On Layered VPN Architecture for Enabling User-Based Multiply Associated VPNs

Yoshihiro Hara[1], Hiroyuki Ohsaki[1], Makoto Imase[1], Yoshitake Tajima[2], Masahiro Maruyoshi[2], and Junichi Murayama[2]

[1] Graduate School of Information Science and Technology, Osaka University 1–3 Machikaneyama–cho, Toyonaka–shi, Osaka, 560–8531 Japan
[2] NTT Information Sharing Platform Laboratories, NTT Corporation 3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan

Abstract. In our previous work, we have proposed a new VPN architecture for enabling user-based multiply associated VPNs [1]. Almost all existing VPN technologies assume that users never simultaneously access more than a single VPN. Thus, for realizing a new VPN service allowing users to simultaneously join multiple VPNs, several fundamental mechanisms, such as dynamically changing user's VPN association status according to the user's request and authorizing user's access to a group of VPNs, are required. In this paper, we propose a layered VPN architecture for realizing user-based multiply associated VPN. Our layered VPN architecture consists of three network levels such as PNL (Physical Network Level), LNL (Logical Network Level), and UNL (User Network Level). First, we discuss and classify functions required for each network level. We then present several approaches for implementing each network level using existing layer 2, 3, and 4 networking technologies, and quantitatively evaluate their advantages and disadvantages from several viewpoints including scalability and transmission speed.

1 Introduction

With recent advancements in network technology, various social activities such as commerce and trade, politics, labor, and other functions are relying more on network communications. In the near future, this may form virtual organizations within the network. We call these virtual organizations "cyber-societies." A "person" in cyber-society needs to establish secure communication and associate with multiple virtual organizations. We believe these virtual organizations can be realized through Virtual Private Networks (VPNs) as network services.

As current technologies for VPN services, there are Provider Provisioned VPN (PPVPN) [2–4] and extranets [5, 6]. However, PPVPN simply builds a VPN between customers' LAN sites. Also, extranets are difficult to manage and transmission performance is degraded when hosts attempt to connect to a lot of VPNs. These problems with existing VPN technology prevent users from associating themselves simultaneously to multiple VPNs at a user level.

To address this problem, we are considering a new VPN architecture that would allow users to simultaneously associate with multiple VPNs [1]. We call

this new VPN "Multiply-Associated VPN (MAVPN)". This paper has two goals. First, we will show that by using a layered model for MAVPN's architecture, MAVPN can be easily realized by integrating existing layer-based technologies. Next, from various perspectives, we will evaluate the advantages and disadvantages of integrating MAVPN into layers 2, 3 and 4 of the network layer model.

2 Layered MAVPN Architecture

In this section we will explain our proposed layered MAVPN architecture. With existing PPVPN, due to its site-to-site VPN tunnel connection method, it is not possible for users to make their own VPN connections with other users. Also, with existing extranet technology it is not possible to simultaneously make a number of VPN connections. To address these problems, we have proposed the MAVPN architecture.

To realize MAVPN, the following three main processes are required. First, provide a base network. Then, build various VPNs on top of the base network. Finally, provide VPN control functions so users can access multiple VPNs securely and simultaneously.

The actual implementation of these processes appears to be complex and difficult. However, by building these three processes on existing network technology through layers, we believe it implementation will be relatively simple.

For example, existing PPVPN builds a logical network over a base network. So we think that it is easy to provide a layer with VPN control functions, for users can access multiple VPNs securely and simultaneously. We think that it is not good to extend logical network for multiple access to VPNs as existing extranet from the point of view of scalability.

Below, we discuss the required features for each of three layered network levels (physical network level, logical network level, user network level). A definition of terms for each network level is shown in Tab. 1.

First, we will discuss the Physical Network Level (PNL). The PNL provides the network that serves as the foundation for building a VPN. Figure 1 is a graphical representation of the PNL. As shown in Fig. 1, nodes such as routers, switches and hosts are connected by links.

Next, we will discuss the Logical Network Level (LNL). In the LNL, a VPN is formed on top of the network provided by the PNL. With PPVPN, the site is the basic unit in forming a VPN. With the MAVPN LNL, however, we introduce the concept of host entity as the basic unit. This entity could be host users, user-level applications or server programs. In this paper, the term "entity" is defined for intended application in VPN services targeted to Application Service Providers (ASP) or for multi-OS usage. Figure 2 graphically represents the LNL. As shown in Fig. 2, an entity-based VPN is created through specifying the entity as the basic unit for authentication. When we implement this layer, we can use various existing network technologies about VPN.

