VPN Architecture Enabling Users to be Associated with Multiple VPNs

Yoshihiro HARA† Hiroyuki OHSAKI† Makoto IMASE† Yoshitake TAJIMA‡
Masahiro MARUYOSHI‡ Junichi MURAYAMA‡ Kazuhiro MATSUDA‡

†Graduate School of Information Science and Technology, Osaka University
1-3 Machikaneyama-cho, Toyonaka-shi, Osaka, 560-8531 Japan
{y-hara, oosaki, imase}@ist.osaka-u.ac.jp

‡NTT Information Sharing Platform Laboratories, NTT Corporation
3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan
{tajima.yoshitake, maruyoshi.masahiro, murayama.junichi, matsuda.kazuhiro}@lab.ntt.co.jp

Abstract

Recent improvements in network technology enable network communications in various social organizations and enable various social organizations to be virtualized in networks. We named the mass of virtual organizations "cyber-society". A "person" in cyber-society needs to establish secure communication associations with multiple virtual organizations. Therefore, we believe that VPN service can help to realize cyber-society because of its security. In this paper, we propose a VPN architecture where a single host can be simultaneously associated with multiple VPNs corresponding to virtual organizations. Because our architecture enables VPN service to be used on a by-host basis, it is more flexible than PPVPN (Provider Provisioned VPN) architecture, which is designed on a customer site basis. Additionally, when compared to an extranet architecture, our architecture has superior forwarding performance because it enables users to directly access destination VPNs.

1 Introduction

Advancement of network technology in recent years has freed social activities from geographical restrictions, allowing social structure to be distributed over wide areas. For instance, rapid increases in network bandwidth availability and the development of web-based applications [1] have caused commercial functions such as commerce and marketing to gradually shift onto the network. Moreover, political functions brought of the e-Japan project [2] and network-based learning continue to emerge. Also, in the business field, intranet/extranet has been widely deployed, leading to widespread use of network-based applications such as intranet database systems and business-to-business transaction systems [3]. Moreover, teleworkers and Small Office/Home Office (SOHO) are increasing their numbers [4]. Widely distributed social structures like this will cause "cyber-societies" to begin to form within the network. A "person" in the cyber-society could, for example, be employed by more than one company. Such a person would have multiple roles and need to easily and securely connect to multiple virtual organizations. For these cyber-societies to function, it is necessary to realize the goal of multiple associations.

Based on this cyber-society background, in this paper we aim to discuss how to allow association with multiple virtual organizations through network services. We use "service" in this context not to mean a commercial product, but a function provided to the user by a network administrator or a service provider. A conventional technology to realize this goal is Provider Provisioned VPN (PPVPN) which has been discussed in the PPVPN working group of the IETF. PPVPN can offer communication services between a limited number of users and is a suitable technology for this purpose.

However, in the current PPVPN specification, VPN is defined as a set of sites, and all users in a site are assumed to belong to the same VPN. The extranet exists as a technology to connect PPVPNs, and is an appropriate technology to associate users with multiple organizations. However, with PPVPN a VPN is constructed per site, making it impossible to construct VPNs for a set of users. For this reason, "persons" in cyber-society belonging to the same VPN site cannot belong to different virtual organizations.

With extranet technology, a "person" in cyber-society can be simultaneously associated with multiple virtual organizations. However, as the number of VPNs increases, various problems such as degradation of transmission speed and increase in management cost will arise. To resolve such issues, in this paper we propose a novel VPN architecture that enables to create of a number of VPNs for sets of users, and allows multiple association of users to a number of different VPNs.

The organization of this paper is as follows. In Section 2, we introduce two conventional VPN technologies — PPVPN and extranet — and discuss their advantages and disadvantages. In Section 3, we explain our VPN archi-

tecture that allows multiple association. In Section 4, we present sample implementations of our proposed VPN architecture. In Section 5, several possible applications of our proposed VPN architecture are described. In Section 6, we finally conclude this paper and discuss future works.

2 Legacy VPN

2.1 PPVPN (Provider Provisioned Virtual Private Network)

Provider Provisioned VPN (PPVPN) architecture is currently under consideration in the PPVPN working group at the IETF [5, 6, 7]. Companies or organizations building secure local area networks have traditionally used leased lines to connect their LANs at various locations. Leased lines are extremely secure, but also are extremely expensive. PPVPN creates a virtual private network inside the service provider network, allowing the service provider to provide network services to customers for significantly cheaper cost than a leased line.

