

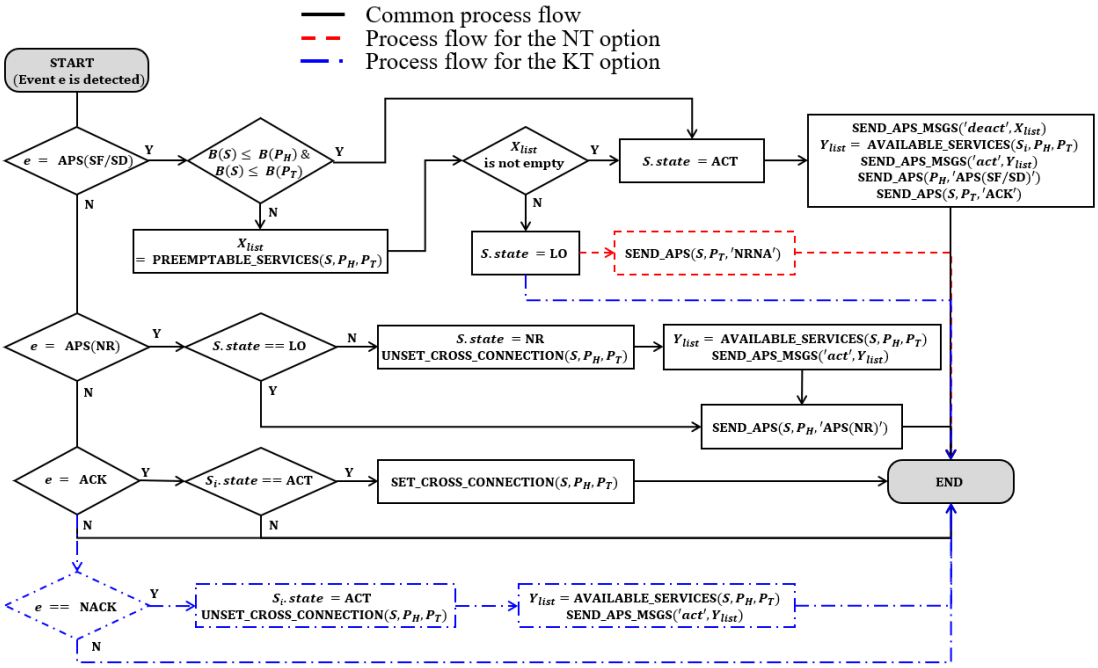

Fig. 5. Intermediate node behavior

there are no resources available and the NT option is used.

When an intermediate node receives ACK and NACK messages, it follows the same procedure as does the tail-end node by considering both ports.

When an intermediate node receives an APS(NR) message and the current state value of *S* is LO, the state of *S* is changed to NR and the establishment of the cross-connection is canceled to stop sending traffic. Then services that can be protected with the free bandwidth created by releasing the resources of *S* are activated, considering both ports. Finally, the node sends an APS (NR) message to an intermediate node in the head-end node direction to release resources preempted by *S*.

3.4.3 Head-End Node Behavior

Fig. 6 shows the behavior of a head-end node using a flowchart. The head-node handles events such as APS(SF/SD) and APS(NR).

When a head-end node receives an APS(SF/SD) message, it begins activating the protection path of S, as does the intermediate node when it receives an APS(SF/SD) message. One difference is that only the bandwidth of the port in the tail-end node direction must be considered. Another difference is that a cross-connection is established immediately after switching because the arrival of the APS (SF/SD) message to the last node (head-end) of the protection path signifies the completion of the activation. When a head-end node receives an APS(NR) message, it follows the same procedure followed by the intermediate node.

