The Multi-layer VPN Management Architecture

E.C. Kim, C.S. Hong, J.G. Song
Telecommunications Network Laboratory, Korea Telecom
463-1 Junmin-dong, Yusung-gu
Taejon,
Korea
{agafe,hongcs,songjg}@kt.co.kr

Abstract

This paper proposes management architecture of multi-layer Virtual Private Network over the broadband network that will play an important role at the initial stage of broadband era. To provide flexible management capabilities with the administrator of the VPN, we adopt layering concept and abstraction mechanism to give a simple view of the real connection at service management level. The multi-layer VPN management architecture we propose includes concept of Customer Network Management for subscriber's control capabilities of their own VPNs, and the information / computational model of VPN with emphasizing layering concept based on ITU-T G.803 and G.805. In addition, some advanced multi-layer VPN features and generic bearer connectivity model are presented. We also outline our early experiences about the implementations of the proposed VPN management architecture based on Common Object Request Broker Architecture and web technologies.

Keywords

Multi-layer VPN, Management architecture, Layering concept, Bearer connectivity, CORBA, Web based CNM.

1. Introduction

At the stage of introduction of the broadband network services, it is expected that broadband Virtual Private Network (VPN) service will play an important role for end customers and telecommunication service providers because it will provide cost-effective and high quality communication capabilities. Unlike "VPN" in Public Switched Telephone Network (PSTN) or Internet paradigm, the first core functionality of the broadband VPN is provisioning of required bandwidth and its flexible management. Therefore the ultimate purpose of the VPN service and its management aspects should be focused on the basic problem such that "How can provide the information transfer capabilities of the VPN connectivity and its management capabilities". This problem relates to the management activities such as design, planning and configuration of VPN connectivity. However due to the complexity of broadband networks, these management activities are not likely to be simple but require more sophisticated management architecture.

To identify and explain such management architecture of the broadband VPN, our approach adopts the layering concept as described in ITU-T G.803 [1] and G.805 [2] to control and manage the VPN connections. ITU-T G.803 and G.805 addresses an essential network model with well defined architectural components based on layering and partitioning concept to simplify and make generic transport capabilities. Because broadband networks are generally multi-layer basis, this layering concept is also useful to address the broadband VPN management architecture. An abstraction methodology for the real transport network resource from the viewpoint of service management level is used to support this layering concept in our approach. Using this abstraction mechanism at service management level, end to end connection across a layer network is abstracted as a generic bearer connectivity that has capability to give the abstract view and status of the VPN connectivity. With considering of these layering concept and abstraction mechanism, this paper proposes efficient management architecture for multi-layer VPN service that enables a VPN administrator to care only specific layer network in the VPN. The proposed VPN management architecture includes ;

- information and computational models for multi-layer VPN management with the generic bearer connectivity model using abstraction at service management level,
- configuring mechanism of VPN connectivity on a specific layer network and its view,
- efficient mechanism to configure the VPN over multiple subscriber domains,
- and customer control capabilities of a VPN using Customer Network Management (CNM) concept.

The remainder of this paper is organized as follows. Section 2 outlines simple description for the concept and benefits of multi-layer VPN, and gives some advanced features for a VPN. In section 3, Information and computational models with the bearer connectivity model for a multi-layer VPN management using object-oriented design method is described. An explanation for early implementation of the proposed VPN management architecture and applied technologies is given in section 4. Finally, section 5 summarizes the experiences we gained during the development and design phase of this work.

2. Multi-layer VPN

Generally, the concept of broadband VPN service which results in a virtually configured participants' own network. has been recognized as management capabilities for end to end communications among distributed members of pre-organized group or subscribers over public broadband network. In this general understanding, we can find several management elements for a broadband VPN.

The first element that should be managed is related to the identification of a specific VPN itself among many others in public network. This means that a VPN can be identified using a unique VPN identifier. In general, a specific VPN identifier and its administrator who has rights to modify or configure the specific VPN can be decided at subscription phase by public VPN service provider.