Figure 1 graphically represents a PPVPN. A network, where all customer's hosts can communicate each other without using the service provider network, is called a site. The CE (Customer Edge) device in Fig. 1 is installed at the border of the customer site. Customer host devices connect to the CE device. A PE (Provider Edge) device is a device which resides in the service provider's network and is directly connected to the CE device. The service provider offers PPVPN service by configuring VPN tunnels between PE devices. Packets received at one end of the VPN tunnel are forwarded to the other side. Packets may not enter the tunnel except through one of the VPN tunnel endpoints.

In the example in Fig. 1, packets sent from VPN A's CE device pass through the tunnel and are forwarded to VPN A's CE device. In this way, the VPN tunnel functions as a virtual private line. The VPN tunnel is created and maintained by tunneling protocols such as IPSec, MPLS, L2TP, GRE and IP-in-IP.

PPVPN has several advantages. First, since only the authorized customers can access the VPN tunnel, unauthorized access by other users can be prevented. Also, since the service provider and customer addressing schemes are independent from each other, customers are free to choose their own addressing schemes.

However, traditional PPVPN also has its disadvantages. According to [5], the smallest component in a PPVPN is the site. As shown in Fig. 1, all hosts connected to the VPN A's CE device are assumed to be associated with VPN A. With PPVPN, if site level authentication is required for VPN access, user level authentication is not required [6]. Because of this, hosts within a single PPVPN site cannot associate themselves with other VPNs.

2.2 Extranet

The extranet exists to allow communication with hosts associated with other VPNs [8, 9]. By using an extranet,

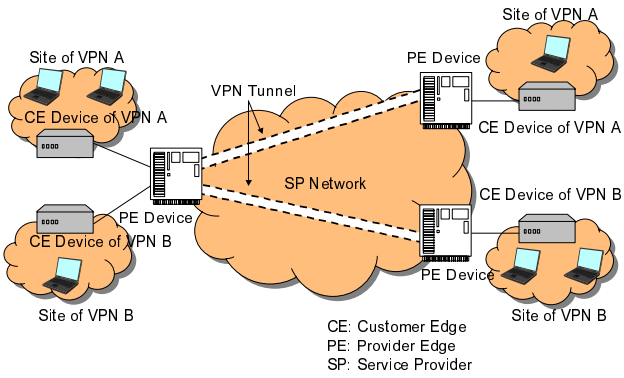

Figure 1: PPVPN Model

hosts are able to communicate with hosts belonging to other VPNs, even if they already belong to a VPN themselves.

To allow communication with multiple VPNs through legacy extranets, VPNs connect to each other through a common VPN. As shown in Fig. 2, VPNs #1 through #4 are connected through a common VPN. Since each VPN is managed under separate policies, a firewall is installed between each VPN and the shared VPN to provide services such as packet filtering and address translation. For communication across VPNs, this results in packet filtering occurring twice — once at each firewall.

Extranets have the following advantages. First, since each VPN is free to set its own firewall and filtering rules, security is maintained even when connecting to foreign VPNs. Secondly, it is possible to connect multiple VPN connections through the common VPN. This enables a single network interface to serve multiple VPN connections.

However, extranets also have the following disadvantages. Since each VPN has its own private addressing scheme, it is necessary to translate these addresses before communication. NAT [10] can be used for this purpose, but not all applications maintain NAT compatibility. Also, filtering rules in the firewall must be appropriately set to ensure an adequate level of security. As the number of connected VPNs increase, additional filtering rules are needed, increasing the connection complexity and administrative burden. Moreover, packet based filtering is thought to negatively impact data transfer performance as more and more filters are applied.

3 MAVPN Architecture Proposal

With PPVPN a VPN is constructed per site, making it impossible to construct VPNs for a set of users. And extranet has problem which filtering burden increases, as the number of VPNs increases. To resolve such issues, in this paper, we propose a VPN architecture with the host as the basic component, which would allow a single host to make multiple simultaneous VPN connections.

Through this type of VPN architecture, multiple VPNs can co-exist inside a single site. Additionally, a single host

