Photonic Network Communications, 7:2, 161–178, 2004

Optical-LSP Establishment and a QoS Maintenance Scheme Based on Differentiated Optical QoS Classes in OVPNs

Mi-Ra Yoon, Ju-Dong Shin, Chang-Hyun Jeong
Pukyong National University, 599-1 Daeyeon 3-Dong Nam-Gu, Pusan, 608-737 Korea
E-mail: {eggshape.jdshin.jch123}@mail1.pknu.ac.kr

Jun-Mo Jo
Kyungpook National University, Department of Computer Engineering, Daegu 702-701, Korea
E-mail: jo2000@mail.tmc.ac.kr

Oh-Han Kang
Andong National University, 388 Song-chon Dong, Andong, Kyoungbuk 760-749, Korea
E-mail: ohkang@andong.ac.kr

Sung-Un Kim*
Pukyong National University, 599-1 Daeyeon 3-Dong Nam-Gu, Pusan, 608-737 Korea
E-mail: kimsu@pknu.ac.kr

Received September 10, 2003; Revised October 15, 2003; Accepted October 20, 2003

Abstract. A ''virtual private network (VPN) over Internet'' has the benefit of being cost-effective and flexible. However, it has difficulties providing sufficient QoS and adequate transmission capacity for high bandwidth services. Given the increasing demand for high bandwidth Internet and the demand for QoS assurances in a ''VPN over Internet'', IP/generalized multi-protocol label switching (GMPLS) based on a control plane combined with a high-bandwidth, dense-wavelength division multiplexing (DWDM) optical network is seen as a very favorable approach for realizing the future ''optical VPN (OVPN) over IP/GMPLS over DWDM''. Within this architecture, providing QoS guaranteed multimedia services with a differentiated QoS guaranteed protocol framework with QoS recovery is one of the key issues to implement. Therefore, we suggest in this paper optical-label switched path (O-LSP) establishment and its QoS maintenance scheme based on differentiated optical QoS-service (DOQoS) classes. They are the key components for this DOQoS framework in assuring end-to-end QoS in an ''OVPN over IP/GMPLS over DWDM'' architecture.

Keywords: OVPN, QoS, DWDM, GMPLS, recovery

1 Introduction

Virtual private network VPN is an enterprise network based on a shared public network infrastructure but providing the same security, management, and throughput policies as applied in a private network. This shared infrastructure can leverage a service provider's IP, Frame Relay, or ATM backbone network and may or may not utilize the public Internet. The primary advantages of ''VPN over Internet'' are cost-effectiveness and flexibility while coping with the exponential growth of Internet. However, the current disadvantages are the lack of sufficient QoS and provision of adequate transmission capacity for high bandwidth services. For resolving these problems, OVPNs over the next generation optical Internet (NGOI) have been suggested [1–3].

*Corresponding author.

Keeping in mind that IETF and ITU-T are standardizing IP/GMPLS over DWDM as a solution for the NGOI, DWDM optical network technology will be used as the NGOI backbone and GMPLS [4] will be used as control protocols for transferring data over IP.

Therefore, an OVPN over IP/GMPLS over DWDM is considered as a major trend for next generation VPNs supporting various real-time multimedia services. Within this architecture, providing QoS guaranteed multimedia services with differentiated QoS guarantee and QoS recovery are the key issues [5].

In this paper, we suggest O-LSP establishment and its QoS maintenance scheme based on DOQoS classes. The suggested scheme considers technologies such as the DWDM optical backbone network, the GMPLS control protocol, OVPN, and QoS.

In Section 2, an architecture and functional procedure of an OVPN over IP/GMPLS over DWDM offering DOQoS is presented. In Section 3, DOQoS classes considered for differentiated QoS in the OVPN and appropriate recovery schemes are suggested. In Section 4, an O-LSP establishment scheme based on DOQoS classes is described. In Section 5, a QoS maintenance scheme is proposed for the QoS-guaranteed protocol framework. Furthermore, types and the recovery mechanism are analyzed. Finally, in Section 6, the conclusion and further study items are presented.

2 Architecture and Functional Procedure of OVPNs

The suggested OVPN structure is composed of customer sites in the electric control domain and the DWDM-based backbone network in the optical control domain, respectively (see Fig. 1). The external customer site is an IP network based on differentiated services (DiffServ) [6]. It aggregates IP packets, which have the same QoS level at the client edge nodes (CE) to reduce network complexity and to make operation simple. The internal OVPN backbone network is a DWDM network based on GMPLS. It consists of the provider edge nodes (PE) and the provider core nodes (P), and it forwards data traffic from the customer sites without electronic–optic–electronic (E–O–E) conversions. There is a QoS traffic policy server (QoS-TP server) for supporting DOQoS among customer sites. It negotiates service level agreement (SLA) parameters describing the service level between customer site and the OVPN backbone network. And, it sets an optical path according to the negotiated parameters. In this way, it can manage the entire network to support the service that satisfies the SLA through the optical path between end users.

The entire procedure of establishing an O-LSP and maintaining QoS by providing DOQoS is shown in Fig. 2. Phases A and B show the establishing procedure of the differentiated optical path for

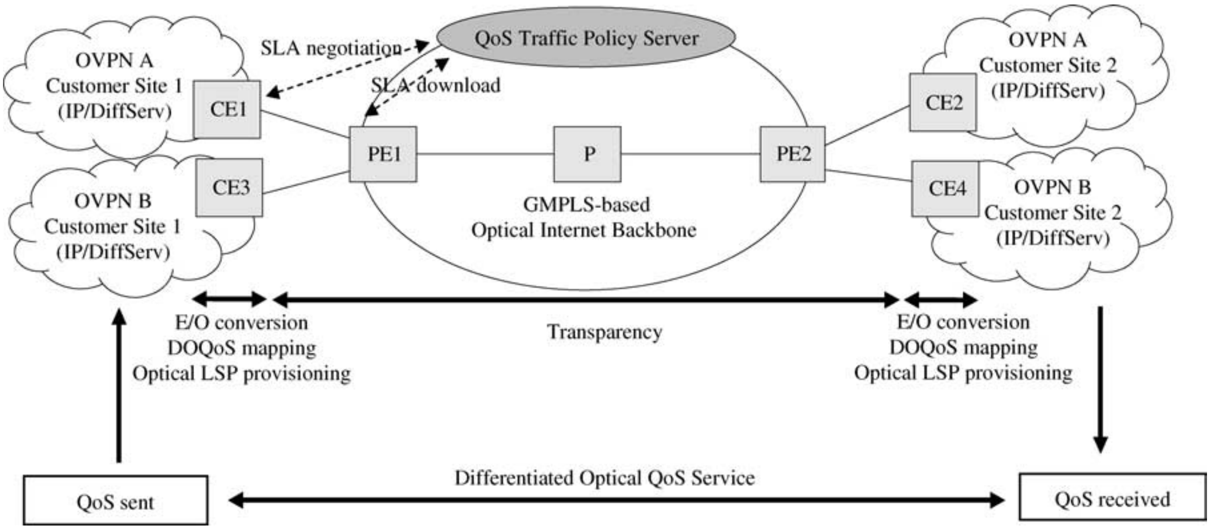


Fig. 1. OVPN model for providing DOQoS.