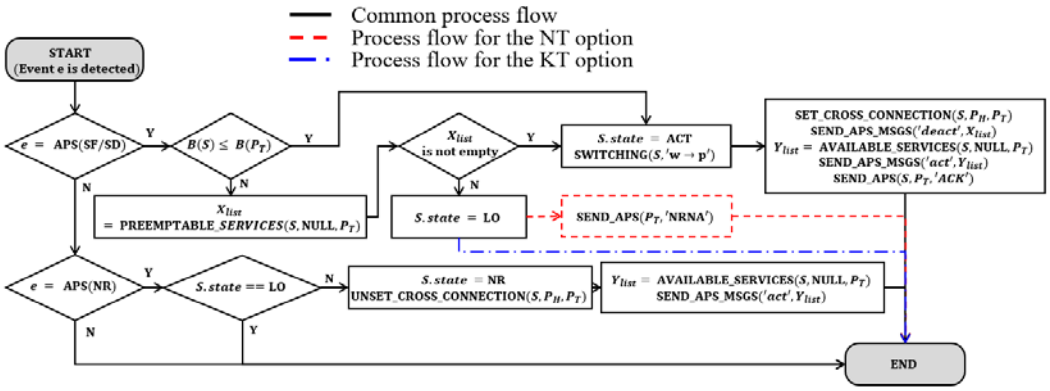

Fig. 6. Head-end node behavior

3.5 Common Algorithms

This section describes three algorithms commonly used by nodes, regardless of their role.

3.5.1 PREEMPTABLE_SERVICES Algorithm

To activate a protection path *S*, a tail-end node must have spare bandwidth for the port in the head-end node direction. In the case of an intermediate node, it must have spare bandwidth in the direction of both ports. In the case of a head-end node, it must have spare bandwidth toward the port in the tail-end node direction. If there is no free bandwidth for these ports, as required by *S*, it is necessary to find services that have lower priority than *S* and are already using the bandwidth of the ports. **Fig. 7** shows the algorithm for finding services that can be preempted by *S*. The time complexity of Algorithm 1 is $O(|\mathfrak{S}|)$ because Algorithm 1 checks the status and priority of services as many as $|\mathfrak{S}| - 1$ times.

Algorithm 1. PREEMPTABLE_SERVICES(S, P_H, P_T)

getRestBand(P): returns the free bandwidth on port P
getLowPrioSrvSFSD(S, P_H, P_T): returns a list of services in ACT state with lower priority than S among services related to at least one of ports P_H and P_T. Services are sorted in ascending order of priority.
has(s, P): returns TRUE if service s uses the bandwidth of port P. Otherwise, FALSE.

```
1:  x_list[], list_low[] ← empty list
2:  B(P_H) ← getRestBand(P_H)
3:  B(P_T) ← getRestBand(P_T)
4:  list_low[] ← getLowPrioSrvSFSD(S, P_H, P_T)
5:  while (TRUE)
6:    s = list_low.getNextItem()
7:    if (There is no service s)
8:      break
9:    if (has(s, P_H) and has(s, P_T))
10:     B(P_H) = B(P_H) + B(s)
11:     B(P_T) = B(P_T) + B(s)
12:     x_list.add(s)
13:   else if (has(s, P_H))
14:     B(P_H) = B(P_H) + B(s)
15:     x_list.add(s)
16:     if (B(P_H) >= B(S) and P_T == NULL)
17:       break
18:   else if (has(s, P_T))
19:     B(P_T) = B(P_T) + B(s)
20:     x_list.add(s)
21:     if (B(P_T) >= B(S) and P_H == NULL)
22:       break
23:   if (has(s, P_H) and B(P_H) >= B(S) and has(s, P_T) and B(P_T) >= B(S))
24:     break
25: return x_list
```

Fig. 7. PREEMPTABLE_SERVICES

3.5.2 AVAILABLE_SERVICES Algorithm

Services should release protection resources in the event of their failure recovery or preemption by other services. Resource utilization is improved if free bandwidth resulting from the release of resources is provided to unprotected services with low priority. **Fig. 8** shows the algorithm for finding services for which the protection process has been stopped due to low priority but now can proceed with the activation of each protection path. The time complexity of Algorithm 2 is $O(|\mathbb{S}|)$ because Algorithm 2 checks the status and priority of services as many as $|\mathbb{S}| - 1$ times.

