濟州大學校 産業技術硏究所 論文集, 第9卷, 1號, pp.110~120, 1998. 6
Cheju National Univ. R.I.I.T. Jour., Vol.9, No.1, pp.110~120, 1998. 6

VPN 관리를 위한 망관리 구조*

송 왕 철** · 김 장 형**

An Architecture for the VPN Service Management

Wang-Cheol Song** and Jang-Hyung Kim**

ABSTRACT

These days the VPN services are provided on basis of the bandwith contracts rather than through leased lines. They require the network managment capabilities. In this paper, hence, an architecture for the VPN service management is proposed on the basis of the structural considerations using the TMN concept. In addtion, the distributed processing technologies are introduced for implementing the architecture. The management architecture for VPN services may be composed of domains for customers and VPN service providers and public network operator/provider, and the domains can be managed via the TMN X interface. Hence, the architecture is modelled hierarchically. It is based on the structuring rule of partitioning and layering on ITU-T G.803 recommendation. On the architecture, the management operations via the X interface can have been performed efficiently by introducing the X.500 directory service and the ODP Trader.

Key words : CTN, VPN, TMN, X.500, Trader, Manager, Agent, X interface

Ⅰ. 서 론

오늘날 많은 기업들은 분산된 기업내의 통신을 위하여 통신 사업자의 전송장비를 임대하여 그들 자신의 사설 통신망을 구축해 왔다. 그러나 기업이 사설 통신망을 구축하여 운용하는 일은 단순하면서도 어려운 일이었다. 비용측면에서 볼 때 일반적으로 전송장비를 소유하거나 임대하는 데는 많은 비용이 들고 회선구성도 두 지점간에는 비교적 쉽지만 여러 지점간을 연결하는 경우는 매우 어려운 과정을 필요로 한다. 통신망의 설계 측면에서도 기업의 사설망 운용자는 각 지점의 통화량과 필요한 통신망 운용요원을 예측해서 최소의 비용으로 최대의 효과를 얻는 망 구축을 해야하는 노력이 따르게 되며, 규모가 큰 기업체일 경우는 시설과 운용요원이 많이 필요하기 때문에 이 부분을 특히 고려해 왔다.

이와 같이 기업의 사설망 구축은 그 범위에 따라 어느 정도 비용이 들게 되므로 써 이용자들은 자연히 통신비용에 대해서 관심을 갖게 되었다. 통신사업자는 이러한 기업의 요구에 맞춰 여러 가지 사업용 통신 서비스를 제공하여 왔으며, 특히 "가상사설망"이라 불리는 서비스 개발을 추진해왔다. 가상 사설망

* 이 논문은 정보통신부, 정보통신정책 연구원 연구비 지원에 의한 것임(과제 번호:신연97-31)
** 제주대학교 정보공학과
Dept. of Information Eng., Cheju Nat'l Univ.

(VPN: Virtual Private Network) 서비스는 가입자 자신이 공중통신망 내에서 소프트웨어적으로 망을 정의하고 변경할 수 있기 때문에 통신망 변경 시에 물리적인 재구성이 필요 없으며 공중통신망을 이용하여 마치 가입자 고유의 사설 통신망을 소유하고 있는 것과 같은 효과를 주는 서비스이다.

가상 사설망을 구축할 때 기존의 PSTN이나 PSDN 망에서는 통신 요구 량에 알맞은 회선을 임대선으로 확보하므로 써 공중망에서의 사설망으로서의 효력을 나타낼 수 있도록 하고 있다. 그러나 근래에 와서는 가상 사설망 서비스에 관리기능을 더하므로 써 임대선에 의한 VPN 구성이 아니라 대역폭 계약 개념에 의해 공중망을 더욱 효율적으로 이용할 수 있도록 하는 가상 사설망 서비스 구조를 고려하고 있다.

실제로 가상사설망(VPN) 구축 시에 그 VPN 서비스 제공자는 고객들의 통신량 및 통신 특성들을 파악하므로 써 그 논리적 가상망에 서비스의 품질과 속도를 보장해야 한다. 이러한 것들을 바탕으로 하면 VPN 서비스 제공자와 공중망 운용자 사이에 가상 패스에 의한 대역폭 개념의 계약으로서 임대회선의 형태를 벗어난 VPN 구축이 가능할 수 있다[1].

그러므로, 본 논문에서는 그러한 가상사설망이 효율적으로 구축되기 위해 필요한 망관리 기능이 구축되어야할 구조에 대하여 제안하였다. 이를 위해 ITU-T 권고안 G.803에 근거한 분할과 계층화라는 개념을 도입하고, TMN의 계층화 개념과 조합함으로써, VPN 관리에 필요한 적절한 구조를 제안하였다.

II. 가상 사설 망 (VPN)

VPN 서비스는 고객에게 사설 망 연결기능을 제공하지만, 공중 스위칭 망자원을 통해 구현된다. 논리적인 통신자원과 공중 스위칭 망의 실질적인 자원과의 모든 맵핑 처리는 VPN 서비스 제공자가 처리-지원하며 이러한 모든 것은 VPN 고객에게는 투명하게 이뤄지게 된다. VPN은 공중망에서 지원되며, 점차 강화되는 고객의 사설망 요구사항, 예를 들어 망 운용에 대한 더 큰 제어권이나 낮은 비용, 보안 등의 요구사항을 실현 가능할 수 있게 한다. 이러한 특징

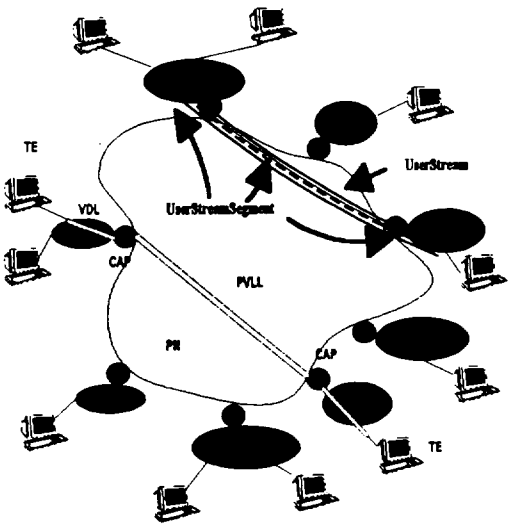

Fig. 1 a VPN model

- CPN : Customer Premises Network
- TE : Terminal Equipment
- CAP : Customer Access Point
- VDL : Virtual Direct Line
- PVLL : Public Virtual Leased Line
- SUG : Service User Group
- VPN : Virtual Private Network)