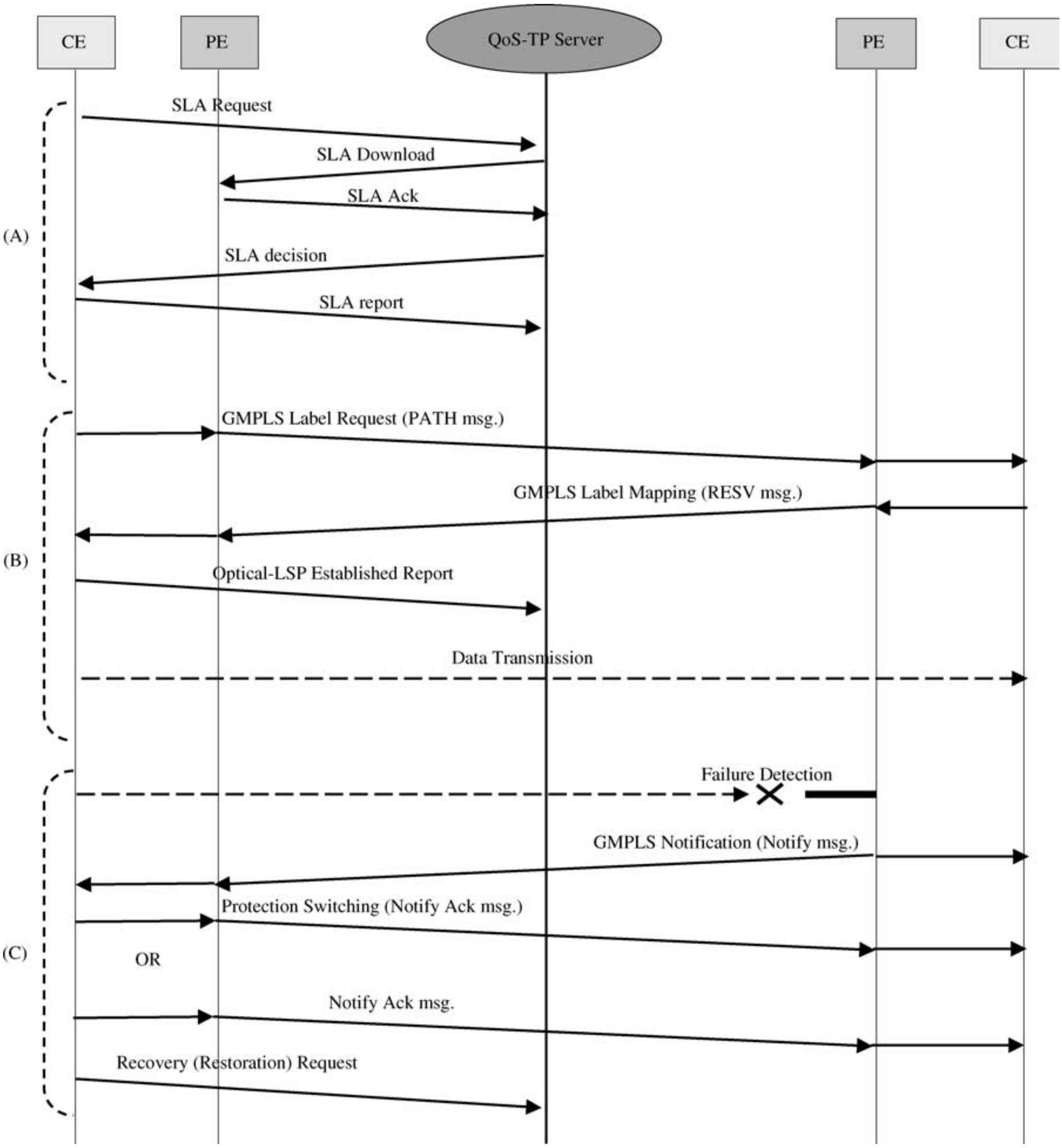

CE
PE
QoS-TP Server
PE
CE
SLA Request
SLA Download
SLA Ack
(A)
SLA decision
SLA report
GMPLS Label Request (PATH msg.)
GMPLS Label Mapping (RESV msg.)
(B)
Optical-LSP Established Report
Data Transmission
Failure Detection
GMPLS Notification (Notify msg.)
Protection Switching (Notify Ack msg.)
(C)
OR
Notify Ack msg.
Recovery (Restoration) Request

Fig. 2. OVPN operation mechanism for providing DOQoS.

providing DOQoS between customer sites, and phase C is a QoS maintenance mechanism by means of a recovery procedure upon failure in the OVPN backbone network.

Phase A represents the SLA negotiation procedure between the customer site and the QoS-TP server. A CE node at the customer site sends a SLA request that specifies the source and destination IP addresses, the customer port identifier (CPI) and provider port identifier (PPI), the aggregated IP flow information, bandwidth, and QoS parameters. When the QoS-TP server receives this request, it verifies the agreements of the traffic contract that was negotiated with the OVPN. If it satisfies the existing traffic contract, then the QoS-TP server downloads the SLA parameters onto the policy agent in the appropriate ingress PE to request a SLA allowance decision. The PE node calculates the QoS guaranteed path, and if it satisfies the demanded bandwidth and specific parameters of the DOQoS class in all the nodes of the path, then the SLA is accepted. If the QoS-TP server receives a return message that the SLA parameters have been accepted by the PE node, then it informs the ingress CE node to negotiate the SLA between the electronic and optic control domains. Further details are described in Section 4.

Phase B is the label distribution procedure of GMPLS to establish an O-LSP in the OVPN. Generally, the GMPLS signaling protocol, the resource reservation protocol with traffic engineering extensions (RSVP-TE +) [7], or the constraint-based routed label distribution protocol with extensions (CR-LDP +) [8] is used. In this paper, RSVP-TE + has been taken as the downstream-on-demand ordered control method to allocate labels. The PATH message allocates a wavelength or port by means of its GMPLS objects such as Generalized Label Request, Suggested Label, Label Set, Upstream Label, and so on. If an ingress CE node receives the RESV message, label distribution is operated on all nodes of the optical path between the end users. This DOQoS signaling procedure using RSVP-TE + will futher be illustrated in Section 4.

Phase C is the QoS recovery procedure for a QoS failure caused by network faults or attacks in the OVPN backbone network. Failures in the OVPN backbone network are detected by interoperation between the power monitoring module (PMM) and the optical resource management agent (ORMA). The localization is determined by the fault management function of the link management protocol (LMP) [9]. Occurrence of a failure is notified to the CE node of the OVPN, and the recovery procedure is processed according to the level of the DOQoS class. This QoS maintenance mechanism will be specified in Section 5.

In order to transmit user data transparently through the OVPN optical backbone network, the protocol layer structure should look like that in Fig. 3.

The OVPN based on DiffServ suggested in this paper reduces network complexity (1) by gathering IP traffic flows that have the same QoS requirements, and (2) by directly mapping the requested service class to the optical channels in the CE node to supply DOQoS. In the electrical–optical/optical–electrical (E–O/O–E) interface layer, IP packets from the higher layers are sorted into the classes 1, 2, and 3 according to specific parameters, as described in the next section. They are given proper GMPLS labels at the level of the DOQoS classes. And, the transmission rate is controled by the payload of the optical transport unit (OTU) that contains IP datagram and GMPLS label. After creating the OTU header, the OTU flows are adapted to the WDM layer by transforming the electrical signal to the optical wavelength according to the appropriate QoS. This E-O/O-E interface layer preserves the quality of the optical signals with the bit error rate (BER), electrical signal-to-noise ratio (el.SNR) and optical SNR (OSNR) for guaranteeing end-to-end QoS at the levels of the various DOQoS classes. The functions are performed by the QoS-TP server and the ORMA. Furthermore, this layer also guarantees end-to-end QoS at the level of the OCh wavelength by transmitting IP packets transparently through the optical channels.

3 DOQoS Classes

Generic classification of application types supported by the NGOI and OVPN may be divided into Class 1: applications that do require absolute QoS guarantees; Class 2: those requiring certain minimal statistical QoS guarantees; and Class 3: those that do not require explicit QoS guarantees at all [10,11]. Premium service (Class 1) for applications that have stringent real-time requirements, guarantees low loss, delay, jitter, and maximum bandwidth. Assured service (Class 2) offers an expected level of bandwidth with a statistical delay bound as a service that exhibits a greater degree of time-sensitivity, e.g., distributed simulation and real-time streaming. Best-effort service (Class 3) corresponds to current Internet services such as file transfer, web browsing, and e-mail that are supported by TCP and UDP.

Within the three services as described above, the DOQoS class is classified according to the parameters of the VPN service level specification (SLS) negotiated upon call setup (delay, jitter, bandwidth, etc.) with respect to BER/el.SNR/OSNR require-

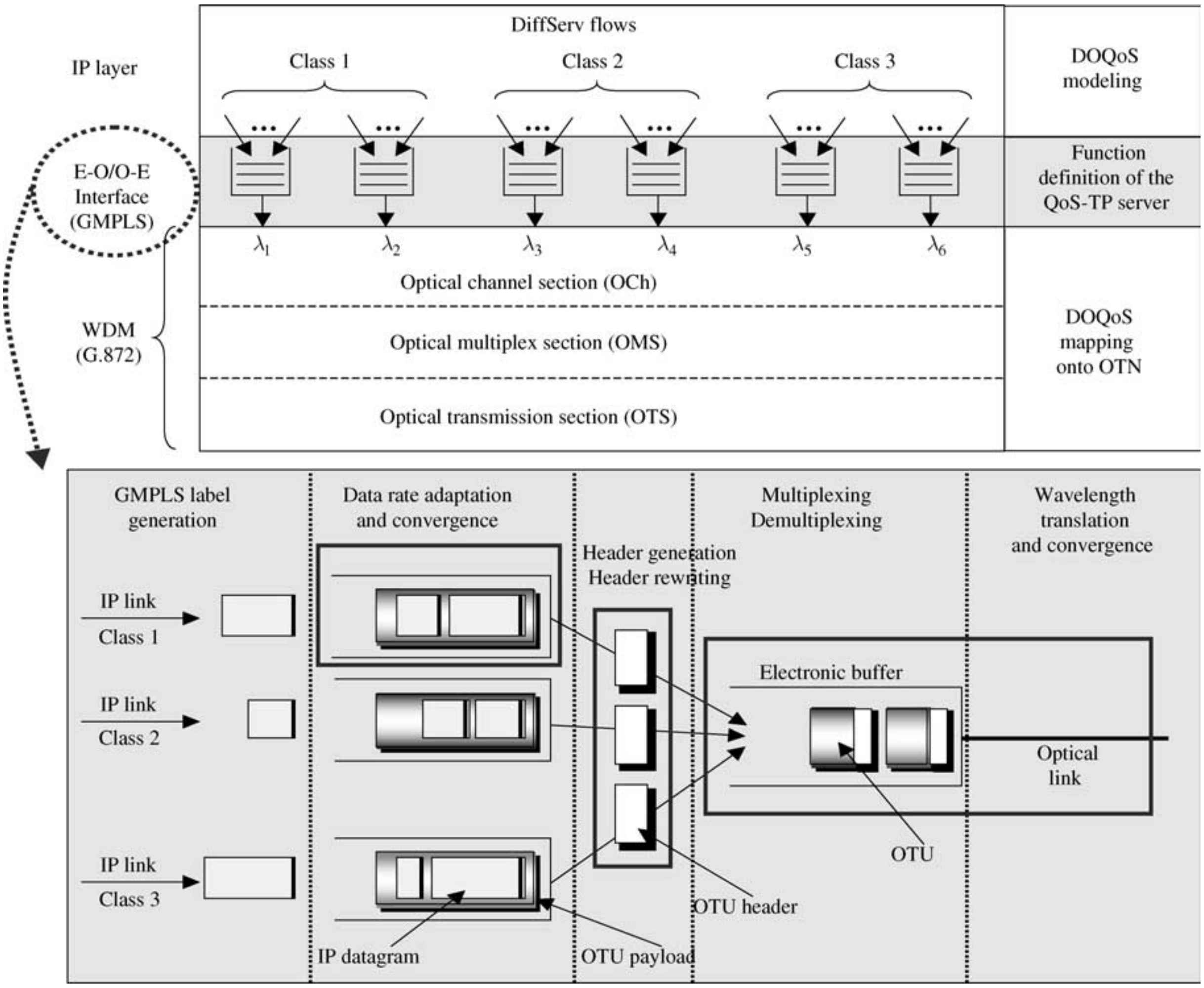


Fig. 3. DOQoS mapping of differentiated IP service in CE.

ments, the optical resource allocation scheme and survivability required against network failure or attack shown in Fig. 4 [12]. This classification will be applied to the suggested OVPN model for providing DOQoS.

