Differentiated Optical QoS Service Framework in Next Generation Optical VPN

차세대 OVPN에서 차등화된 광 QoS 서비스 제공 프레임워크 연구

A thesis submitted in partial fulfillment of the requirements

for the degree of

Master of Engineering

in the Department Telematics Engineering, Graduate School,

Pukyong National University

February 2004

윤미라의 공학석사 학위논문을 인준함

2004년 12월 26일

주 심 공학박사 김 석 태 (인)

위 원 공학박사 주 문 갑 (인)

위 원 공학박사 김 성 운 (인)

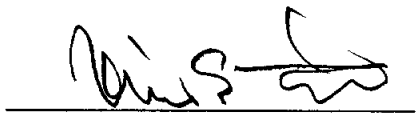
Differentiated Optical QoS Service Framework
in Next Generation Optical VPN

A Dissertation

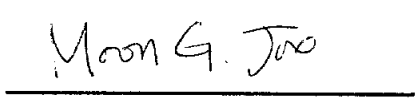
by

Mi-Ra Yoon

Approved as to style and contents by:



(Chairman) Seok-Tae Kim



(Member) Moon-Gab Joo

(Member) Sung-Un Kim

December 26, 2003

Contents

Differentiated Optical QoS Service Framework in Next Generation Optical VPN

Mi-Ra Yoon

Department of Telematics Engineering, Graduate School

Pukyong National University

Abstract

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. 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. Keeping in mind that IETF and ITU-T are standardizing IP/generalized multi-protocol label switching (GMPLS) over dense-wavelength division multiplexing (DWDM) as a solution for the NGOI, DWDM optical network technology will be used as the NGOI backbone and GMPLS 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.

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

I. Introduction

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].

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.

II. Architecture and Functional Procedure of OVPNs

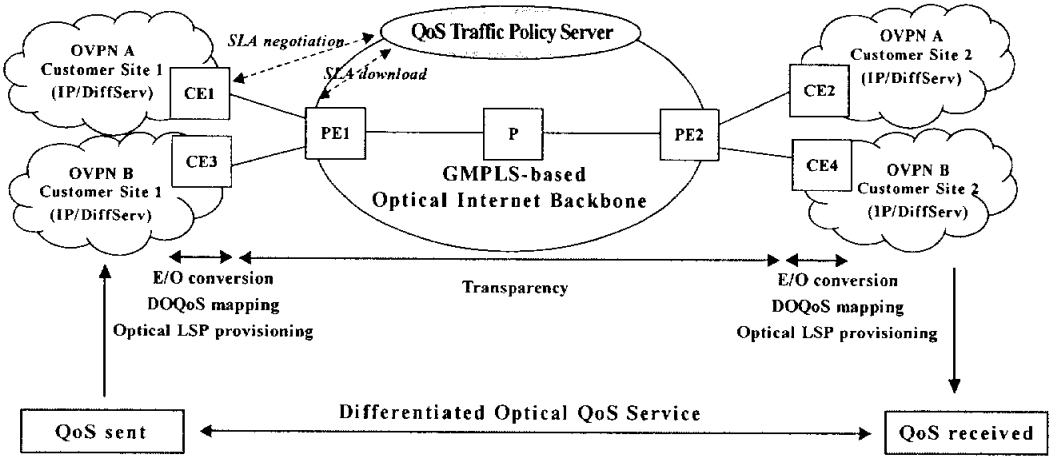


Figure 1. OVPN model for providing DOQoS

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. 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.

Tradition method to guarantee QoS emphasizes control plane and data plane, while neglecting the indispensable management plane. Ref. [7] point out that only by collaboration with these planes can QoS control of IP VPN be effectively relized. This is because that QoS management involves so many interwaved factors distributed in all planes that it is necessary to harmonize control and data plane by management plane. So it is necessary to integrate three planes to provide QoS control. Flexible policy management offer decision-making service to each agent of management plane, for example SLS subscription and invocation need corresponding negotiation policy, traffic engineering needs resource allocation policy, routing and network planning need constraint routing policy. If policy is tightly coded within the management plane, it will be difficult to adjust the policies to meet dynamic request, which is stated in Ref [8]. So we separate policy management from management plane as shown in Figure 2.

Figure 2 depicts the functional block of the OVPN nodes for providing DOQoS.

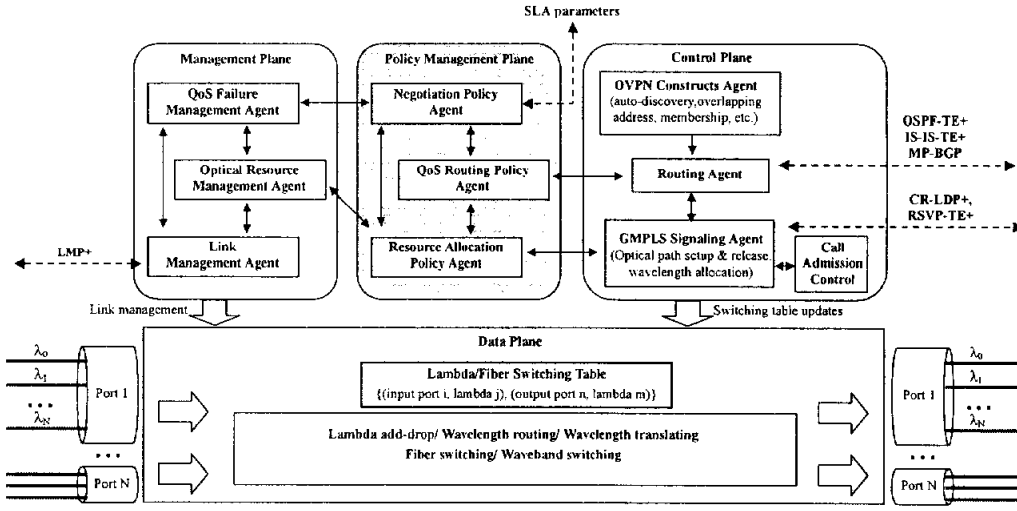


Figure 2. Functional block of the OVPN nodes

- **OVPN Constructs Agent**

  Accomplishment of auto-discovery, overlapping address, membership functions for optical LSP establishment offering OVPN service

- **Routing Agent**

  Calculation of the QoS guaranteed path

- **GMPLS Signaling Agent**

  Reservation of the optical resource (allocation of the label) along the QoS guareented path through GMPLS signaling protocol; The resource reservation protocol with traffic engineering extensions (RSVP-TE+) [9] or the constraint-based routed label distribution protocol with extensions (CR-LDP+) [10]

- **Call Admission Control Agent**

  Examination of the requested bandwidth and specific parameters of the DOQoS class in the signaling message to see whether or not it is possible to establish the O-LSP

- **Negotiation Policy Agent**

  Management of the O-LSP establishment for guaranteeing SLA requirements; The SLA requirements are recived from the QoS-TP server.

