An Architecture of a QoS Management System for Next Generation Internet

Taesang Choi, Yoonhee Jung, Sungwon Sohn
Electronics Telecommunications Research Institute
161 Kajong-Dong Yusung-Gu
Taejon City, KOREA
E-mail: {choits, yhjung, swsohn}@etri.re.kr

Abstract

Seamless end-to-end Internet Quality of Service (QoS) management is very challenging not only because Internet management is not well understood and practiced in the real world but because the nature of the Internet is hard to predict and manage. Secure transmission, transport reliability, ability to differentiate service qualities, QoS-based intelligent routing, QoS monitoring, and customer-oriented service management are essential technical huddles to be coped with. Despite of these difficulties, the Internet becomes the platform of choice for the next generation applications and services. Without a solid management solution, it is not easy to deploy high quality commercial services. In this paper, we propose an architecture of seamless end-to-end Internet QoS Management System and describe the design principles and system components of our developing prototype system.

1. Introduction

The Internet is growing with enormous speed and is becoming an integral part of everyday business operation. It is undoubtedly becoming the platform of choice for the emerging innovative network and application services. In order to support such services, several unsolved technical issues have to be resolved. Secure transmission, transport reliability, ability to differentiate service qualities and intelligent routing are some of the essential technical huddles to be coped with. Industries, academia and research communities of the IT advanced countries are actively engaged in developing products, conducting researches, establishing test-beds and performing performance and interoperability tests for next generation Internet technologies. Unlike the existing Internet, which is mainly based on best-effort service, the emerging next generation Internet [4] can provide secure, reliable, and qualitatively differentiated commercial services. For the success of this emerging Internet and its services, the importance of automated seamless end-to-end Internet service and network management cannot be over-emphasized. It will play a very important role for both customers and service providers. Customers can request a service with quality of their choice, monitor how the requested service behaves and report troubles when faults occur through the automated service management interface. Internet service providers (ISPs) can provision the requested services via service/network provisioning processes, monitor the service/network status and requested qualities, and act proactively when the faulty situation occurs such as identifying the faults, analyzing the problems, fixing them, and sending trouble status reports to the customers, etc. Also ISPs can exchange service orders and trouble tickets among themselves.

In the current Internet, very limited set of configuration, fault, performance, accounting management for the network elements only are used for most ISPs and enterprise networks. Network management is far from the reality, let alone the service management. But, as the Internet becomes the platform for various network services, the customers want to consider the service they are using as a total solution. To meet this requirement, customer care management, service management, network management and network element management should tightly work together to provide automated seamless end-to-end Internet management.

In telecommunications environments, this issue was raised and work have been progressed to address it. TeleManagement Forum (TMF) [1] is a leading industry consortium that recognized the issue and is providing a number of solution sets. Its Service Management Business Process Model (SMBPM) [2] defines a number of processes including customer care processes, service management processes, network management processes, and information systems management processes. Each process has its own functions and interfaces for the interaction with other processes. These management processes are not fully defined yet, and even those defined ones are specifically designed for telecommunications services. However, the concept is very useful to the next generation Internet management and can be augmented for this purpose.

Recently, in the Internet community, automation of QoS control for IP networks has become a hot issue. Internet Engineering Task Force (IETF) policy framework working group has published an internet draft on policy-based network management (PBNM) architecture [3]. Its main objective is to provide secure and scalable management framework for automated policy-based QoS control in the Internet. Also, Internet2's QBONE bandwidth broker working group [4] is defining a specification for bandwidth broker. It provides an automated end-to-end resource allocation mechanism between customers and service providers. These two activities mainly focus on network management issues with little service management aspects. They are very Internet specific but lack overall service and network management framework. Hence, marriage between TMF's SMBPM and these two activities can produce very interesting service and network management framework for the next generation Internet.

This paper proposes an architecture of seamless end-to-end Internet QoS Management System based on the three management frameworks mentioned above. In the next section, some of the major Internet management issues are summarized. In Section 3, we describe the TMF's business process model and relate it with our management processes. Then, the functional management architecture is explained. In Section 4, our prototype implementation based on the proposed architecture is explained in detail. Finally, we conclude our work with summary and itemize the remaining future work.

2. Major Internet Management Issues

It is very important to understand the current and next generation Internet before we start considering how to manage them. In comparison with network management for telecommunications network and service, the Internet management is not well studied and practiced. One main reason for this is because that the Internet was not considered as a commercial service platform until recently. Most mission critical applications were used over relatively secure and reliable privately owned or leased network infrastructure. People have tendency to be tolerable for the current low quality best-efforts Internet services. However, as the Internet becomes a commercial service platform, the situation is completely different. Business excellence of an ISP can be judged by the robust management processes.