들을 가상망을 통해 제공하므로 써, VPN은 공중망 사용비용으로 기존의 사설망보다 더욱 큰 탄력성과 유연성을 가지게 된다. 서비스 공급자는 서비스 제공 방식을 고객의 요구에 맞출 수 있게 된다. VPN은 고객의 통신량을 크게 변화시키는 것에도 쉽게 맞춰나갈 수 있을뿐더러, 지리적으로도 넓은 지역에 분포되어 있는 여러 컴퓨터들을 서로 연결하는 서비스를 할 수도 있으며, 가상 사설망에 대한 모델은 Fig. 1에서 볼 수 있다[1].

2.1. VPN 자원 모델과 일반적 역할

2.1.1 자원들

초고속 망 고객에 의해 인식되는 가장 추상적인 레벨의 통신자원이나 설비들은 자기와 관련된 관리시설들을 가지고 있으며 이러한 설비들은 Fig. 2에서와 같이 나타낼 수 있으며 그 요소들은 다음과 같다.

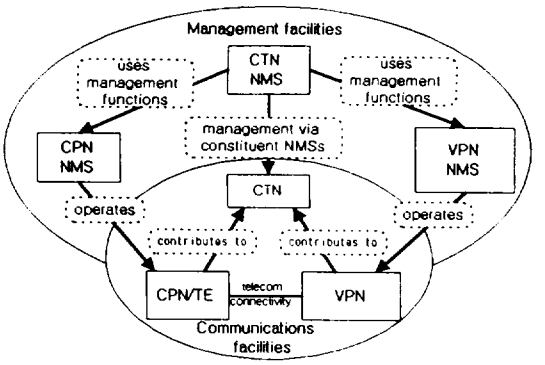

Fig. 2 CTN resources of VPN services

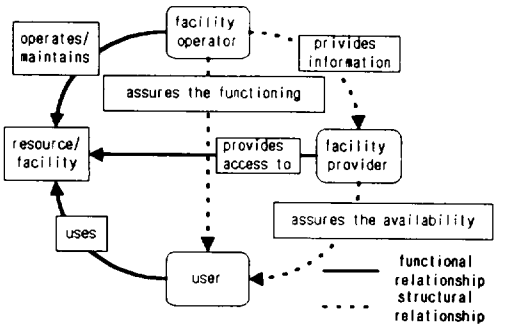

Fig. 3 Generic entities and their relationships

- CTN : 고객 조직체에 속해 있거나 지원하면서, 종단 사용자 서비스들을 제공하는 종합통신 하부구조이다.(참고, CTN은 CPN과 TE, VPN으로 이뤄진 가상 개체이다. 그것의 주요역할은 CPN과 VPN의 이질적인 환경을 가로질러 종단간 관리를 하는 것과 관련 있다.)
- VPN : 공공 영역에 위치한 CTN의 일부분으로서 지리적으로 떨어진 여러 싸이트들을 연결하여 전체 CTN을 구성하는 일을 한다.
- CPN/TE : 단일 싸이트에 있는 통신 하부구조로서 좁은 범위의 지역에 대해 종단 사용자 서비스를 제공한다.

이러한 유형의 CTN 구성에 있는 초고속 망 VPN은, 종단 사용자 서비스에 비교해서, 하위 계층 통신 서비스를 제공한다. CTN NMS의 역할은 VPN NMS 관리 기능을 이용하여 개별적인 CPN NMS 관리 기능들을 통합하려는 것으로써, 연관된 모든 망들을 가로질러 종단에서 종단까지의 종단 사용자 서비스들에 대한 관리를 하려는 것이다.

2.1.2. 역할과 관계들

일반적인 자원들과 마찬가지로 사람으로서의 역할을 갖는 사용자와 운용자, 공급자와 같은 개체들의 일반적인 역할들에 대해서도 구별되어야 한다. 이들에 대한 차이점은 어떤 자원(CTN, VPN, CPN)에 대한 공급자와 운용자 사이에서 구분될 수 있다. 이러한 차이점은 인터페이스를 정의하는 목적을 지원하게 되는데, 이는 통신 서비스의 경우 ISDN의 U, S 참조점이나 X.25에서의 DCE와 같은 인터페이스를 정의하는 것과 통신망 관리의 경우에서 TMN X-인터페이스를 정의하는 것과 같이 그 역할의 차이에 따라 인터페이스 정의의 목적이 달라질 것이다.

관련된 조직체 개체 영역 내부에서의 일반적 개체들의 일반적인 역할은 Fig. 3에 나타나 있다. 종단 사용자 역할은 "사용" 관계를 갖는 자원에 연결된다. 구조적 관계는 운용자 역할에 종단 사용자 역할을 연결하므로 써 이뤄지는데, 이는 운용자가, 그 자원이 사용자의 수요에 따라 동작한다는 것을 확실하게 할 책임과 의무가 있다는 것을 뜻한다. 이 관계는, 종단 사용자가 제공자 역할의 존재를 인식할 수 만 있게 하는 방식을 통해 간접적이 될 수도 있다.

제공자 역할과 종단 사용자 역할 사이의 구조적 관계는, 공급자가 종단 사용자에게 제때에 맞춰, 합의된 요건 QoS로써 자원을 공급할 의무가 있다는 것이다.

2.1.3. Outsourcing

영역들에 있는 역할과 자원의 위치는 "outsourcing"이라는 말로 표현될 수 있다. 운용자가 그 자원과는 다른 영역에 위치한다면, 그것이 책임의 outsourcing이라는 경우이다. 반대로 자원이 제공자나 운용자와는 다른 영역에 위치해 있다면 그것은 "소유권 outsourcing"이라는 경우이다.