The contents of the VPN SLS [13] include the essential QoS-related parameters, including scope and flow identification, traffic conformance parameters, and service guarantees. More specifically, the VPN SLS has the following fields: scope, shows the topology range in which the policy will be put into force; flow descriptor (Flow Id), represents the IP stream that shares at least one common feature; traffic descriptor, describes the traffic features of the IP packet stream corresponding to the Flow Id; excess treatment, indicates the parameter that describes how to process excessive traffic beyond the agreed profile; and performance parameters, consisting of delay, jitter, packet loss, and throughput.

In the GMPLS header, there is an experimental (Exp) field that is reserved for experimental use [14]. By using this field for the class of service (CoS) to implement differentiated optical Internet service, it can process packets according to the priority indicated by the Exp value of the packets specifying the application service. Because GMPLS Exp can classify totally eight services by three bits, the mapping according to the service features in this paper is given in Table 1.

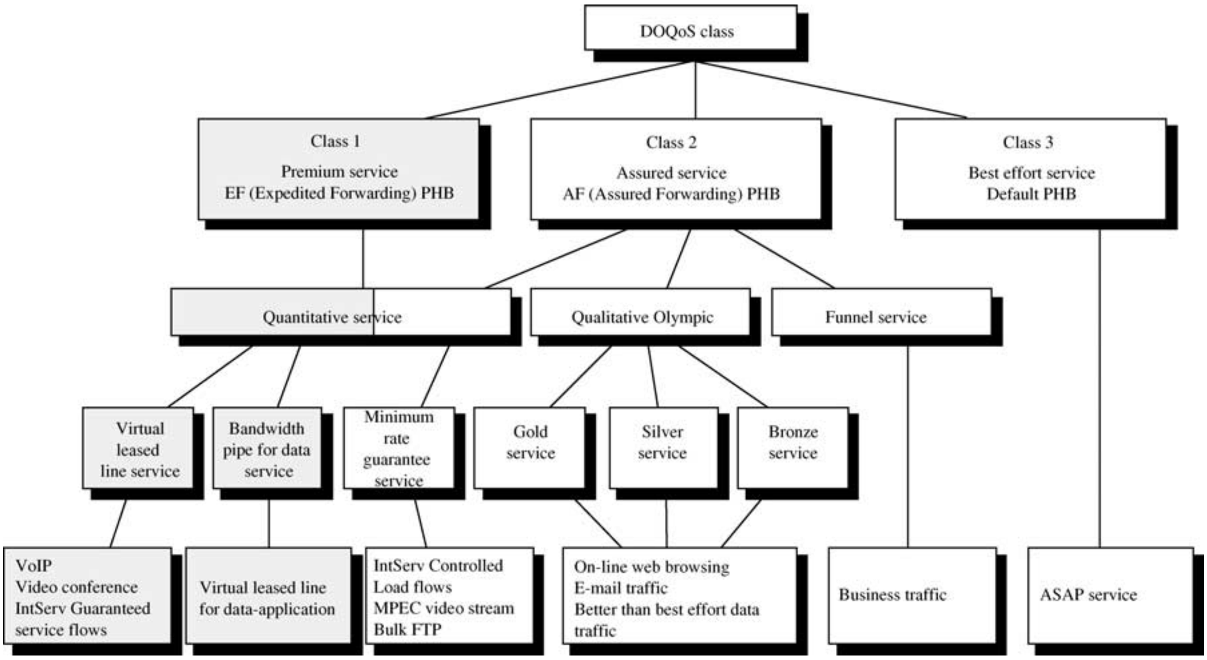


Fig. 4. DOQoS specification.

Table 1. The value of GMPLS Exp according to service types.

Service Type	GMPLS Exp field
Quantitative service	
Virtual leased line service	111
Bandwidth pipe for data service	110
Minimum rate guarantee service	101
Funnel service	100
Qualitative Olympic service	
Gold	011
Silver	010
Bronze	001
Best effort service	000

In a DWDM network, a source-destination pair has many optical paths. To determine the quality of the optical service on each path, it is necessary to define features such as BER, delay, jitter, and the protection scheme characterizing each optical path. While traveling through the components of the optical path such as optical cross-connects (OXC), fiber segments, and erbium doped fiber amplifiers (EDFAs), the optical signal may be changed by several causes such as jitter, wander, crosstalk, and amplified spontaneous emission (ASE). As signals propagate to the egress node, the transmission signal tends to be less or more modified so that the quality of optical signal may rapidly degrade. Most of these modifications can be determined by calculating BER in the receiving node. Therefore, BER is one of the most important parameters for the measurement of the optical path performance. However, it is very difficult to measure BER at the optical level, since data in an O-LSP of an OVPN is sent transparently without O–E conversion. Therefore, in order to measure performance of the optical transmission, the BER in this paper is obtained by the Q-factor [15]. The Q-factor is a new parameter evaluating signal quality, which measures the signal-to-noise ratio (SNR) based on assuming Gaussian noise statistics in the eye-diagram. The correlation among BER, el.SNR, OSNR, and Q-factor can be expressed by the following Equations (1) to (3) [16]. Therefore, a DOQoS class is classified by defining the limits of BER, el.SNR, and OSNR as QoS requirements. Then the factors are used for detecting failures caused by network faults and attacks.

$$\mathrm{BER}(Q) \cong \left(\frac{1}{\sqrt{2\pi}}\right) \cdot \left(\frac{\exp(-Q^2/2)}{Q}\right). \tag{1}$$

$$\mathrm{el.SNR} = 10 \log Q^2. \tag{2}$$

$$\mathrm{OSNR}_{0.1\,\mathrm{nm}} = \frac{(1+r)\cdot(1+\sqrt{r})^2}{(1-r)^2} \cdot \frac{\mathrm{Be}}{\mathrm{Bd}} \cdot Q^2, \tag{3}$$

$r = 0.15$ (extinction ratio of the transmitted optical signal)
$\mathrm{Be} = 0.75 \times f_0$ (effective electrical noise bandwidth due to bit rate f_0)
$\mathrm{Bd} = 12.6\,\mathrm{GHz}$ or $0.1\,\mathrm{nm}$ (optical bandwidth for OSNR measurement)

An EDFA optical amplifier provides a relatively flat and wide gain curve so that it is commonly used for transferring optical signals. In particular, it has a gain band available in the C-band ranging from 1530 to 1565 nm and also has a low attenuation factor of 0.28 dB/km. In terms of the influence of temperature, the bands up to 1625 nm can be used for transferring optical signals, whereby the L-band has an attenuation factor of 0.35 dB/km [17]. Therefore, the C-band is selected for an O-LSP of the premium service to provide high reliability and the L-band is used for an O-LSP of the assured or best-effort service [18]. Thus, the entire currently available band of wavelengths is divided into three categories in a proper proportion (premium: 10%, assured: 30%, best-effort: 60%), thereby gaining the load balancing effect by avoiding heavy loaded links and failing optical path settings.

Since in general the optical signal has a high data rate capacity, a failure would result in considerable losses of data. Accordingly, protection and restoration mechanisms are very critical to ensure that optical paths are transparent against various problems such as a broken optical line and a damaged wavelength. The premium service that transmits real-time data like sound requires very high reliability. This service is protected by a local QoS protection mechanism on the optical channel level or a GMPLS backup procedure within a recovery time of 50 ms or less. Reliable QoS of the assured service requires using an O-LSP restoration scheme of GMPLS that generates a backup path upon any occurrence of incidents. The O-LSP restoration scheme has to find the recovery O-LSP dynamically to replace a damaged optical path between ingress and egress PEs, so it requires longer recovery time than that in premium service (tens to hundreds of ms). This scheme may have better resource utilization but lower recovery success so that there is a trade-off. Best-effort service recommends an O-LSP restoration scheme at the IP level, where best-effort service with service interruption due to any failure is compensated by retransmission of TCP within a service time ranging from 100 ms to several seconds.

Based on the above considerations, the DOQoS classes in the next generation OVPN are suggested as shown in Table 2 [19].