Figure 1 [5] may best illustrate the architecture of the Internet today, which includes the diversity of end-user connectivity, the mix of retail and wholesale environments, the ability to undertake multiple upstream services, and the existence of point of presences (PoPs) and exchange points at various locations within the Internet. Physically, future Internet will be similar to the current architecture except higher capacity PoPs (Giga PoPs), exchange points, and transmission links. But functionality will be quite different. More sophisticated bandwidth management, congestion control, traffic policing, and quality of service control will be added.

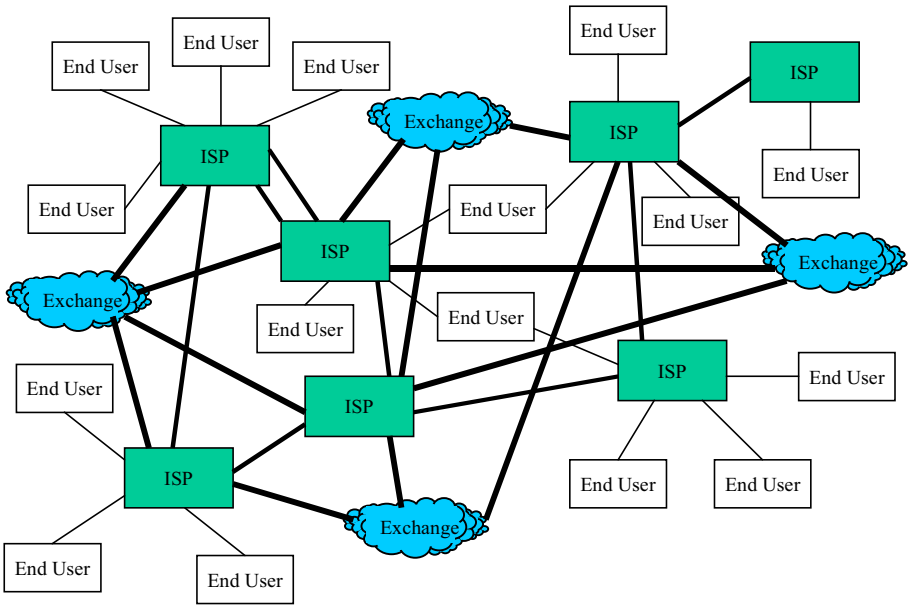

Figure 1: The Current View of Internet Structure

Some of the important issues to consider for managing such complex physical and logical components of the new Internet can be identified best in terms of ISO's five major functional areas of network management, that is, configuration, fault, performance, accounting and security management. For proper identification of issues, we need to look at the Internet architecture described in Figure 1 from the management point of view. Figure 2 shows functional components for management and their relationships at the top most level. For seamless automated end-to-end Internet management, end-customers should be able to participate in the management processes via customer care management interfaces. An ISP not only has to interact with end-customers but with other ISPs, network operators or suppliers for the end-to-end service and network management. More details on internal processes and interfaces will be discussed in the following section.

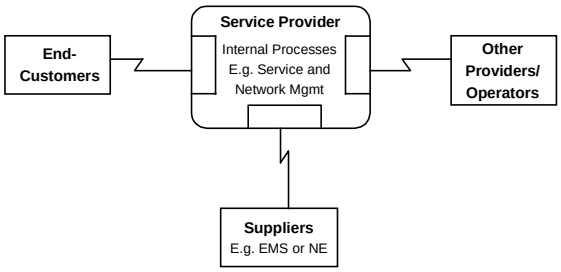

Figure 2: High-level Internet Management Business Context and Scope

- Configuration Management

Configuration management is the process of monitoring and inventorying the current state of resources and their inter-relationships (e.g., network topology) and controlling the configuration, state and relationships between resources. The former is a very important process but the latter has attracted more attention from the Internet management community recently. Traditionally, remote control of the network resources was done through telnet or SNMP set operations although remote configuration management requires scalable, reliable and convenient way of controlling network resources. It can be viewed from different levels: service management, network management and network element management.

- From the service management viewpoint, service topology monitoring, intra- and inter-service provisioning, service inventory control, and Service Level Agreement (SLA) negotiation with end-customers and other ISPs are main tasks.
- From the network management viewpoint, service provisioning data (e.g., QoS parameters, security parameters, etc.) should be mapped to network provisioning data and network topology should be mapped to service topology. It checks resource availability and policy conflicts for the requested provision and decides which network elements should be chosen for the final enforcement. These checks can be done based on known topology, inventory and policy information.
- From the network element management viewpoint, element specific data can be enforced to setup the requested functionality (e.g., a queuing discipline, filtering rules, etc.). It also collects topology and inventory specific data to be used by network management layer.