Finally, we will discuss the User Network Level (UNL). The UNL controls access from the entity to each VPN when the entity simultaneously connects to, or

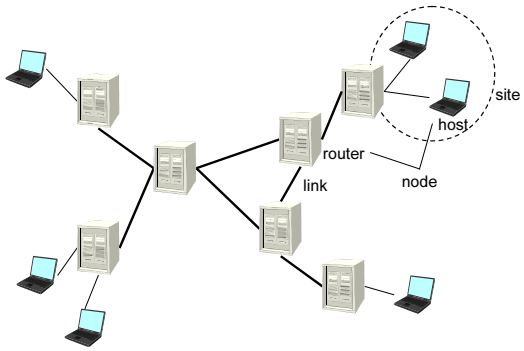

Fig. 1. Physical Network Level (PNL) in MAVPN architecture

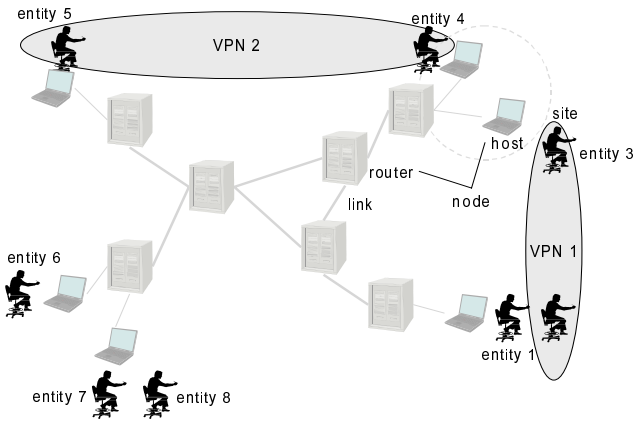

Fig. 2. Logical Network Level (UNL) in MAVPN architecture

is multiply associated with, multiple VPNs. Specifically, it provides the controls which let the entity transparently connect to and use multiple VPNs, as well as preventing unauthorized access across any other associated VPNs. Figure 3 is a graphic representation of the UNL. When we implement this layer, we can transfer the packets from a entity to the target VPN using various information of the packets. This transfer functions may be implemented in edge routers or other devices. The layer of the information of packet for transfer depends on the implement technology.

3 Three Typical MAVPN Architecture

Because current wide-area connection services are commonly provided through network layer 2 or layer 3, we consider the PNL to be realized through network

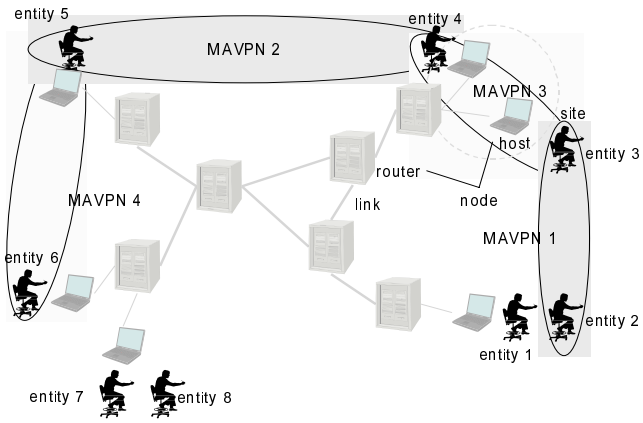

Fig. 3. User Network Level (UNL) in MAVPN architecture

Table 1. Definition of terms

Terms for Physical Network Level	
Host	Terminal, PC
Node	Devices like Hosts, routers, and switches
Link	Physical line between nodes
Terms for Logical Network Level	
Entity	Users, user-level applications, and server programs on hosts
VPN	Virtual closed network consist of entities
User for Logical Network Level	
Multiple Association	A single entity simultaneously connects to multiple VPNs

layer 2 or 3. Likewise, we consider the UNL to be realized through Layer 3 or Layer 4. Therefore, in this paper, we will discuss the following three MAVPN architecture types which are based on the three layered network levels.

3.1 Architecture 2-3-4

Architecture 2-3-4 uses different network layers for each of the physical, logical, and user network levels. Architecture 2-3-4 is explained below.

First, the PNL is realized from information in network layer 2. The layer 2 network could be provided by Ethernet or MPLS [7], for example.

Second, the LNL is realized from information in network layer 3. The layer 3 network could be provided through MPLS-VPN [8], for example.

Next, the UNL is realized from information in network layers 4 and higher. For this method, the LNL, using information in packets from layer 4 or higher, would send packets from the entity to the appropriate multiply-associated VPN.

3.2 Architecture 2-2-3

Architecture 2-2-3 uses network layer 2 information for PNL and LNL, and network layer 3 information for the UNL. Architecture 2-2-3 is explained below.

First, the PNL is realized from information in network layer 2. The layer 2 network could be provided by Ethernet or MPLS, for example.