4 O-LSP Establishment Scheme based on DOQoS Classes

In this section, the E–O/O–E interface layer for mapping the actual differentiated IP service flow onto the optical channel, the QoS-TP server, and the ORMA function are defined in the control plane of the OVPN node for implementing an effective wavelength assignment mechanism. Moreover, the establishing procedure of an O-LSP for providing DOQoS is suggested.

The QoS-TP server handles dynamic management of the SLA between the customer sites and the OVPN service provider and provides load-balancing management needed for improving network utilization. It also manages recovery operations for QoS failure due to network fault or attack. Furthermore, it manages the entire network to provide services that meet the SLA through the optical path between the end users.

When an OVPN backbone network is given a new set of service features or functions, it is important that the changes on the customer side should be minimized. The routers of the customer site should be used just as they were before, even if there are many changes in the OVPN backbone network. In this context, it seems to be good to take a centralized approach in which a central policy server provides a user interface, which can exchange the dynamic SLA negotiation parameters with a secured communication channel, and in which it performs a centralized QoS path computation and controls the optical nodes inside the OVPN backbone network.

However, this approach will lead to performance bottleneck problems when the network size becomes large. We therefore propose a decentralized approach in which the central policy server only performs SLA management, whereas the QoS path computation and

Table 2. DOQoS classes.

	Class 1		Class 2					Class 3
	Premium Service: Expedited Forwarding (EF) PHB		Assured Service: Assured Forwarding (AF) PHB					Best Effort (BE) Service: Default PHB
Classification criteria	Virtual Leased Line Service	Bandwidth Pipe for Data Service	Minimum Rate Guarantee Service	Qualitative Olympic Service			Funnel Service	
Scope	(1|1)	(1|1)	(1|1)	(1|1) or (1|N)			(N|1)	All
Flow descriptor	EF, *S-D* IP-A	EF, *S-D* IP-A	AF1x	MB1			AF1x	None
Traffic descriptor	$(b, r), r = 1$	NA	(b, r)	(b, r), r indicates a maximum CIR			(b, r)	NA, the full link capacity is allowed
Excess treatment	Dropping	NA	Remarking	Remarking			Dropping	NA
Performance parameters	$D = 20$ $(t = 5,$ $q = 10\text{E} - 3),$ $L = 0\ (R = r)$	$R = 1$	$R = r$	Gold Delay or Loss must be indicated qualitatively	Silver	Bronze	NA	NA
GMPLS Exp field	111	110	101	011	010	001	100	000
BER (Q)	10^{-12} (7)		10^{-9} (6)~10^{-7} (5.1)					10^{-5} (4.2)
el. SNR	16.9 dB		15.5 dB~14.2 dB					12.5 dB
OSNR ($f_0 = 10$ Gbit/s)	19.5 dB		18.2 dB~16.8 dB					15.1 dB
Resource allocation	Pre-specified percentage (10%) for this service (C band: 1530 nm–1565 nm)		Pre-specified percentage (30%) for this service (L band: 1565 nm–1625 nm)					Best use of the remaining bandwidth (L band: 1565 nm–1625 nm)
Recovery scheme	Local protection/backup λ-LSP		λ-LSP restoration					Restoration at IP level
Recovery time	< 50 msec (Detection time: < 100 msec)		50–100 msec (Detection time: 0.1 msec–100 msec)					1–100 sec (Detection time: 100 msec–180 sec)

(b, r): token bucket depth and rate (Mb/s), p: peak rate, D: delay (ms), L: loss probability, R: throughput (Mb/s), t: time interval (min), q: quantile, *S-D*: source and destination, IP-A: IP address, MBI: may be indicated, NA: not applicable, CIR: committed information rate.

resource reservation are performed in the PEs in a distributed manner.

ORMA manages, classifies, and reserves optical resources in a real time manner by interacting with the LMP. And it also preserves available wavelengths, links, nodes, and optical amplifiers and so on for establishing optical paths dynamically. Moreover, it receives data about the monitored Q-factor to calculate the BER value for the decision of the necessity for using the recovery mechanism by verifying limitations of the corresponding service class. It also decides about call acceptance/rejection according to the performance of the available optical resources by interacting with the call admission control (CAC). Finally, it gathers network status information and reserves optical resources by interacting with the signaling agent (see Fig. 5).

4.1 SLA Negotiation Procedure

In order to support differentiated optical service through the OVPN backbone network, an implementation of the SLA negotiation procedure between the customer site and the QoS-TP server is needed as has been shown in Fig. 2 (Phase A). Fig. 5 depicts the SLA negotiation procedure and the functional blocks in the OVPN node.

First, a policy agent of the CE sends a SLA request that specifies the source and destination IP addresses

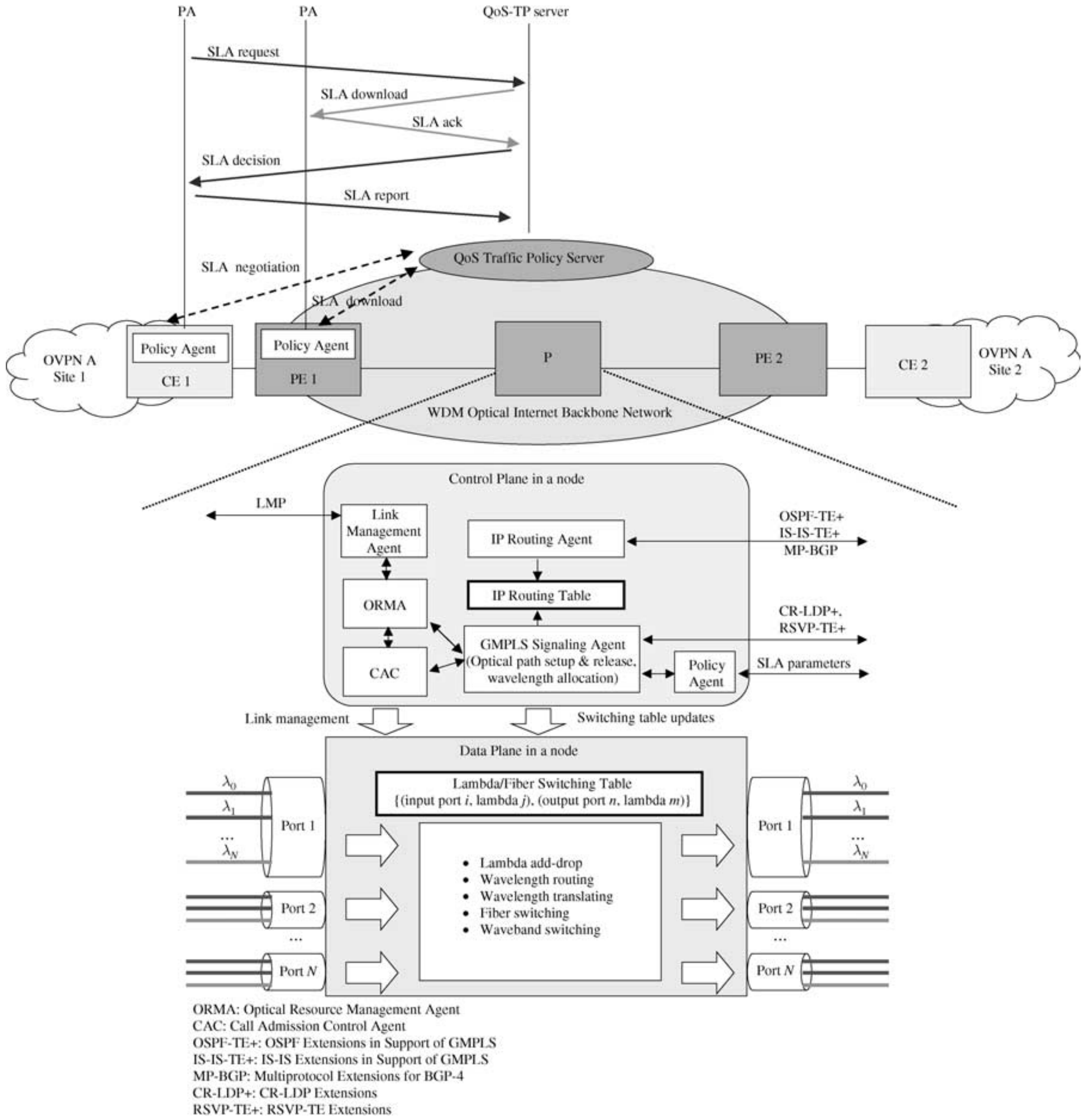


Fig. 5. SLA negotiation procedure and functional blocks in an OVPN node.

and the CPI/PPI, the aggregated IP flow information, bandwidth, and QoS parameters. When the QoS-TP server receives this request, it verifies the pre-negotiated traffic contract with the OVPN service provider. If it satisfies the traffic contract, then the QoS-TP server downloads the SLA parameters onto the policy agent in the appropriate ingress PE (PE1 in Fig. 5) to request a SLA allowance decision, which in turn establishes an O-LSP using RSVP-TE + signaling.