The second thing is the configurable element, a VPN member from the viewpoint of configuration management (at the service management level) that is geographically distributed. A VPN member can be a specified physical port of a Customer Premise Network (CPN) or a Customer Premise Equipment (CPE) attached to the public broadband network. In the both cases, the specified physical ports of a CPN or a CPE have network addresses that are used in the provisioning of connections between them. As a result, registering these VPN members in a VPN allows the VPN administrator to make a connection between them. Furthermore one VPN member can be registered in the multiple VPNs over different subscriber domains because a VPN can be configured over multiple subscriber domains. The simple case can be found in federated broadband VPN for business alias between different corporations (or business units) as depicted in Figure 1. Such a VPN over multiple subscriber domains requires different mechanisms for control and monitoring because it covers different management authorities. In this case, a subscriber who owns a VPN member should export the permission rights to the other subscriber who wants to share this exported VPN member. Exporting permission rights to the other subscriber means that the VPN member has the attribute, which allows other subscribers to make a connection using it. For example, exporting a VPN member "A" on a subscriber "X" domain to the other subscriber "Y" allows a subscriber "Y" to get the permission to make a connection using the VPN member "A". This mechanism, so called "permission exporting" will be described more in next section.

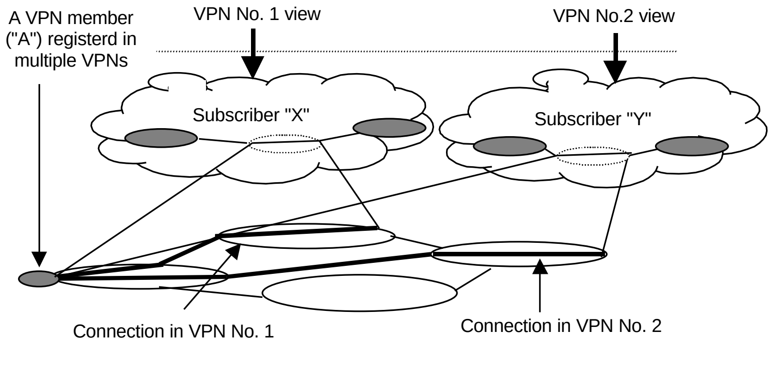


Figure 1: Abstract view for each VPN and VPNs sharing a VPN member

Finally, the element to be managed is a connection between VPN members. The connection that can be configurable, of course, makes a VPN complete and it can be existed on any layer network. Because the assumption that the broadband networks are based on multiple network layers is reasonable, a configurable connection in a VPN may be on ATM Virtual Channel (VC) layer, Virtual Path (VP) layer or even Frame Relay layer. Therefore, the layering concept as in ITU-T G.803, G.805 can be applied to these VPN connections on the different layer networks so that the VPN administrator can configure the VPN connection of each layer network separately. To do this, the VPN service provider should provide the each layer network view to the VPN administrator because a connection of the server layer (e.g., ATM VP layer) network must be configured a priori in order to configure the connection on the client layer (e.g., ATM VC layer) network. For example, to configure a ATM VC layer trail, the VPN administrator has to configure a VC port and a VC link a priori. In this case, the VPN administrator requests to configure a VC port and a VC link to the VPN service provider and then he/she can request to setup a VC trail upon the configured VC port and link using abstracted VC layer view (See Figure 2) as a partial of multi-layer VPN. In the same manner, to configure end to end VP layer trail, the VPN administrator only request to setup VP trail with VP layer view including VP ports and VP links (where a VP link is equivalent to a physical connectivity at User Network Interface).

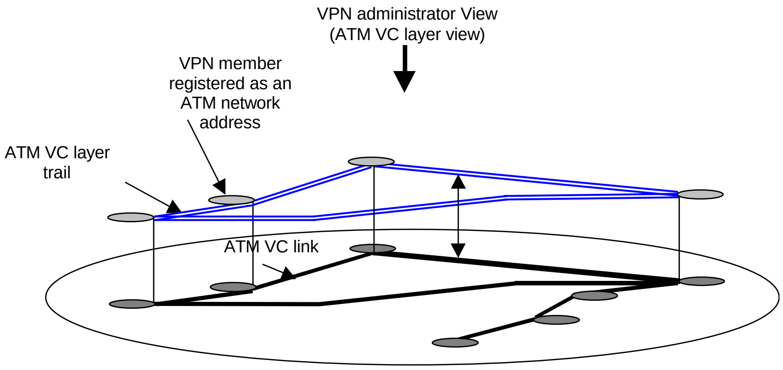


Figure 2 : ATM VC layer view of multi-layer VPN

Using this approach that adopts layering concept in the broadband VPN service management, we can get several useful aspects. First, the VPN administrator cares only the characteristics of the specific layer network connection that originally he/she intended so as to configure, monitor, and plan simply and easily. For example, in the case that the legacy data connections on VP layer and the real time connections on VC layer are mixed in one VPN, the VPN administrator can get VP layer view or VC layer view separately. This enables the VPN administrator to modify, reconfigure the layer network easily with the configured topology including trail, link, link termination point (LTP), traffic and fault information related to specific layer network.