Fig. 4에서는 CTN에 있는 두 가지 유형의 자원을 보여주고 있는데, 역할들과 자원들 사이의 관계들에 대해 다음과 같은 유형들을 보이고 있다.

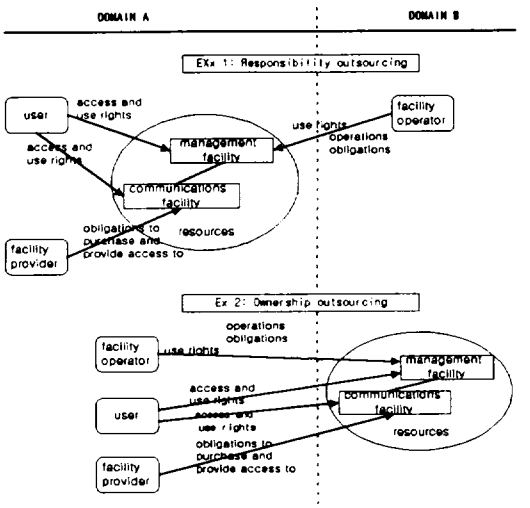

Fig. 4 Relationships between roles and resources in the CTN environment

- 사용(권)
- 구매 및 접근 제공(책임)
- 운용(의무)

또한 Fig. 4에서는 outsourcing의 두 가지 시나리오를 볼 수 있는데, 그림 상단에서는 책임 outsourcing의 예가 있다. 고객의 통신설비를 운용할 책임이 다른 조직체에 위치해 있는 것이다. 그림의 하단에는 소유 outsourcing의 예를 보이고 있는데, 고객에 의해 쓰이는 설비들이 개별 조직체들에 의해 소유되어 있고 고객 조직체에서는 이를 임대해서 사용하는 경우이다. 세 번째 예로서 종단 사용자가 영역 A에 그 역할만이 위치한 경우를 생각할 수 있는데, 이는 고객의 통신설비들과 관련 제공자/운용자 역할들 모두에 대한 outsourcing 상황이라 하겠다.

2.2. 정보 모델 정의

VPN 서비스 정보요건을 구현하는 정보모델은 다중 영역 위에 구현된다. VPN 서비스 레벨에서 이들은 VASP 영역이라 불리며, 고객의 여러 싸이트들에 퍼져 있는 많은 CPN 영역들로 이뤄져 있다.

VASP 영역에 모든 정보객체를 구현하기 쉽게 하기 위한 정보에 관점으로부터 여러 VASP 영역에 위에서 정의한 정보 객체들을 분산시키려면 여러 가지 요건들이 필요하다. 이러한 요건들은, 일부 정보들에 대한 제어권은 고객에게 남기면서, 동시에 어떤 관리 책임은 외부로 위탁하는 방식에 근거하게 된다. 그러므로 이러한 요건들에 따르면, 서비스 사용자 그룹 정보 객체는 VASP 영역에서 지원되어야 하는 반면, 단말 장비와 종단 사용자 객체들은 CPN 영역에서 지원되어야 할 것이다.

정보 관점은 또한 정보 객체의 위치에 대해 몇 가지 요건을 붙이게 되는데, 특히 VDL과 PVLL을 표시하고 관리하는 것에 대한 경우는, VPN 서비스 레벨에서, 실제 자원이 존재하는 영역에 그 객체의 위치를 자연스레 묶어 놓게 될 것이다. 그러므로, VDL은 CPN 영역에서 지원되는 반면, PVLL의 경우는, PVLL의 요소적인 자원들은 여러 다른 공중망 영역에 존재하므로, 이 공중망 영역들을 직접적으로 관리하는 VASP 영역에서 지원될 것이다. PVLL들의 종단점들은 PVLL 그 자신들과 같이 동일한 영역에 존재하므로, 고객 접근점 정보 객체 역시 VASP 영역에서 지원된다.

사용자 스트림은, 고객 요건에 의해 그 제어권이 다양한 레벨의 outsourcing과 직접 제어 방식들로 조합되어 있기 때문에, 사용자 스트림 정보 객체는 CPN과 VASP 영역 모두에 의해 지원된다. 이로 인해 이 정보 객체에 의해 표현되는 자원들은 그 관리에 있어서 유연성을 부여받는다. 이러한 유연성은 기본적으로, 사용자 스트림에 연관된 종단간 정보가 VASP 영역에서 중앙집중형태로 관리되느냐 아니면 CPN 영역들에 의해 좀더 분산된 형식으로 관리되느냐 하는 방식들 간의 차이에서 온다.

실제 정보 모델은 여러 가지 정보 객체들과 그들을 적절히 여러 영역들로 분산시켜 놓은 것을 그대로 반영하게 된다. Fig. 5는 관리 객체 클래스들에 대한 포함 트리를 보이고 있고, Fig. 6에서는 상속 트리를 볼 수가 있다[1].

고객 정보 객체는 특정 고객에 관련되는 다른 MO들 모두를 포함한 customer MO와 접속 및 서비스 프로필에 대한 정보를 담고 있는 customerProfile MO로 나누어져 있다. CPN 영역과 VASP 영역들로 정보 객체들이 분산된 것을 반영하기 위해, 포함 트리에서 정보 모델의 나머지를 두 개의 하부 트리로