Algorithm 2. AVAILABLE_SERVICES (S, P_H, P_T)

getRestBand(P): returns the free bandwidth on port p
getLowPrioSrvLO(S, P_H, P_T): returns a list of services in LO state with lower priority than S among services related to at least one of ports P_H and P_T. Services are sorted in descending order of priority.
has(s, P): returns TRUE if service s uses the bandwidth of port P. Otherwise, FALSE.

```
1:  y_list[], list_low[] ← empty list
2:  B(P_H) ← getRestBand(P_H)
```

```
3:   B(P_T) ← getRestBand(P_T)
4:   list_low[] ← getLowPrioSrvLO(S, P_H, P_T)
5:   while (TRUE)
6:     s = list_low.getNextItem()
7:     if (s == NULL)
8:       break
9:     if (has(s, P_H) and has(s, P_T))
10:      if (B(P_H) – B(s) > 0 and B(P_T) – B(s) > 0)
11:        B(P_H) = B(P_H) – B(s)
12:        B(P_T) = B(P_T) – B(s)
13:        y_list.add(s)
14:    else
15:      if (has(s, P_H))
16:        if (B(P_H) – B(s) > 0)
17:          B(P_H) = B(P_H) – B(s)
18:          y_list.add(s)
19:      if (has(s, P_T))
20:        if (B(P_T) – B(s) > 0)
21:          B(P_T) = B(P_T) – B(s)
22:          y_list.add(s)
23:  return y_list
```

Fig. 8. AVAILABLE_SERVICES

3.5.3 SEND_APS_MSGS Algorithm

If the protection of service is not allowed due to activation of other higher priority services, the protection of the service must be prevented. Therefore, the establishment of the cross-connection must be canceled immediately. An NRNA message is then sent to the tail-end node (NT option), or a NACK message is sent to the neighboring node in the tail-end node direction (KT option). However, if the protection of service was stopped because of a lack of protection resources, but the resources necessary for protection become available, the protection of the service can be restarted or resumed. Therefore, an NRA message is sent to the tail-end node (NT option), or an ACK message is sent to the neighboring node in the tail-end node direction (KT option). **Fig. 9** shows the algorithm that sends APS messages to services that must stop the activation of their protection paths immediately or services that should resume the activation of their protection paths. The time complexity of Algorithm 3 is $O(|\mathfrak{S}|)$ because Algorithm 3 checks the status and priority of services as many as $|\mathfrak{S}| - 1$ times.

Algorithm 3. SEND_APS_MSGS(*mode*, *list*)

```
     list: list of services to receive messages.
     mode: indicates whether to activate or deactivate the services in list.
1:   while (TRUE)
2:     s = list.getNextItem()
3:     if (mode is "act")
4:       if (NT option is used)
5:         SEND_APS(s, P_T, "NRA")
6:       else if (KT option is used)
7:         SEND_APS(s, P_T, "ACK")
8:     else if (mode is "deact")
9:       UNSET_CROSS_CONNECTION(s, P_H, P_T)
10:      if (NT option is used)
11:        SEND_APS(s, P_T, "NRNA")
```

```
12:       else if (KT option is used)
13:         SEND_APS(s, P_T, "NACK")
14:     if there is no next item on list.
15:       return
```

Fig. 9. SEND_APS_MSGS

4. Experiments

This section compares performance by implementing each SMP mechanism with the NT and KT options. The SMP mechanisms using each option are compared in terms of the average number of transactions, the number of protected services, and the average protection switching time.

4.1 Experimental Setup

To measure performance in a realistic experimental environment, we used a North America network topology [29] (**Fig. 10**) modeled on a real American network. The reason for adopting this topology in the experiment is that existing studies related to SMP ([26], [29]) performed experiments on this topology. For verification of realistic scenarios, we assumed that there could be data-center cities for full-mesh connections. To reflect the control overhead in the experiment, we assumed that T_α and T_β are approximately 4.9 and 2 ms (referring to [26]) for the simulation experiments described in **Table 3**. Note that these parameter values can vary depending on the system and the implementation. We also assumed that the hold-off time is zero so that the confirmation time at each node is in between $(k - 1) \times$ CC_Period and $k \times$ CC_Period + T_{prop_r} where T_{prop_r} denotes the latency of a continuity check (CC), periodic control message, from the impairment location to the end node, CC_Period denotes the CC message interval, and k takes values in the interval $3.25 \leq k \leq 3.5$. According to previous studies, the working path is assumed to be the shortest path [22, 23] or given properly [24]. Additionally, we assumed that the second-shortest path, disjointed from the working path, is