- Fault Management

Fault management is the process of identifying faults, isolating, responding, and resolving them quickly. Typically fault management was the realm of network administrators or managers and, thus, end-customers were not aware of what was going on inside of the ISP's network. However, as the Internet becomes a platform to provide meaningful commercial services, end-customers no longer want to consider it as a black box. Instead, they want to be well informed as to the nature of the fault, the status of resolution and expected time for the resolution. This requirement leads to ISPs to be more open and interactive with end-customers and other ISPs. Fault management can also be viewed from different levels of management.

- From the service management viewpoint, trouble handling process is the main task. Through the automated interfaces between an end-customer and ISP(s), the state and information regarding fault management processes can be shared seamlessly. Especially, new functional components for QoS control need to be managed properly.
- From the network management viewpoint, identification, detection, and resolution of network specific faults are important tasks. It has to interact with service management layer and network element management layer. Identification of network faults can trigger the trouble handling process in the service management layer to notify the faults to the affected customers or other ISPs. Customer trouble reports can trigger network fault management process as well in the reverse direction. It is very important to automate these processes and integrate them for the seamless end-to-end service/network management.
- From the network element management viewpoint, network elements in the next generation Internet add new hardware and software components to be managed such as active bandwidth management mechanisms, queues, policing and shaping components. Fault monitoring of these components and timely resolutions are essential to provide end-to-end QoS guarantee.

- Performance Management

Performance management is the process of collecting data relating to the usage of resources, analyzing them to make meaningful statistics, feeding them to fault management process, and applying them to capacity planning and deployment. Managing performance is one of the most challenging aspects of Internet management, especially next generation Internet management. For QoS guaranteed services, service provisioning is just

beginning and constant monitoring of the requested service quality is more important. Let's look at the performance management from three different management levels.

- From the service management viewpoint, end-to-end service quality monitoring is the main task. ISPs have to keep track of performance metrics regarding end-to-end aspects such as one way delay, two-way delay, delay variance, and packet loss rate, etc. On the other hand, end-customer's main interest is whether the service quality they requested is well met. This task can be achieved by defining automated interface between an end-customer and an ISP for performance reporting. This is a very important process that most current Internet service providers is missing and should be an essential part of customer care processes for next generation Internet.
- From the network and network element management viewpoints, interests are in network or network element level. Performance metrics for a particular network or a network element are collected and analyzed, for instance, single diff-serv [6] domain performance metrics, a single RSVP [7] flow delay variance in a given network domain, and a router's queuing performance metric, etc. Aggregation of all these metrics can be used to provide an end-to-end performance metric.

● Accounting Management

Accounting management is the process of gathering resource usage data and assigning that usage to a end-customer whose use is to be accounted. Unlike telecommunications environment, resource usage accounting in the Internet is not a trivial task. Currently, there are two different mechanisms are widely used by the ISPs, that is, simple accounting method used by Radius [8] and TACACS+ [9] and interior accounting method defined by IETF Realtime Traffic Flow Measurement (RTFM) [10] working group and Cisco's Netflow [11]. The former collects aggregate usage data per customer and the latter accounts for per service basis so that a separate tariff can be applied. But because of the IP traffic characteristics, the second methods have several problems to be solved. Besides them, end-to-end accounting management when multiple ISPs involved for providing a particular service has to be addressed. Also when different quality of service is provided, the tariff structure becomes much more complex.

● Security Management

Security management is the process of managing the security environment of a network including detection of security violations and maintaining security audits and performing the network management task in a secure way. For detection of security violation, there are issues such as fault-tolerant and scalable intrusion detection mechanisms and real-time intrusion tracking mechanisms both for IP-based enterprise networks and ISP networks. For secure network management operations, issues such as secure management information transport with reasonable overheads and remote controlling of network resources in a secure manner become very important.

