Service Management Architecture for MPLS VPN Service Provisioning with High-speed Access Network

Chan Kyu Park, Daniel W. Hong , Dongsik Yun
Network Technology Lab., Korea Telecom
463-1 Jeonmin-dong Yusung-gu, Daejeon 305-811 Korea
{pck, wkhong,dsyun}@kt.co.kr,

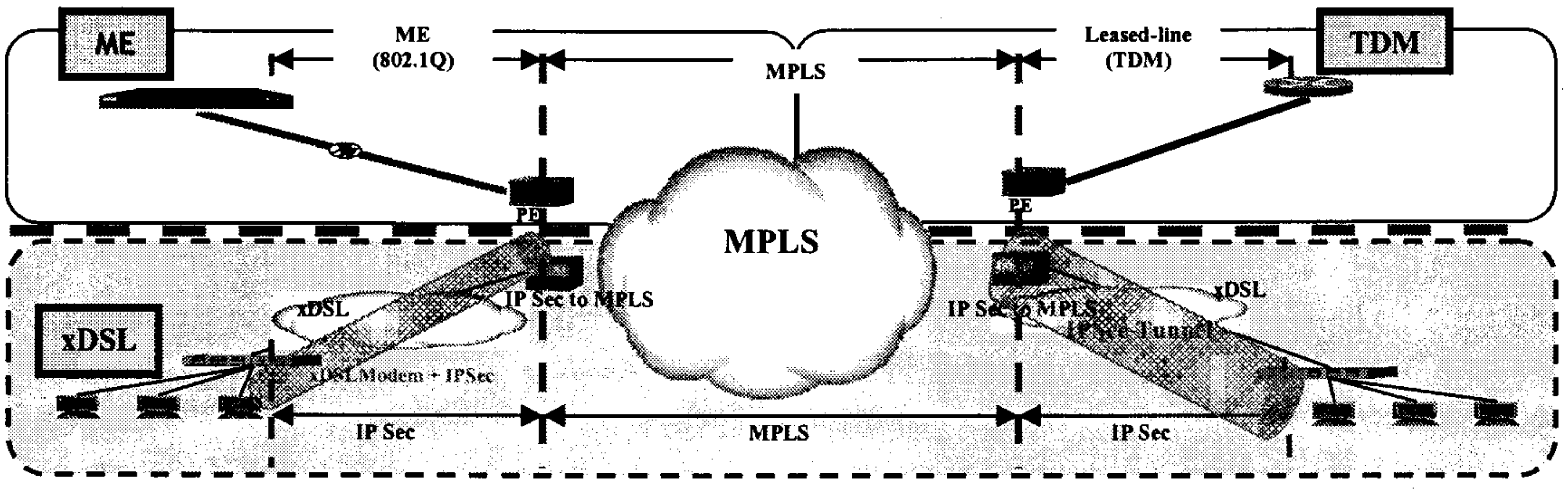
ABSTRACT

To compensate the loss of leased-line subscribers and the excessive increase of residential xDSL (Digital Subscriber Line) ones of KT (Korea Telecom), the paper proposes the service model by which it can reinstate the subscription ratio status through employing next generation OSS (Operations Support System) and high-quality MPLS (Multiprotocol Label Switching) VPN (Virtual Private Network). It also describes diverse modules comprising NeOSS (New OSS) of KT, followed by detailed accounts regarding the service delivery process of KT VPN. Shortly visited are the primary constituents as well as configuration parameters of MPLS VPN. Finally the network topology along with a feasible service model case is presented.

I. INTRODUCTION

In recent years, many subscribers of KT VPN service have been compromised to adopt to purchase third-party-provided VPN CPE (Customer Premise Equipment) at a considerably low price to get the access to the Internet offered through xDSL lines. And more subscribers are expected to follow this trend since they can appreciate VPN service provisions not only at a lower price but also with higher bandwidth due to the fact that the service is provided through broadband lines up to 100Mbps. Taking into account that the top-tier rate of subscribers of KT-VPN services comprising more than 70% are the ones that are using these broadband lines, it can certainly be a frightening factor to undermine business revenue stacks of KT. So there arises the need to provide a service to meet the customers' needs by offering VPN service through broadband access in public Internet that intersects with high-quality MPLS VPN. KT is currently provisioning VPN service called 'X4Biz' to accommodate this type of customers' need.