- **QoS Routing Policy Agent**

  QoS routing and network planning that are satisfied with the SLA requirements

- **Resouce Allocation Policy Agent**

  Allocation of the network resource and the traffic engineering that are satisfied with the SLA requirements

- **QoS Failure Management Agent**

  Accomplishment of the QoS recovery function, when a failure occurred by the network faults or attacks; 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.

- **Optical Resource Management Agent**

  Management, classification, and reservation of the optical resource in a real time manner

- **Link Management Agent**

  Management and mornitoring of the conrtol and data channel along the optical path through the link management protocol (LMP) [11] and LMP-WDM [12]; LMP runs between neighbor nodes and is used to manage traffic engineering (TE) links. LMP-WDM is extentions to LMP to allow it to be used between a peer node and an adjacent optical line system (OLS).

Each agents of the policy management plane interact with the agents of the control and management planes, and management of the O-LSP establishment for gureenting DOQoS. After O-LSP establishment, data traffic will be forwared through label switching that collated with the Lambda/Fiber Switching Table.

In order to transmit user data transparently through the OVPN optical backbone network, the protocol layer structure should look like that in Figure 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 controlled 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 guarantying end-to-end QoS at the levels of the various DOQoS classes. The functions are performed by the QoS-TP server and the optical resource management agent (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.