However, as is often the case, if the VPN administrator wants to view and plan entire layer networks, then the public VPN service provider should give the integrated layer network views for his/her own VPN. Using these layer network views as the second useful point, the VPN administrator can request to modify bandwidth from the physical layer network (e.g., DS3 physical links) to the top layer network (e.g., ATM VC layer) so that he/she can plan or modify his/her own VPN. An integrated layer network view of a multi-layer VPN as shown in the Figure 3 depends on the ITU-T G.803 and G.805 layering concept.

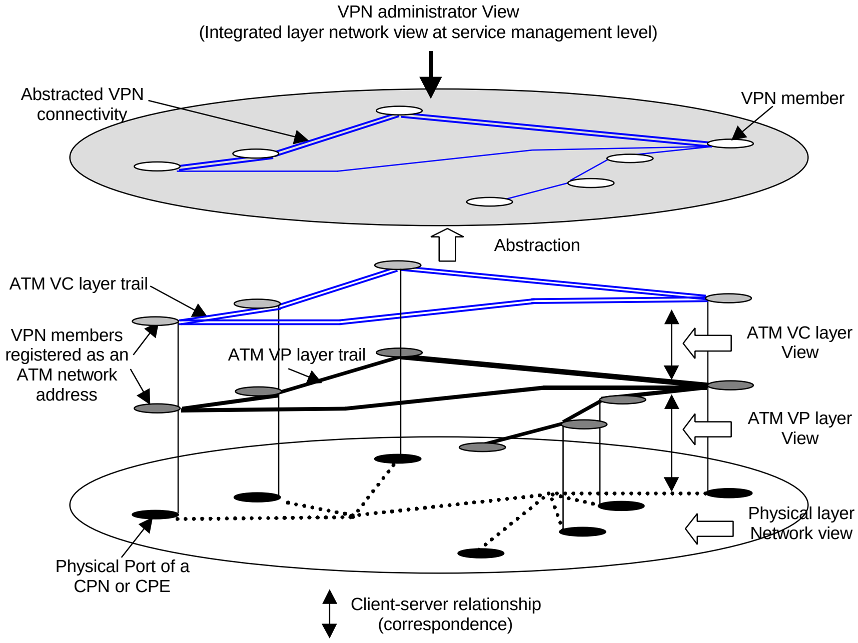

VPN administrator View
(Integrated layer network view at service management level)
Abstracted VPN connectivity
VPN member
Abstraction
ATM VC layer trail
VPN members registered as an ATM network address
ATM VP layer trail
ATM VC layer View
ATM VP layer View
Physical layer Network view
Physical Port of a CPN or CPE
Client-server relationship (correspondence)

Figure 3 : Layer network view for Multi-layer VPN

3. Modeling of multi-layer broadband VPN

For the developing the management model of multi-layer VPN, we adopt the information and computational viewpoints of the five Reference Model of Open Distributed Processing (RM-ODP) viewpoints [3], [4]. The information model from the information viewpoint of RM-ODP gives the management information view of entire multi-layer VPN model, resulting in the definition of VPN member and generic bearer connectivity that is used as an abstraction of VPN connection on different network layer. The computational model describes the components for the control and monitoring management information based on the information model. At the stage computational modeling, CNM concept defined in [5] and [6] is also refered. However, at this work, CNM ability is used for highlighting customer control capabilities for a VPN. Reference [7] and [8] gives the detailed description and research activities of CNM for a broadband VPN for custom control abilities.

3.1. Information Model

The multi-layer VPN basically consists of information objects that are managed by the VPN administrator. Figure 4 shows these configurable information objects such as VPN member, VPN Network Flow End Point (NFEP) and VPN Network Flow Connection (NFC) and their relationships using Rumbaugh's Object Modeling Technique (OMT) notation [9].