This service offers competitive technological aspects such as the service being provisioned through MPLS VPN which supports a number of QoS (Quality of Service) functionalities; CR-LDP (Constraint Routed Label Distribution Protocol), RSVP-TE (Resource Reservation Protocol – Traffic Engineering), Diffserv (Differentiated Service), and etc [1] [6]. This can be a significant advantage since the VPN constructed on public Internet network with a third-party vendor CPE attached at a customer's premise lacks the security- and quality-wise functionalities to a considerable degree.



ME: Metro Ethernet
TDM: Time Division Multiplexing
xDSL: Digital Subscriber Line
MPLS: Multiprotocol Label Switching
IPSec: Secure Internet Protocol

Figure 1. Network topology

In addition, MPLS VPN allows users to apply their policies according to the traffic and security priorities of their own, and optimizes WAN (Wide Area Network) bandwidth at a customer's VPN to consistently process network traffics at the overall network topology [2] [7]. Subscribers also should note that they can achieve altitudinous scalability because it is not necessary to have full-mesh type of configuration of virtual connections in MPLS VPN so that a certain user group may easily create and delete its own VPN [2]. Figure 1 shows the network topology of the service. Table 1 also shows the increase and decrease of lines for each service over 12 months from July 2003 to June 2004.

	Leased	ATM	xDSL	VPN
July, 2003	378,517	11,648	156,139	3,022
June, 2004	361,418	6,839	216,649	2,994
Inc/Dec	**-17,099**	**-4,809**	**+60,510**	**-28**