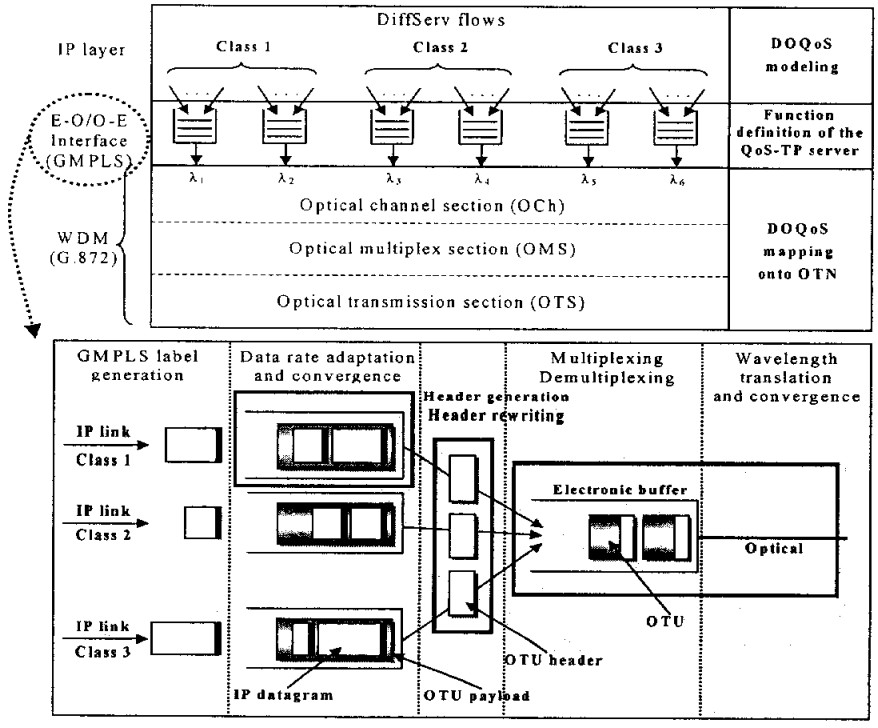


Figure 3. DOQoS mapping of differentiated IP service in CE

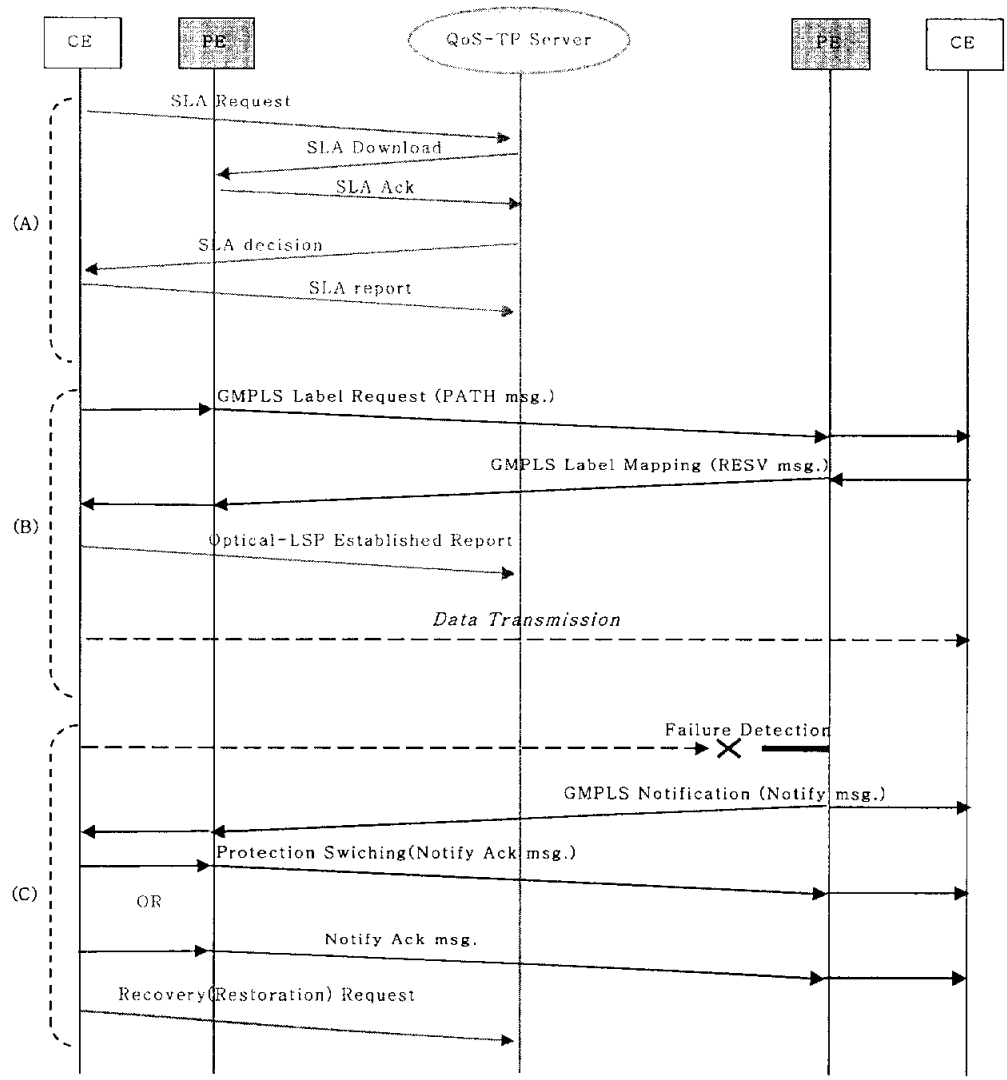


Figure 4. OVPN operation mechanism for providing DOQoS

The entire procedure of establishing an O-LSP and maintaining QoS by providing DOQoS is shown in Figure 4. Phases A and B show the establishing

procedure of the differentiated optical path for 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 RSVP-TE+, or the CR-LDP+ 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 LMP. 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.

III. DOQoS Classes

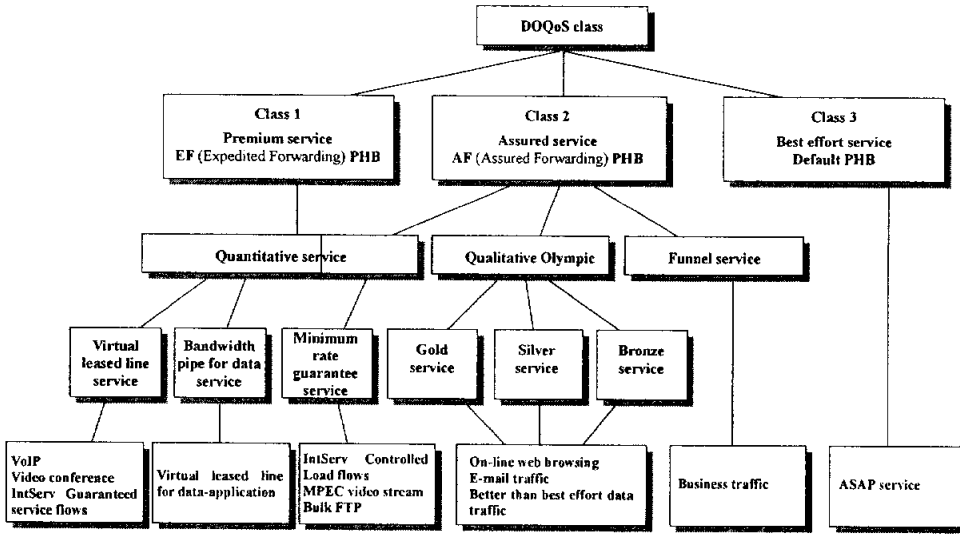


Figure 5. DOQoS specification

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 [13, 14]. Premium service (Class 1) for applications that have strigent 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 requirements, the optical resource allocation scheme and survivability required against network failure or attack shown in Figure 5 [15]. This classification will be applied to the suggested OVPN model for providing DOQoS.

The contents of the VPN SLS [16] 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 [17]. 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.

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 travelling 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 [18]. 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 [19]. 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.

$$BER(Q) \cong (1/\sqrt{2\pi}) \cdot (\exp(-Q^2/2)/Q) \qquad (1)$$

$$el.SNR = 10\log Q^2 \qquad (2)$$

$$OSNR_{0.1nm} = \frac{(1+r)\cdot(1+\sqrt{r})^2}{(1-r)^2} \cdot \frac{Be}{Bd} \cdot Q^2 \qquad (3)$$

r = 0.15 (extinction ratio of the transmitted optical signal)
Be = 0.75 × fo (effective electrical noise bandwidth due to bit rate fo)
Bd = 12.6 GHz or 0.1 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 a attenuation factor of 0.35 dB/km [20]. 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 [21]. 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 re-transmission 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 is suggested as shown in Table 2 [22].

Table 2. DOQoS Classes

Classification criteria	Class 1		Class 2					Class 3
	Premium service: Expedited Forwarding (EF) PHB		Assured service: Assured Forwarding (AF) PHB					Best Effort (BE) service: Default PHB
	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	MBI			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=10E-3), L=0 (R=r)	R=1	R=r	Gold	Silver	Bronze	NA	NA
				Delay or Loss must be indicated qualitatively				
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