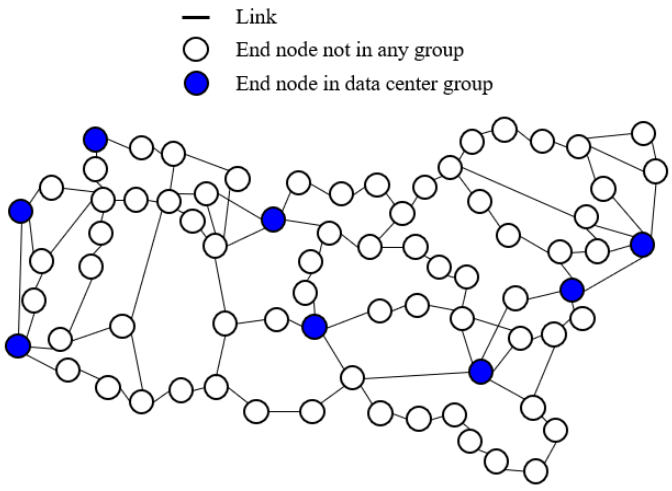

Fig. 10. North America network topology with data center end nodes

set as the protection path in order to provide traffic delay similar to the working path and availability similar to a linear protection. Therefore, we assumed that there is one working path (shortest path) and one protection path (second-shortest path) between any two data-center cities where the working and protection paths are disjointed. The demand for bandwidth between two data-center cities was assumed to be proportional to the product of their populations and inversely proportional to the distance between the cities. The capacity of a link was set to be greater than the maximum bandwidth required between any two data-center cities, and less than the sum of all required bandwidths. Through experimentation, the following two parameters were found to be most sensitive: the sharing rate related to the capacity of the link and the number of failures that can occur probabilistically. We defined a sharing rate [26], which indicates the degree to which the protection paths share the capacity of a link. The sharing rate for the links we set is expressed as a percentage, and the smaller this value, the more the resources are shared. We assume that a link cut occurs in any link and up to two link cuts can occur at a given time in our simulated network. The direction of each link cut was randomly selected in a unidirectional or bidirectional manner. Two link cuts can cause both a working and a protection path to fail at the same time. However, the service does not require any shared resource when a failure occurs on the protection path of a service. The simulation was conducted on MATLAB. We continued the experiments until the values of the average number of transactions and the average protection switching time stabilized. We observed that the results stabilized after considering five thousand cases of different link cuts.

4.2 Problem Formulation of Protection Switching Time for SMP

Before performance analysis, we formulated the protection switching temporal model for SMP by referring to the standard of a generic protection switching [30]. Protection switching time (T_P) can be expressed as:

$$T_P = T_C + T_T + T_R \tag{1}$$

where confirmation time (T_C) is the time from the occurrence of the network impairment to the instant when the triggered SF/SD is confirmed as requiring protection switching operations. The recovery time (T_R) is the time interval between the completion of protection switching operations and the full restoration of protected traffic. The transfer time (T_T) is the time interval between the confirmation of an SF/SD and the completion of protection switching operations. Accordingly, the transfer time is affected by the implemented SMP mechanism because it is the time required to make decisions related to protection switching or transmission of the control signals. **Table 4** describes the notations used in following formulas.

Referring to [26], we assume that a service succeeds in protection after N_f attempts to preempt the resources of the protection path. If the NT option is used, the tail-end node waits until it receives the NRNA message and then restarts the activation of the protection path from the tail-end node. Thus, the transfer time in this case is formulated as follows:

$$T_T = \operatorname{sgn}(N_f)\sum_{i=1}^{N_f}\{T_{fn}(N_d(i), N_s(i)) + T_w(i)\} + T_s(N_h) \tag{2}$$

where

$$T_{fn}(N_d(i), N_s(i)) = \mathrm{sgn}(N_d(i)) \left(\begin{array}{l} T_\alpha (N_d(i) - N_s(i) + 1) \\ +2 \sum_{j=1}^{N_d(i)} T_p(j) \end{array} \right) + T_\beta, \quad (3)$$

$$T_s(N_h) = T_\alpha N_h + \sum_{j=1}^{N_h - 1} T_p(j) + T_p(N_h - 1) + T_\beta \quad (4)$$