Table 1. Service line increase and decrease in 1 year

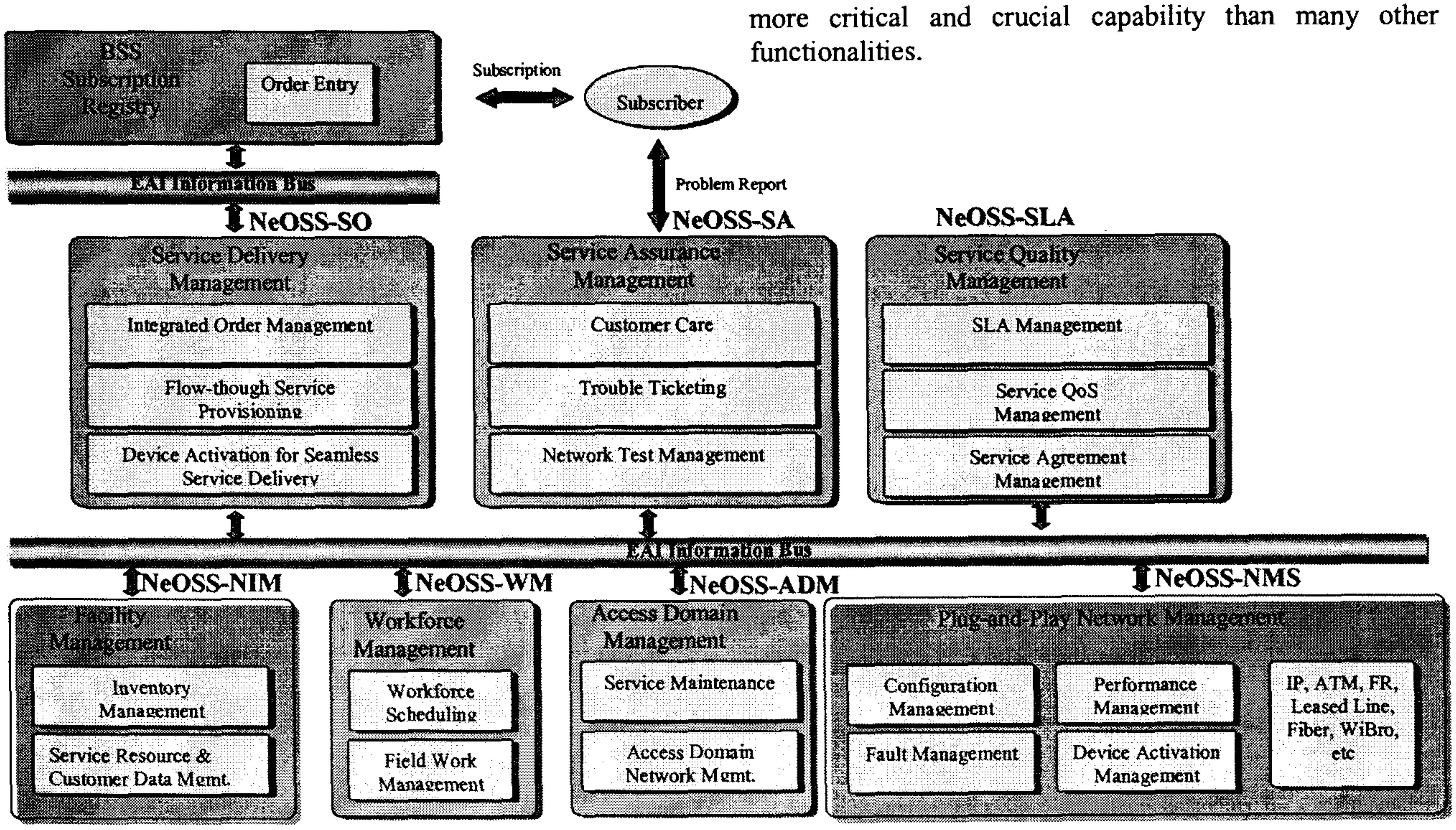
II. NEXT GENERATION VPN OSS: NeOSS

KT launched delivering commercial VPN service in 2000. Even though it has expanded and augmented its services and systems over time, it was not until quite recent years that it has landed on developing the next generation VPN operations support systems – NeOSS (New OSS), which includes service delivery system, fault management system, as well as network inventory management system and other essential systems of OSS such as provision/activation systems. Figure 2 shows the building blocks of NeOSS architecture.

Before NeOSS comes into place, KT VPN services were made only possible to be provisioned through disparate and separately-developed systems, each handling its own number of core functionalities of OSS. Not to mention, if all other KT services taken into consideration, it was literally a jungle of heterogeneous systems taking lengthy time and efforts to collaborate with other silos due to the lack of standards and different platforms.

Significant parts of NeOSS referenced by NGOSS (Next Generation OSS) and e-TOM (enhanced Telecom Operational Map) models of TMF (TeleManagement Forum) and other standard technologies, namely, XML Web Services, EAI (Enterprise Application Integration), and so forth, NeOSS successfully brought these overwhelming amount of home-grown systems into one picture [3] [4] [5]. Since it was agreed to choose MS Windows as its platform, NeOSS has also been able to take full advantage of lavish classes that the .NET framework offers in its development process.

Now that KT VPN comprises NeOSS, it can accommodate a supplementary service in the future as agilely as NeOSS can while fully appreciating workflow capability of BPM that Micro Soft BizTalk Server 2004 provides. When it is not less than common situations that many requests arise from operators and users in front office day by day to modify business processes partly or wholly, it is much more critical and crucial capability than many other functionalities.



SO: Service Ordering
NIM: Network Inventory Management
SLA: Service Level Agreement
NMS: Network Management System

SA: Service Assurance
WM: Workforce Management
ADM: Access Domain Management
NetIS/NE: Network Information System/Network Engineering