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

1. SLA Negotiation Procedure

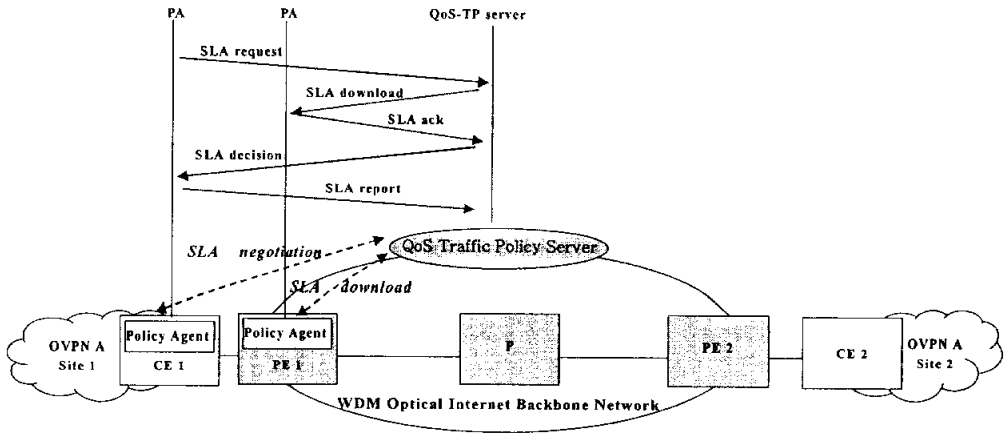


Figure 6. SLA negotiation procedure in an OVPN node

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 Figure 4 (Phase A). Figure 6 depicts the SLA negotiation procedure in the OVPN node.

First, a policy agent of the CE sends a SLA request that specifies the source and destination IP addresses 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 Figure 6) to request a SLA allowance decision, which in turn establishes an O-LSP using RSVP-TE+ signaling.

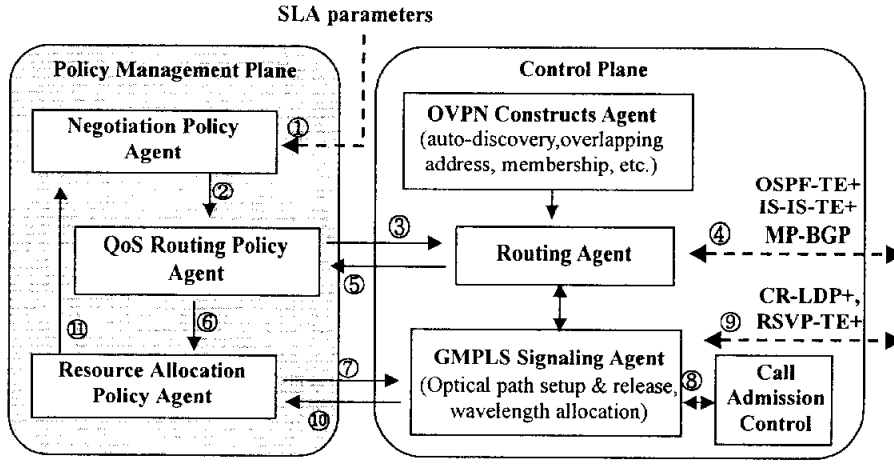


Figure 7. Functional blocks of an OVPN node for the SLA negotiation

When the negotiation policy agent in ingress PE receives a trigger for setting up an O-LSP, it asks the QoS routing policy agent to find the best QoS-guaranteed path (①-② in Figure 7). The QoS routing policy agent asks the routing agent in the control plane which uses OSPF extensions in support of GMPLS (OSPF-TE+) [23] or IS-IS extensions in support of GMPLS (IS-IS-TE+) [24] 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) [25] 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. The routing agent informs the QoS routing policy agent thet the QoS guaranteed path is calculated, and then the QoS routing policy agent asks the resource allocation policy agent to reserve the optical resource along the path. The resource allocation policy agent requests the GMPLS signaling agent to reserve the optical resource along the calculated QoS path with RSVP-TE+. 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 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 TP server gets the result, it informs the policy agent of the CE that the SLA negotiation had been completed. After SLA negotiation between the customer site and the OVPN backbone network, the GMPLS signaling procedure is started along the performance guaranted path.