The policy agent conveys the parameters to the GMPLS signaling agent so that it can establish the GMPLS O-LSP from the ingress PE to the egress PE and can reserve resources along the path. When the GMPLS signaling agent receives a trigger for setting up an O-LSP, it asks the routing agent which uses

OSPF extensions in support of GMPLS (OSPF-TE +) [20] or IS-IS extensions in support of GMPLS (IS-IS-TE +) [21] to find the best QoS-guaranteed path to that egress PE router. The address of this egress PE is resolved by using the multiprotocol extensions of the BGP-4 (MP-BGP) [22] reachability information. MP-BGP is the extension of BGP-4 to enable it to carry routing information for multiple network layer protocols (e.g., IPv6, IPX, etc.). Therefore, it is used for exchanging routing information among the customer sites in the same OVPN. At each transit node, where the QoS guaranteed path is calculated in the routing agent, the requested bandwidth and specific parameters of the DOQoS class in the message are examined by the CAC and the ORMA to see whether or not it is possible to establish the O-LSP. Then it sends the result to the QoS-TP server. As soon as the QoS-TP server gets the result, it informs the policy agent of the CE to negotiate the SLA between the electronic and optic control domains.

Fig. 6 gives a flowchart of the SLA negotiation procedure considering DOQoS classes between CE and QoS-TP server. SLA negotiation is applied differently according to the service class levels. For the premium service, as defined in Section 3, the SLA negotiation is decided by selecting a working path and backup path satisfying the QoS requirements in the pre-allocated wavelength part (10%) in the C-band. For the assured service and the best effort, having inferior priority compared to the premium service, the

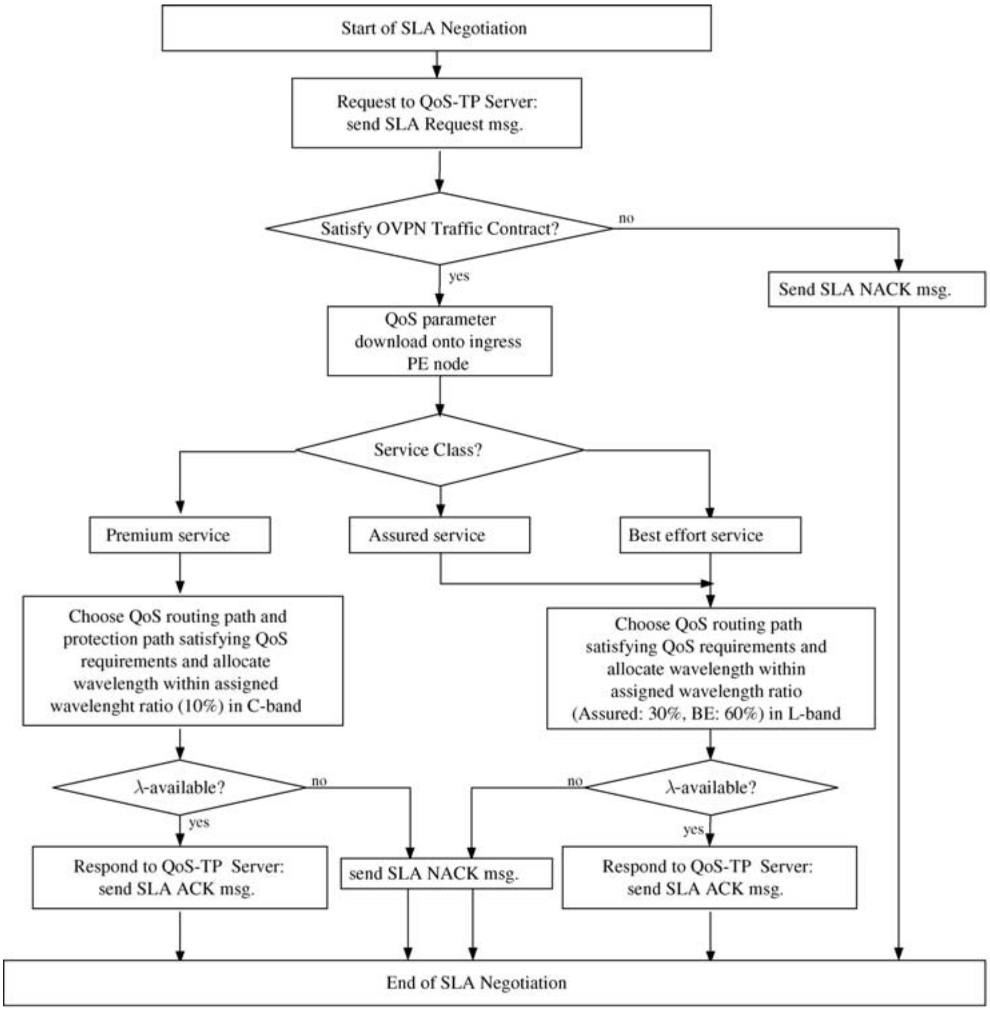

Start of SLA Negotiation
Request to QoS-TP Server: send SLA Request msg.
Satisfy OVPN Traffic Contract?
no
yes
Send SLA NACK msg.
QoS parameter download onto ingress PE node
Service Class?
Premium service
Assured service
Best effort service
Choose QoS routing path and protection path satisfying QoS requirements and allocate wavelength within assigned wavelenght ratio (10%) in C-band
Choose QoS routing path satisfying QoS requirements and allocate wavelength within assigned wavelength ratio (Assured: 30%, BE: 60%) in L-band
λ-available?
no
yes
λ-available?
no
yes
Respond to QoS-TP Server: send SLA ACK msg.
send SLA NACK msg.
Respond to QoS-TP Server: send SLA ACK msg.
End of SLA Negotiation

Fig. 6. SLA negotiation procedure.

SLA is decided by selecting a working path that satisfies QoS requirements in the pre-allocated wavelength part (assured: 30%, best effort: 60%) in the L-band.

4.2 Signaling for Establishing an O-LSP

After SLA negotiation between the customer site and the OVPN backbone network, the GMPLS signaling procedure is operated for O-LSP establishment. In this paper, RSVP-TE + , one of the GMPLS signaling protocols, is used for label distribution. The operation of RSVP-TE + is illustrated in Fig. 7 with the messages needed to reserve resources such as the PATH and RESV messages. For establishing differentiated O-LSP based on DOQoS classes, the Exp field in the GMPLS header is used as CoS function to allocate different values for each service class. The traffic of each DOQoS class and QoS parameters are defined with the traffic descriptor (Tspec), the service specification (Rspec), and the Adspec object in RSVP-TE + . As the resources are reserved with these parameters, differentiated QoS can be guaranteed.

Table 3 shows the parameters belonging to the Tspec, Rspec, and Adspec objects needed to support applications desiring guaranteed service.

Premium service requires a strict end-to-end delay bound as well as no packet loss, but only for a packet flow that agrees with the given traffic specification. Therefore, in order to satisfy strict QoS requirements, the flow should guarantee for constant bandwidth rate. For this, an egress CE seeks for *r*, *b*, *p* and *m* information from the Tspec as well as Qmindel, Error contents (C_{tot}, D_{tot}), PathMTU and Bpath from the Adspec. The end-to-end worst-case queuing delay (Qdelreq) can be obtained by subtracting Qmindel from the maximum delay time required by the egress CE. *R* can be obtained by applying Qdelreq, C_{tot}, D_{tot}, *M*, *r*, *b* and *p* to Equations (4) to (6).

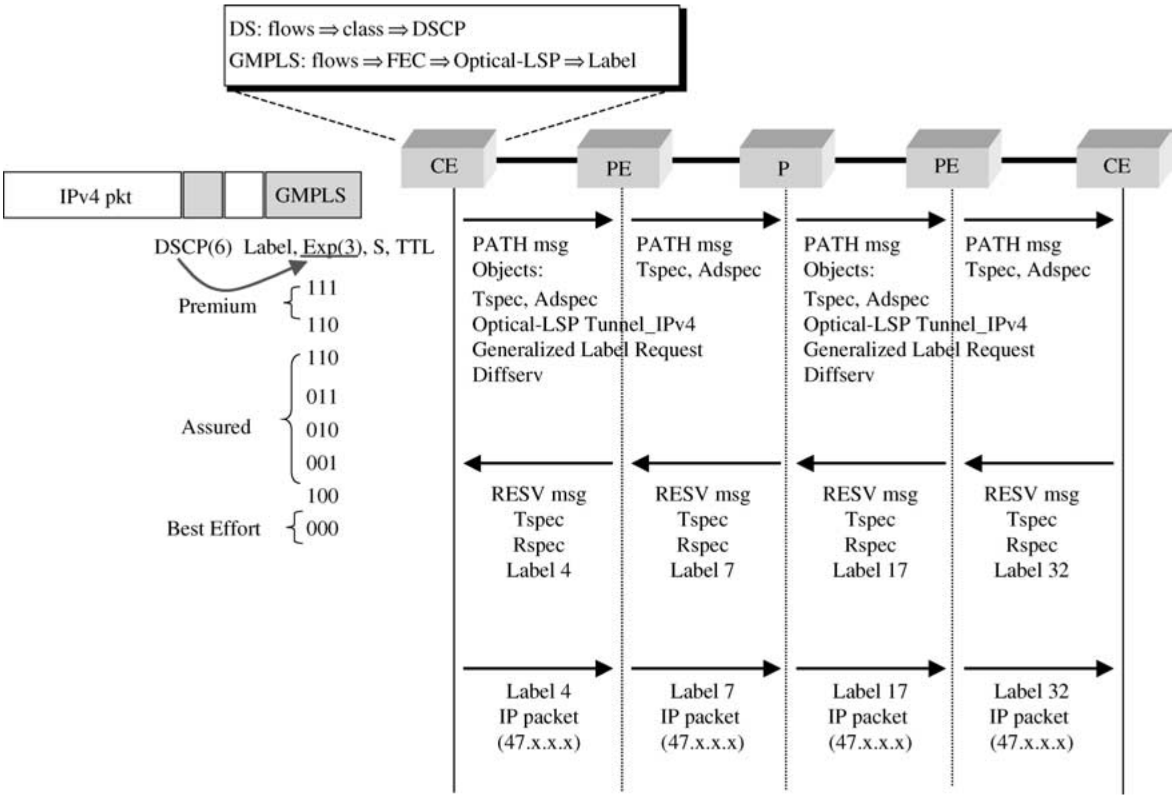


Fig. 7. RSVP-TE + operation mechanism for assuring QoS.

