DBpia

Performance Management and Analysis for Guaranteed End-to-End QoS Provisioning on MPLS-based Virtual Private LAN Service(VPLS)

Seong-Woo Kim*, Chul-Kim**, Young-Tak Kim**　Regular Members

ABSTRACT

Internet/Intranet has been continuously enhanced by new emerging IP technologies such as differentiate service(DiffServ), IPSec(IP Security) and MPLS(Multi-protocol Label Switching) traffic engineering. According to the increased demands of various real-time multimedia services, ISP(Internet Service Provider) should provide enhanced end-to-end QoS(quality of service) and security features. Therefore, Internet and Intranet need the management functionality of sophisticated traffic engineering functions.

In this paper, we design and implement the performance management functionality for the guaranteed end-to-end QoS provisioning on MPLS-based VPLS(Virtual Private LAN Service). We propose VPLS OAM(Operation, Administration and Maintenance) for efficient performance management. We focus on a scheme of QoS management and measurement of QoS parameters(such as delay, jitter, loss, etc.) using VPLS OAM functions. The proposed performance management system also supports performance tuning to enhance the provided QoS by re-adjusting the bandwidth of LSPs for VPLS. We present the experimental results of performance monitoring and analysis using a network simulator.

Ⅰ. Introduction

Because of the rapidly increasing needs of real-time multimedia services, the performance management has become an important issue in Internet/Intranet to provide guaranteed end-to-end QoS, to guarantee the user-requested QoS, and to keep the network at the optimal operation status. The performance management functionality continuously monitors and analyzes various parameters related to the network performance, such as QoS, network/operation status, and SLA(Service Level Agreement), from the moment of network deployment.

Recently, IETF(Internet Engineering Task Force) introduced various technologies, such as differentiate service(DiffServ)[1] and IPSec for QoS and security on IP network. A VPN(Vitual Private Network) applying those technologies has been widely studied to provide QoS and security for private IP services. But the performance management functionality for the support of QoS in MPLS[2]-VPLS are not well defined yet.

VPNs are becoming a popular technology for interconnecting CPNs(Customer Premises Networks) and have been recommended as a promising approach to implement enterprise networks covering several branches of a company distributed around world. Currently, those networks are often built with corporate network technology using leased lines in the wide area to interconnect the subnetworks of the company. These leased lines usually guarantee QoS; but the utilization of the fixed-bandwidth leased line is usually very poor without flexibility.

In this paper, we design and implement the management functionality for end-to-end guaranteed QoS on MPLS-based VPLS[1-3] that is also known as TLS(Transparent LAN Service) and VPSN(Vitual Private Switched Network) service. VPLS's basic

* 경북전문대학 멀티미디어정보통신과(ksw@kbc.ac.kr),
**영남대학교 대학원 정보통신공학과 차세대네트워킹 연구실(goldfe@nownuri.net, ytkim@yu.ac.kr)
논문번호 : 030010-0107, 접수일자 : 2003년 1월 7일

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr

framework is taken from L2-VPN(Layer 2 VPN). We discuss the performance management functions such as QoS monitoring and performance analysis in VPLS. In this paper, we focus on the scheme of QoS management with measurement of the QoS parameters(such as delay, jitter, packet loss, etc.) using the designed VPLS OAM functions. We present experimental results of the performance monitoring and analysis using network simulator.

The rest of paper is organized as follows: In section II, we first look briefly at the VPLS. In section III, we describe the consideration points of VPLS performance management and the measurement points for the performance monitoring on VPLS. Also, we propose the VPLS OAM for performance management. In section IV, we deal with the simulation of performance management functionality on VPLS using a network simulator, and in section V we summarize and conclude the paper.

Ⅱ. MPLS-based Virtual Private LAN Service(VPLS)

The virtual private LAN appears in almost all respects as a LAN to the ISP customer. However, in a VPLS, the customers are not all connected to a single LAN; the customers may be spread across a metro or wide area. In essence, a VPLS interconnects several individual LANs across a metro area to appear and function as a single LAN[3,4].

VPLS's basic framework is taken from L2-VPN; the service offered is a L2-VPN. In the case of VPLS, however, the customers in the VPN are connected by a multipoint network, in contrast to the usual L2-VPN which is point-to-point topology in nature.

Fig. 1 depicts the MPLS-based VPLS architecture where an L2PE(Layer 2 Provider Edge) node is used for layer 2 aggregation. The L2PE is owned and operated by ISP. The PE and L2PE devices are "VPLS-aware" which understands the VPLS service being offered.

In contrast, the CE(Customer Edge) is "VPLS-unaware"; as far as the CE is concerned, it is same as to be connected to the other CEs in the VPLS via the layer 2 switched network. This means that there is no need to change the CE device, neither to the hardware nor to the software, in order to offer VPLS. Note that a CE device may be connected to a PE or an L2PE via layer 2 switches that are VPLS-unaware. From the VPLS point of view, such layer 2 switches are invisible. Furthermore, an L2PE may be connected to a PE via layer 2 or layer 3 devices. The PEs are assumed to be full-meshed with tunnels.