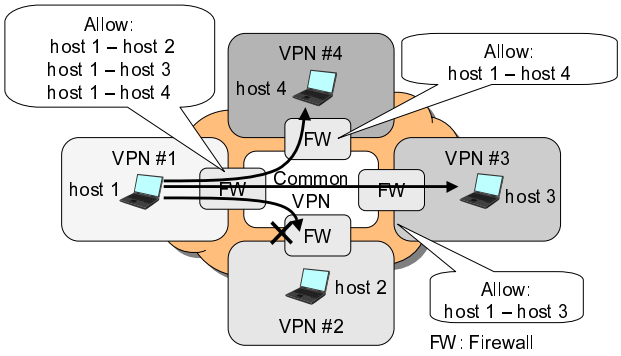

Figure 2: Extranet Model

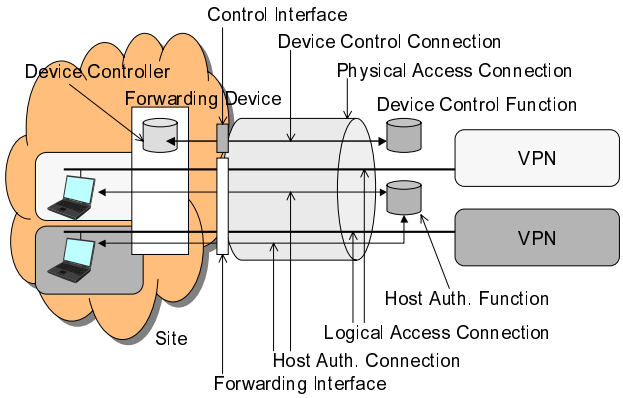

Figure 3: MAVPN Architecture

can be associated with multiple VPNs. We call this VPN architecture Multiply-Associated VPN (MAVPN).

See Fig. 3 for the MAVPN architecture. For this architecture, an MAVPN service is provided for each host. The MAVPN service provides a forwarding interface and a control interface to the host. User data forwarding functions are handled through the forwarding interface, while other functions are serviced through the control interface. See below for description of functions provided to the host:

a) Functions provided via the forwarding interface:

- VPN Access

  At the physical layer, one physical interface connects the site to the network. At the data link or network layer, multiple logical access connections to VPN are provided.

- Host Authentication

  VPN authentication is performed at the access connection level. In other words, authentication of VPN access requests is performed not at the site level but at the host level.

- VPN Adressing

  The host receives an assigned address for each VPN access connection. This address is assigned from a VPN address pool predefined by the administrator of the target VPN. Therefore, same address may be assigned to hosts associated with deferent VPNs. This address confliction must be tolerated.

b) Functions provided via the control interface:

In the MAVPN architecture, it is necessary to prevent forwarding devices in the site (such as routers) from inadvertently or illicitly connecting separate VPNs. To prevent this, the control interface provides a control function to forwarding devices (Fig. 3).

4 MAVPN Sample Implementation

4.1 Host-based VPN

Before explaining the MAVPN sample implementation, first we will explain a VPN sample implementation using the host as the basic unit. We call this type of implementation “host-based VPN.” This sample implementation assumes a service provider providing host-based VPN service.

As shown in Fig. 4, it is possible to configure the service provider’s network access connection with VLAN as specified in IEEE802.1Q [11] and PPP [12]. The service provider connects different VPNs with corresponding VLAN-IDs. A VLAN switch in the customer site would allow hosts to isolate and allocate a VPN for each VLAN. If each host uses PPPoE [13] to access the service provider network, it is possible to select, authenticate and connect to a VPN on a host-by-host basis. If hosts are attached to different port VLAN segments, address confliction between hosts is tolerated. The control interface between the service provider network and the CE device can be used to allow SNMP traffic over IPSec, for instance. In this case, the SNMP manager is installed inside the service provider network as a device control server, while the CE device in the customer site functions as the SNMP agent.

The sample implementation in Fig. 4 allows each host in the customer site to associate with different VPNs. By doing this, the VPN configuration is a host-based, thereby resolving the problems inherent in PPVPN.

4.2 Host-based MAVPN

Figure 5 shows an MAVPN sample implementation where a single host is simultaneously connected to multiple VPNs. We will call this sample implementation “Host-based MAVPN.” This sample implementation assumes a service provider providing host-based MAVPN service.

As in the previous VPN implementation example, with MAVPN we also configure the service provider’s network access connection with VLAN as specified in IEEE802.1Q and PPP. The service provider connects different VPNs with