3. System Architecture

3.1. Business Process Model

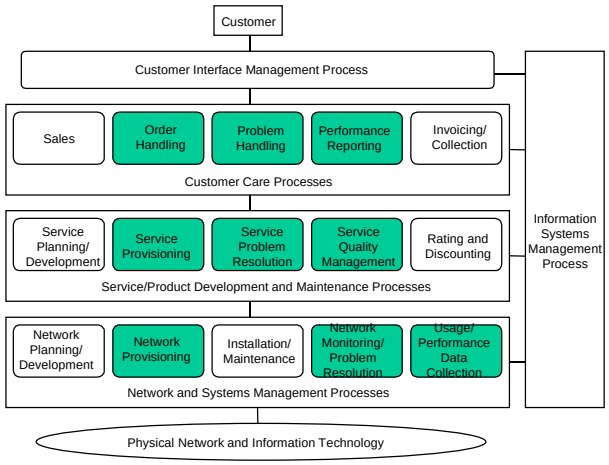

Figure 3: TMF's Service Management Business Process Model

In section 2, we described major management issues based on ISO's five major functional areas of network management from the TMN's service management, network management, and network element management viewpoints [12]. These management functionalities can be grouped into layers whose components are a set of management processes. Each process performs specific management functions and interacts with other processes in the same layer or different layers for seamless management operations. TMF defined a process model, SMBPM, for this purpose. It is shown in Figure 3.

The first two layers show management processes relating to the service management and the third layer shows network management processes. Each process shown as a small box actually consists of very complex internal functions and interfaces for the interactions with other processes. This model covers five management functional areas. The shaded boxes represent management processes that this proposal is interested in, namely, service configuration (especially including QoS provisioning), fault management (including trouble administration), and performance monitoring (particularly QoS monitoring).

Based on this model, we would like to provide a management platform for seamless end-to-end Internet QoS management. A simple scenario is as follows. Customers can request a particular service to an ISP, say VPN via a customer care interface. SLA includes service specific QoS parameters for provisioning. The ISP receives the request, processes it, and interacts with customers while the requested service is provisioned. The ISP's QoS service manager converts the QoS parameters and other parameters (e.g., security, access control, etc.) into proper policies, stores in the policy

repository for further processing, and then notifies QoS network manager about the request. The QoS network manager retrieves the stored policy, performs some housekeeping functions (e.g., policy conflict checking, resource availability, etc.) and enforces the required resource reservation to necessary network elements. If the requested service provisioning requires more than one ISP's involvement, the same process has to be repeated between the ISPs. Once the provisioning is completed, the results will be notified to the QoS service manager and the QoS service manager, in turn, will notify the customer. Also QoS service manager constantly monitors the service quality with the help of QoS network managers. It regularly reports to the customer about the QoS status to meet the SLA. Customers can send any trouble reports regarding the requested service via the same customer care interface and the service provider processes them by interacting with a QoS fault manager for the identification, detection, and resolution of possible faults. QoS network manager can also detect faults and notifies the customer if it affects service qualities. Meantime, the status of the resolution process is promptly notified to the customer.

The mapping between this conceptual business process model and real functional model with implementation details will be described in the following sections in detail.

3.2. Functional Architecture

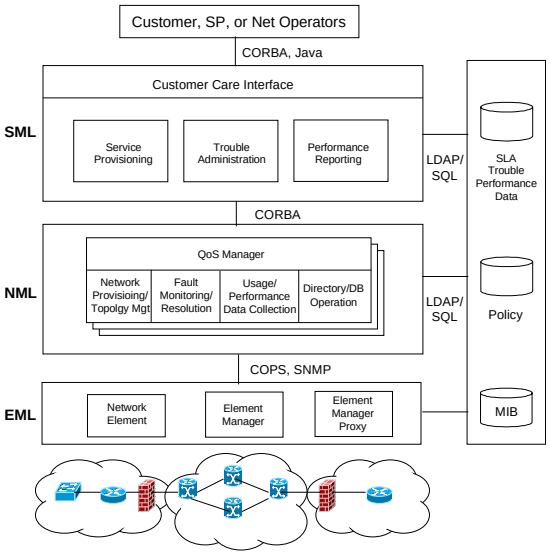

Figure 4: Functional Architecture of the Proposed Management System

Figure 4 shows the functional architecture of our proposed QoS management system. As the figure illustrates, this architecture is based on the TMN model [12] for the overall management framework, TMF's SMBPM for automated business processes workflow, and IETF's PBNM for network and element management especially in the area of QoS-based resource provisioning. The system currently covers configuration, fault, performance, and part of security management functional areas. However, the system architecture is scalable to expand other management functional areas such as accounting and other security management. As the system matures, we are planning to add those functionality as well in the future.