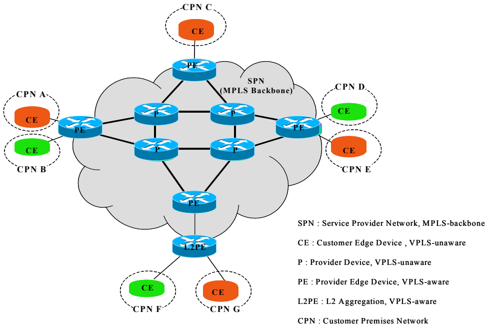

CPN C
CE
PE
SPN
(MPLS Backbone)
CPN A
CE
PE
P
P
PE
CPN D
CE
CE
CPN B
P
P
CE
CPN E
PE
L2PE
CE
CPN F
CE
CPN G
SPN : Service Provider Network, MPLS-backbone
CE : Customer Edge Device , VPLS-unaware
P : Provider Device, VPLS-unaware
PE : Provider Edge Device, VPLS-aware
L2PE : L2 Aggregation, VPLS-aware
CPN : Customer Premises Network

Fig. 1. MPLS-based VPLS

A VPLS offers a mulitpoint layer 2 service over tunnels across a common packet switched network. This requires following functional elements[3]:

- Endpoint discovery: the process by which VPLS-aware devices find all the customers' port that belong to the same VPLS.
- Signaling: Once discovery is done, each pair of PEs in a VPLS must be able to establish LSPs to each other. Signaling is also used to initiate "relearning", and to transmit certain characteristics of the PE regarding a given VPLS.
- MAC(Medium Access Control) address learning: The key distinguishing feature of VPLS is that it is a multipoint service. This means that the entire SPN should appear as a single logical learning bridge for each VPLS that the SPN supports.
- Flooding: When a bridge receives a packet to a destination that is not in its FIB(forwarding Information Base), it floods the packet on all the other ports. Similarly, a VE(VPLS Edge : PE or L2PE) will flood packets to an unknown destination to all other VEs in the VPLS.
- Spanning tree: Learning bridges typically run

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr

STP(Spanning Tree Protocol) to avoid flooding loops. However, running an instance of STP for each VPLS may produce scalability problem. By mandating a full mesh of PE-to-PE tunnels, we obviate the need for STP across the SPN.

As shown in Fig. 1, CE-PE links establish VLAN(or Ethernet) flows, (L2PE)PE-P links establish VC(Virtual Circuit) LSP, and P-P links establish Tunneled-LSP. Fig. 2 depicts the MPLS tunnelling levels in VPLS.

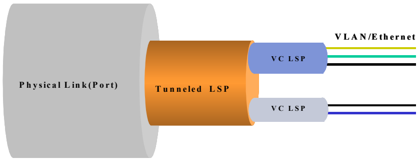


Fig. 2. MPLS tunnelling level

An Ethernet port is used to connect a customer CE to the PE acting as an LER(Label Edge Router). Customer traffic is subsequently mapped to a specific MPLS-based VPLS by configuring L2 FECs(Forwarding Equivalence Classes) based upon the input port ID and/or VLAN index depending upon the VPLS service.

Broadcast and multicast services are available over traditional LANs. MPLS does not support such multicasting services currently. Sites that belong to the same broadcast domain and connected via an MPLS network expect broadcast, multicast and unicast traffic to be forwarded to the proper locations. This requires MAC address learning on a per LSP basis, packet replication across LSPs for multicast/broadcast traffic and for flooding of unknown unicast destination traffic. Internet draft[6] describes a solution to support point-to-multipoint VPLS over MPLS.

Ⅲ. Performance Management of MPLS-based VPLS

3.1 Consideration Points of Performance Management for MPLS-based VPLS

A proper bandwidth management is one of the critical issues in designing a scalable VPLS[4]. Customer broadcast traffic, whether explicit or implicit due to unknown L2 destinations, as well as certain native L2 protocols run by customers, are frequently seen as a problem of the stability of ISP networks. Therefore, a bandwidth management must be able to guarantee an ISP network's stability by the control of all customer L2 traffic.

In order to carry out the performance management, a bandwidth management module measures the following key parameters:

- Total capacity: the total available network capacity
- Services capacity: the total allocated capacity for service offering.
- Actual capacity: the allocated capacity for service offering actually.

Once services have been offered to customers, the ISP's concern is to make sure that the customer traffic, whether intentional or not, does not exceed the allocated share of network capacity. This can be accomplished by dividing all transfers into two mode of operations, and then by proper management of each mode[7]:

- CRTM(Committed Rate Transport Mode) represents an ISP's commitment to a particular service level. All packets falling into the CRTM category will be forwarded according to the advertised characteristics associated with them. The characteristics include delay, bandwidth, jitter, etc. In this mode, all transport parameters have been determined, and all necessary network resources have been allocated and guaranteed for the duration of the service.
- BETM(Best Effort Transport Mode) represents an ISP's unwillingness to commit to any specific characteristics of the service beyond the promise of best effort. Namely, this mode is similar to the traditional IP best effort transport mode. In this mode, the transport parameters are not deterministic and may be changed at any time after the service has been offered.

These two modes can be supported by DiffServ and traffic engineering in MPLS-based VPLS. The requirements of L2 services such as VPLS, specify particular types of connectivity between sites without

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr

mandating uniformity in the traffic parameters. The requirements define the service as LAN-style, many-to-many connectivity between all points, but it does not require the traffic characteristics to be identical between all points in the VPLS. Namely, in the VPLS, the many-to-many connectivity topology will be covered at least by the best effort mode, BETM.

A provider may guarantee certain traffic characteristics on this network through CRTM. For example, it can offer CRTM for traffic from one particular site (i.e. company headquarters) to all others (i.e. company branches). All traffic flows to and from the headquarters are guaranteed, but the traffic flows between the branches are supported in best effort manner.