In the case of the SMP mechanism with the KT option, it resumes the activation of the protection path from the intermediate node that failed to preempt resource. Thus, the transfer time of this case is formulated as follows:

$$T_T = \mathrm{sgn}(N_f) \sum_{i=1}^{N_f} \{T_{fk}(N_d(i), N_s(i)) + T_w(i)\} + T_p(N_h - 1) + T_\beta \quad (5)$$

where

$$T_{fk}(N_d(i), N_s(i)) = \mathrm{sgn}(N_d(i)) \left(\begin{array}{l} T_\alpha (N_d(i) - N_s(i) + 1) + T_\beta \\ + \sum_{j=N_d(i-1)}^{N_d(i)} T_p(j) \end{array} \right), \quad (6)$$

Whenever activation fails, the double of $T_p(j)$ is added repeatedly to T_{fn}, but $T_p(j)$ is added to T_{fk} only once. Therefore, as N_f increases, protection switching can be performed faster when the KT option is used than when the NT option is used.

Table 4. Notations used in the formulas for protection switching time

Symbol	Description
N_f	Number of failed activation attempts before a service succeeds in the protection switching for an SF/SD. The number of activation failures depends on the relationship with the services sharing resources and their priority.
$N_d(i)$	Index of the segment denied by higher priority service/services in the i-th activation attempt of the service. This value is the same as the hop count from the tail-end node to the first node of the corresponding segment. Note that $N_d(0) = 1$.
$N_s(i)$	The number of nodes where link resources are not shared on the protection path in a range from the tail-end node to the $N_d(i)$-th node.
$T_w(i)$	Waiting time from the end of the i-th activation attempt to the start of the (i+1)-th activation attempt.
N_h	Total hop count from the tail-end node to the head-end node.
$T_{fn}(N_d(i), N_s(i))$	Time from the start of the i-th activation attempt to reception of the NRNA message of the failed i-th activation at the tail-end node when the NT option is used.
$T_{fk}(N_d(i), N_s(i))$	Time from the start of the i-th activation attempt to reception of the NRNA message of the failed i-th activation at the tail-end node when the KT option is used.
T_s	Time from the start of the last activation attempt to the protection switching completion of all nodes on the protection path.
T_α	Time between the reception of a protection event; e.g., SF/SD event or SMP message, and the sending of the SMP message to the next node.
T_β	Time between the reception of a protection event; e.g., SF/SD event or SMP

	message, and the end of the traffic switching.
$T_p(j)$	Propagation delay from j-th node to (j+1)-th node.
$\mathrm{sgn}(x)$	Sign function that extracts the sign of a real input number x and is defined as follows: $$\mathrm{sgn}(x) = \begin{cases} 1 \text{ if } x > 0, \\ 0 \text{ if } x = 0. \end{cases}$$

4.3 Average Number of Transactions

We experimented with the number of APS messages occurring in the network on a transaction basis. A transaction in a network environment can be defined as a logical unit of work in which a destination point performs an operation related to a message sent from a source point. If there are few transactions, the SMP-related load for each node is reduced. In addition, traffic loss can be reduced because decisions about which protection path should be protected are made quickly. **Fig. 11** shows the average number of transactions for the data-center cites. The lower the sharing rate, the greater is the difference between the number of transactions for the SMP with the NT option and the SMP with the KT option. If the NT option is used, an NRNA or NRA message is sent to the end node when the resource is not available; therefore, more related messages are sent later. On the other hand, if the KT option is used in the same situation, it will not produce messages. Based on these results, we confirmed that the KT option reduces the load on each node and contributes to protection faster than does the NT option.