In the service management layer, three management processes are defined. It has a single integrated customer care interface with which customers, other ISPs, or human enterprise/ISP's network managers interact. In other words, the system provides two different ways of interaction. One possible scenario is when customer network management system or other ISP's service management system interacts with it via a programming interface. Another case is when human administrators want to access the management system directly via its graphical user interface. The former is using a CORBA IDL interface [13] and the latter supports web access via Java/CORBA mapping. Three processes also communicate with QoS network manager in the network management layer through the CORBA IDL interface. Another important interaction is with a directory/DB server for storing and retrieving SLAs, trouble tickets, and performance reports. SLA is stored in two different forms: service provisioning independent and dependent information. The latter is translated into the policy schema (e.g., QoS policy, routing policy, and security policy) which will be used by a QoS network manager later.

In the network management layer, more than one QoS network manager can exist. Each is responsible for its own network domain, for example, a single Diff-Serv domain. Each handles network resource provisioning, fault monitoring and resolution, performance data collection, and policy schema administration. It interacts with service management processes through a CORBA IDL interface. Invocation of a management operation can be either direction. For example, a service provisioning process initiates network provisioning via QoS manager interface. On the other hand, the QoS network manager can send a performance data to a performance reporting process in the service management layer. For network resource provisioning, the QoS manager interacts with a directory server to retrieve appropriate policy schema (e.g., QoS policy, access control policy, etc.) and network topology information. The QoS network manager then decides what policies to be applied to which network elements. Before provisioning takes place, it converts the policy schema into information objects that both QoS manager and network element manager have a common understanding. Common Open Policy Service (COPS) protocol [14] is used for transport of these information. Fault, performance, and network topology management use SNMP.

In the network element management layer, a few different types can coexist. The first kind is a network element which plays a role of a COPS client and an element management agent. This is the simplest case where the QoS manager directly controls the network

element. Another kind is a network element manager which manages one or more same type of devices. In this case, it plays an agent role towards the QoS manager and plays a manager role for its device(s). For network elements provisioning, it intercepts COPS messages and enforces them to the appropriate network elements. If the element supports COPS client functionality, the COPS message for the QoS manager transparently pass through. If not, the element manager plays a role of proxy for that particular network element. Fault, performance, and topology management can be performed via SNMP.

4. Implementation

We are currently implementing our system based on the proposed architecture. Our initial implementation focus is end-to-end QoS-based resource provisioning. The prototype system consists of three components: a QoS Service Manager, a QoS Policy Server, and a QoS Client.

4.1. QoS Service Manager

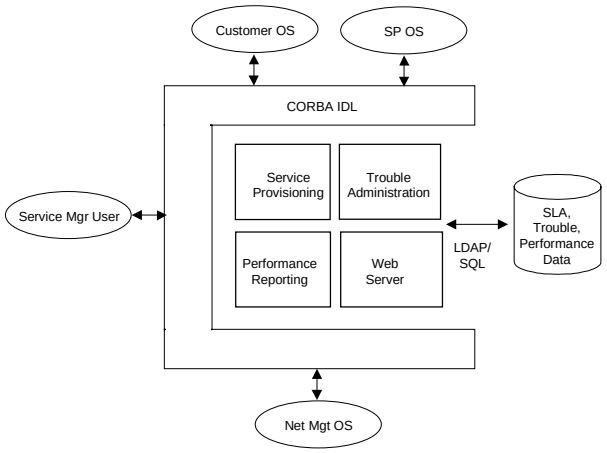

Figure 5: A QoS Service Manager Implementation Architecture

As mentioned in the previous section, TMF's Service Management Automation Reengineering Team (SMART) [15] has defined technical specifications for service order handling [16], customer-to-service provider trouble administration [17], and performance reporting [18]. These documents define information models and service interfaces independent of underlying communications technologies. The range of resources and services, problem types, status codes, service orders, performance metrics etc. are defined primarily to cover telephony service. In order for these service management processes to support the Internet services, extension of the above resource types is inevitable. However, their functional requirements, state model, and basic protocol mechanisms are designed in such way that no or trivial modifications are needed.

Our QoS service manager implementation is based on the functional behaviors defined in these specifications and extension of resource types suitable for the next generation Internet environment. Also these specifications lacks the capability to interact with network management layer processes. However, for the true seamless end-to-end QoS management of the Internet, integration of service management layer and network management layer is very important requirement to be fulfilled. Thus, our QoS service manager implementation extends the existing interface specifications to cover this requirement.

One more user of the QoS service manager is network administrators or managers of an enterprise network or an Internet service provider. Unlike the previous cases which require a programming interface for communications, a user friendly and easily accessible user interface is recommended for those users. The QoS service manager exposes its services via Java applet to those users. This way they can access QoS service manager's interface via their web browser. The detailed implementation architecture of the QoS service manager is illustrated in Figure 5.