To support the end-to-end QoS, we need an identification of each VPLS endpoint. For this purpose, this paper uses VCID(Virtual Circuit Identifier) field in the VC FEC(L2FEC) TLV as a customer's VLAN. In other words, SLA is made for customer's VLAN between the provider and a customer. When a VPLS service begins, customer VLAN traffic flow is mapped to proper VC-LSP by the VC FEC according to the negotiated SLA. For this purpose, when configuring VC FEC, we use customer ID and VC ID which are the physical port ID and VLAN ID respectively. Mapping to a proper VC-LSP should be accomplished by DiffServ and/or traffic engineering in ingress PE. In MPLS tunneling levels shown in Fig. 2, a VC label for identification of VC-LSP can not be determined until the packet reaches at the egress PE.

An ISP should provide the end-to-end guaranteed-QoS to its customers with continuous performance measurement to check whether the negotiated SLA is satisfied or not for each VC-LSP. VPLS can provide the QoS and CoS(Class of Service) by two way. Once a L2 frame's priority is decided by 802.1p priority or PE's class, that frame can mark proper CoS or can map to specific QoS LSP. The CoS can be provided by EXP field in MPLS header that decides the queuing characteristics used at all hops through the LSP. We'll use VPLS-OAM for performance management. The VPLS-OAM will be explained in detail in section 3.2.

To carry out the performance management, the QoS management function measures following key parameters:

- delay : end-to-end delay and segment delay at VC-LSP and Tunneled-LSP for packet
- jitter : end-to-end jitter and segment jitter at VC-LSP and Tunneled-LSP for packet
- packet loss : the number of dropped(discarded) packets at each node on the VC-LSP(Tunneled-LSP)
- throughput and utilization : throughput/utilization of the VC-LSP and Tunneled-LSP

3.2 VPLS-OAM

For the provisioning and support of QoS in VPLS, VPLS-OAM functionality is required. In this paper, we extend the MPLS-OAM[8] in order to provide VPLS-OAM functions. We add the Tunneled LSP Identifier and the VC LSP Identifier fields to MPLS-OAM. The VPLS-OAM packet is periodically delivered through the same user data path. But the return path of the VPLS-OAM results is configured through the MPLS control channel by MPLS signaling such as RSVP-TE or CR-LDP. Fig. 3 depicts the VPLS-OAM packet structure for the performance management.

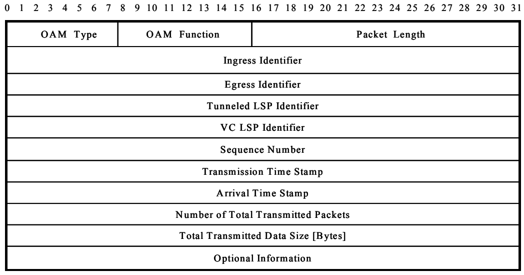


Fig. 3. VPLS-OAM packet structure

The ingress identifier and egress identifier can be specified at both PE and P(LSR). The transmission/arrival time stamp values are the record of the OAM packet transmission time and the arrival time, and are used to calculate the end-to-end/section packet delay from the ingress PE/LSR(P) to the egress PE/LSR(P). The calculated end-to-end/section transmission delay is also used to calculate the jitter.

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr

Fig. 4 shows the point of delay measurement using OAM function.

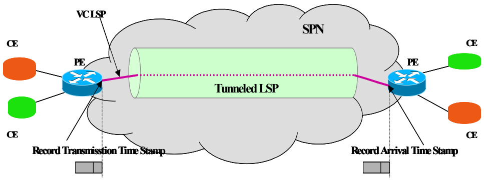


Fig. 4. Point of end-to-end delay measurement using OAM function

The calculations of the end-to-end/section packet transfer delay and jitter is defined as follows:

(i) delay : the interval between the reception time and the transmission time of the packet P(k).

$$d(k) = t_{arrival}(k) - t_{transmission}(k)$$

This delay value is calculated from the arrival time stamp value and the transmission time stamp value.

We can calculate the average end-to-end delay for VC-LSP(i) and the Tunneled-LSP(i) as follows:

$d_{VC\text{-}LSP(i)}$ =

$$\frac{\sum d(k)}{number\ of\ total\ measured\ packets} = \frac{\sum_k [t_{arrival}(k) - t_{transmission}(k)]}{number\ of\ total\ measured\ packets}$$

$d_{Tunneled\text{-}LSP(i)}$=

$$\frac{\sum d_{VC-LSP(i)}}{number\ of\ VC\ LSP\ in\ the\ same\ Tunneled\_LSP}$$

Where the VC-LSP(VC-LSP(i)) belongs to the same Tunneled-LSP.

(ii) jitter : packet delay variation for packet P(k)

$$j(k) = d(k) - d(k-1)$$

We can calculate the average end-to-end jitter for VC-LSP(i) and Tunneled-LSP(i) as the follows:

$j_{VC\text{-}LSP(i)}$ $= \frac{\sum_{k=2}^{n} j(k)}{n-1} = \frac{\sum_{k=2}^{n}[d(k) - d(k-1)]}{n-1}$, n = the number of VC-LSPs in the same Tunneled-LSP(i)

$j_{Tunneled\text{-}LSP(i)}$ =

$$\frac{\sum j_{VC\_LSP(i)}}{number\ of\ VC\_LSP\ in\ the\ same\ Tunneled\_LSP}$$

The delay and jitter need the time synchronization for precisional measurement. Therefore we get the time synchronization of the delay and jitter using the VGC(Virtual Global Clock)[9]

In order to monitor the packet loss, the performance measurement OAM also contains the total transmitted packet count and the amount of data after the transmission of the previous performance measurement OAM packet. With these data, the egress PE can calculate the transferred data size for the interval(e.g. 1 second) and the packet loss in the interval.