Figure 2. NeOSS architecture

- *Service Ordering (SO)*
  To realize flow-through business processes, Service Ordering module employed workflow-based Business Process Management (BPM) methodology. It allows core VPN business processes to quickly adapt to new services and systems modifications while this process previously held by tedious manual coding. KT VPN process workflows can be altered in-flight without stopping and starting the system again. As a next generation OSS, NeOSS fully supports the end-to-end service delivery process. Detailed process flow will be visited later in this paper.
- *Service Assurance (SA)*
  The integrated fault management system SA is the one-stop service assurance process that provides unified dashboard interfaces from generating trouble tickets through analyzing them to dispatching technicians to customer sites. It also accompanies the automated test capability across the entire network topology to deliver an end-to-end connectivity testing to operators.
- *Network Inventory Management (NIM)*
  NIM is an integrated SQL database built to manage an excessive amount of physical and logical facilities, location information, and subscribers' original records. It regularly updates itself by polling data from network elements containing traffic and device configuration contents.
- *Workforce Management (WM)*
  To derive maximized efficiency of operational management and customer satisfaction, WM has integrated manual processes that were individually built and operated in each division of workforce. WM supports PDA (Personal Digital Assistant) to transmit and receive SO/SA data at the site of servicing for POTS (Plain Old Telephone Systems), broadband, and dedicated-line services, and aids to request necessary data for line testing as well as reporting the task results.
- *Network Management System(NMS)*
  Network Element (NE) configuration management, performance management, traffic control and network monitoring are the primary profiles of NMS. To provide consolidated management across different silos, NMS collaborates with SO, SA, FM, and SLA.
- *Access Domain Management (ADM)*
  As an integrated management system of access domain facility, ADM interoperates with NE in real-time to process service orders and trouble tickets, and performs provisioning/activation and testing functionalities. Among the facilities it monitors are DSLAM (Digital Subscriber Line Access Multiplexer), FLC (Fiber Loop Carrier), and AGW (Access GateWay). These are mainly access domain edge equipment, terminal devices, and transmission machines. ADM module consists of configuration, fault, network monitoring, and flow managements.
- *Service Level Agreement (SLA)*
  As part of efforts to guarantee service quality, SLA module superintends a variety of data to check service order quality, trouble ticket quality, and network quality. If any violation detected against subscriber contracts, it notifies BSS to trigger proper billing adjustment for the benefits of subscribers. To ensure the flawless collaboration with SO, SA, and NMS for gathering accurate and timely data, SLA utilizes standardized way of commutation based on XML messages and .NET platform.