Table 3. Tspec, Rspec and Adspec objects.

Tspec	p	The maximum rate at which packets can be transmitted (bytes/s).
	r	The rate at which tokens arrive at the token bucket (bytes/s).
	b	The size of the token bucket (bytes).
	m	The maximum packet size that can be accepted (bytes).
	M	Any packet with a size smaller than m will be counted as m bytes (bytes).
Rspec	R	The service rate or bandwidth requirement (bytes/s).
	S	The extra amount of delay that a node may add that still meets the end-to-end delay requirement (ms).
Adspec	Bpath	The amount of bandwidth available along the path followed by a data flow.
	Qmindel	The minimum packet delay of a hop or a path.
	PathMTU	The maximum transmission unit (MTU) along a path.
	C_{tot}	The sum of C over a path (C: Rate-dependent error term, measured in byte).
	D_{tot}	The sum of D over a path (D: Rate-independent error term, measured in units of 1 microsecond).
	Csum	The partial sum of C between shaping points.
	Dsum	The partial sum of D between shaping points.

$$\text{Qdelreq} = \frac{(b-M)(p-R)}{R(p-r)} + \frac{M + C_{\text{tot}}}{R} + D_{\text{tot}} \quad (p > R \geq r). \tag{4}$$

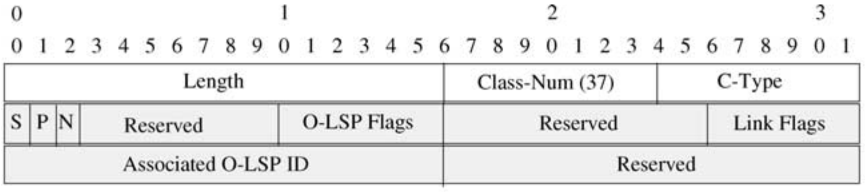
$$\text{Qdelreq} = \frac{M + C_{\text{tot}}}{R} + D_{\text{tot}} \quad (R \geq p \geq r). \tag{5}$$

$$\text{Qdelreq} = \frac{b}{R} + \frac{C_{\text{tot}}}{R} + D_{\text{tot}} \quad (R \leq r). \tag{6}$$

For a successful requested resource reservation, R should be reduced if R is greater than the value of Bpath. The egress CE sets Rspec with the calculated R. And the RESV message containing Rspec is sent to the ingress CE through the path. Then the required QoS can be guaranteed.

Assured service does not require specific values for delay time and packet loss, since it permits a certain range of values. Traffic parameters are defined by Tspec and Rspec. Unlike premium service, the p value in Tspec is not specified since it permits a certain amount of packet loss depending on the network situation.

Since best effort service does not need to reserve specific resources, the ingress CE node can establish an O-LSP tunnel without resource reservation by sending a PATH message containing Tspec set to zero. And, if it receives a RESV message containing the Tspec and Rspec parameters set to zero, an unreserved resource O-LSP tunnel between the end-to-end CEs is established.



- S: When set to 1, this bit indicates that the requested O-LSP is a secondary O-LSP. When set to 0 (default), it indicates that the requested O-LSP is a primary O-LSP.
- P: When set to 1, this bit indicates that the requested O-LSP is a protecting O-LSP.
- N: When set to 1, this bit indicates that the control plane message exchange is only used for notification during protection switching. When set to 0 (default), it indicates that the control plane message exchanges are used for protection switching purposes.
- O-LSP Flags: Indicates the desired end-to-end O-LSP recovery type. (Unspecified/Extra Traffic/ Unprotected/Shared Mesh/Dedicated 1:1 (with Extra Traffic)/Dedicated 1+1 Unidirectional/Dedicated 1+1 Bidirectional).
- Link Flags: Indicates the desired link protection type.
- Associated O-LSP ID: Identifies the O-LSP protected by this O-LSP or the O-LSP protecting this O-LSP.

Fig. 8. The format of the protection object.

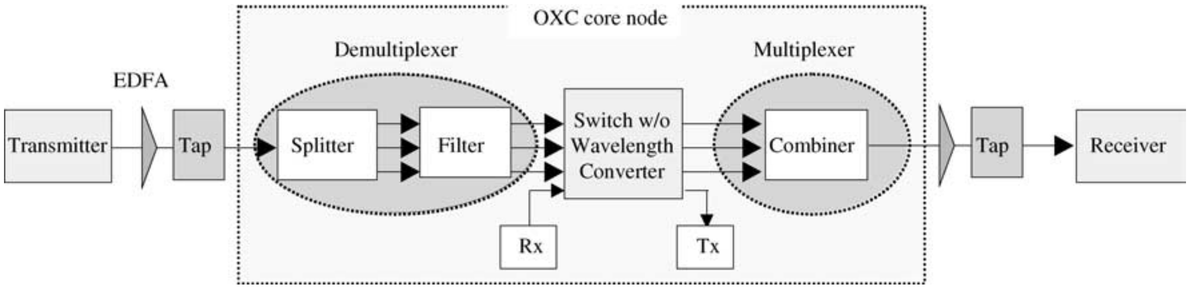


Fig. 9. The model of the OVPN optical backbone network.

For assured or best effort service, which uses the restoration scheme of GMPLS or IP level as recovery mechanism, only the working path is established. But, for premium service that uses the GMPLS protection scheme, an additional protection path is needed. To do this, it is necessary to set the P bit to one using the protection object of the Path message as shown in Fig. 8, which indicates that the requested O-LSP is a protecting O-LSP. The protection object represents the end-to-end O-LSP recovery type (1 : 1, 1 + 1, shared mesh, extra -traffic, etc.) and the descriptor of the working path protected by the protection path (associated O-LSP ID field in Fig. 8) [23]. Such a protection path like the working path reserves resources with the Tspec, Rspec, and Adspec objects. When a failure occurs on the working path, the traffic on the working path is switched over to the protection path by the swichover request of the Notify message.

5 QoS Maintenance Mechanism

The OVPN optical backbone network is a DWDM all-optical transport network composed of transparent OXCs. Fig. 9 represents the DWDM system composed of the basic optical elements. In this model, a lightpath consists of a number of intermediate OXCs between the source and the destination nodes, interconnected by fiber segments, amplifiers and optional taps. The optical components that constitute a DWDM node in general include a cross-connect switch (with or without wavelength conversion functionality), a demultiplexer comprising of (optional) signal splitters and optical filters, and a multiplexer made up of signal combiners.

In this section, QoS failures are analyzed due to network faults or attacks in the OVPN optical backbone network, and a QoS recovery mechanism for each service class is suggested, including a detection mechanism.

5.1 Analysis of QoS Failures

QoS failures in OVPNs can be considered in three types. Firstly, a failure caused by the violation of initial negotiated traffic contract with the OVPN service provider. Secondly, a service disruption caused by system malfunction as a result of a sudden fault or intentional attack of active elements in the optical network. Finally, a service degradation caused by the gradual attenuation of signal quality. Table 4 summarizes a QoS failure classification and its corresponding detection mechanisms.

First of all, a failure caused by violation of the traffic contract between the customer and the QoS-TP server upon request of establishing a CE-to-CE O-LSP can happen. The QoS-TP server informs the failure of the SLA negotiation to the customer, and requests the traffic contract to readjust.

Secondly, service disruption caused by a fault or intentional attack due to severance of fiber or transmitter causing laser malfunction can be classified into three levels such as link, channel, and node level as shown in Table 4. Since, these service disruptions incur the loss of optical signals, it is possible to extract the loss of light (LOL) alarm from the PMM located in each node (see Fig. 10).

Finally, service degradation is caused by noise from random fluctuation, pulse distortion, or crosstalk. Especially, the random fluctuation can be dealt with the Gausian process such as ASE or relative intensity noise (RIN). Generally, these degradations of signal quality can be detected by analyzing the overhead of data at the electrical level after the optical to electrical conversion (For example, in case of using the B1, B2 bytes in the SDH system). However, an O-LSP of the OVPN, which does not convert between optical–

Table 4. QoS failure classification and detection mechanism.