VC-LSP Packet loss($L_{VC\text{-}LSP}$) is calculated from the number of total transmitted packets(P_{total}) and the number of arrived packets($P_{arrived}$) through the egress PE during the interval.

Packet Loss Ratio(VC-LSP) =

$$\frac{L_{VC\_LSP}}{number\ of\ total\ transmitted\ packets} = \frac{P_{total} - P_{delivered}}{P_{total}}$$

The packet loss and packet loss ratio for the same Tunneled-LSP can be calculated as the following:

Packet Loss Ratio(Tunneled-LSP) =

$$\frac{\sum_k L_{VC\_LSP_k}}{\sum_j number\ of\ total\ transmitted\ packets\ in\ the\ Tunneled\_LSP_j}$$

For the actually used bandwidth(actual throughput), the egress PE counts the total delivered data size through the allocated VC-LSP for each interval(1 second).

actual throughput(actualBW) = $\frac{total\ delivered\ data\ size[bytes]}{interval(1\ [\mathrm{sec}])}$

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr

This value is same as the throughput value of a VC-LSP.

We can calculate the actual throughput of Tunneled-LSP by following equation:

$$\mathrm{ActualBW}_{Tunneled\text{-}LSP(i)} = \sum_{i=1}^{n} ActualBW_{VC\_LSP(i)}$$

The VC-LSP utilization can calculate the VC-LSP throughput for allocated bandwidth(services capacity) of VC-LSP.

$$\mathrm{Utilization}_{VC\text{-}LSP} = \frac{VC\_LSP_{throughput}}{BW_{services}\ \ of\ \ VC\_LSP}$$

With this result, we can be calculated from the utilization of Tunneled-LSP as follows:

$$\mathrm{Utilization}_{Tunneled\text{-}LSP} = \frac{\sum_{i=1}^{n} VC\_LSP(i)_{throughput}}{BW_{services}\ \ of\ \ Tunneled\_LSP}$$

The VPLS OAM function for each section(except PE-PE) is optionally executed by the request from the EMS/NMS that specifies section with degraded performance on VC/Tunneled LSP.

These measured performance values are compared to the agreed QoS parameters that have been specified in the SLA. If a severe performance degradation below the predefined threshold is measured, the LSP is evaluated as a “severely degraded LSP” and the egress PE sends the performance degradation notification message to the ingress PE that performs the fault restoration procedure for the erred LSP.

The proposed VPLS-OAM provides performance measurement, connectivity verification, and fault detection for the segments between PE-PE, PE-P, P-PE and P-P as shown in Fig. 5.

To carry out the performance measurement for each section, we measure the PE-P/P-PE link, P-P link, PE-PE link, and intermediate P-P link on VC-LSP/Tunneled-LSP using VPLS OAM. With these results, we can find which section is most degraded in performance o n a VC-LSP/Tunneled-LSP.

For the VPLS-OAM functions, we assume that each node(PE, P) has TE-agent(traffic engineering agent) which handles the performance measuring of VC-LSP/Tunneled-LSP, fault notification and other traffic engineering tasks. Also, the TE-agent communicates with SPN EMS/NMS.

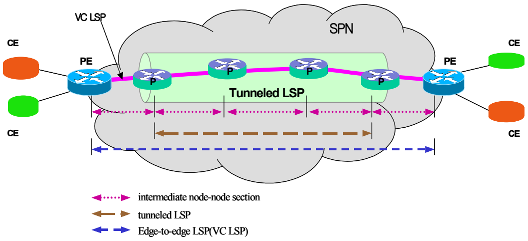


Fig. 5. Operation of VPLS OAM functions for each section

3.3 Measurement Points for Performance Management on MPLS-based VPLS

A good guideline is to drop excess traffic as soon as the metering module determines that the packet exceeds the committed rate. Typically three logical measurement points are defined in the network[10]:

- provider ingress
- tunnel ingress
- provider egress

Customer traffic is first checked at the entry to the provider’s network. Soon after that, it is evaluated again after the tunnel to the destination PE has been determined. If the packet is following a CRTM transport mode, it is evaluated against committed traffic parameters, and it could be dropped if it exceeds the threshold. If the packet travels along a BETM transport mode, it is still evaluated and possibly dropped with the difference that the criteria are totally at the discretion of the provider. After the packet reaches the destination PE, it is evaluated for the last time before it is delivered to the customer CE. Unlike the previous measurement points, this one does not play any vital role in protecting the stability of the provider’s network, rather, it enforces the terms of the agreement with the customer. Of course, in CRTM, each ingress PE node must determine the tunneled-LSP to let the packet to be forwarded to the destination PE. The VPLS should offer proper means

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr

to support CRTM and/or BETM according to the service configuration.

To carry out the performance management proposed in this paper, we consider following measurement points:

- customer sites(inner CE area) : using Intranet performance management
- CE-PE section : measurement for VLAN/Ethernet traffic flows
- VC-LSP(PE-PE section) : measurement for VC-LSP ingress and egress
- Tunneled-LSP(P-P section) : measurement for Tunneled-LSP ingress and egress
- intermediate node-to-node section : measurement for intermediate node-to-node on VC-LSP/Tunneled-LSP
- each node in SPN : measurement for status and throughput/utilization of PE, P devices
- CE-CE section : measurement for end-to-end QoS

Customer sites can be managed by various Intranet management system. In this paper, we used DPE-based performance management system[11]. In CE-PE section, we can periodically measure the performance parameters such as packet loss, throughput, utilization, bandwidth and connectivity for CE-PE(Ethernet/ VLAN) traffic flows. The Intranet EMS/NMS reports the measured results to ISP NMS(EMS) periodically. If measured values do not satisfy the already negotiated SLA between the customer and ISP, the Intranet EMS/NMS notify these results to ISP immediately. Fig. 6 depicts the interoperation between ISP NMS/EMS and Intranet NMS/EMS.