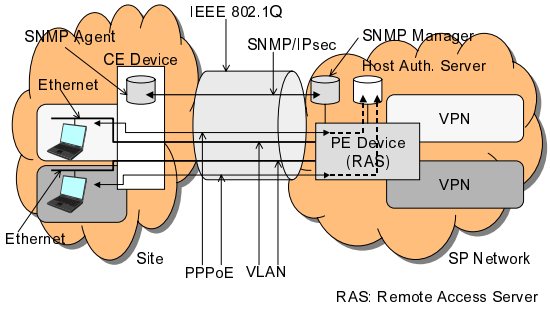

Figure 4: Host-based VPN Sample Implementation

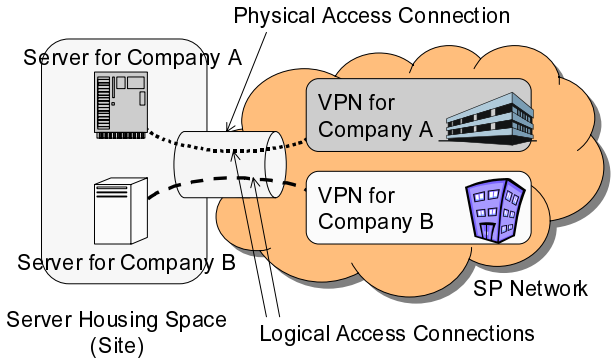

Figure 6: Housing Service for Businesses

corresponding VLAN-IDs. With host-based MAVPN, multiple VLANs are assigned to a single host. The host must use a single access connection configured with multiple VLANs.

If the host does not support VLAN tagging, another device between the host and VLAN switch must be employed to assign VLAN-IDs. The host receives address assignments from multiple VLAN segments and will have multiple network addresses. Moreover, the host must authenticate and connect to multiple VPNs with multiple PPPoE sessions.

In a traditional extranet, connection policies between VPNs become more complex as more VPNs are connected and more filtering rules are added. This causes a corresponding increase in the administrative burden. In addition, forwarding performance is impacted by packet-based filtering as additional filtering rules are applied. With host-based MAVPN, the host is directly connected to the target VPN, thereby eliminating these problems. When selecting the target VPN, host authentication provides the necessary security, thereby eliminating the packet filtering requirement. The forwarding performance issue caused by packet filtering disappears, and performance is improved when compared to extranet. Administrative overhead is also reduced because filtering rules are not required.

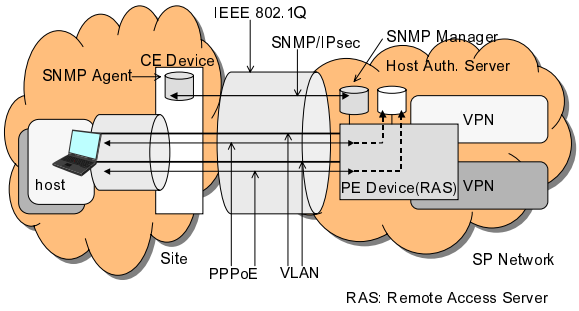

Figure 5: Host-based MAVPN Sample Implementation

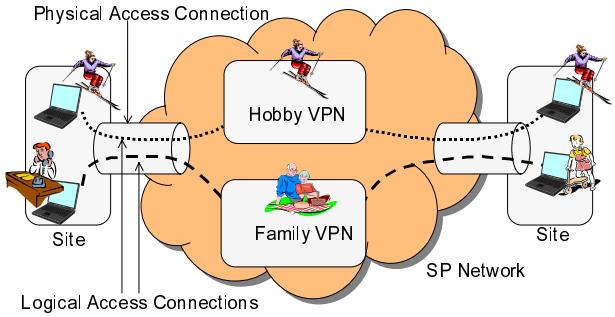

Figure 7: Home User VPN Service

5 MAVPN Applications

5.1 Applications for Host-based VPN

First, we discuss host-based VPN applications. We will discuss applications for host-based VPN for servers and host-based VPN for clients.

- Server housing service for businesses

  We consider an application where a server housing service is provided to house business' important servers. As precaution against disaster, it is important to maintain a server separated from the main company office. By leveraging host-based VPN as in Fig. 6, a housing service provider can use a single server housing facility to safely house servers belonging to several different VPN-associated organizations. This service can be provided at a low cost by sharing a single housing site among multiple customers.

- Home User VPN Service

  By using host-based VPN to create VPNs at the host level, it should be easy for home users to make their own VPNs (Fig. 7). For example, it would be possible to provide VPNs to single user-level groups for specific applications such as hobbies or family.