4.4 Average Number of Protected Services

We experimented with the number of services protected with each option. **Fig. 12** shows the average number of protected services for data-center cites. In SMP networks for the given data-center cities, working paths handling approximately 4.5 services are unable to deliver traffic when one or two link cuts occur. At this time, the number of services protected for the options differ. On average, the number of protected services varies from approximately 0.2 to 0.6. If the NT option is used, the service traffic is blocked from the tail-end node when the resource is not available. Conversely, if the KT option is used in the same situation, it consumes the resources of other links, except for those resources of links that cannot be secured. Based on these results, we confirmed that the NT option is more suitable for increasing the utilization of resources than the KT option.

4.5 Average Protection Switching Time

The speed with which traffic is switched to the protection path after a failure occurs on the working path is the most important indicator of protection designed to reduce traffic loss. We measured the protection switching time for each option. **Fig. 13** shows the average protection switching time for the data-center cites. In the same situation, the difference between the protection switching times for the NT and KT options ranges from 30 to 280 ms. In the case of the NT option, the activation process for the protection path restarts from the tail-end node in any situation. Conversely, the KT option resumes the activation from the point at which a resource is unavailable. Based on these results, we confirmed that the KT option performs faster protection switching than the NT option.

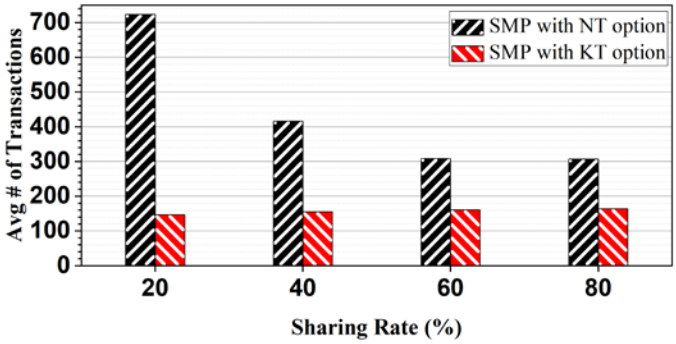

Fig. 11. Average number of transactions for data-center cites

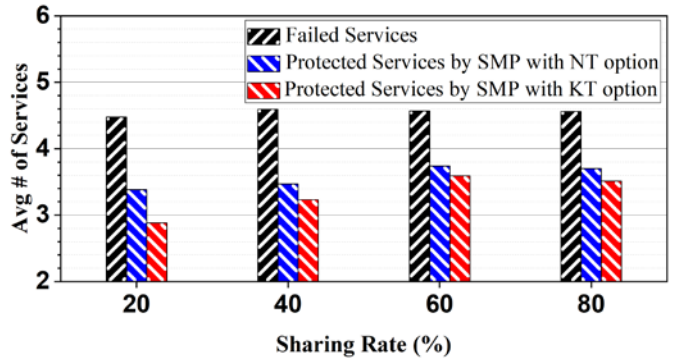

Fig. 12. Average number of protected services for data-center cites

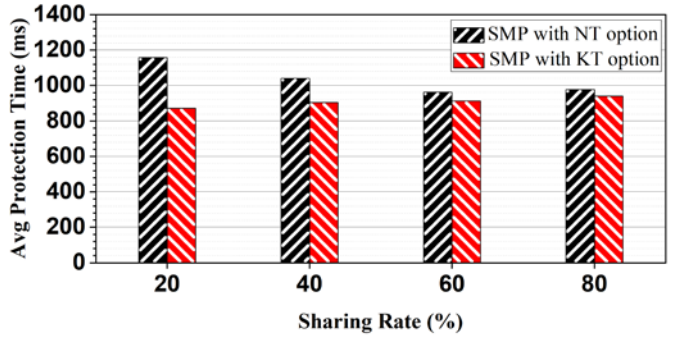

Fig. 13. Average protection switching time for data-center cites

5. Conclusion

In this paper, we have defined the SMP mechanism, including operations for NT and KT options, by detailing behaviors of tail-end, intermediate, and head-end nodes. The main actions for each node role were defined using flow charts. Further, the action to preempt certain services was defined in the PREEMPTABLE_SERVICES algorithm, the action of finding an available service was defined in the AVAILABLE_SERVICES algorithm, and the action of sending APS depending on the situation was defined in the SEND_APS_MSGS algorithm. To