In PE-PE section(that includes PE-P section), we can measure the previously negotiated SLA between the customer and ISP for VC-LSP(ingress/egress PE). It periodically measures the performance parameters such as delay, jitter, packet loss, bandwidth and connectivity, using VPLS-OAM.

In P-P section, we measure the previously determined QoS grade for Tunneled-LSP between penultimate LSR(P)s. In CE-CE section, we periodically measure the performance parameters such as delay, jitter, packet loss, bandwidth, throughput, utilization and connectivity, using Intranet management functions only[11]. The end-to-end delay is measured over layer 3 since the CE-PE link is constructed by VLAN/Ethernet traffic flows. We separate the network performance parameters between L2 and L3. We focus on the measurement of QoS parameters for the end-to-end/section in SPN based on the above mentioned measurement points and VPLS OAM.

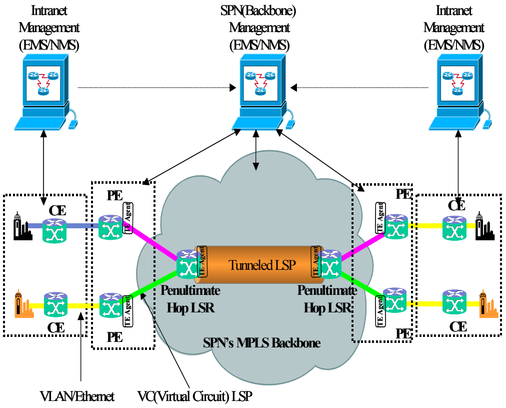


Fig. 6. Interoperation between Intranet EMS/NMS and SPN EMS/NMS

3.4 Example SLA for MPLS-based VPLS

The SLA is established between the customer and the provider. In a multi-provider secnario a provider needs to access the management of peer providers, where one provider plays the role of a customer. This can be expressed by setting up an SLA between providers. The SLA parameters(such as network latency, network packet delivery, nework availability, and service quality) should be mapped to the network performance parameters(such as delay, jitter, loss, and thoughput/utillization). The performance management system measures the network performance parameters and the measurement data compresses into nework status and usage information at the network layer. Subsequently, these measurement data are compared to pre-negotiated SLA values. If this result does not satisfy the range of pre-negotiated SLA values, then proposed system starts performance tuning action with closed-loop control. The range of pre-negotiated SLA

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr

values may represent the criteria of severly degraded network performance. The performance tuning using closed-loop control is explained in the next section. Table 1 shows an example of SLA for United States IP VPN Dedicated Access in WordCom[12].

Table 1. Example of Service Level Agreement

ISP	Guarantee Items	Guarantee Target	Guarantee Remedy
MCI WorldCom	Access Latency	average round trip transmission of 120 milliseconds or less between Customer premise routers for an IP VPN with all of its sites in North America	compensate five days charge
	Access Availability	the dedicated access portion of the IP VPN Total Access Service available 99.9% of the time, for Customers with ten or more IP VPN Total Access dedicated sites and 99.8% of the time, for Customers with three to nine IP VPN Total Access dedicated sites	compensate five days charge

The SLA also contains the boundary of the valid VPLS area. Referring to Fig. 1 where CPN networks A to G might belong to the same organization and be located at different remote locations, and any site may want to establish a connectin with another under the same contract. Therefore, this boundary defines the perimeter of the VPLS area and is stored in the SLA database of SPN EMS/NMS as source and destination addresses. The user authentication process prohibits malicious users from setting up unauthorized tunnel and access network resources illegally. The SLA, however, allows users to add new VPLS areas to their current contracted list of valid VPLS areas.

The SLA for MPLS-based VPLS, proposed in this paper contains following tuple:

- User Id
- Password
- Maximum BW in Mbps
- Kind of Service
- Source Address and Destination Address

The first two parameters(User Id and Password) specify the user's identification. The rest of parameters specify the maximum amount and type of traffic that the user can send and/or receive through a VC-LSP/Tunneled-LSP. These parameters are stored in SLA database.

Ⅳ. Simulation

4.1 Network Simulation Configuration

For the evaluation of the proposed VPLS OAM functions, we used the NIST GMPLS network simulator, GLASS[13]. The network simulation topology of the MPLS-based VPLS is as shown in Fig. 7. There are three customers distributed on three remote areas. CE 1 and CE 2 of customer A are connected by a VC-LSP with label 500 that is tunneled by Tunneled-LSP with label 7. CE 1 and CE 2 of customer B connected by a VC-LSP with label 300 that is tunneled by Tunneled-LSPs with label 5. CE 1 and CE 2 of customer C are connected by a VC-LSP with label 100 that is tunneled by Tunneled-LSP 1. The traffic flows between CEs and PEs are VLAN traffic flows. We assume that the LSP is bi-directional, and the return path for VPLS OAM packet flow is maintained.

The transit network is configured with full-mesh topology. Each PE establishes VC-LSP for each customer pair with traffic parameters individually. The physical links have been programmed to have the link specifications as shown in Table 2. The traffic generation conditions are as shown in Table 3. The average traffic rate at CE1-CE2 of customer A is 1.7 Mbps. CE1-CE2 of customer B has the packet stream of average rate 2.7 Mbps. CE1-CE2 of customer C has the packet stream of average rate 1.3 Mbps. The Internet traffic generation has the properties of random exponential distribution in the packet interval and the packet size has normal distribution to make

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr

the simulation more realistic.