4.2. QoS Network Manager

This component is an NM OS which is responsible for managing configuration, fault, performance, part of security aspects of a network in the Internet. Its implementation architecture is based on the IETF's PBNM architecture. PBNM defines four major components: Policy Management Tool, Policy Repository, Policy Decision Point (PDP), and Policy Enforcement Point (PEP). Policy Management Tool presents services, interacts with users, and coordinates PDPs. PDP stores the policies provided by users into a policy repository as schematic forms, checks any local domain conflicts, exchanges policies with PEPs and, possibly, with other PDPs. PEP participates policy management (e.g., sending request, reports, and accounting info., etc.) and enforces policies received by a PDP. Policy repository contains policies stored in a certain schema. There is, currently, no standardized common schema but work is under progress in IETF policy framework working group. Policy can represent a variety of information such as QoS, routing, security, etc. Policy information is exchanged between PDP and PEP via COPS protocol.

The scope of current PBNM mainly covers policy-based QoS service provisioning which is only a subset of the configuration management. Yet, QoS fault and performance monitoring and proactive QoS problem management are significant aspects to be considered as well. Our QoS Network Manager is built on PBNM with additional functionality expanded. Towards SML, it has a CORBA IDL interface for necessary interactions with customer care processes. For network QoS provisioning, we are implementing PDP functions, LDAP for policy repository, and COPS-PR [19] server functions for policy information exchange. Network topology monitoring and update functions are added for intra- and inter-domain network resource provisioning. Network fault management and network QoS performance data collection funtionality is included. SNMP is a protocol

used for the associated management operations and the network provisioning process shares manager MIB. For the common understanding of these management information between the service manager and the network manager, mapping functions between manager MIB and information objects consumed by the service manager are provided.

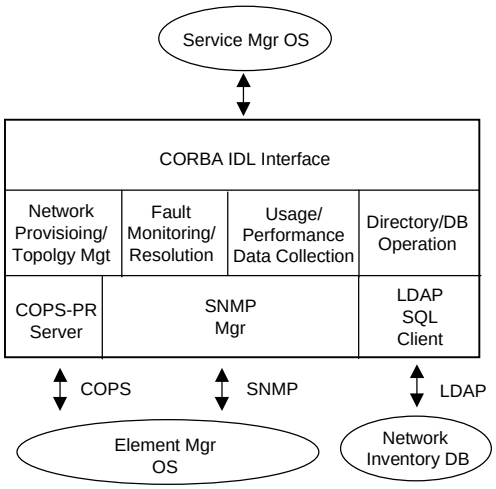

Figure 6: A QoS Network Manager Implementation Architecture

IETF defined Realtime Traffic Flow Measurement (RTFM) architecture for realtime network performance monitoring. It consists of four main components: meter, meter reader, meter manager, and analysis applications. QoS Network Manager implements a meter manager and a meter reader. Figure 6 shows an implementation architecture of the QoS Network Manager.

4.3. QoS Element Manager

The main requirement of our QoS Element Manager is to provide platform transparent QoS control. There are many different types of network elements in the Internet: routers and a variety of switches (L2/L3/L4, FastEthernet, Gigabit Ethernet, ATM, MPLS, etc.). Each one has different means of controlling its QoS features. Our Element Manager provides a platform neutral interface for QoS control towards the QoS network manager and has an adaptation layer which interacts with a particular platform. For QoS provisioning of a network element, QoS Element Manager plays COPS client role. It supports both COPS enabled network elements and non-COPS compliant network elements. For the former, it transparently pass the COPS messages to network elements. For the latter, it plays a role of COPS client proxy for those network elements.

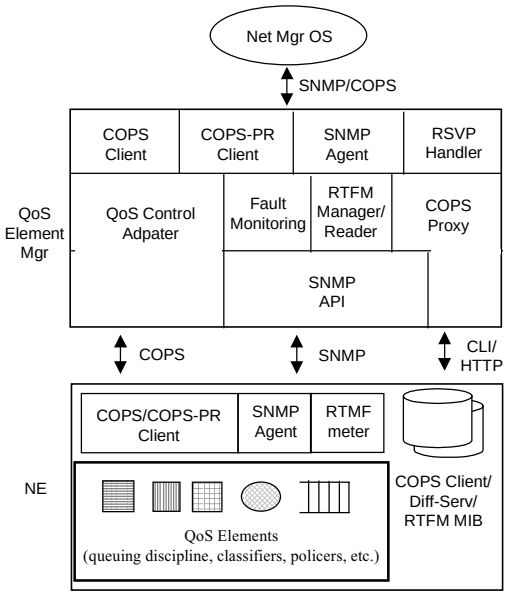

Figure 7: A QoS Network Element Manager Implementation Architecture

It also performs fault and performance management functions. IETF Diff-Serv and RAP working groups are still defining Diff-Serv MIB [20] and COPS client MIB [21]. We try to implement those MIBs and will align the changes as the drafts mature. For performance monitoring it implements RTFM components for a network element or a subnetwork that has homogenous network element types. This information will be used by the QoS network manager for network wide performance monitoring. We describe the detailed implementation architecture in Figure 7.