III. SERVICE DELIVERY PROCESS

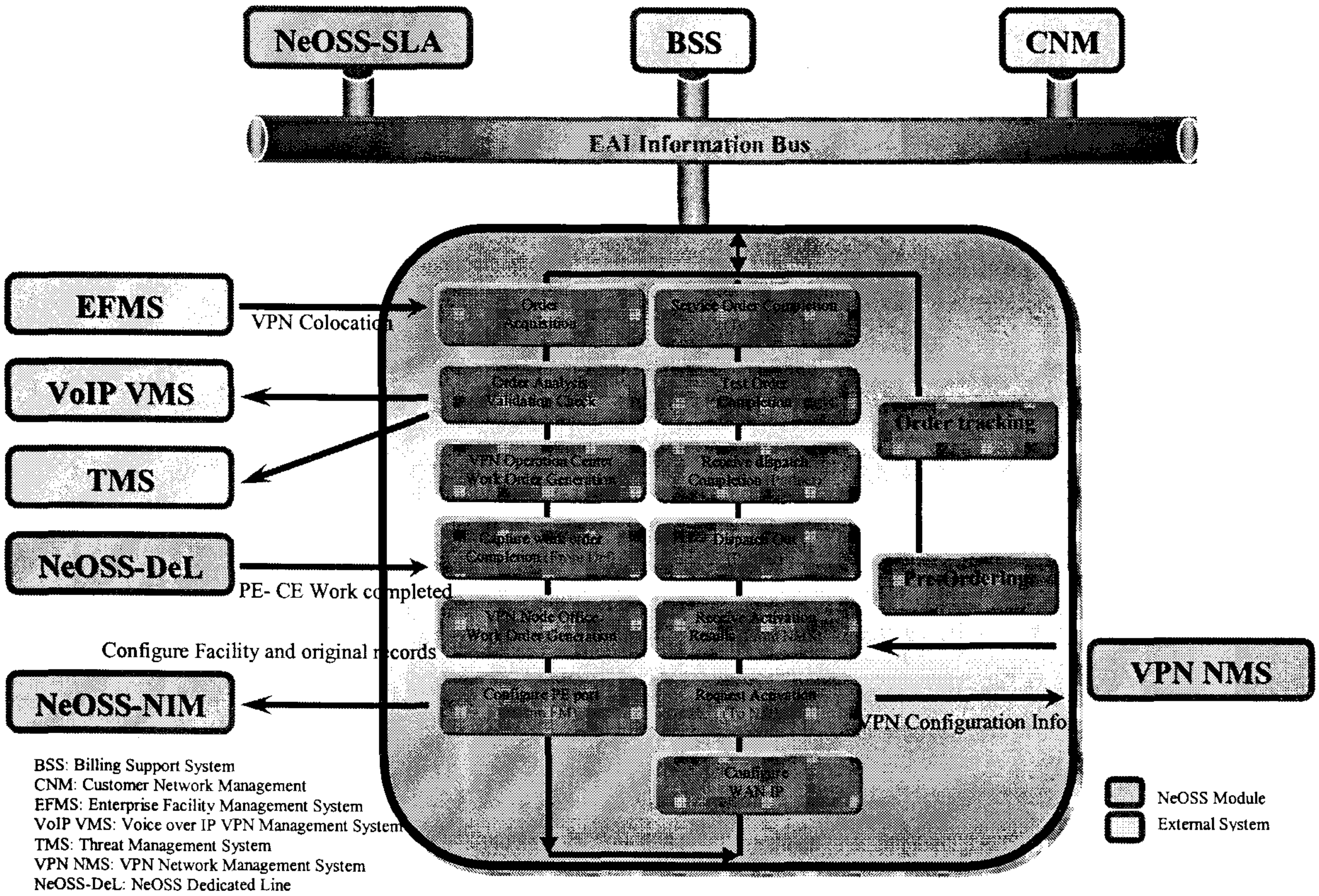
Now, let us examine detailed procedures of service delivery system, i.e., SO module of NeOSS. Figure 3 depicts the flow diagram of KT VPN service.

i. *Service Order Acquisition*
   A service order can be acquired through only one route, that is, from ICIS (Integrated Customer Information System), the KT's BSS (Billing Support System), to NeOSS. Other types of VPN service orders may take a different route via one of the collaborated systems of VPN to finally be acquired by the order acquisition part in NeOSS. Once the service order makes an entry inside NeOSS, it is passed to the next function block to be validated and analyzed.
ii. *Service Order Validation Check and Analysis*
   The service order must be required to be through validation check. In this procedure, the order is analyzed and checked whether there is any missing data item, whether there is any incorrect data field, or whether the order data have valid formats or not.
iii. *Work Order Generation I*
   Once the service order successfully passes the validation check, it is now ready to generate a work order including VRF, RD, and RT to be completed by operators at the VPN operation center. This work order is distinguished from the type of work orders that will be described later when we get to the point 'v. Work Order Generation II' in the sense that this work order is comprehensive, namely, it includes all the work order items that the work order for node office operators consists of.
iv. *Work Order Completion Capture*
   After an operator at VPN operation center finishes fulfilling the work order items, the work order completion is sent back to NeOSS and captured by it.
v. *Work Order Generation II*
   This time the work order is generated to be used by an operator at a node office. The node office operator configures the order items on Web GUI, and then notifies the order completion at the node office level to the operator at VPN operation center.
vi. *Physical Facility Configuration*
   An operator in a node office or at the VPN operation center configures relevant equipment

settings on Web GUI, saves them, and the configuration data are transferred to Network Inventory Management to reserve the necessary facility to deliver the requested service.

vii. *Logical Facility Configuration*
Most of the time the operator in the node office configures the IP settings within the allowed range of IP coverage. In doing so, segmentation and desegmentation of IPs are performed to generate a number of IPs corresponding to the operator's request.

viii. *Activation Request*
All the configurations of physical and logical facilities saved to a local database of SO module are now cast to VPN NMS (Network Management System) to activate necessary resources. This is the process that actually deals with operating a variety of network devices and equipment. The preview functionality which allows operators to check a set of functions and test them in advance before a real activation takes place comes handy to facilitate the critical, but complicated task of equipment activation.