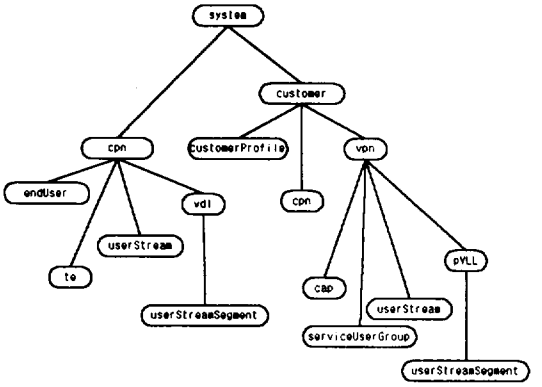

Fig. 5 Containment Tree

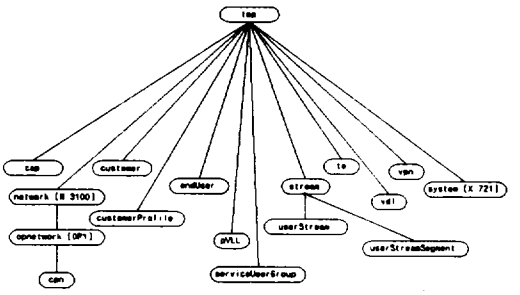

Fig. 6 Inheritance Tree

나누어 놓았다. cpn MO가 포함하고 있는 MO들은 CPN 영역에 있는 객체들인 반면, vpn MO에 포함된 하부 트리는 VASP 영역에 속한 것들이다. cpn MO는 또한 그 싸이트의 접촉과 서비스프로필에 관한 정보를 포함하고 있다.

위에서 언급하였지만, userStream MO는 CPN과 VASP 영역 모두에 포함되어 있다. 추가된 MO인 userStreamSegment는 단일 영역 내부에 있는 사용자 스트림에 필요한 자원들을 표시한다. 사용자 스트림은 PVLL과 VDL에 의해서 규정된 경로 상에서만 셋업될 수 있기 때문에 userStreamSegment는 PVLL과 VDL에서 사용 가능한 자원들만을 이용한다. 그러므로 userStreamSegment가, 이것이 이용하는 자원들인 VDL과 PVLL MO 내에 포함되면, 이들 자원들의 할당이 쉽게 관리될 수 있다.

하지만, 단일 사용자 스트림에 대하여, userStream MO를 단지 하나만 인스턴스화 하더라도 그 사용자 스트림의 종단간 특성에 대하여 이 MO는 자세한 정보를 모두 포함하고 있다. 만일 사용자 스트림 관리에 대한 중앙 집중식 접근법이 적용된다면, 통신경로에 대하여 사용자가 요청하게 되면 이는 바로 VASP 영역에 있는 userStream MO를 생성해내게 될 것이다. 공중망과 CPN을 가로질러 있는 자원들에 대한 관리는 관련영역(각 VASP와 CPN 영역들)에 있는 관련 VDL이나 PVLL 상에 존재하는 userStreamSegment MO를 통해 표시하므로써 수행할 수 있다. 이 접근법 상에는 VASP 외부에서는 어떠한 userStream MO도 인스턴스화되지 않는다. 그러나 분산화된 방식에서는 사용자 스트림에 대한 정보를 요청하는 사용자가 있는 CPN 영역에서 자세한 정보를 담고 있는 userStream MO가 인스턴스화될 것이다. 이것은, 관련 VDL MO와 결합된 userStreamSegment MO를 인스턴스화 하므로써 수행된다. 그 경로를 제대로 관리하기 위해서 두 번째 userStream MO가 VASP 영역에서 인스턴스화 되게 되는데, 이것은 종단간 경로에 대해 전체적으로 자세한 정보를 담는 것이 아니라, 요청 CPN 영역의 CAP으로부터 그 경로에서 필요한 다른 TE까지에 대해서만 자세한 정보를 제공하게 된다. 이러한 정보로부터 VASP 영역은 관련 PVLL과 연관된 VASP에 있는 userStreamSegment들은 물론 그 영역에서의 관련 VDL들과 연관된 원거리 CPN에 있는 userStreamSegment들을 인스턴스화 하게 된다.

또한, 지금까지 언급된 여러 MO들을 관리하기 위해서는 그 MO들을 전역적으로 유일하게 명명할 수 있는 전역적 명명 방식이 필요하다. 그래야 자기 영역은 물론이고 다른 영역에 있는 MO들에 대한 적절한 관리가 이루어 질 수 있다[2)-4)].

III. 분할 및 계층화 개념

논리적 망 자원 위에서의 VPN은 토폴로지와 연결성이라는 항목으로 그 특성을 가지고 있다는 것을 고려하면, 일반적인 망 정보모델의 개념과 정확히 일치한다.

3.1. 일반적 망 정보 모델

일반적 망 정보모델은 G.803 권고안의 개념과 원

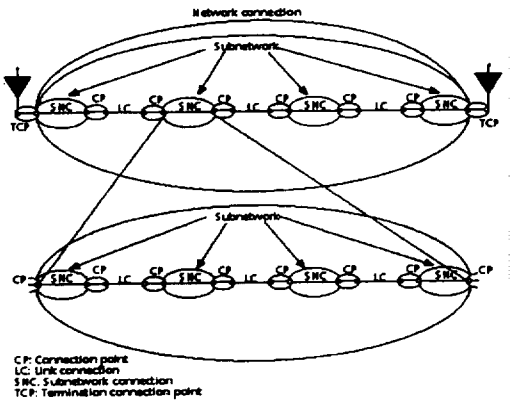

Fig. 7 Structuring Principles : Partitioning and Layering

칙들에 바로 기초하고 있다. 그 권고안의 주요 초점이 SDH 망이기는 하지만, 이 권고안은, 어떠한 망의 토폴로지와 연결성도 그 기술에 무관하게 묘사하는데 쓰일 수 있는 수많은 일반적 개념을 제공하고 있다. 더욱이, G.803 권고안은, Fig. 7에서 보듯이, 분할과 계층화라는 아주 강력한 구조화 원칙을 도입하고 있다. 분할이란 어떠한 망이라도 원하는 레벨까지 자세하게 나타낼 수 있는 궤환적 분해를 가능하게 한다. 다시 말하면, 분할이란 하부망을 바로 다음 레벨에서 더 하위에 있는 하부망의 자세한 사항들을 추상화시킴으로써 계층 구조를 정의하는 것이다. 계층화는, 근접 계층 사이의 클라이언트/서버 관계를 이용하여 하나의 트랜스포트 망을 서로 독립적인 수많은 트랜스포트 망 계층으로 분해하므로써 이루어지는 것이다. 이러한 관계에 있어서 클라이언트 계층에 있는 링크연결은 서버 계층에 있는 하나의 trail에 의해 제공된다.