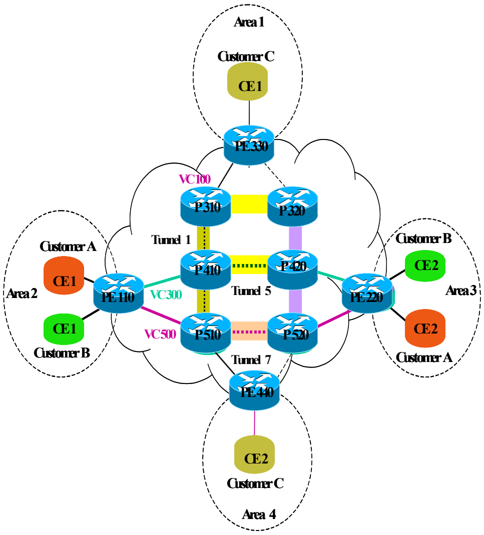


Fig. 7. Network Simulation Topology

Table 2. Transmission Link Specifications in the Simulation

Physical Link		Bandwidth	Propagation Delay
Customer A	CE1-PE110 CE2-PE220	4 Mbps	5 ms
Customer B	CE1-PE110 CE2-PE220	6 Mbps	3 ms
Customer C	CE1-PE330 CE2-PE440	3 Mbps	5 ms
Core	PE110-P410 PE220-P420 P510-P520	10 Mbps	10 ms
Core	P320-P420 P410-P420	12 Mbps	5 ms
Core	P310-P410 P410-P510 P420-P520	8 Mbps	15 ms
Core	PE330-P310 PE330-P320 PE110-P510 PE220-P520 PE440-P510 PE440-P520	6 Mbps	10 ms

In the experimental simulation, we use WFQ(Weighted Fair Queuing) MPLS LSP packet schedulers at each P. The packet generation at each CE has been programmed to have different duration, so as to vary the network link utilization along the simulation.

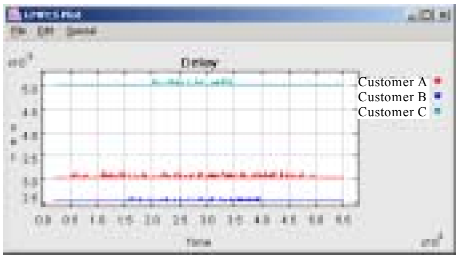
Table 3. Traffic Generation in Simulation

Src-Dest (VC-LSP Label)		Traffic Type	Traffic Parameter [Mbps]	Packet Schedu-ling at P(LSR)	Routing	Traffic Genera-tion Period [sec]
Customer A	CE 1 - CE 2	CBR	PDR:2 CDR:1.5	WFQ	Explicit routing	50 - 500
Customer B	CE 1 - CE 2	CBR	PDR:3 CDR:2	WFQ	Explicit routing	150 - 400
Customer C	CE 1 - CE 2	CBR	PDR:1.5 CDR:1	WFQ	Explicit routing	200 - 350

4.2 Performance Measurement and Analysis

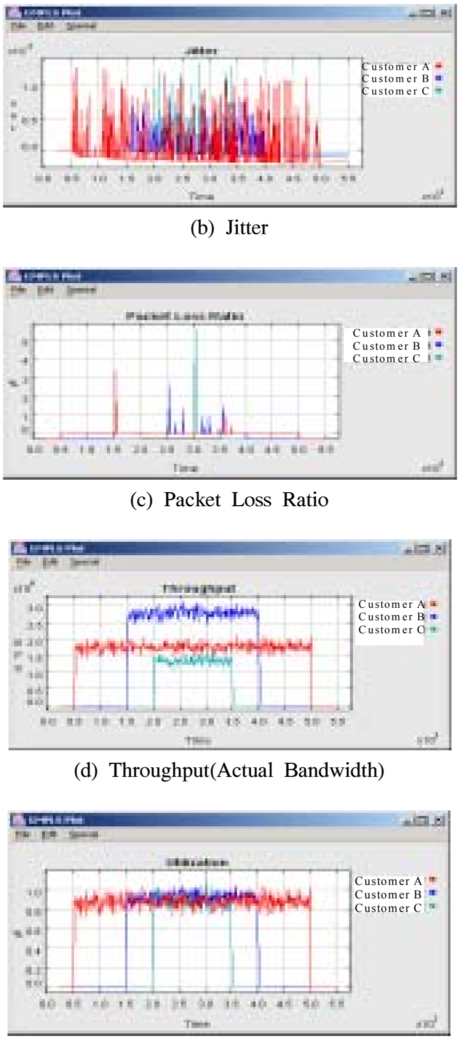
By using the VPLS OAM, we can measure actual throughput and utilization through the VC-LSP/Tunneled-LSP, end-to-end delay from the ingress PE to the egress PE, jitter, and packet loss. Each performance parameter is calculated by the equations in section 3.2. The performance measurement is executed at each egress PE.

For the performance monitoring of LSP, the OAM packets are generated by the ingress PE at every 1 second(default interval), and transferred through the user data LSP to the egress PE. At the egress PE, the performance of the VC-LSP is analyzed by calculating the performance parameters, such as the actual throughput, packet data size, the PE-to-PE packet transfer delay, the amount of jitter, and the amount of packet loss(ratio). Fig. 8 shows the results of performance measurement for each customer.