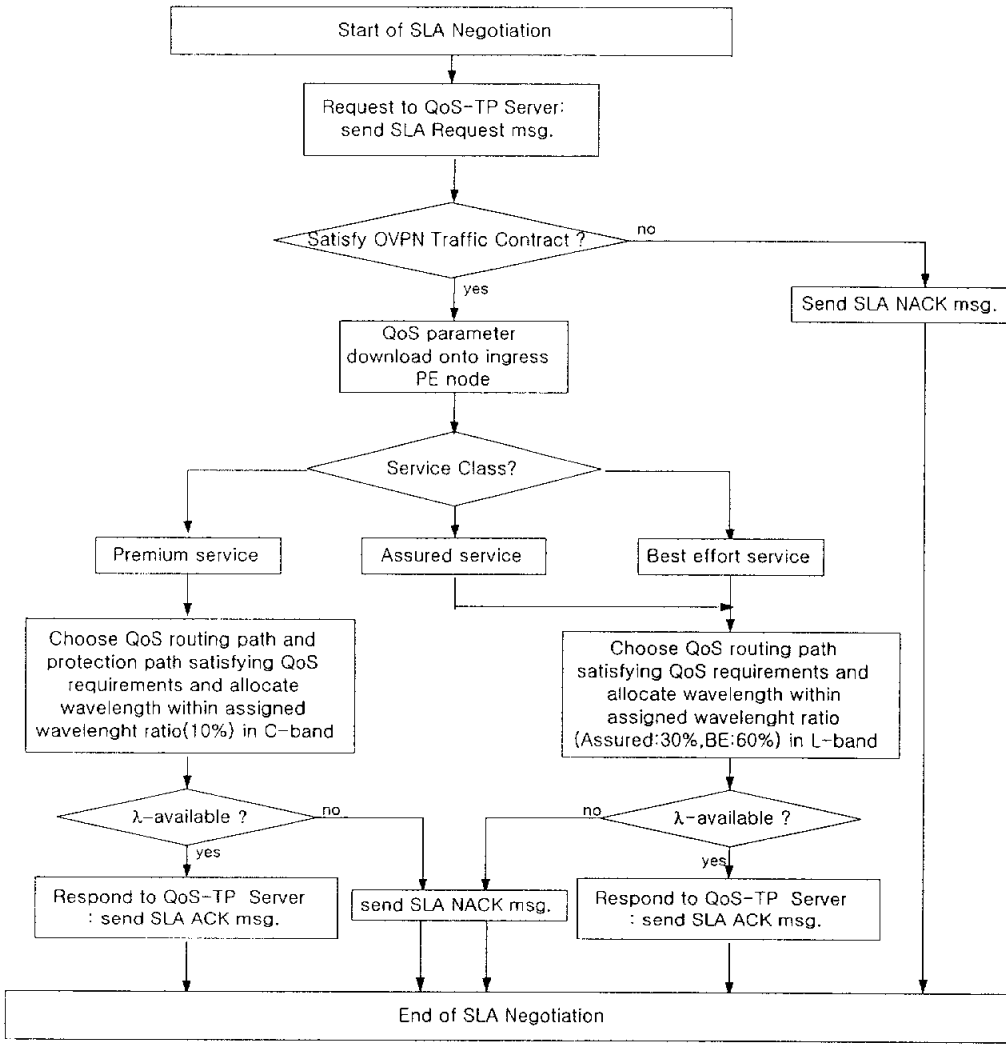


Figure 8. SLA negotiation procedure

Figure 8 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 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.

2. Signalling for Establishing an O-LSP

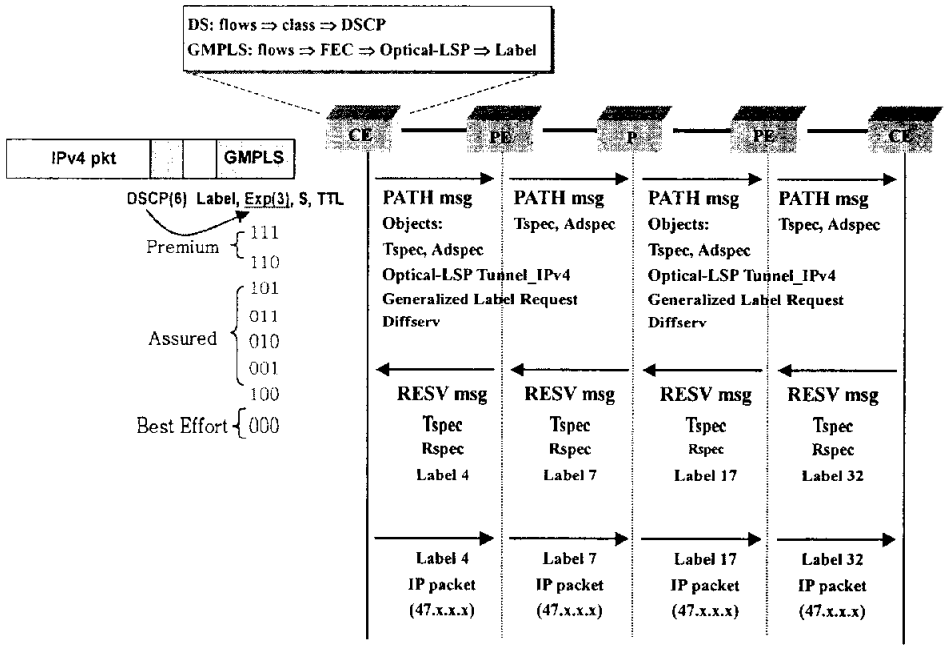


Figure 9. RSVP-TE+ operation mechanism for assuring QoS

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 Figure 9 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. Tspec, Rspec and Adspec Objects

Tspec	p	The maximum rate at which packets can be transmited (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.
	Ctot	The sum of C over a path. (C: Rate-dependent error term, measured in byte)
	Dtot	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.

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 (Ctot, Dtot), 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, Ctot, Dtot, M, r, b and p to equations 4 to 6.

$$Q\,delreq = \frac{(b-M)(p-R)}{R(p-r)} + \frac{M+C_{tot}}{R} + D_{tot} \quad (p > R \geq r) \qquad (4)$$

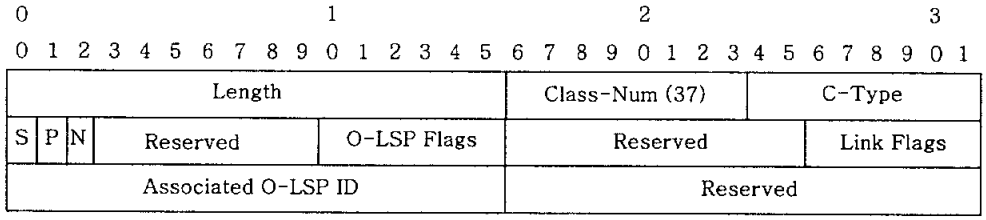
$$Q\,delreq = \frac{M+C_{tot}}{R} + D_{tot} \quad (R \geq p \geq r) \qquad (5)$$

$$Q\,delreq = \frac{b}{R} + \frac{C_{tot}}{R} + D_{tot} \quad (R \leq r) \qquad (6)$$

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.

Figure 10. The format of the Protection Object

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 Figure 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 Figure 8) [26]. 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.

V. QoS Maintenance Mechanism

The OVPN optical backbone network is a DWDM all-optical transport network composed of transparent OXCs. Figure 11 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.

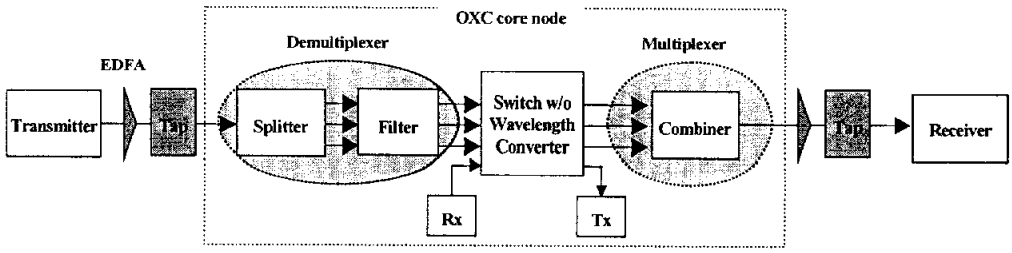


Figure 11. The model of the OVPN optical backbone network

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.