Category		Cause	Characteristic	Detection
Traffic Contract Violation		By violation of pre-negotiated traffic contract	SLA rejection	SLA management function of QoS-TP server
Service Disruption	Link level	Physical fiber link breakdown	Loss of light (LOL)	LOL alarm from Power Monitoring Module
	Channel level	Wavelength channel blocking		
	Node level	Node breakdown		
Service Degradation	By noise	Amplified spontaneous emission Relative intensity noise	Gradual attenuation of signal quality	BER/e1.SNR/OSNR Estimation by Q-factor
	By distortion	Chromatic dispersion Nonlinearities (SPM, XPM, FWM...)		
	By crosstalk	Interferometic crosstalk		

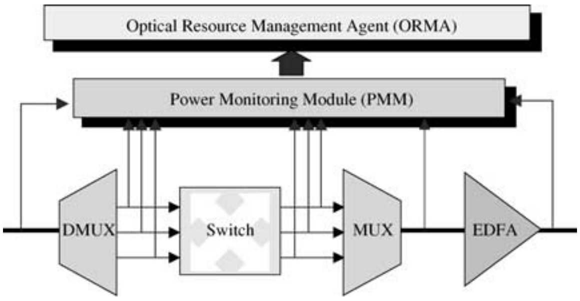

Optical Resource Management Agent (ORMA)
Power Monitoring Module (PMM)
DMUX
Switch
MUX
EDFA

Fig. 10. The model of QoS failure detection.

electrical signals, requires monitoring at the optical level. The Q-factor [15] obtained from the eye diagram is the method to measure quality of signal without O–E conversion used in this paper.

5.2 QoS Recovery

QoS Recovery is in general operated in the sequential order of failure detection, failure localization, failure notification, and QoS recovery (protection/restoration) [24].

5.2.1 Failure Detection

One of the QoS failures, the violation of traffic contract, can be detected during the procedure of the SLA negotiation. On the contrary, service disruption or degradation happens during the process of data transmission through the O-LSP. So there is detection mechanism required.

A QoS failure detection model is shown in Fig. 10. The PMM of each node detects system failures in the multiplexer/demultiplexer, switch, or amplifier. It further detects LOL by monitoring the input power and it sends the monitored BER information with the Q-factor to the ORMA (see Fig. 11).

The ORMA detects service disruption with the LOL alarm from the PMM. The service degradation is obtained by comparing the regularly monitored BER value with the limits specified in the service class (Premium: 10^{-12}, Assured: $10^{-4} \sim 10^{-7}$, Best-effort: 10^{-5}).

5.2.2 Failure Localization

Failure localization is the localizing step that informs the place of failure origin and separates the malfunction elements from the existing traffic, and it uses the fault management function of LMP, the link

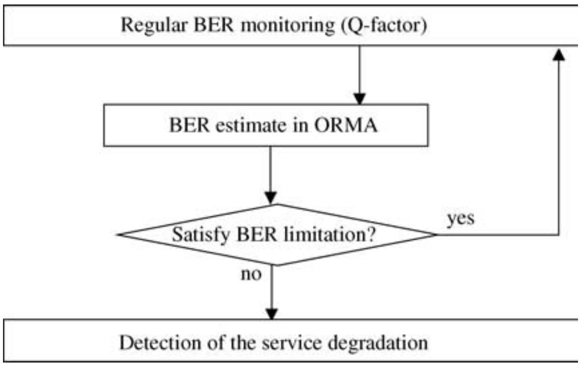

Regular BER monitoring (Q-factor)
BER estimate in ORMA
Satisfy BER limitation?
yes
no
Detection of the service degradation

Fig. 11. The detection mechanism of service degradation.

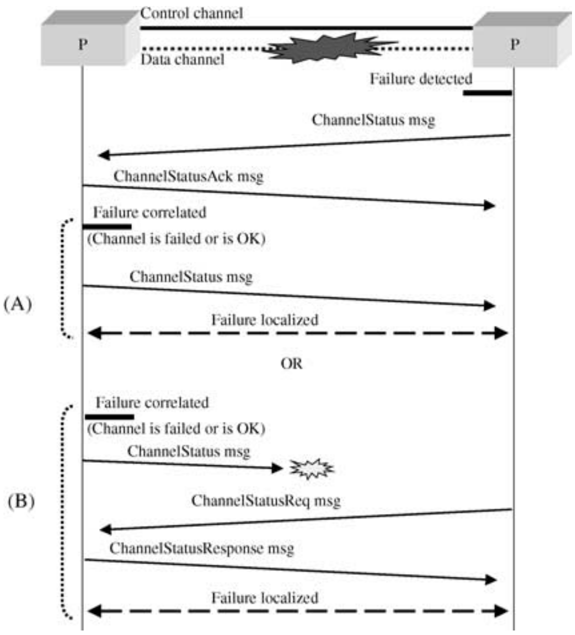


Fig. 12. Failure localization using LMP.

management protocol of GMPLS as shown in Fig. 12. If the failures defined in Table 4 are detected in the ORMA (as shown in Fig. 10), the LMP informs the adjacent upstream node about the failure using a Channel Status message containing a Channel Status object as defined in Fig. 13.

The Channel Status object represents the descriptor of the data link (Interface_Id field in Fig. 13), the status of the data link (Signal Okay, Signal Degrade, Signal Fail), and the direction of the data channel. When the upstream node receives the Channel Status message, it sends a Channel Status Ack message back to the downstream node and checks if the O-LSP has another failures. Next, it localizes the failure between the two nodes by notifying the downstream node by means of a Channel Status message as shown in Fig. 12 (A). If there is no Channel Status message after recognition of a failure, it should be localized by sending a Channel Status Request message as shown in Fig. 12 (B).

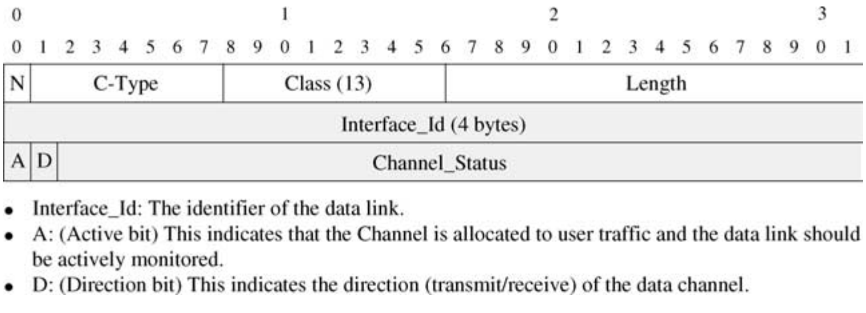
5.2.3 Failure Notification

Failure notification for informing failure localization notifies the failures to the intermediate nodes on the O-LSP and the node that has responsibility for the recovery scheme operated by using a Notify message in RSVP-TE + .

In the case of premium service, a Notify message, which represents a ''Working Path Failure; Switchover Request'', is transmitted to the ingress CE as shown in Fig. 14 (A). The Notify message informs about the failed working link descriptor and the failure information such as signal degradation, signal failure and so on. When the ingress CE receives these Notify messages, it switches to a prepared protection path that is shown in Fig. 14 (B), and it informs the egress CE using a Notify Ack message as shown in Fig. 14 (C).

In the case of assured service, the restoration path should be obtained dynamically by replacing the damaged optical path between nodes. Therefore, a Notify message is sent to the ingress CE that a failure has been occurred (the same as in Fig. 14 (A)). Then, the CE replies with a Notify Ack message (the same as in Fig. 14 (C)) and asks for calculation of a new path satisfying the QoS requirements to the QoS-TP server (the same as in Fig. 14 (F)).

In the case of best effort service, it uses a restoration scheme at the IP level. As soon as the ingress CE receives a Notify message of the failure, it



```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-------------+---------------+-------------------------------+
|N|   C-Type    |  Class (13)   |            Length             |
+-+-------------+---------------+-------------------------------+
|                     Interface_Id (4 bytes)                    |
+-+-+-----------------------------------------------------------+
|A|D|                       Channel_Status                      |
+-+-+-----------------------------------------------------------+
```

- Interface_Id: The identifier of the data link.
- A: (Active bit) This indicates that the Channel is allocated to user traffic and the data link should be actively monitored.
- D: (Direction bit) This indicates the direction (transmit/receive) of the data channel.

Fig. 13. The format of the Channel Status Object.

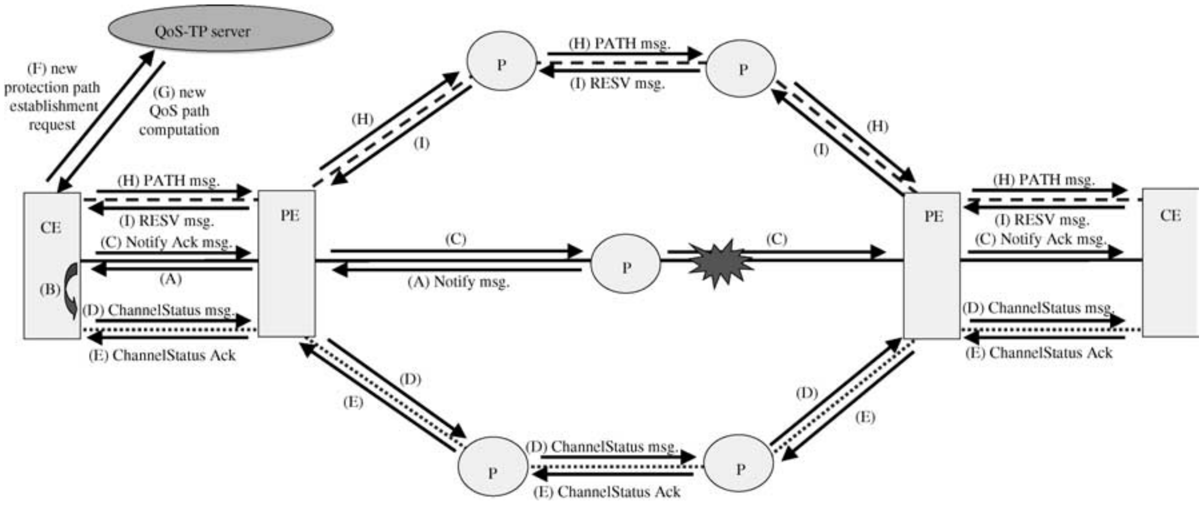


Fig. 14. Recovery procedure of premium service.

replies with the Notify Ack message (the same as in Fig. 14 (A) and (C)) and compensates through TCP retransmission.