가시성의 개념은, 전체 네트워킹 구조가 고려되는 추상화 레벨을 표현하기 위해 도입되어져 왔다. Fig. 8과 같은 일반적인 요소에 의해 지원되는 궤환성과 분할원칙을 이용한 분해를 최적으로 이용하려면, 각 가시성 레벨에서는 많아야 한 단계 정도의 분할이 이루어져야 한다. 결국, 각 가시성 레벨에서 정보 모델은 동일 가시성 레벨 및 가능한 그 다음 하위 레벨의 모든 요소들을 포함하게 된다.

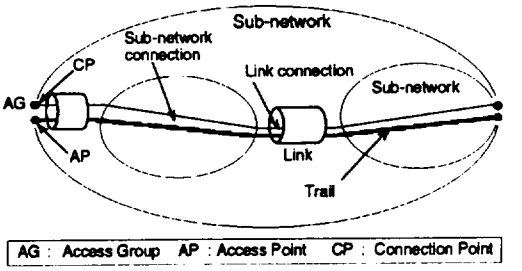

Fig. 8 Generic elements

Ⅳ. TMN 개념에 의한 VPN 관리

4.1. VPN 관리 구조

앞서 기술한 개념과 원리들은 VPN 정보구조 전체를 규정하는 데 쓰일 수 있다. Fig. 9에서 볼 수 있듯이, VPN 구조는 계층적이며, 계층화와 분할이라는 원리를 이용한다. 여기서는 4레벨의 가시성 레벨로 그 구조를 나타낼 수 있다. 공중망의 복잡도에 따라, 그 레벨과 스위칭 요소 레벨 사이에 중간 가시성 레벨이 필요할 수도 있다.

CTN 레벨은 VPN 전체 구조를 나타내는 부분으로, 필요 통신 용량을 응용들에 제공하는데 관계된 통신자원의 종단 대 종단 관점을 제공한다. 그러므로 CTN 레벨은 사설 및 공중영역 모두를 포함하며 통신 응용들에 대한 서버로서 작용한다.

VPN은 CTN레벨에서 하위 망으로서 나타나 보이지 않고 CPN들 사이에 설정된 링크회선들의 모음으로 보인다. 어떤 두 CPN 사이에 정의된 모든 회선들은, 그 회선들의 QoS 요건에 따른 하나 이상의 가상 사설선로(VPN 레벨 trail)에 의해 서비스되는 것이다.

이러한 계층구조는, TMN 개념에 의한 VPN 서비스에 대한 관리구조를 고찰해 볼 경우, 망 운용자의 OSF 쪽에서는, 스위칭 요소 레벨은 망요소 관리 계층, 공중망 레벨은 망관리 계층, VPN 레벨은 서비스 관리 계층에 해당되며, VPN 서비스 운용자의 OSF 쪽에서는 CTN 레벨이 서비스 관리 계층에 해당한다.

또한, 각 망 운용자 OSF와 VPN 서비스 운용자 OSF는 서로 X 인터페이스를 통해 관리 정보를 주고받게 된다(Fig. 10).

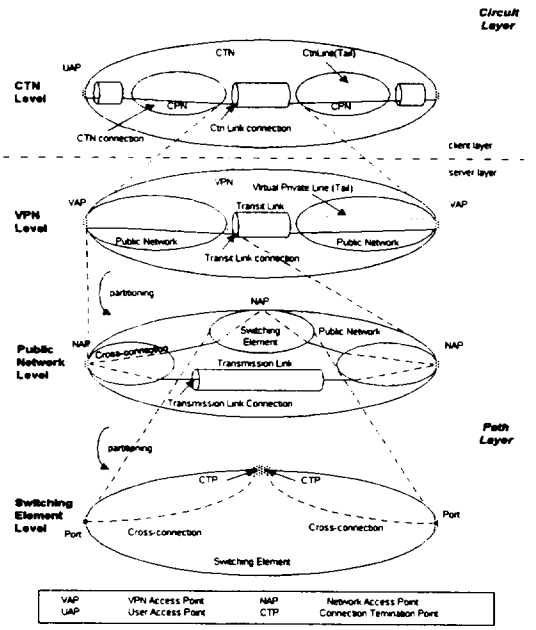

Fig. 9 VPN information Architecture

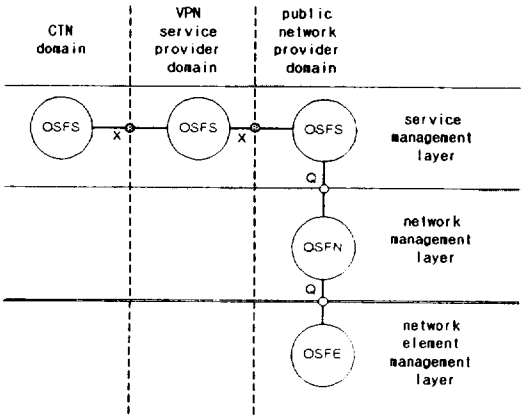

Fig. 10 Relationships between OSFs in their domains of the TMNs

결국, 이러한 구조는 TMN의 개념에서 고찰했을 때, 논리계층구조(LLA, Logical Layered architecture)에 입각하여 분할화와 계층화라는 구조화 기법을 도입한 관리 구조 형태를 띨 것이다.