BSS: Billing Support System
CNM: Customer Network Management
EFMS: Enterprise Facility Management System
VoIP VMS: Voice over IP VPN Management System
TMS: Threat Management System
VPN NMS: VPN Network Management System
NeOSS-DeL: NeOSS Dedicated Line
NeOSS-NIM: NeOSS Network Inventory Management

Figure 3. Service Delivery Process

ix. *Activation Result Acquisition*
After the required activations are successfully executed, then the consequent results are notified to the requesting party in SO module. The notifications are carried out through Web Service communication or in rare times through MSMQ (Micro Soft Message Queuing).

x. *Dispatch Request*
A dispatch out is forwarded to a field technician to install a CPE at the customer's site. Depending on the type of services, a dispatch in is also forwarded to an operator in a central office to fulfill the required job inside the central office. KT holds partnerships with third party vendors to efficiently handle dispatch out and CPE installation for each VPN service.

xi. *Field Work Completion Acquisition*
A field technician completes the assigned work order, and informs the VPN operations center of the completed task through Web GUI.

xii. *Service Order Completion Test*
Prior to the final notice of the requested service order, a test is performed to make sure that the service delivery is ready to take place by OSS.

xiii. *Service Order Completion Notification*
By fulfilling this procedure, the acquired service order to OSS is transmitted back to BSS to notify it should start billing process to a subscriber.

IV. MPLS VPN

Throughout the telecommunication industry at the global level, it is not difficult to find out that a good number of telecoms are deploying MPLS VPN in their networks. KT also embarked to commercially provision such a service a few years ago since it proposes attractive cost savings to customers compared to traditional leased-line subscription.

As to technological facets, it offers far more list of advantages than just a cost benefit owing to supporting QoS (Quality of Service), TE (Traffic Engineering), multi protocol such as IPv4, IPv6, Apple Talk, and so forth. The fact that MPLS uses a rather simple-to-use switch than a router as hardware platform, and exploits table lookup methods along with streamlined hardware-like packet transmission makes it enhance cost to performance ratio.

KT MPLS VPN is comprised of 3 elements; P (Provider) router, PE (Provider Edge) router, and CE (Customer Edge) router as illustrated in Figure 4. And the access from a customer site to MPLS backbone is only granted through the link between CE and PE. PE should possess a forwarding capability to distinguish incoming packets in terms of VPN.

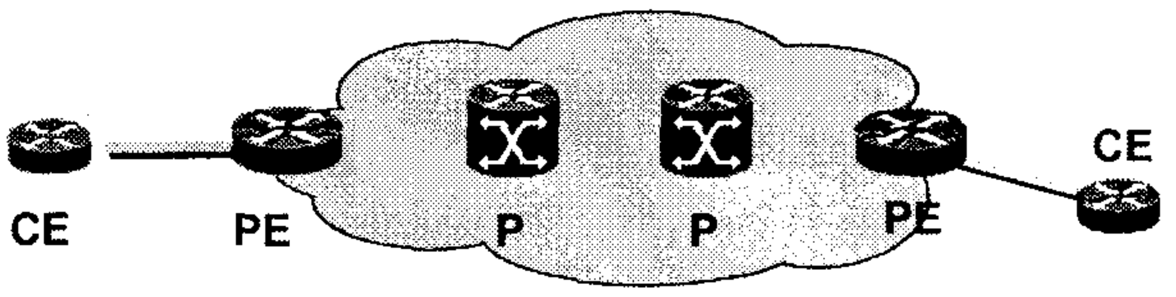


Figure 4. MP-BGP basic layout

- P: It does not involve in MPLS routing. It only forwards labels exchanged at PE. This is the router located at the path of LSP (Label Switched Path) between Ingress and Egress routers. It searches LFIB (Label Forwarding Information Base) by the label attached to a packet.
- PE: This router is connected to CE router of a customer, and it generates a unique VRF (VPN Routing and Forwarding) for each subscriber. A LSP is created between a destination PE router of the customer and a source PE while using LDP (Label Distribution Protocol) and RSVP (Resource Reservation Protocol). PE routers exchange VPNv4 routing information through MP-BGP (Boarder Gateway Protocol).
- CE: This is the gateway to the access domain network at the customer side; It connects to the actual customer's network. It does not carry any configuration with regards to MPLS VPN. Communicating through static, OSPF (Open Shortest Path First), RIP (Routing Information Protocol), it establishes a connection to PE.