1. Analysis of QoS Failures

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/el.SNR/OSNR Estimation by Q-factor
	By Distortion	Chromatic dispersion Nonlinearities (SPM, XPM, FWM...)		
	By Crosstalk	Interferometic crosstalk		

QoS failures in OVPNs can be considered in three types.

- **Traffic Contract Violation**

  A failure caused by the violation of initial negotiated traffic contract with the OVPN service provider.

- **Service Disruption**

  A service disruption caused by system malfunction as a result of a

sudden fault or intentional attack of active elements in the optical network.

- **Service Degradation**

  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 power-monitoring module (PMM) located in each node (see Figure 12).

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 amplified spontaneous emission (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-electrical signals, requires monitoring at the optical level. The Q-factor [18] obtained from the eye diagram is the method to measure quality of signal without O-E conversion used in this paper.

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) [27].

2.1. Failure Detection

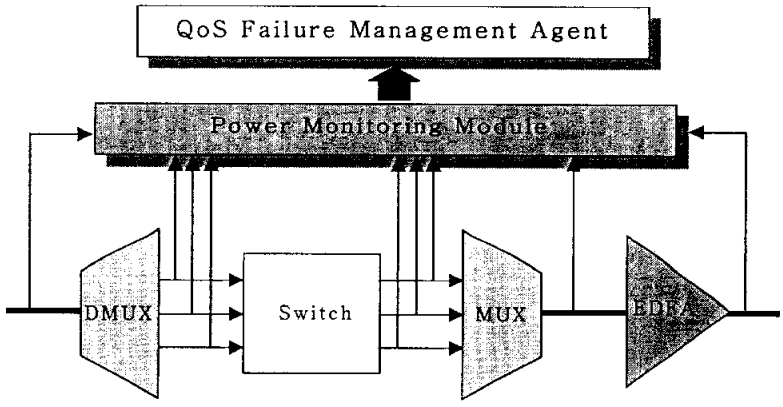


Figure 12. The model of QoS Failure detection

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 Figure 12. 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 QoS failure management agent (QoS-FMA).

The QoS-FMA 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: 10-4~10-7, Best-effort: 10-5).

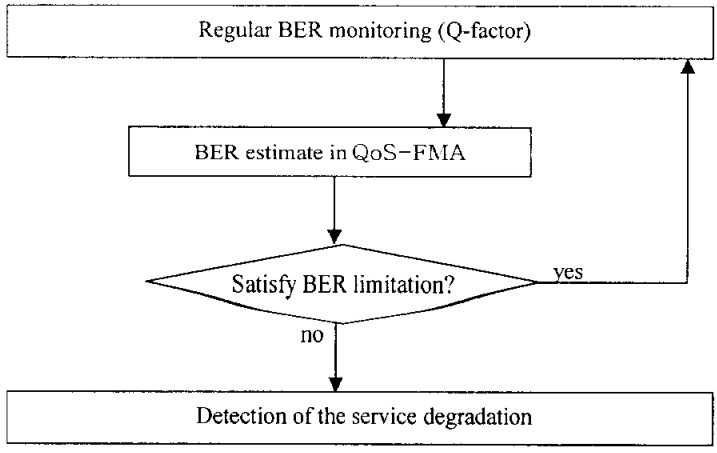


Figure 13. The detection mechanism of service degradation

2.2. Failure Localization

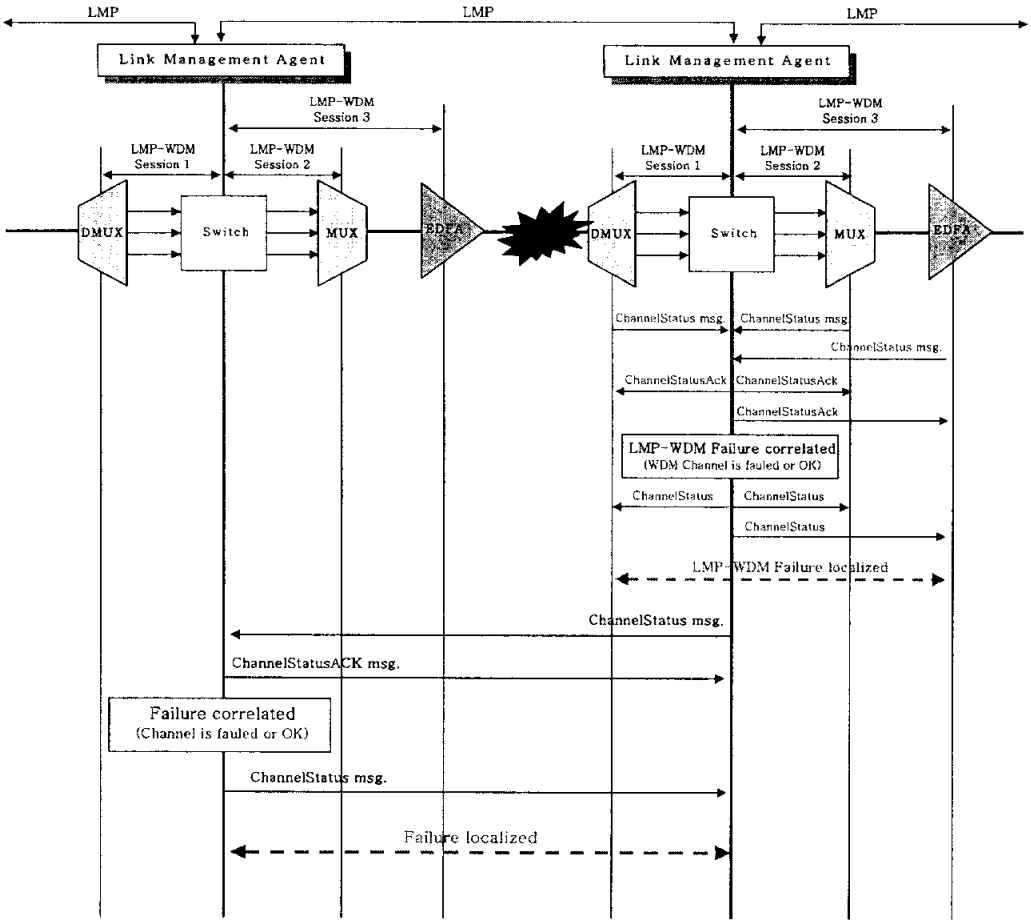
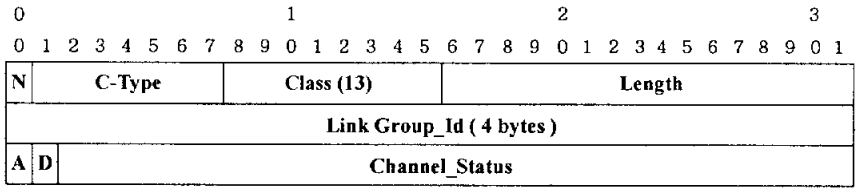