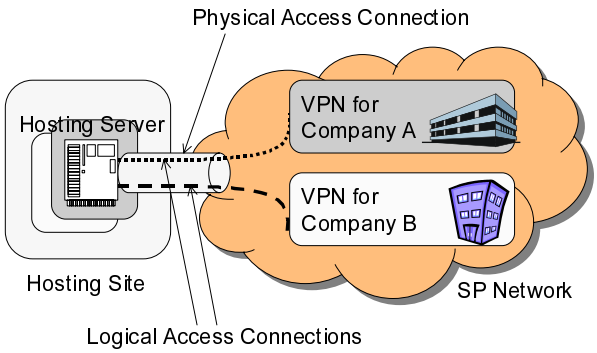

Figure 8: Hosting Service

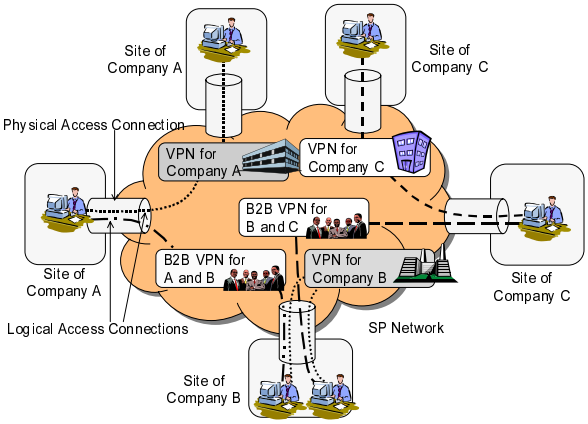

Figure 9: B2B Corporate Network Service

5.2 Applications for Host-Based MAVPN

We will discuss host-based MAVPN applications for servers and host-based MAVPN applications for clients.

- Hosting Service

  It is common for hosting service providers to rent server space to businesses and individuals. By using host-based MAVPN, hosting service providers can provide these hosting services to their customers at a lower cost. As shown in Fig. 8, single physical server can be shared among multiple customers by associating it with multiple VPNs, thereby allowing hosting service provider to provide the hosting service at a lower cost.

- Constructing corporate networks for B2B

  For Business to Business (B2B), companies use VPNs to create extranets to conduct commercial transactions. By using host-based MAVPN as shown in Fig. 9, companies can create not only VPNs of their own employees but also other B2B VPNs that include members of foreign companies as well.

6 Conclusion

In this paper we have proposed a MAVPN architecture which uses the host instead of the site as its basic component. We have also shown how the MAVPN architecture allows a single host to be simultaneously associated with multiple VPNs. In addition, we have shown the superiority of our MAVPN architecture over traditional VPN architectures. Future topics for discussion include proposing a multi-layer MAVPN architecture, evaluating MAVPN performance, and testing a MAVPN prototype.

References

[1] S. J. Vaughan-Nichols, "Web Services: Beyond the Hype," *IEEE COMPUTER*, vol. 35, pp. 18–21, Feb. 2002.

[2] N. Ohyama, "Progress of e-Government in Japan," *IPSJ Magazine*, vol. 44, pp. 455–460, May 2003. (in Japanese).

[3] Ministry of Public Management, Home Affairs, Posts and Telecommunications, "Communications Usage Trend Survey in 2001 (in Japanese)," May 2002. available at `http://www.johotsusintokei.soumu.go.jp/yusei/adapter.Main`.

[4] Japanese Telework Association, "Teleworker Population Survey (in Japanese)," July 2002. available at `http://www.soumu.go.jp/s-news/2002/020705_4.html`.

[5] M. Carugi *et al.*, "Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks," *Internet Draft* <draft-ietf-l3vpn-requirements-00.txt>, Apr. 2003.

[6] A. Nagarajan, "Generic Requirements for Provider Provisioned VPN," *Internet Draft* <draft-ietf-l3vpn-generic-reqts-01.txt>, Aug. 2003.

[7] R. Callon *et al.*, "A Framework for Layer 3 Provider Provisioned Virtual Private Networks," *Internet Draft* <draft-ietf-l3vpn-framework-00.txt>, Mar. 2003.

[8] J. Miyoshi, I. Imaida, K. Isagai, J. Murayama, and S. Kuribayashi, "A Mechanism of Policy-Based Service Control in Communication between VPNs," *IEICE Technical Report* SSE99-171, vol. 99, pp. 61–66, Mar. 2000. (in Japanese).

[9] H. Hara, J. Murayama, K. Isagai, and I. Imaida, "IP-VPN Architecture for Policy-Based Networking," *IEICE Technical Report* IN2000-101, vol. 100, pp. 39–46, Oct. 2000. (in Japanese).

[10] K. Egevang and P. Francis, “The IP Network Address Translator (NAT),” *Request for Comments (RFC) 1631*, May 1994.

[11] IEEE Standards for Local and Metropolitan Area Networks, “Virtual bridged local area networks,” *IEEE Standard 802.1Q-1998*, Dec. 1998.

[12] W. Simpson, “The Point-to-Point Protocol (PPP),” *Request for Comments (RFC) 1661*, July 1994.

[13] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, and R. Wheeler, “A Method for Transmitting PPP Over Ethernet (PPPoE),” *Request for Comments (RFC) 2516*, Feb. 1999.