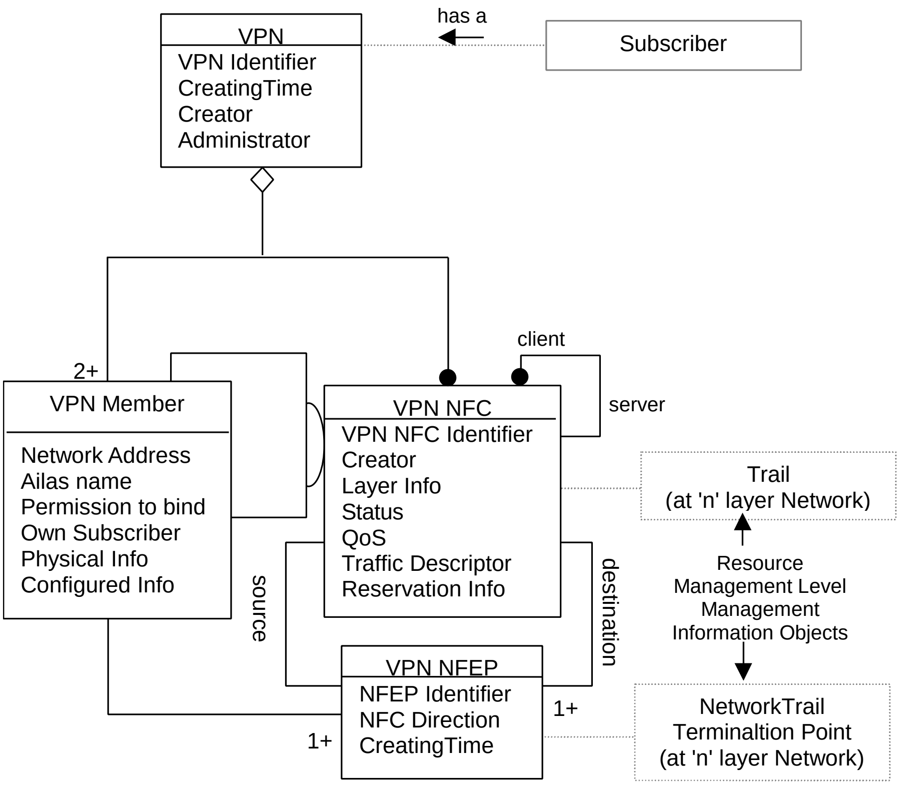


Figure 4 : Information Model of the multi-layer VPN

Some of information objects including a VPN itself with a public network-wide unique identifier and VPN Members are created (at the instance level) when the customers subscribe to the VPN service provider with a contract using VPN service. Because one subscriber can have multiple VPNs, whenever a customer created his/her own VPN, these information objects are newly created. After this subscription phase, a VPN consists of some other information objects at the step for configuring VPN by a VPN administrator.

The VPN member as discussed in the previous section, identifies an end point of that layer network, thus means a network address. Note that the VPN member is an abstract model of the physical port of a CPN or a CPE which connects to the port of edge Network Element (NE) via User Network Interface (UNI). Therefore it is logically viewed as T_B point between B-NT1 and B-NT2 from the viewpoint of B-ISDN reference model and has other attributes which represent the physical layer information (e.g., SDH, DS1/3 characteristics) of the port and the configured information. The attribute, "Configured Info" represents, for example, maximum number of VPC/VCC, maximum VPI/VCI bits (most of these items can be derived from standard Management Information Base for CNM purpose, see [5] and [10]) in the case of using ATM.

In addition, the VPN member has another attribute, "Permission to bind" that is used to "permission exporting" mechanism as addressed in the previous section. For the "permission exporting" mechanism, this attribute is designed to represent its owner's (i.e., subscriber's) agreement so that the other subscriber can make a connection using this VPN member. So, this attribute has information such as the identifier of the subscriber who has permission to make a connection using this VPN member and the traffic descriptors / Quality of Service (QoS) parameters of the connection that can be terminated at this VPN member. Therefore, once the owner of the VPN member writes these values, the other subscriber can make a connection to this VPN member under the limitation as represented in these attribute values. The description of this attribute using Object Management Group (OMG) Interface Definition Language (IDL) syntax is as follows ;

```
typedef    string       subscriberId_t;
struct     trafficDescriptor_t {
           atmTd_t      forwardAtmTd;
           atmTd_t      backwardAtmTd;
           frTd_t       forwardFrTd;
           frTd_t       backwardFrTd;
};
struct     qosParameter_t {
           short        forwardQos;
           short        backwardQos;
};
struct     permissionToBind_t {
           subscriberId_t          permittedSubscriber;
```

```
          trafficDescriptor_t   permittedTd;
          qosParameter_t        permittedQos;
};
typedef   sequence<permissionToBind_t>          permissionToBindList_t;
interface vpnMember {
          attribute permissionToBind_t   permissionToBind;
          // other attributes and operations
};
```