The operators at both VPN operation center and node offices must be able to determine 3 major configuration values to provide MPLS VPN to subscribers. They are VRF, RD (Route Distinguisher) and RT (Route Target).

- VRF: This is required to efficiently manage a unique routing table for each customer. It contains 2 labels regarding data packets and the information for a next hop including MP-BGP data from another PE router and CE router information.
- RD: When different customers have same private IPs, address overlapping occurs. To avoid this conflict, a singular RD should be assigned to each customer. It follows the form of AS:NN where AS is autonomous system number given to a network (for example, KT's KORNET network is 4766), and NN denotes 5-digit RD number such as 10000.
- RT: This is an attribute attached to VPNv4 BGP route to express VPN membership. This value is added to the customer route when IPv4 route gets converted to VPNv4 at PE router. Simply put, this is required to make routings possible in MPLS VPN. The source PE to send out the customer route has the 'export RT', and the destination PE to receive has the 'import RT'. Each PE router contains a pair of the export and import RTs. See Figure 5 for the illustration.

V. DELIVERING THE SERVICE

Taking advantages of MPLS VPN stated above along with well-constructed access infra of xDSL wired lines of KT, the aforementioned VPN service, X4Biz, is to have the following network topology.

An exuberant variety of auxiliary 'access' services that KT VPN catalogue presents ought to be possible to be available when customers subscribe to intra and extranet services since it is via MPLS VPN. Subscribers should be allowed to have their own IPs for the same reason as well. As in the existing premium VPN service, Internet service comes into play utilizing firewalls and NAT (Network Address Translation) at the MPLS gateway. However, direct access to Internet from the customer side is prohibited essentially. KT makes it possible by operating terminal devices at the customer site by itself and also monitoring the attempts from the center.

The table below summarizes comparison between a residential xDSL service and business xDSL (X4Biz) service. Advantages of business xDSL are added at the last column.

	Residential xDSL	Business xDSL	Advantages
Backbone	PublicIP Network	MPLS Dedicated Network (Private)	Enhanced Security
Structure	Hub-Spoke	Full Mesh	Scalability
Management	separately managed Line, Network	Integrated management of Line, Network	Integrated Management
Customer Equipment	Separate modem, VPN equipment	built-in Modem+VPN	Lower initial investment
Service	Simple line provisioning	Line + VPN + QoS + TE + Security(anti-virus) + Multicasting	Differentiated business service

Table 2. Residential vs. Business xDSL

One feasible model to provision the intranet service is as follows. This case has hosts residing inside VPN. For the backbone network, MPLS VPN collaborates with TDM

(Time Division Multiplexing) and metro-Ethernet networks via VRF, RD, and RT. For the access network, the connection is established through IPSec tunnels for security purposes. And between customer LAN sites, only static routing should be allowed at the initial stage of the service while fine-tuning PE performance so that the dynamic routing may be available later. The model is depicted in Figure 5 below.