(a) End-to-End Packet Delay

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr



(b) Jitter

(c) Packet Loss Ratio

(d) Throughput(Actual Bandwidth)

(e) Utilization

Fig. 8 Performance Measurement Results using VPLS-OAM Functions

Fig. 8 shows the results of performance measurement using VPLS OAM function at normal status in each customer. In Fig. 8(c), we can see the performance degradation of packet loss ratio(172.09 second for customer A, 254.07 second for customer B, 300.15 second for customer C). The performance degradation is detected at the egress PE that does not notify this result to ingress PE, because the increased packet loss ratio is occurred by temporary congestion and the values are under the pre-defined threshold as shown in Table 4.

4.3 Performance Tuning

Table 4 shows an example of the criteria of severely degraded LSP performance. In this paper, we checked the performance degradation of the available bandwidth, excessive end-to-end delay and jitter, and excessive packet loss ratio, degraded throughput and utilization. According to the characteristics of the user's application service, the criteria of service degradation of LSP performance can be defined differently. For example, the real-time multimedia communication service will require strict end-to-end transfer delay and jitter limitation while allowing moderate packet loss ratio. The bank transfer applications, on the other hand, will require strict packet loss limit and bandwidth while allow moderate end-to-end transfer delay and jitter.

Table 4. Criteria of severely degraded performance (example)

Traffic/QoS parameter	Threshold of severe degradation
End-to-end delay	More than 120% of agreed end-to-end delay limit
jitter	More than 200% of agreed jitter limit
packet loss	More than 20 % of transmitted data
available bandwidth	Less than 80% of CDR

Fig. 10 shows the detection of the performance degradation at the egress PE and the notification to the ingress PE for each customer. The egress PE detects the performance degradation according to the criteria shown in Table 4.

OAM Degradation Report
LSP ID : 500
Ingress LER : 220
Egress LER : 110
Detection Time : 253.0903
Packet Loss Warning : 20.19579395
Node(220) Module(pmProc)

Fig. 10. Detection and Notification of Performance Degradation.

To maintain the predefined network performance, the performance management needs the closed-loop control that is supported by traffic engineering. The closed-loop control has three major functions: short-term optimization, mid-term optimization and long-term optimization. The short-term optimization is real-time per-flow optimization that sets router

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr

parameters such as bandwidth allocation, queuing and packet scheduling. The mid-term optimization executes the operations such as the re-configuration of logical topology(traffic trunk). The long-term optimization performs the operation such as the network planning and facility provisioning. Fig. 11 depicts the closed-loop control for performance management. In Fig. 11, the performance management functionality monitors each node performance. From these monitored performance information, the performance management functionality analyzes each node performance and network performance. By these results, the NMS/EMS(TE Agent) catches the end-to-end performance level and executes the proper closed-loop control.

By the result of Fig. 10, Fig. 12 shows the results of closed-loop control for performance degradation in customer A(PE110-PE220, VC500). In Fig. 12(a), the packet loss ratio for the customer A is severly increased at the 253 seconds. The reason of this severly increased packet loss ratio is a congestion on the link between CE1 and CE2 in customer A. Therefore the egress LER(PE220) notifies the performance degradation to ingress LER(PE110). By notification from PE220, the TE-agent in PE110 executes the performance tuning that is bandwidth re-distribution as short-term closed-loop control by using following rule.

```
if(threshold-crossing for packet loss on LSPi)
  if(allocated bandwidth+20% > available bandwidth
      threshold)
  then
        notify_to_NML_or_operator();
  else
        modify_link_capacity(LSPi, allocated
                                    bandwidth + 20%);
```

In Fig. 12(a) and (b), we knows that the packet loss ratio and utilization are remarkably decreased by the bandwidth re-distribution. The TE-agent also communicates with the NMS/EML of SPN to exchange the management messages for performance tuning.

By these simulation results, we can see the VPLS OAM function monitors correctly the degraded performance. For connectivity test, we check a specified timeout period(e.g 3 × target end-to-end transfer delay) at the egress PE for any user data packet and the periodic performance measurement OAM packet.

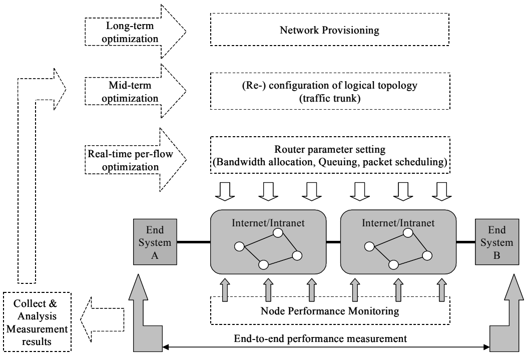
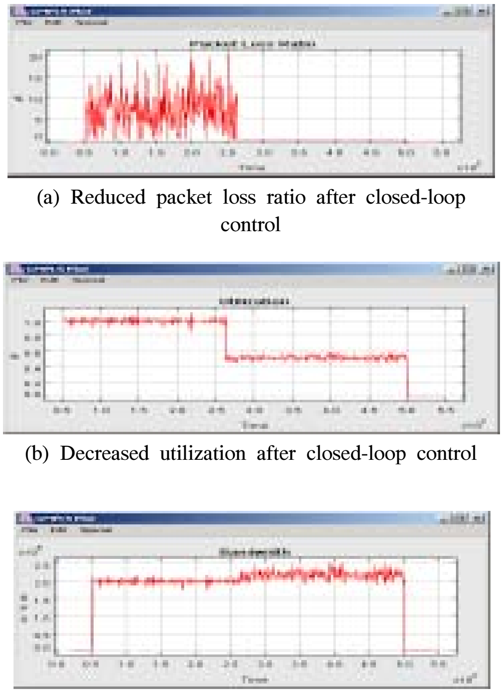

Long-term optimization
Network Provisioning
Mid-term optimization
(Re-) configuration of logical topology (traffic trunk)
Real-time per-flow optimization
Router parameter setting (Bandwidth allocation, Queuing, packet scheduling)
End System A
Internet/Intranet
Internet/Intranet
End System B
Collect & Analysis Measurement results
Node Performance Monitoring
End-to-end performance measurement

Fig. 11. The Closed-loop Control in performance management.