The VPN NFC models the generic bearer connectivity which is an abstraction of real layer network resources to make information flow between information source and sink points from the viewpoint of service management level. The VPN NFC can be mapped into the trail in a specific layer network domain from the viewpoint of network resource management. On the other hand, because it has service concept, it can be viewed as a committed contract to use network resource between public network provider and subscriber. Thus, the VPN NFC has attributes to express characteristics of the contract for connection, which are traffic descriptor and QoS parameter and so on. In our modeling, the VPN NFC has attribute "Layer Info" which represents mapping relationship between VPN NFC and its correspondent network resource information object at network management level. For example, in the case that a specific VPN NFC is abstraction of ATM VC layer trail, "Layer Info" attribute of that VPN NFC keeps the identifier of VC layer trail and its link.

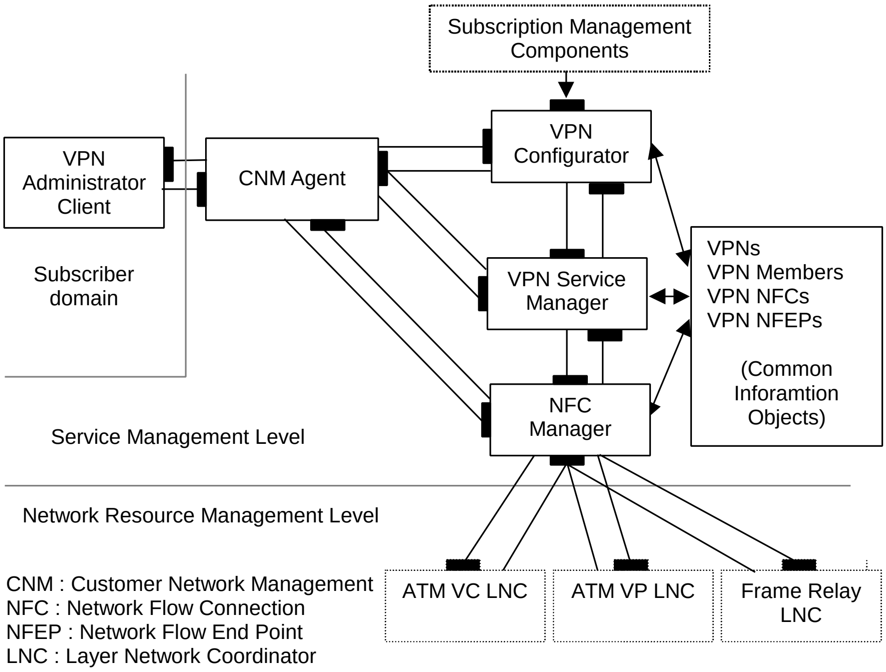
The VPN NFC's ending points are modeled as a VPN NFEP in our approach. The VPN NFEP can be either a source or consumer for information flow and its view from resource management may be mapped to network trail termination point. For the point to point ATM VC connection, there are two VPN NFEPs at each source and destination port (VPN member), and their identifiers ("NFEP Identifier") are simply VPI/VCI or DLCI (Data Link Connection Identifier) values. Because the VPN NFEP has meaning of binding information between public network-side network resource and its termination at customer's network access point, its instance is created at the specific VPN member whenever the connection (i.e., VPN NFC) is made between two VPN members.

3.2. Computational Model

The computational model of the multi-layer VPN illustrates the entire system's structure so as to make our approach for functional aspects visible. These functional aspects, which are based on Telecommunication Information Networking Architecture (TINA)'s separation concept [11] between access and service core, are classified into 3 categories.

The first category is responsible for access capability to the service core logic. The second is responsible for a multi-layer VPN logic itself. Final category has a role for selecting and mapping the multi-layer VPN information objects at service management level into the resource management level information objects. With this guiding principle in the design of the computational model, several computational objects are defined. These objects are VPN Administrator Client, CNM Agent, VPN Member Configurator, VPN Service Manager, and NFC Manager as shown in Figure 5.