improve resource efficiency, three APS messages were also defined. In the experiment, a traffic scenario between data-centers was assumed in a topology with nodes based on major cities in the United States. We compared the NT and KT options in terms of the average number of transactions, the number of protected services, and the average protection switching time. The experimental results show that the KT option results in the generation of approximately half (or fewer) as many APS messages as that are produced when using the NT option. In addition, the protection switching time is up to 280 ms faster when using the KT option, compared with the use of the NT option. Therefore, the KT option is preferred over the NT option, both in terms of the number of transactions and the protection switching time. Conversely, the number of protected services increases by 0.6 when using the NT option, compared to that with the use of the KT option. Therefore, the NT option is preferred over the KT option in terms of the number of protected services, indicating resource efficiency. As expected, we could see a difference in performance depending on which option was chosen within the same SMP mechanism. We hope that the results in this paper will contribute to the development of future standards for SMP and serve as a reference for network managers seeking to apply SMP to their networks.

References

[1] *Optical Transport Network: Linear Protection*, document ITU-T Rec. G.873.1, 2017. https://www.itu.int/rec/T-REC-G.873.1/en

[2] *Ethernet Linear Protection Switching*, document ITU-T Rec. G.8031, 2015. https://www.itu.int/rec/T-REC-G.8031-201501-I/en

[3] J. D. Ryoo, T. Cheung, D. King, A. Farrel, and H. van Helvoort, "MPLSTP linear protection for ITU-T and IETF," *IEEE Commun. Mag.*, vol. 52, no. 12, pp. 16–21, Dec. 2014. Article (CrossRef Link)

[4] *MPLS Transport Profile (MPLS-TP) Linear Protection*, document RFC 6378, IETF, 2011. https://tools.ietf.org/html/rfc6378

[5] *ODUk Shared Ring Protection*, document ITU-T Rec. G.873.2, 2015. https://www.itu.int/rec/T-REC-G.873.2/en

[6] *MPLS-TP Ring Protection*, document ITU-T Rec. G.8132/Y.1383, 2017. https://www.itu.int/rec/T-REC-G.8132

[7] J. D. Ryoo, H. Long, Y. Yang, M. Holness, Z. Ahmad, and J. K. Rhee, "Ethernet ring protection for carrier Ethernet networks," *IEEE Commun. Mag.*, vol. 46, no. 9, pp. 136–143, Sep. 2008. Article (CrossRef Link)

[8] *Optical Transport Network (OTN) - Shared Mesh Protection*, document ITU-T Rec. G.873.3, 2017. https://www.itu.int/rec/T-REC-G.873.3

[9] *Requirements for MPLS Transport Profile (MPLS-TP) Shared Mesh Protection*, document RFC 7412, IETF, 2014. https://tools.ietf.org/html/rfc7412

[10] *Generic Protection Switching – Shared Mesh Protection*, document ITU-T Rec. G.808.3, 2012. https://www.itu.int/rec/T-REC-G.808.3

[11] *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*, document RFC 4090, IETF, 2005. https://tools.ietf.org/html/rfc4090

[12] *Topology Independent Fast Reroute using Segment Routing*, document draft-ietf-rtgwg-segment-routing-ti-lfa-05, IETF, 2018. https://datatracker.ietf.org/doc/draft-ietf-rtgwg-segment-routing-ti-lfa/

[13] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks. Part I-Protection," in *Proc. of IEEE INFOCOM*, New York, USA, pp. 744–751, 1999. Article (CrossRef Link)

[14] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks. Part II—Restoration," in *Proc. of IEEE Int. Conf. Commun. (ICC)*, Vancouver, Canada, pp. 2023–2030, 1999. Article (CrossRef Link)