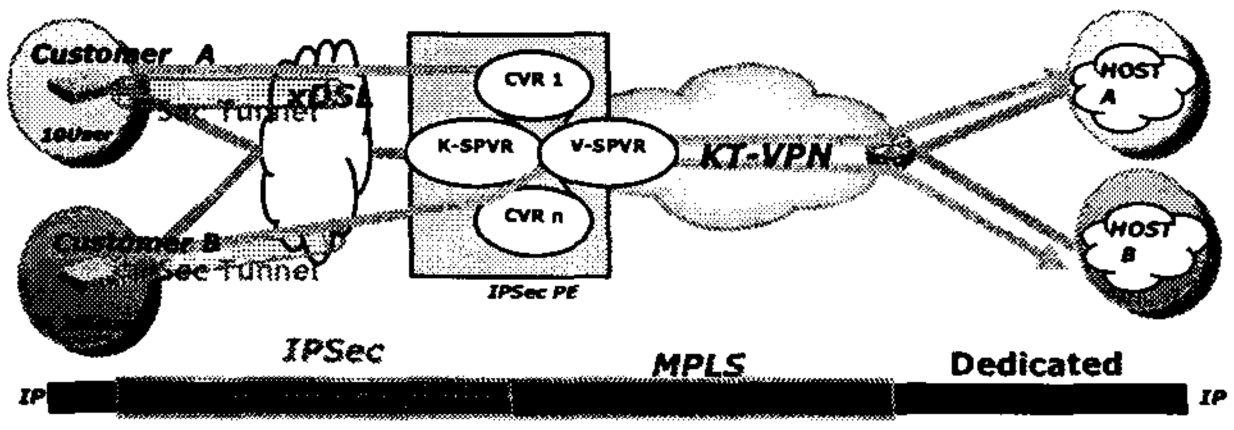


Figure 5. Service Provision Example

VI. CONCLUSION

During the year charted in the table 1, the number of increased subscribers toward residential xDSL service is approximately 60,000. This amounts to 5,000 subscribers per month. One can not help but to be drawn to resort to this number to find a reasonable explanation to count the loss of 17,000 dedicated line subscribers during the same period.

Today's hyper competitive market leads many subscribers to turn into lower price with higher bandwidth even at a negligible difference. To sustain a healthy reservoir of subscriber pool for VPN and leased-line services, a new type of VPN service is proposed to be delivered in full scale at KT constituting the service with well-established access infra and MPLS VPN.

The proposed service model incorporates next generation OSS, a.k.a., NeOSS to furnish end-to-end service delivery by implementing flow-through BPM workflows. And we described each component module of NeOSS in small detail. We also examined the service delivery process starting from the front office in BSS through the back office of NeOSS operators to field technicians of partners.

Various points of MPLS VPN were visited including technical and financial advantages it owns compared to traditional private line network, and it was followed by the accounts illustrating basic operations among the major building blocks of MPLS VPN as well as primary configuration parameters.

Finally, we proposed the network topology of the stated service including a feasible service provision model for intranet service, and presented a table of comparison between the residential and business xDSL services.

With the proposed service model, KT can provide thousands of subscribers with broadband bandwidth on top of numerous high quality functionalities that MPLS VPN can only support, while all of these offered at an affordable price. Not to mention the standard-based technologies upon which its service delivery system has been built. It can quickly and easily adapt to agile business environment. KT is standing at the heart of dramatic shift to new paradigm in telecommunication industry. By the proposed service model, it will be able to blow the wind driving the tide in favor of itself.

REFERENCES

[1] Ivan Pepelnjak, Jim Guichard, MPLS and VPN Architectures, Cisco Press, January 2004.

[2] Nam-kee Tan, Building VPNs with IPSec and MPLS, McGraw-Hill, 2003

[3] TMF 050.v.2.0, "NGOSS Overview", TMF document, July 01, 2001

[4] TMF 053.v.2.0, "NGOSS Architecture", TMF document, July 01, 2001

[5] Microsoft, ".NET", http://www.microsoft.com/net

[6] Daniel W. Hong, Choon Seon Hong, Dongsink Yun, "A Flow-through Workflow Control Scheme for BGP/MPLS VPN Service Provision," in Proceeding of the 3rd European Conference on Universal Multiservice Networks, Published in Lecture Notes in Computer Science, Vol.3262, pp.397-406, October 2004

[7] Daniel W. Hong, C.S. Hong, Y.I. Kim, J.W.Kim, S.B. Kim, C.S. Kim, J. W. Park, D.S. Yun, and C.H. Ahn, "A Workflow-based Service Delivery Architecture for Providing MPLS VPN Service," in Proceedings of the 8th World Multi-Conference on Systemics, Cybernetics, and Infomatics, Vol. 3, pp.427-430, July 2004