In the first category, VPN administrator Client and CNM Agent objects are defined. CNM have been already well described in the standardization organization [5], [12], [13] and various papers [14], [15] and its concept is widely accepted for customer control capability of their own private network. Especially recent studies [7] and [8] have emphasized the control ability than the traditional approach which limits the customer's ability to the monitoring only. Our approach also adopts the concept for granting rights to control their network resources through the computational objects at the service management level. Therefore a specific VPN administrator with use of VPN Administrator Client object can request connection setup, release and monitor the VPN status via CNM Agent computational object in the network side. CNM Agent performs these functions per subscriber basis while the other components do not.



CNM : Customer Network Management
NFC : Network Flow Connection
NFEP : Network Flow End Point
LNC : Layer Network Coordinator

Figure 5 : Computational Model of the multi-layer VPN

The VPN Configurator and VPN Service Manager computational objects are defined for the responsibility in the second category. The VPN Configurator computational object has computational interfaces for creating a new VPN information object in the public broadband network, assigning an unique VPN identifier, setting the related attributes and initializing information objects whenever a new VPN is created. The VPN Service Manager computational object performs most of VPN service logic. It registers/de-registers VPN members in the multi-layer VPN, validates rights to use VPN members in the different subscriber's VPN, and checks whether the requests from subscriber domain are affordable for subscription parameters.

The composition of selecting and mapping relationship between service management level information objects and resource management level information objects is NFC Manager computational object's role. Thus, requests for establishing/releasing/modifying VPN connections from the VPN Service Manager computational object (of course, it is originally issued from the VPN Administrator Client object and passed CNM Agent object) are performed at NFC Manager to create/delete/modify VPN NFC and VPN NFEP information objects. The NFC Manager object also has responsibility to find the proper layer network and to exchange information to/from related Layer Network Coordinator (LNC) objects that reside in the resource management level in order to monitor/control end to end VPN connections. The LNC computational object on the basis of TINA's network resource management concept [16] has a responsibility to cover and coordinate the entire specific layer network. Please refer to [16] and [17] for detailed information for LNC and its architecture.

4. Implementation

For the realization of the multi-layer VPN management architecture we proposed, a Common Object Request Broker Architecture (CORBA) Object Request Broker (ORB) [18] implementation is used as a middleware. The CORBA have been known as a well defined distributed object-oriented methodology for integrating distributed system components. We use IONA's Orbix 2.x for CORBA ORB products and Orbix Names which is complying to Common Object Service Specification (COSS) naming service specification [19]. We also use Internet Inter-ORB Protocol (IIOP) to guarantee interoperability for communicating between all CORBA components.

Web technologies (based on Microsoft's Internet Information Server 3.0 with Active Server Page capability and some Active-X based control objects) are used also for CNM implementation. Recent web technologies such as direct interfaces between Database Management System and web server and server side scripts can provide capability of migration from static HyperText Markup Language (HTML) to dynamic one. Thus they can promote the programmable web interfaces resulting in giving more flexibility and easiness and these features are suited for customer control ability of a CNM system.

In addition, Information objects as described above are implemented by using an

Object-Oriented Database Management System (OODBMS) and CORBA adapter for OODBMS so that all information object implementations can be viewed as CORBA objects via transparent CORBA interfaces. For this purpose we used Object Store OODBMS and Orbix Object Store adapter so that all information objects acts as CORBA objects with persistency.

Especially, the shared common information object concept that is similar to TMN Shared Management Knowledge concept [20] is applied to implement these information objects. The shared common information object concept gives several benefits in reducing the number of information exchange between distributed computational objects, maintaining the integrated view of entire system's knowledge and getting ride of unnecessary operations to handle information integrity.