(a) Reduced packet loss ratio after closed-loop control

(b) Decreased utilization after closed-loop control

(b) execution of the closed-loop control(bandwidth re-distribution) for performance degradation(packet loss ratio)

Fig. 12. Results of Closed-loop Control for Performance Degradation in Customer A

Ⅴ. Conclusion

In this paper, we proposed a performance

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr

management scheme of MPLS-based VPLS using VPLS OAM functions. And we analyzed the consideration issues and measurement points of the performance management for MPLS-based VPLS. The proposed VPLS OAM functions provide the end-to-end QoS monitoring and its analysis.

The detail procedure of the periodic performance monitoring and the detection of severe performance degradation were designed and implemented. By this VPLS OAM function, the provisioning of guaranteed QoS can be continuously monitored and analyzed.

We simulated the VPLS OAM functions using NIST GMPLS Network Simulator-GLASS. The simulation results showed the correct operation of OAM functions for performance monitoring, detection of performance degradation and notification. We could confirm that the proposed VPLS OAM functions can be efficiently applied to MPLS-based VPLS performance management. We expect the proposed VPLS OAM functions to be applied to enhance the performance of MPLS-based VPLS.

References

[1] IETF RFC2475, “An Architecture for Differentiated Services,” Dec. 1998.

[2] IETF RFC3031, “Multiprotocol Label Switching Architecture,” Jan. 2001.

[3] IETF draft, Virtual Private LAN Service, “draft-kompella-ppvpn-vpls-00.txt,” Nov. 2001.

[4] IETF Draft, Architecture and Model for VPLS, “draft-augustyn-vpls-arch-00.txt,” Nov. 2001.

[5] IETF Draft, Decoupled Virtual Private LAN Servce, “draft-kompella-ppvpn-dtls-01.txt,” Nov. 2001.

[6] IETF Draft, Virtual Private LAN Service over MPLS, “draft-lasserre-vkompella-ppvpn-vpls- 02.txt,” June 2002.

[7] IETF Draft, Bandwidth Management in VPLS Network, "draft-augustyn-vpls-bw-00.txt," Nov. 2001.

[8] Young-Tak Kim, Eun-Hyuk Lim, Byung-Jae Kim, Yong-Gi Lee, “A Design and Implementation of the MPLS OAM Functions for Performance Monitoring, Fault Detection and Localization,” KT Journal, 2002.

[9] 신동진, 김영탁, “인터넷 환경에서의 VGC/Loopback을 이용한 멀티미디어 통신의 동기화 기법 연구”, 한국통신학회논문지, 2001. 7

[10] IETF Draft, Extensions of for QoS Support in Transparent VLAN Services over MPLS, “draft-lau-ppvpn-qos-tls-mpls-00.txt,” Mar. 2002.

[11] Seong-Woo Kim, Chul-Kim, Jae-Kwang Shin, Young-Tak Kim, “Performance Measurement and Analysis of Intranet using DPE-based Performance Management System,” KICS pp282-2-4, Vol. 27 No.4C, Apr. 2002.

[12] WorldCom, “http://www.worldcom.com/us/ legal /sla/ servicessupported /vpn.xml”.

[13] NIST GMPLS Lightpath Agile Switching Simulator, “http://dns.antd.nist.gov/glass/,” Dec. 2002.

김 성 우(Seong-Woo Kim) 정회원

1997년 2월 : 경일대학교 전자공학과 졸업

1999년 2월 : 영남대학교 대학원 멀티미디어통신공학과 졸업(공학석사)

2003년 2월 : 영남대학교 대학원 정보통신공학과 졸업(공학박사)

2001. 3 ~ 현재 : 경북전문대학 멀티미디어정보통신과 전임강사

<관심분야> TINA, SNMP, TMN, NGI, ATM/B-ISDN, MPLS, VPN

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr

김 철(Chul Kim) 정회원

1998년 2월 : 영남대학교 전기전자공학부 졸업

2000년 2월 : 영남대학교 대학원 정보통신공학과 졸업 (공학석사)

2001년 3월~현재 : 영남대학교 대학원 정보통신공학과 박사과정재학

<관심분야> NGI, ATM/B-ISDN, MPLS, Traffic Engineering

김 영 탁(Young-Tak Kim) 정회원

1984년 2월 : 영남대학교 전자공학과 졸업

1986년 2월 : KAIST 전기 및 전자공학과 졸업 (공학석사)

1990년 2월 : KAIST 전기 및 전자공학과 졸업 (공학박사)

1990년 3월~1994년 8월 : 한국통신 통신망연구소 전송망구조연구실 선임연구원

1994년 9월~현재 : 영남대학교 공과대학 정보통신공학과 부교수

2001년 2월~2002년 1월 : NIST Guest Researcher

<관심분야> Broadband networking, ATM/B-ISDN, MPLS

Copyright (C) 2003 NuriMedia Co., Ltd.
www.dbpia.co.kr