Figure 14. Failure Localization using LMP

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 and LMP-WDM, the link management

protocol of GMPLS as shown in Figure 14. If the failures defined in Table 4 are detected in the QoS-FMA (as shown in Figure 12), the LMP-WDM informs the link management agent (LMA) about the failure using a Channel Status message containing a Channel Status object as defined in Figure 15. The Channel Status object represents the descriptor of the data link group (Link Group_Id field in Figure 15), the status of the data link (Signal Okay, Signal Degrade, Signal Fail), and the direction of the data channel. When the LMA receives the Channel Status message, it sends a Channel Status Ack message back to the OLSs and checks if the O-LSP has another failures. Nextly, it localizes the failure between the node and the OLSs by notifying the OLSs by means of a Channel Status message as shown in Figure 14 (A).

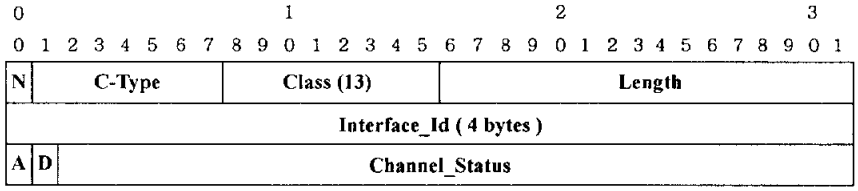


- **Link Group_Id**: The identifier of the data link group.
- **A**: (Active bit) This indicates that the Channel is allocated to user traffic and the data link should be actively monitored.
- **D**: (Direction bit) This indicates the direction (transmit/receive) of the data channel.

Figure 15. The format of the Channel Status Object on the LMP_WDM

And then, a failure between the upstream and downstream node should be localized. Therefore the LMP informs the adjacent upstream node about the failure using a Channel Status message containing a Channel Status object as defined in Figure 16. The Channel Status object represents the descriptor of the data link

(Interface_Id field in Figure 16), the status of the data link, 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. Nextly, it localizes the failure between the two nodes by notifying the downstream node by means of a Channel Status message as shown in Figure 14 (B).



- **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.

Figure 16. The format of the Channel Status Object on the LMP

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 Figure 17 (A). The Notify message informs about the failed working link descriptor and the failure information such as signal degrade, signal fail and so on.

When the ingress CE receives these Notify messages, it informs the egress CE using a Notify Ack message as shown in Figure 17 (B), and it switches to a prepared protection path that is shown in Figure 17 (B).

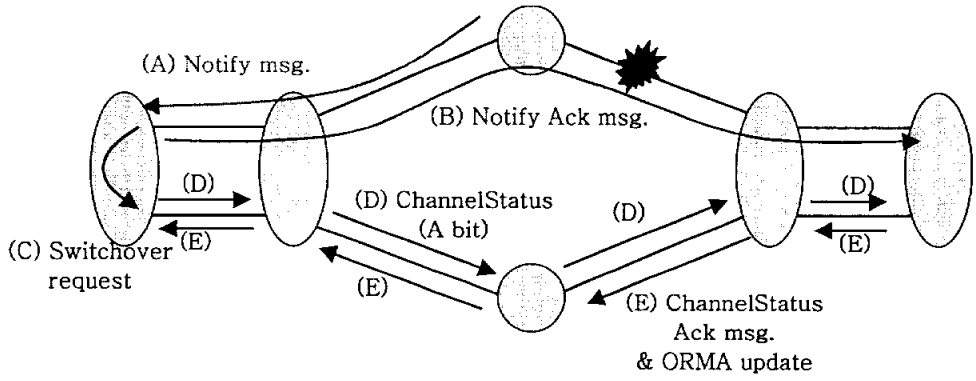


Figure 17. Recovery procedure of Premium Service

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 as shown in Figure 18 (A). Then, the CE replies with a Notify Ack message as shown in Figure 18 (B)) and asks for calculation of a new path satisfying the QoS requirements to the QoS-TP server as shown in Figure 18 (C).

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 replies with the Notify Ack message (the same as in Figure 17 (A) and (C)) and compensates through TCP retransmission.

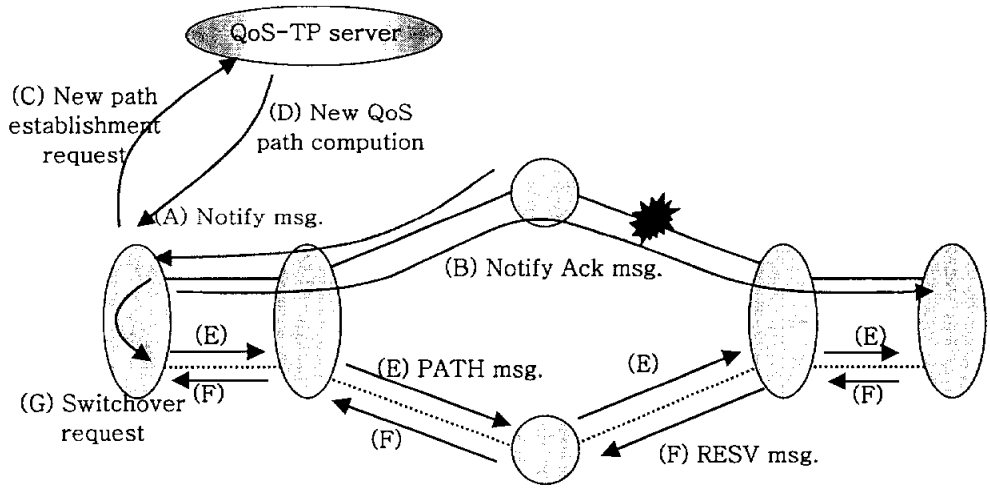


Figure 18. Recovery procedure of Assured Service

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 Figure 17 (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 Figure 17 (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 (the same as in Figure 18 (C)). 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 Figure 9.