4.4. Testbed and Target Application Services

Figure 8 shows our testbed configuration. The testbed is built in the lab environment that simulates a real next generation Internet. It is made of five network domains with four autonomous systems (ASs) and has eight routers: one Cisco 7507 router, four Linux-based routers [22], two FreeBSD-based routers [23], and one Fore Powerhub. Three domains (domain 1, 2, and 4) are IPOA clouds, domain 3 is fast ethernet cloud, and domain 5 is Ethernet cloud. Four domains (domain 1, 2, 3, and 4) support Diff-Serv model. Each border router runs BGP4. Our proposed QoS Management System runs in domain 1, 2, 3, and 4.

Our initial target application service is Virtual Private Network (VPN). Users can setup a VPN by using our proposed QoS Management System and monitor the provisioned QoS. Both intra-domain provisioning and inter-domain provisioning is possible. When an unexpected problem occurs such as performance degradation can generate a trouble report which initiates a trouble resolution process.

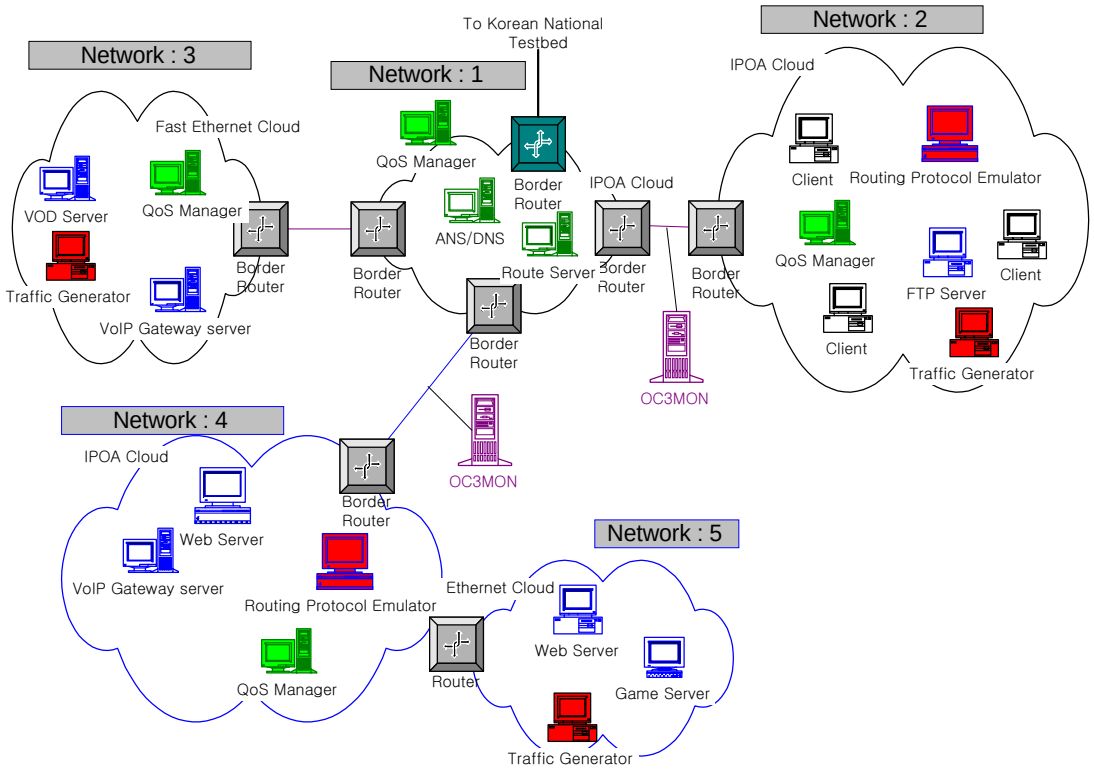

Figure 8: Our Testbed Configuration

5. Summary and Future Work

In this paper, we proposed an architecture of seamless end-to-end QoS Management System and described the design principles and system components of our developing prototype system. It is based on the TMN architecture for the overall management framework, TMF's SMBPM for automated workflow process integration, IETF's PBNM for QoS provisioning, and IETF's RTFM for QoS performance monitoring. We extended the existing models to provide an integration solution. For the system's scalability, object-oriented technology is adpated for the integration of the service management and the network management. For reliability and security, COPS protocol is used to convey security sensitive network provisioning information between the network manager and the network elements. For user friendliness, Jave-based web user interface is provided.