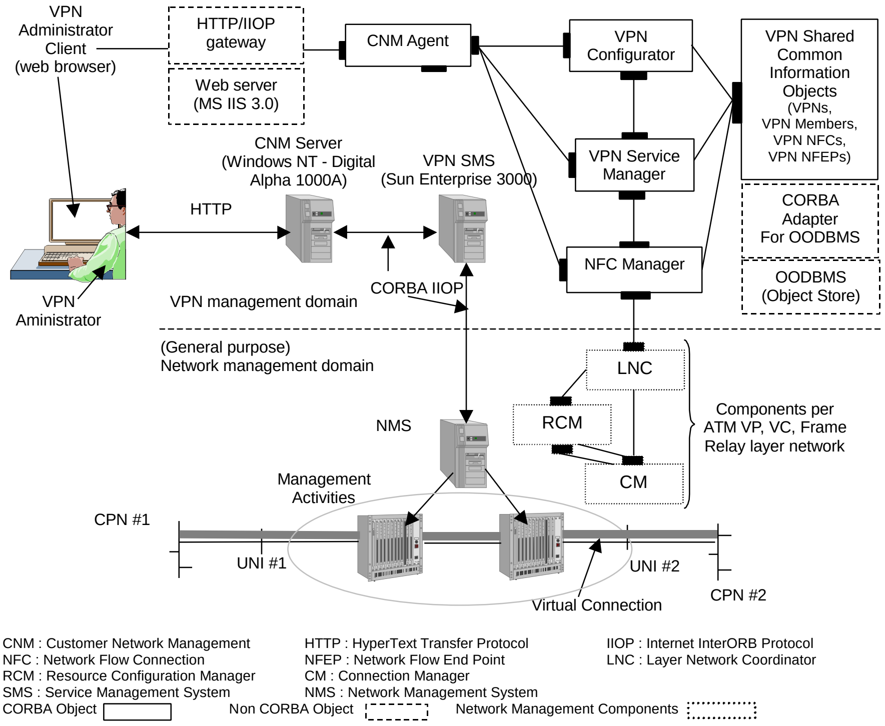

VPN Administrator Client (web browser)
HTTP/IIOP gateway
Web server (MS IIS 3.0)
CNM Agent
VPN Configurator
VPN Shared Common Information Objects (VPNs, VPN Members, VPN NFCs, VPN NFEPs)
CNM Server (Windows NT - Digital Alpha 1000A)
VPN SMS (Sun Enterprise 3000)
VPN Service Manager
HTTP
CORBA Adapter For OODBMS
NFC Manager
OODBMS (Object Store)
VPN Aministrator
CORBA IIOP
VPN management domain
(General purpose) Network management domain
LNC
RCM
CM
NMS
Components per ATM VP, VC, Frame Relay layer network
Management Activities
CPN #1
UNI #1
UNI #2
CPN #2
Virtual Connection
CNM : Customer Network Management
NFC : Network Flow Connection
RCM : Resource Configuration Manager
SMS : Service Management System
HTTP : HyperText Transfer Protocol
NFEP : Network Flow End Point
CM : Connection Manager
NMS : Network Management System
IIOP : Internet InterORB Protocol
LNC : Layer Network Coordinator
CORBA Object
Non CORBA Object
Network Management Components

Figure 6 : Overview of implementation for VPN management

Figure 6 gives an overview of key components used for the multi-layer VPN management system implementation. In VPN management domain, computational objects we designed such as CNM Agent, VPN Configurator, VPN service Manager, NFC Manager and Shared Common Information Object are implemented.

In network management domain, LNC component and other components such as Resource Configuration Manager (RCM) and Connection Manager (CM) are developed based on TINA Network Resource Architecture [17] and Connection Management Architecture [16]. Note that these components are existed per specific layer network (For example, ATM VC LNC, VC RCM, VC CM components are responsible for ATM VC layer and VP LNC, VP RCM, VP CM components are responsible for ATM VP layer).

5. Conclusion

The layering concept and abstraction mechanism for broadband VPN management has some important benefits. First, it is much simpler to plan, configure each layer network separately in the VPN than all transport capabilities are managed in one VPN as a whole. This feature, of course, is resulted from the architectural viewpoint (i.e., a layer network is able to have its own operation abilities) as addressed in ITU-T G.803 and G.805. The second benefit is that it is possible to change a layer network in a broadband VPN without much consideration about affecting other layer networks because each layer network connection can be defined independently of the others. In addition, usefulness like these is stimulated by the integrated layer network view of the broadband VPN by using abstraction mechanism we proposed. This abstracted mechanism enables for the VPN administrator to picture out all the alternatives of the VPN topology at that layer network. The "permission exporting" feature also gives some advanced feature for configuration of the broadband VPN over multiple subscriber domains.

However, the aspects of operation and maintenance, including trouble reporting of fault and Service Level Agreement (SLA) of performance are not much considered in this work. Features such as handling fault recovery and monitoring SLA parameters is critical issues to the VPN administrator and the VPN provider. In the current our VPN management system prototype, the ability of the system to process a large number of transactions is not carefully handled. However, because this capability for scalable management in public networks is essential to support high rates of operation requests, we are studying on this issue.

References

[1]. ITU-T Recommendation G.803, "Architectures of transport networks based on the Synchronous Digital Hierarchy (SDH)," March 1993.