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 Figure 18 (C). If the QoS-TP server has calculated a restoration path, then the resources are reserved by the mechanism explained in Section 4 and as shown in Figure 18 (D-F).

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.

VI. 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-TP server and the policy agents 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 between many control protocols (MP-BGP, OSPF-TE+/IS-IS-TE+, RSVP-TE+ /CR-LDP+, LMP) in an OVPN environment that guarantees DOQoS.

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-ccamp7-gmpls-architecture-07.txt, IETF Internet Draft, May 2003.

[5] Jigesh K. Patel, Sung U. Kim and 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, January 2002, pp. 5-18.

[6] Chava Vijaya Saradhi and 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] P. Trimintzios et al.: A management and control archiecture for providing

IP differentiated services in MPLS-based networks, IEEE Communication Magazine, vol. 39, no. 5, May 2001, pp. 80-88.

[8] M. Brunner, J. Quittek: MPLS Management using Policies, Integrated Network Management Proceedings, 2001 IEEE/IFIP international Symposium on, 2001, pp. 515-528

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

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

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

[12] A. Fredette et al.: LMP for DWDM Optical Line Systems, draft-ietf-ccamp-lmp-wdm-02.txt, IETF Internet Draft, March 2003.

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

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

[15] 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.

[16] F. Chiussi et al.: Framework for QoS in Provider-Provisioned VPNs, draft-

chiussi-ppvpn-qos-framework-01.txt, IETF Internet Draft, March 2003.

[17] E. Rosen et al.: MPLS Label Stack Encoding, IETF RFC 3032, January 2001.

[18] 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.

[19] G. Bendelli et al.: Optical performance monitoring techniques, ECOC 2000 (Munich, Germany, September 2000), paper 11.4.1, pp. 113-1168.

[20] Lucent's White Contribution COM 15-39-E: L-and C-Band Attenuation in Installed Fibre Links, ITU-T SG15 Contribution.

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

[22] 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.

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

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

December 2002.

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

[26] 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, February 2003.

[27] 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.

차세대 OVPN 에서 차등화된 광 QoS 서비스 제공 프레임워크 연구

윤 미 라

부경대학교 대학원 정보통신공학과

국 문 요 약

IP 망을 활용한 VPN(Virtual Private Network)은 비용과 운용측면에서 효율적이지만 QoS 보장 메커니즘과 광대역 서비스 제공에 많은 문제점을 가진다. 이러한 IP 기반의 VPN 에서 QoS 보장과 광대역폭 제공에 대한 해결책으로 차세대 광 인터넷을 통한 OVPN(Optical VPN) 기술이 제시되고 있다. 차세대 광 인터넷 백본망 기술은 DWDM(Dense Wavelength Division Multiplexing) 광 네트워크 기술을 활용하고, IP 전달을 위한 제어 프로토콜은 GMPLS(Generalized Multi-Protocol Label Switching) 기술을 사용하는 IP/GMPLS over DWDM 프로토콜 프레임워크로 표준화되고 있는 현실에 비추어, IP/GMPLS over DWDM 백본망을 통한 OVPN(OVPN over IP/GPMLS over DWDM)은 차세대 가상사설망으로써 멀티미디어 서비스 제공을 위한 유일한 대안이다. 차세대 DWDM 광 인터넷 백본망을 활용한 OVPN 에서 종단간 QoS 보장을 요구하는 멀티미디어 서비스 제공을 위해서는 차등화된 광 QoS 서비스(DOQS: Differentiated Optical QoS Service) 제공 메커니즘이 필수적으로 요구된다. 따라서, 본 논문에서는 OVPN over IP/GMPLS over DWDM 에서 종단간 QoS 제공을 위한 DOQS 프로토콜 프레임워크의 핵심 기술인 "차등화된 광 QoS 클래스를 고려한 Optical-LSP(Label Switched Path)의 설립과정 및 QoS 유지방안"을 제안한다.

Acknowledgements

I would like to express my heartfelt thanks to Prof. Kim, Sung-Un. He gives time and effort unsparingly to guidance and his unselfish sharing of ideas made this dissertation possible. Moreover, I am very thankful to Prof. Kim, Seok-Tae, Prof. Joo, Moon-Gab for examining this dissertation along with much good advice. And I appreciate precious advice of Prof. Jo, Jun-Mo and Prof. Lee, Jae-Dong. Of course, I acknowledge several professors in Dept. of Telematics Engineering, Pukyong National University for considerable instructions and encouragement till now. Meanwhile, I thank my big seniors in the protocol engineering laboratory, who gave much advice and help to me during my master's degree course. I would like to acknowledge many seniors: Jae-Yun, Young-Suk, Sung-Su, Jae-Ho, Heung-Sik, eui-Sub, Seong-Kil, Seon-Kyu, Ik-Seob, Mi-Kyoung and Du-Jin who were already graduated, and especially, Hyun-Soo, Ju-Dong, Jung-Hyun who help to me in every respect. I thank Chang-Hyun, Mi-Seon, Kwang-Hyun, Seok-Jin, kyong-Dong, Jin-Ho and Jeong-Mi, too.

Above all, I would like to acknowledge my parents who have devoted themself to supporting me even despite many difficulties, as well as my sisters, Mi-Hwa and Young. I love you with all my heart. I am also thankful to other acquaintances, juniors, seniors and my friends as missed on this paper.