Our developing prototype system is at the beginning stage and requires lots of additional extensions. It currently covers QoS-based service provisioning and monitoring aspects. We need to consider QoS-based routing management aspect and more. It deals with Diff-Serv based network only and have to extend to cover RSVP network as well. Once a proof-of-concept implementation is completed, the system's reliability and performance has to be evaluated.

Acknowledgment

The work reported in this paper is supported by the Ministry of Information and Communication of Korea.

References

[1] TMF, http://www.tmforum.org.
[2] NMF, A Service Management Business Process Model, 1995.
[3] G. Waters, J. Wheeler, A. Westerinen, L. Rafalow, R. Moore, "Policy Framework Architecture," Internet Draft, Mar. 1999.
[4] Internet2, http://www.internet2.org/qos/qbone.
[5] Geoff Huston, ISP Survival Guide: Strategies for Running a Competitive ISP, Wiley, 1999.
[6] S. Blake, D. Black, M. Carlson, et., "An Architecture for Differentiated Services, Internet Draft, Oct. 1998.
[7] IETF, "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification, RFC2205, Sep. 1997.
[8] C. Rigney, et al, Remote Access Dial In User Service, Internet Draft, Feb. 1995.
[9] C. Finseth, "An Access Control Protocol, Sometimes Called TACACS", RFC 1492, Jul. 1993.
[10] N. Brownlee et al, "Traffic Flow Measurement: Architecture", Internet Draft, Jun. 1999.
[11] Cisco, http://www.cisco.com/warp/public/732/netflow/.

[12] ITU-T Recommendation M.3010, “Maintenance: Telecommunications Management Network”, Oct. 1992.
[13] OMG, “The Common Object Request Broker: Archtecture and Specification”, Revision 2.2, Feb. 1998.
[14] J. Boyle, “The COPS (Common Open Policy Service) Protocol”, Internet Draft: draft-ietf-rap-cops-03.txt, 1998.
[15] TMF, http://www.tmforum.org/smart.
[16] NMF, “Ordering SP to SP Interface Business Agreement”, NMF 503, SMART Ordering Team, Jul. 1997.
[17] NMF, “Customer to Service Provider Trouble Administration Requirement Specification”, NMF 501, SMART Trouble Administration Team, Aug. 1996.
[18] NMF, “Customer to Service Provider Performance Reporting Requirement Specification”, 1995.
[19] F. Reichmeyer, K. Chan, D. Durham, R. Yavatkar, S. Herzog, et al, “COPS Usage for Policy Provisioning”, Internet Draft, Feb. 1999.
[20] F. Baker, “Management Information Base for the Differentiated Services Architecture”, Internet Draft, Jun. 1999.
[21] A. Smith, D. Partain, J. Seligson, “Definitions of Managed Objects for COPS Protocol Clients, Jun. 1999.
[22] W. Almesberger, “Differentiated Services on Linux”, Internet Draft, Jun. 1999.
[23] A. Terzis, et al, "A Prototype Implementation of the Two-Tier Architecture for Differentiated Services", RTAS99, Vancouver, Canada.

최태상 (choits@etri.re.kr)
1995.12: Ph.D in Computer Network & Telecommunications, U. of Missori-Kansas City
1996.4 - 1998: Multimedia Communications Section, ETRI
1999 – Now: Internet Architecture Team, ETRI

Research Interests:
- Internet QoS Management
- Interactive Multimedia Service System
- Network, System, and Service Management

정윤희 (yhjung@etri.re.kr)
1990.2: 한양대학교 산업공학과 학사
1992.2. 한국과학기술원 산업공학과 석사
1992.3. - 현재: 한국전자통신연구원

주요관심분야:
- 차세대 인터넷 QoS 분야

손승원 (swsohn@etri.re.kr)
1984년 경북대학교 공과대학 전자공학과 졸업(학사)
1994년 연세대학교 산업대학원 전자전공 졸업(석사)
1999년 충북대학교 컴퓨터공학과 졸업(박사)
1991년 8월 ~ 현재 한국전자통신연구원 인터넷구조팀장

주요관심분야:
- 차세대인터넷
- QoS 보장 기술
- 라우팅 구조 및 알고리즘
- 인터넷 네트워킹