[2]. ITU-T Recommendation G.805, "Generic functional Architectures of transport networks," November 1995.

[3]. ITU-T Recommendation X.902, "Information technology - Open Distributed Processing ? Reference Model : Foundations," November 1995.

[4]. ITU-T Recommendation X.903, "Information technology - Open Distributed Processing ? Reference Model : Architecture," November 1995.

[5]. ATM-Forum af-nm-0019.000, "Customer Network Management (CNM) for ATM Public Network Service (M3 Specification)," Revision 1.04, October

1994.

[6]. GR-1117-Core, "Generic Requirements for Phase 1 Exchange PVC CRS Customer Network Management Service," Issue 1, June 1994.

[7]. M.C.Chan, A.A. Lazar and R. Stadler, "Customer Network Management and Control of Broadband VPN Services," Proc. IFIP/IEEE International Symposium on Integrated Network Management, May 1997.

[8]. Jong-Tae Park, Jae-Hong Lee, and James Won-Ki Hong, Customer Network Management System for Managing ATM Virtual Private Networks," IEICE Trans. Comm. Vol. E80-B, No.6, June 1997.

[9]. James Rumbaugh, Michael Blaha, William Prmerlani, Fredrick Eddy and William Lorenson, "Object-Oriented Modeling and Design," Prentice Hall, 1991.

[10]. IETF RFC 1695, "Definitions of Managed Objects for ATM Management, Version 8.0 using SMI v2," August 1994.

[11]. TINA-C baseline, TB_MDC.012_1.3_94, "Definition of Service Architecture," November 1994.

[12]. ITU-T Recommendation X.160, "Architecture for Customer Network Management Service for Public Date Networks," October 1996.

[13]. NM-Forum FRF.6, "Frame Relay Customer Network Management Implementation Agreement," March 1995.

[14]. Jacqueline Aronsheim-Grotsch, "Customer Network Management : CNM," Proc. IEEE/IFIP Network Operations and Management Symposium, April 1996.

[15]. M. Hinchliff and N.Cook, "Customer Network Management and ATM Networks," Proc. IEEE/IFIP Network Operations and Management Symposium, April 1996.

[16]. TINA-C baseline, TB_JJB.005_1.3_94, "TINA Connection Management Architecture," January 1995.

[17]. TINA-C baseline, NRA_v3.0_97_02_10, "TINA Network Resource Architecture Ver 3.0," February 1997.

[18]. OMG, "The Common Object Request Broker : Architecture and Specification," Revision 2,0, July 1995.

[19]. OMG, "CORBAservices : Common Object Services Specification," Revised edition, March 1995.

[20]. ITU-T Recommendation M.3010, "Principle for an Telecommunication Management Network," January 1996.

Biography

Eun Chul Kim is a member of technical staff for the broadband networking system at Telecommunications Netowork Lab, Korea Telecom. Since joining Korea Telecom in 1993, he has been working for the broadband networking system design and its control architecture and is currently developing integrated CNM system. His research interests includes open service control and management for broadband network, distributed object processing such as CORBA, DCOM and Web based management. He has B.S in electronic engineering from Yonsei University in 1990 and M.B.A in management science from GSMIS, HUFS in 1993.

Choong Seon Hong received his B.S., M.E. in electronic engineering from Kyung Hee University, Seoul, Korea, in 1983, 1985, respectively. In 1988 he joined Korea Telecom, where he worked on N-ISDN and Broadband Networks as a member of technical staff. He received the Ph.D. degree at Keio University in March 1997. He is now working for Telecommunications Network Lab, Korea Telecom as a senior member of technical staff. His research interests includes the service networking architecture on distributed processing environment, fault-tolerant process management for distributed objects and mobility services between heterogeneous networks.

Joong Goo Song received his B.S., M.E., and Ph.D in electronic engineering from SungKyunKwan University, Seoul, Korea, 1979, 1987 and 1995, respectively. From 1980 to 1983, he had worked in ETRI (Electronic & Telecommunication Research Institutes), Korea. In 1984 he joined in Korea Telecom, where he has worked of networks management system development for POTS and data networks in Korea Telecom. He is now working for Telecommunications Network Lab, Korea Telecom as a principal member of technical staff and a director of data networking team. His research interests include QoS management for multimedia networking services, distributed objects technology & distributed management, ATM/IP management for multi-layered networks and traffic management.