[15] H. Zang, C. Ou, and B. Mukherjee, "Path-protection routing and wavelength assignment (RWA) in WDM mesh networks under duct-layer constraints," *IEEE/ACM Trans. Netw.*, vol. 11, no. 2, pp. 248–258, Apr. 2003. Article (CrossRef Link)
[16] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks," *J. Lightw. Technol.*, vol. 21, no. 4, pp. 870–883, Apr. 2003. Article (CrossRef Link)
[17] C. Ou, H. Zang, N. K. Singhal, K. Zhu. L. H. Sahasrabuddhe, R. A. MacDonald, and B. Mukherjee, "Subpath protection for scalability and fast recovery in optical WDM mesh networks," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 9, pp. 1859–1875, Nov. 2004. Article (CrossRef Link)
[18] Y. Miyao and H. Saito, "Optimal design and evaluation of survivable WDM transport networks," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 7, pp. 1190–1198, Sep. 1998. Article (CrossRef Link)
[19] C. Ou, J. Zhang, H. Zang, L. H. Sahasrabuddhe, and B. Mukherjee, "New and improved approaches for shared-path protection in WDM mesh networks," *J. Lightw. Technol.*, vol. 22, no. 5, pp. 1223–1232, May 2004. Article (CrossRef Link)
[20] M. Kodialam and T. V. Lakshman, "Dynamic routing of bandwidth guaranteed tunnels with restoration," in *Proc. of IEEE INFOCOM*, Tel Aviv, Israel, pp. 902–911, 2000. Article (CrossRef Link)
[21] B. T. Doshi, S. Dravida, P. Harshavardhana, O. Hauser, and Y. Wang, "Optical network design and restoration," *Bell Labs Tech. J.*, vol. 4, no. 1, pp. 58–84, Jan./Mar. 1999. Article (CrossRef Link)
[22] B. G. Józsa and D. Orincsay, "Shared backup path optimization in telecommunication networks," in *Proc. of DRCN*, Budapest, Hungary, pp. 251–257, 2001. Article (CrossRef Link)
[23] G. Li, D. Wang, C. Kalmanek, and R. Doverspike, "Efficient distributed restoration path selection for shared mesh restoration," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 761–771, Oct. 2003. Article (CrossRef Link)
[24] Y. Liu, D. Tipper, and P. Siripongwutikorn, "Approximating optimal spare capacity allocation by successive survivable routing," *IEEE/ACM Trans. Netw.*, vol. 13, no. 1, pp. 198–211, Feb. 2005. Article (CrossRef Link)
[25] C. H. Cho, T. Cheung, and J. D. Ryoo, "Priority assignment algorithms for shared mesh protection switching," *IEEE Trans. on Comm.*, vol. 67, no. 3, pp. 2130–2143. Mar. 2019. Article (CrossRef Link)
[26] C. H. Cho and J. D. Ryoo, "Minimizing protection switching time in transport networks with shared mesh protection," *Int. J. Netw. Manag.*, vol. 31, no. 4, 2020, Art. no. E2136. Article (CrossRef Link)
[27] O. Lemeshko, O. Yeremenko, B. Sleiman, and M. Yevdokymenko, "Fast ReRoute Model with realization of path and bandwidth protection scheme in SDN," *Inf. Commun. Technol Serv.*, vol. 18, no. 1, pp. 23-30, Mar. 2020. Article (CrossRef Link)
[28] *Requirements of an MPLS Transport Profile*, document RFC 5654, IETF, 2009. https://tools.ietf.org/html/rfc5654
[29] A. Deore, O. Turkcu, S. Ahuja, S. J. Hand, and S. Melle, "Total cost of ownership of WDM and switching architectures for next-generation 100Gb/s networks," *IEEE Commun. Mag.*, vol. 50, no. 11, pp. 179-187, Nov. 2012. Article (CrossRef Link)
[30] *Generic Protection Switching - Linear Trail and Subnetwork Protection*, document ITU-T Rec. G.808.1, 2014. https://www.itu.int/rec/T-REC-G.808.1

CHOONG-HEE CHO received the B.S. degree in computer science from Sahmyook University, Seoul, in 2010, and the Ph.D. degree in network technology from the Korea University of Science and Technology (UST), Daejeon, South Korea, in 2019. He is currently a postdoctoral researcher at the Information & Electronics Research Institute Department, Korea Advanced Institute of Science and Technology. His current research interests include SDN, OpenFlow protocol, NFV, Protection for Transport Network, and Reinforcement Learning.