5.2.4 *QoS Recovery (Protection/Restoration)*

The premium service using the GMPLS protection scheme switches traffic with a prepared protection path for traffic recovery after receiving a Notify message in the ingress CE. At this time, each node informs about the allocation of the user's traffic and requests constant monitoring using the A bit in the Channel Status message of the LMP to activate the control channel as shown in Fig. 14 (D). The downstream nodes receiving these messages reply with a Channel Status Ack message, and update the optical status of the ORMA that manages the optical resources as shown in Fig. 14 (E). Then, for the establishment of a new protection path, the ingress CE asks the QoS-TP server to calculate a new protection path that satisfies the QoS requirements as shown in Fig. 14 (F). If the QoS-TP server calculates the new protection path, then the resources are reserved by the mechanism explained in Section 4 and shown in Fig. 14 (G–I).

On the contrary, in assured service, which seeks the restoration path after the presence of a network failure, for establishing an O-LSP, the ingress CE requests the QoS-TP server to calculate a restoration path that satisfies the QoS requirements as shown in Fig. 14 (F). If the QoS-TP server has calculated a restoration path, then the resources are reserved by the mechanism explained in Section 4 and shown in Fig. 7.

Finally, in best effort service that does not require explicit QoS guarantees a failure is compensated by TCP retransmissions since it uses the restoration scheme of the IP level.

6 Conclusion

In this paper, DOQoS classes are considered for supporting real-time service that is sensitive to delay and requiring high bandwidth in an OVPN over IP/GMPLS over DWDM. In order to implement an effective wavelength usage mechanism in the E–O/O–E interface layer, the QoS traffic policy server and the ORMA are used for establishing an O-LSP for supporting DOQoS. And, by analyzing QoS failures caused by network faults and attacks, a QoS maintenance scheme has been suggested for each DOQoS class.

In future research, it is needed to study specific functional extensions and interoperation among many control protocols (MP-BGP, OSPF-TE + /IS-IS-TE +, RSVP-TE + /CR-LDP +, LMP) in an OVPN environment that guarantees DOQoS.

Acknowledgment

We appreciate the precious comments of Dr. Harmen Van As for the completion of this paper. This work was supported by grant No. (R01–2003–000–10526–0) from Korea Science & Engineering Foundation.

References

[1] H. Ould-Brahim, et al., Generalized Provider-provisioned Port-based VPNs using BGP and GMPLS Toolkit, draft-ouldbrahim-ppvpn-gvpn-bgpgmpls-03.txt, IETF Internet Draft, March 2003.

[2] Tomonori Takeda, Layer 1 Virtual Private Network Generic Requirements and Architectures, ITU-T Draft Rec. Y.l1vpnsdr, November 2002.

[3] Y. Qin, et al., Architecture and analysis for providing virtual private networks with QoS over optical WDM networks, Optical Network Magazine, vol. 2, no. 2, (April 2001), pp. 57–65.

[4] Eric Mannie, Generalized Multi-Protocol Label Switching (GMPLS) Architecture, draft-ietf-ccamp-gmpls-architecture-07.txt, IETF Internet Draft, May 2003.

[5] Jigesh K. Patel, Sung U. Kim, David H. Su, QoS recovery schemes based on differentiated MPLS services in all-optical transport next generation internet, Photonic Network Communications, vol. 4, no. 1, (Jan. 2002), pp. 5–18.

[6] Chava Vijaya Saradhi, C. Siva Ram Murthy, A framework for differentiated survivable optical virtual private networks, Photonic Network Communications, vol. 4, no. 3, (July 2002), pp. 457–487.

[7] L. Berger, GMPLS Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions, IETF RFC 3473, Jan. 2003.

[8] P. Ashwood-Smith, L. Berger, GMPLS Signaling Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions, IETF RFC 3472, Jan. 2003.

[9] J. P. Lang, et al., Link Management Protocol, draft-ietf-ccamp-lmp-09.txt, IETF Internet Draft, June 2003.

[10] V. Jacobson, et al., An Expedited Forwarding PHB, IETF RFC 2598, June 1999.

[11] J. Heinanen, et al., Assured Forwarding PHB Group, IETF RFC 2597, June 1999.

[12] P. Triminitzios, et al., A management and control architecture for providing IP differentiated services in MPLS-based networks, IEEE Communication Magazine, vol. 39, no. 5, (May 2001), pp. 80–88.

[13] F. Chiussi, et al., Framework for QoS in Provider-Provisioned VPNs, draft-chiussi-ppvpn-qos-framework-01.txt, IETF Internet Draft, March 2003.

[14] E. Rosen, et al., MPLS Label Stack Encoding, IETF RFC 3032, Jan. 2001.

[15] Rec. G.976, Test methods applicable to optical fiber submarine cable systems, COM15R68 (TSB, 7 Nov. 1996), Sect. 7.6.1.1: Measurement of Q-factor, pp. 172–174 and Annex A.4: ‘‘Q-factor’’ p. 17.

[16] G. Bendelli, et al., Optical performance monitoring techniques, ECOC 2000 (Munich, Germany, Sept. 2000), paper 11.4.1, pp. 113–1168.

[17] Lucent’s White Contribution COM 15–39-E, L- and C-Band Attenuation in Installed fiber Links, ITU-T SG15 Contribution.

[18] KDDI’s White Contribution D.97 (WP4/15), Recent technical information on C- and L-bands in optical transmission systems, ITU-T SG15 Contribution, Feb. 2001.

[19] Jae-Dong Lee, Sung-Un Kim, et al., Differentiated wavelength assignment with QoS recovery for DWDM next generation internet backbone networks, Photonic Network Communications, vol. 5, no. 2, (March 2003), pp. 163–175.

[20] K. Kompella, Y. Rekhter, OSPF Extensions in Support of Generalized MPLS, draft-ietf-ccamp-ospf-gmpls-extensions-09.txt, IETF Internet Draft, Dec. 2002.

[21] K. Kompella, Y. Rekhter, IS-IS Extensions in Support of Generalized MPLS, draft-ietf-isis-gmpls-extensions-16.txt, IETF Internet Draft, Dec. 2002.

[22] T. Bates, et al., Multiprotocol Extensions for BGP4, IETF RFC2858, June 2000.

[23] J. P. Lang, et al., RSVP-TE Extensions in support of End-to-End GMPLS-based Recovery, draft-lang-ccamp-gmpls-recovery-e2e-signaling-02.txt, IETF Internet Draft, Feb. 2003.

[24] D. Papadimitriou, E. Mannie, Analysis of Generalized MPLS based Recovery Mechanisms (including Protection and Restoration), draft-ietf-ccamp-gmpls-recovery-analysis-02.txt, IETF Internet Draft, May 2003.

Mi-Ra Yoon received her B.S. degree in Telematics Engineering from Pukyong National University, Korea, in 2002. She is currently pursuing the master’s degree. Her research interests include OVPN, QoS, GMPLS, NGN and survivability.

Ju-Dong Shin received his B.S. degree in Telematics Engineering from Pukyong National University, Korea, in 2002. He is currently pursuing the master’s degree. His research interests include optical network, VPN and network survivability.

Chang-Hyun Jeong received his B.S. degree in Telematics Engineering from Pukyong National University, Korea, in 2003. He is currently pursuing the master's degree. His research interests include OVPN, QoS, DWDM and survivability.

Jun-Mo Jo received his B.S. from Iowa State University, USA, in 1991 and his M.S. degree in Computer Engineering from Kyungpook National University, Korea. He is now a Ph.D. candidate at Kyungpbuk National University. Since 1998, he has been an assistant professor in the Department of Internet Security, Tong-Myong College, Korea. His research interests include OVPN, GMPLS, Network Security, and Information Assurance.

Oh-Han Kang is an associate professor of computer education at the Andong National University, Korea. He was a visiting scholar at the Center for Distributed and Mobile Computing at the University of Cincinnati in 1999. He worked as a senior engineer for Qnix Computer Corp., from 1984 to 1993. He received his B.S. degree in electrical engineering from Kyungpook National University, Korea, in 1982 and M.S. and Ph.D. degrees in computer science from the Korea Advanced Institute of Science and Technology in 1984 and 1992, respectively. His research interests include parallel and distributed computing, mobile computing, and multimedia service in OVPN.

Sung-Un Kim received his B.S. from Kyungpook National University, Korea, in 1982 and his M.S. and Ph.D. degrees in Computer Science from the University of Paris 7, France, in 1990 and 1993, respectively. He joined Electronics and Telecommunications Research Institute (ETRI, Korea) in 1982 and then Korea Telecom Research Labs (KTRL) in 1985, where he has developed protocol testing systems for LAN, B-ISDN and Intelligent Network and developed also a protocol validation tool. He was also an editor for ITU-T SG7 Q.23 on data communication protocol testing. Since 1995, he has been an associate professor in the Department of Telematics Engineering, Pukyong National University, Korea. His research interests include protocol engineering, GMPLS, DWDM optical network and QoS.