4.2 분산망 관리기법의 도입

지금까지 살펴온 VPN 구조는 분할과 계층화 방식

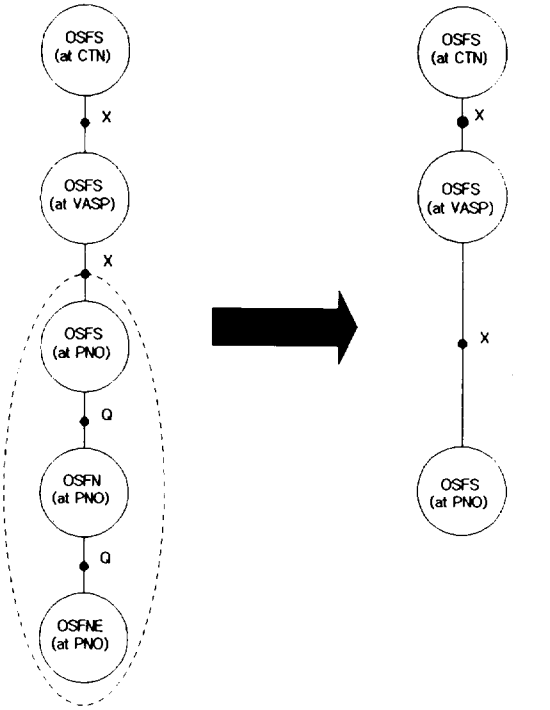

Fig. 11 Simplified relationships between OSFs in their domains of the TMNs

에 의한 계층적 구조를 가지고 있다. 그러나, 이러한 VPN에 대한 관리는 고객 영역과 VPN 서비스 제공자 영역, 망 제공자 영역 등의 각 TMN 영역들 사이의 inter-TMN 관리 운용이 수행되어야 한다. 그러므로, X 인터페이스를 통한 관리 동작의 특성이 제한된 관리 권한을 부여받을 뿐만 아니라 다른 TMN 영역 내에서 어떤 TMN 대리자가 어떤 서비스를 제공하는 지에 대한 정보가 제한되어 있으므로, 분산 시스템에서의 관리 기법을 도입하므로써 효율적인 관리가 이뤄질 수 있을 것이다. 그러므로, 먼저 Fig. 10에서 TMN 내부에서의 Q 인터페이스에 대해서는 계층화를 간략화 시켜 보이므로써, Fig. 11과 같은 형태로 OSF들 사이의 관계를 기본 모델로 하자.

X.500 디렉토리 서비스[5),6)]는 이미 개발되어 널리 알려진 분산처리 기술로서 전자적 화이트 페이지로서만 쓰이는 것이 아니라, 다양한 목적으로 널리 쓰이고 있다[7),8)]. 이는 X.500이 강력한 정보 모델링 용량 및 일반적인 명명 방식과 간단한 접근 인터페이스,

전역적 서비스 가용성 등을 제공하기 때문이다.

반면에, ODP 트레이더는 아직도 표준화 과정에 있는 것으로서, 아직까지도 완성된 규정을 가지고 있지 않다. ODP 트레이더는 ODP[9),10)] 환경을 구성하는 하나의 요소인데, ODP의 목적은 ODP 객체들 사이에 match-making 도구를 제공하려는 것이다. ODP트레이더의 주요 이점은, 객체들이 사용할 수 있는 서비스들을 인식할 수 있도록 할 필요가 있는 분산 환경에서 아주 유용하다는 것이다. 트레이더는, ODP 환경 내에 있는 서비스나 서비스 제공자에 대해서 먼저 알지 않고서도, ODP 객체들이 그 환경 속에 형성될 수 있도록 한다. 트레이더는 클라이언트들과 서버들 사이에서 역동적인 서비스 선택 및 링크를 가능하게 하는 제 3자로서 동작하기 때문에 앞에서 언급한 서비스들이 가능해지는 것이다.

다양한 관리 기능들을 수행하는 TMN 대리자들은 X.500 디렉토리 서비스와 ODP 트레이더 서비스 모두를 이용한다. 예를 들어, TMN 대리자들은 시스템 초기화 시에 다양한 자원 관련 정보들을 디렉토리로 저장하거나 갱신한다. 그러한 정보들을 필요로 하는 TMN 관리자와 다른 대리자들은, 그들이 자신의 관리 기능을 수행해 나감에 따라 요구되는 정보들을 디렉토리 서비스에 접근하여 얻어낼 것이다. TMN 관리자 및 대리자 모두는 DAP(Directory Access Protocol)를 이용할 것이다. DAP는 디렉토리에 정보를 저장하기 위해 X.500 권고안에 저장된 디렉토리 서버 접근용 프로토콜이다[5),6)]. X. 500 디렉토리 서비스는 분산망에서 TMN 대리자의 위치 정보를 제공하므로써, 위치 투명성을 제공하고, 다소 정적인 특성을 가지는 관리대상 객체(MO)에 대하여 저장소 역할을 하게 된다. 또한, 분산된 MO들에 대한 전역적 명명 방식을 제공하므로 그 이름을 이용하여 전역적으로 유일하게 식별해낼 수 있게 한다. X.500 디렉토리 서비스에 의해 쓰이는 정보 모델은 TMN 표준과 OSI 관리 표준에서와 동일한 객체지향 모델링 기법을 사용하고 있으므로, 디렉토리로 접근함에 있어 데이터의 변환을 필요로 하지 않는다.

TMN 환경에서, 다양한 관리 서비스가 다양한 관리자 및 다른 관리 서비스들에 의해 사용가능하고 또 쓰이고 있다. 이러한 서비스들은 이용하기 이전에 반드시 등록되거나 여러 정보들이 그 사용자들에게 알려져야 한다. ODP 트레이더는 이러한 작업을 수행한다. 즉, 어떤 사용자가 사용하고자 하는 서비스에 대한 정보들을 역동적으로 제공하는 일을 수행한다. 즉, 서비스 제공자들은 트레이더에게 각 서비스의 속성들을 가지고 자신들의 서비스들을 "exporting"하므로써 서비스 등록을 하게된다. 그러면, 어떤 서비스를 필요로 하는 사용자는, 자신의 목적에 맞는 서비스의 위치를 파악하기 위해 트레이더에게 문의하므로써 서비스에 대한 정보를 얻을 수 있다. 일단 서비스 위치가 파악되면, 요청는 그 서비스를 "import"하여 그것을 이용하게 된다. 그러므로, ODP 트레이더는 분산 처리에 대하여 브로커의 역할을 담당하기 때문에 TMN 관리자는 여러 TMN 대리자에 분산되어 있는 MO들에 대해 관리 운용을 수행할 수 있다. 이러한 트레이더는 다분히 동적인 망관리 정보 및 서비스들에 대하여 관리자 및 관리 응용들이 운용동작을 취할 수 있게 해준다.

그러므로 Fig. 12와 같은 관리 시스템의 구조가 가능할 것이다. 하지만, 여기서 제공되는 트레이더는 계층화된 구조를 반영하는 서비스를 제공하여야 할 것이다.

V. 구현 방식 고찰

본 논문에서 제안한 시스템은 TMN LLA에 근거하여 VPN을 효율적으로 관리하고자 하는 것이다. 이를 위하여 X.500 디렉토리 서비스와 ODP 트레이더를 이용하여, 효율적인 관리가 이뤄지도록 하였다. 이들은 분산망 관리에서 도입될 수 있는 서비스들이기 때문에, 분산망 관리가 필요한 TMN X 인터페이스가 있는 x-참조점에 도입하였다. TMN 내부에 있는 q-참조점에 대해서는 TMN 자체 내부에 있는 정보에 대한 관리에 해당하므로 반드시 분산 처리 기법을 도입할 필요가 없으므로 고려하지 않았다. 그러나, 이들 역시 필요하다면 확장은 가능할 것이다.

본 논문에서는 isode 8.0과 osimis 4.0을 플랫폼으로 사용하여 구현하였고, X.500 디렉토리 서비스는 isode 8.0에 구현되어 있는 것을 이용하였다[11),12)].

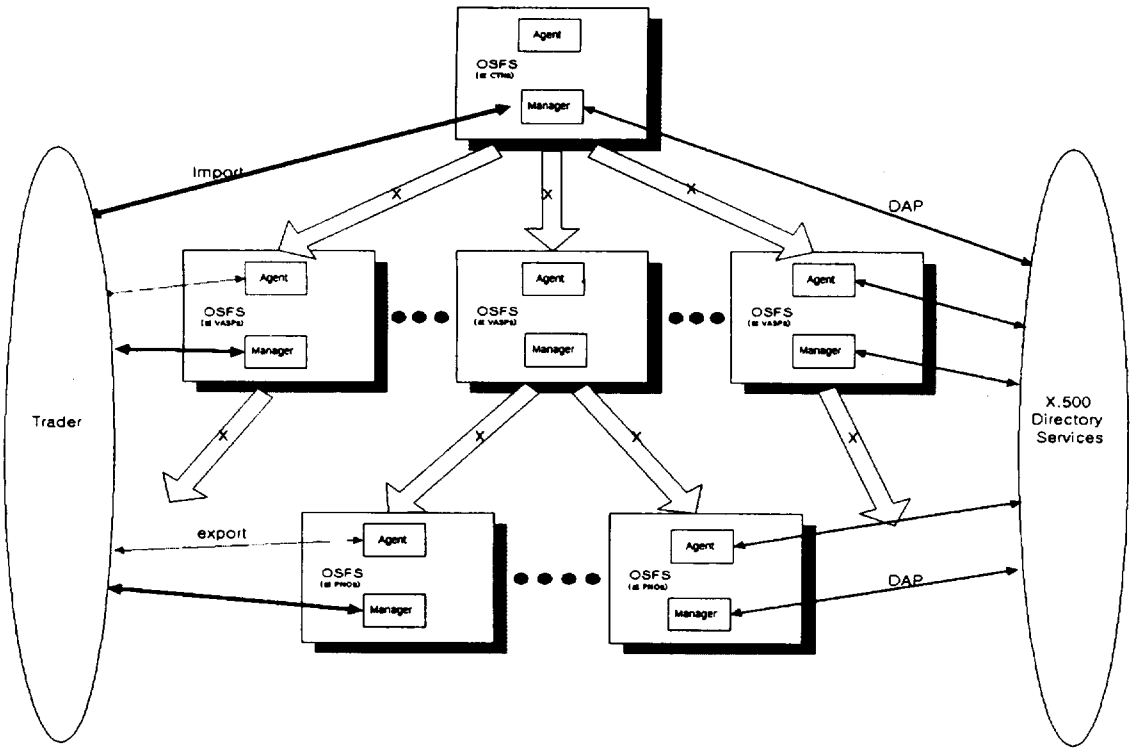

Fig. 12 The hierarchically distributed VPN management architecture using the Trader and the X.500 Directory Service

본 논문에서 도입한 트레이더는 LLA를 반영하여 계층적으로 구성된 VPN 관리 구조에 대하여 각각의 TMN 영역을 각각의 도메인으로 설정하여 서비스한다. 본 논문에서 구현되는 트레이더는 TMN 대리자와 TMN 관리자가 사용할 수 있는 두 가지 함수들에 대하여 정의하였다. 먼저, TMN 대리자는 트레이더에게 "export" 하므로써 자신의 서비스를 등록하므로, TMN 대리자가 이용할 수 있는 기능들은 다음과 같다.

```
agent_export([in] domain_id,
             [in] agent_id,
             [in] attribute [, attribute]*,
             [out] service_id):
    : TMN 대리자의 서비스를 export함.

agent_withdraw([in] domain_id,
               [in] service_id):
    : 이미 등록된 TMN 대리자의 서비스
      를 취소함.

agent_update([in] domain_id,
             [in] attribute [, attribute]*,
             [in] service_id):
    : 이미 등록된 TMN 대리자의 서비스
      의 속성을 갱신함.

domain_id : TMN 영역을 표시
agent_id : TMN 대리자를 표시
attribute : TMN 대리자의 서비스
            속성 표시
service_id : 트레이더에 등록된
             서비스 id
```

이러한 함수들을 이용하여 등록된 TMN 대리자들에 대하여 TMN 관리자는 자신이 속한 TMN 영역

의 하위 계층의 도메인에 속한 TMN 대리자들에 대해서만 필요 서비스를 import하여 관리 동작을 수행한다. Importer로서 TMN 관리자가 사용할 수 있는 기능은 다음과 같다.

```
manager_import([in] domain_id,
               [in] attribute[, attribute]*,
               [out] service_id[, service_id]*):
    : TMN 대리자의 서비스를 import함.
```

이와 같은 기능 함수들을 통해 각 계층마다의 망관리 동작은 원활히 이뤄질 수 있으며, 이는 바로 CNM 관리자와 같은 VPN 고객 망의 관리자가 어떤 관리 서비스를 요청했을 때, 공중망 관리자에게까지 그 관리 동작이 효율적으로 전달되어 효율적인 VPN 서비스가 이뤄질 수 있도록 할 것이다.

Ⅵ. 결 론

본 논문에서는 분산망에서 망관리 동작 기법을 이용하여 VPN 관리 구조를 제안하고 또 이를 위한 관리 기법에 대하여 고찰하였다.

근래의 VPN 서비스는 임대선 방식의 서비스가 아니라 광대역 통신망을 기반으로 하는 대역폭 계약 방식의 서비스이다. 이러한 서비스가 효율적으로 고객에게 서비스되려면, 망관리 기능이 반드시 제공되어야 한다.

VPN 서비스에서 고객에 의해 인식되는 가장 추상적인 레벨의 통신 자원이나 설비들은 CTN과 VPN, CPN/TE 등이다. 특히 CTN은 CPN과 TE, VPN으로 이뤄진 가상 개체로서 CPN과 VPN의 이질적인 환경을 가로질러 종단간 관리를 하게된다. 또한 CTN 구성에 있어서의 VPN은 하위 계층 통신 서비스를 제공하게 된다. 이러한 관계 속에서 CTN NMS의 역할은 VPN NMS 관리 기능을 이용하여 개별적인 CPN NMS 관리 기능들을 통합하려는 것으로, 연관된 모든 망들을 가로질러 종단에서 종단까지의 종단 사용자 서비스들에 대한 관리를 행하게 된다. 따라서 본 논문에서는 이들에 대한 각 NMS 기능들을 TMN 관점에서 각 영역에서의 OSF들로 대응시켜 살펴보았으며, 이들은 각기 각 영역 내부에서는 Q 인터페이스를 통해서, 다른 영역의 OSF들과는 X 인터페이스를 통하여 관리정보를 주고받게 된다.

이러한 VPN 서비스에 의한 CTN의 구성과 이러한 CTN의 가상 사설망으로서의 역할이 제대로 이루어지기 위해서는 VPN 서비스와 VPN 관리 기능 사이에 역동적인 상호작용이 있어야 한다. 이는 자원을 최대한 효율적으로 이용하여 가상 사설망 서비스를 제공하려는 것이다. 따라서 이러한 사설망에 대한 고객들 자신의 관리 요구는 높을 수밖에 없으므로, 최근에는 고객에 의한 VPN 관리에 대한 연구가 활발히 진행되고 있다. 고객이 필요로 하는 관리 정보는 최대한 추상화된 정보객체로서, 공중망을 통과하는 하나의 통신 회선은 그 하부 망에 대한 정보를 전혀 가지고 있지 않다. 그러므로, 본 논문에서는 이러한 VPN 서비스 환경에 대해 분산처리 기법을 도입하여, X. 500 디렉토리 서비스와 ODP 트레이더를 도입하여 VPN 서비스 관리 구조를 정의하고, 이에 대한 구현 방식에 대하여 고찰하였다.

그러나, 본 논문에서 prototype만을 고려하였으며, 실제로 본 논문에서 제시한 구조에서는 트레이더가 중요한 역할을 담당하는 만큼 대규모 망에 대한 분산처리를 위해서는 일관성에 대한 고려, 트레이더의 import 기능의 다양화 등과 같은 더욱 많은 고찰이 필요하다 하겠다.

참 고 문 헌

1) 송왕철, 김장형, 이상준, 1998, "초고속정보통신망에 근간한 가상사설망에 관한 연구," 정보통신부 정보통신정책연구원.

2) Song Wang Cheol, Kang Chang Eon, 1995, "Globally Unique Names for Network Management between TMNs," JTC-CSCC'95, Japan.

3) 송 왕철, 강 창언, 1995, "Relationship을 이용한 OSI 망관리 Naming Method," 한국통신학회논문지, 20권 8호, pp. 2207-2220.

4) Song Wang Cheol. Baek Lee Hyun. Kang Chang Eon. 1997. "Naming method and its extension to an access control model using the GRM." *IEE Electronics Letters*. Vol.33. No.10. pp. 838-839.

5) CCITT. 1988. *The Directory - Overview of Concepts. Models and Services. CCITT X.500 Series Recommendations.* CCITT

6) CCITT. 1991. *The Directory - Overview of Concepts. Models and Services. Draft CCITT X.500 Series Recommendations.* CCITT

7) Hong J. W.. Bauer M. A.. and Bennett J. M.. 1993. Integration of the Directory Service in the Network Management Framework. *Proc. of the Third International Symposium on Integrated Network Management.* pp. 149-160. San Francisco CA.

8) Stathopoulos C.. Griffin D.. and Sartzetakis S. 1995. Handling the Distribution of Information in the TMN. *Proc. of the Fourth International Symposium on Integrated Network Management.* pp. 398-411. Santa Barbara CA.

9) ITU-TS. 1992. *Basic Reference Model of Open Distributed Processing Part 1: Overview and Guide to the Use of the Reference Model.* ITU-TS Rec X.901. ISO/IEC 10746-1.

10) ITU-TS. *Draft* 1994. *ODP Trading Function.* ITU-TS SG7.Q16 Draft Recommendation.

11) Pavlou G.. McCarthy K.. Bhatti S.. and Knight G.. 1995. The OSIMIS Platform: Making OSI Management Simple. *Proc. of the Fourth International Symposium on Intergrated Network Management.* pp. 480-493. Santa Barbara. CA.

12) Robbins C. J. and Kille. S. E.. 1992. *The ISO Development Environment: User's Manual Version 8.0.* X-Tel Services Ltd.

13) Song Wang Cheol. Baek Lee Hyun. and Kang Chang Eon. 1995. "Design and Implementation of a Security Management System." SICON/ICIE. Singapore.