Second, the LNL is realized from information in network layer 2. The layer 2 network could be provided by IEEE 802.1Q VLAN [9] or L2TP [10], for example.

Next, the UNL is realized from information in network layer 3. For this method, the LNL, using information in packets from layer 3, would send packets from the entity to the appropriate multiply-associated VPN.

3.3 Architecture 3-3-3

Architecture 3-3-3 uses network layer 3 information for each of the physical, logical and user network levels. Architecture 3-3-3 is explained below.

First, the PNL is realized from information in network layer 3. The layer 3 network could be provided by IP or other protocols, for example.

Second, the LNL is realized from a tunneled layer 3 network. The tunneling used in layer 3 could be provided by IPSec [11] or other protocols, for example.

The UNL is realized from information in network layer 3. For this method, the LNL, using information in packets from layer 3, would send packets from the entity to the appropriate multiply-associated VPN.

For each of these MAVPN architectures, Fig. 4 shows the relation of the three levels (physical, logical, user) and the layers in the OSI reference model.

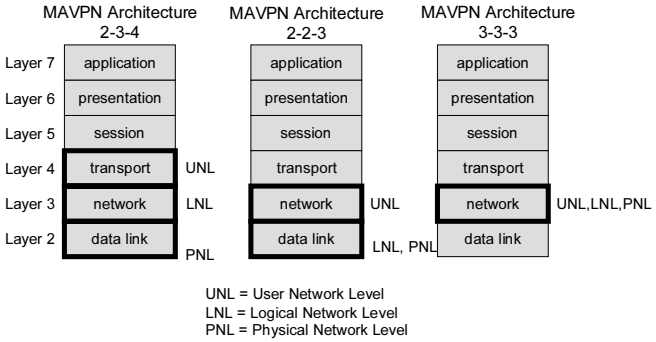

Fig. 4. Three typical MAVPN architectures

4 Evaluating MAVPN Architecture from Several Viewpoints

In this paper, from several viewpoints, we will quantitatively evaluate the advantages and disadvantages of these three MAVPN architecture types.

When considering its expected application in the formation of a cyber-society, MAVPN must be able to operate on an extremely large network. For this reason, it is most preferable to have a high degree of scalability in numbers of nodes, VPNs and entities. Therefore, it is necessary to evaluate the scalability of these objects.

Also, in the past few years, the size of content on the Internet has mushroomed. For this reason, it is most preferable that transmission speeds under MAVPN are fast and efficient. Therefore, it is necessary to evaluate transmission speed.

Additionally, it is preferable that MAVPN users be able to use various types of network services. Therefore, it is necessary to evaluate the numbers of usable services.

Finally, it is preferable that MAVPN be flexible enough to meet user needs through ease of VPN configuration and VPN connection to entities. Therefore, it is necessary to evaluate entity and VPN manageability.

5 Evaluating MAVPN

5.1 Scalability (Number of Nodes, VPNs and Entities)

We evaluate the three MAVPN Architectures 2-3-4, 2-2-3, and 3-3-3 from the viewpoint of node, VPN and entity scalability.

Node Scalability Scalability of nodes in MAVPN is determined by the scalability of nodes in the PNL. These are considered below for each of the MAVPN architecture types.

- Architecture 2-3-4
  The physical network layer is created through network layer 2. Because of this, node scalability is more negatively impacted than Architecture 3-3-3 which uses network layer 3. For example, a typical layer 2 protocol like Ethernet is more negatively impacted in terms of scalability than a typical layer 3 protocol like IP.
- Architecture 2-2-3
  The physical network layer is created through the network layer 2. For this reason, node scalability is more negatively impacted than Architecture 3-3-3. On the other hand, scalability is comparable to Architecture 2-3-4, which also uses network layer 2 for the PNL.
- Architecture 3-3-3
  The physical network layer is created through the layer 3 network. For this reason, scalability is excellent as compared to Architecture 2-3-4.

Based on the above examination, Architecture 3-3-3 excels most in node scalability.

VPN Scalability VPN scalability in MAVPN is determined by VPN scalability in the LNL. These are considered below for each of the MAVPN architecture types.

- Architecture 2-3-4
  For the LNL, the scalability of number of VPNs is determined by what type of layer 3 network is used. For example, if using MPLS VPN, by stacking MPLS labels, a high degree of scalability is possible.
- Architecture 2-2-3
  For the LNL, the scalability of number of VPNs is determined by what type of layer 2 network is used. For example, if using IEEE 802.1Q tagging VLAN, by stacking tags, a high degree of scalability is achievable.
- Architecture 3-3-3
  For the LNL, the scalability of number of VPNs is determined by what type of layer 3 network is used. For example, if using a common tunneling technology like IPSec, it is necessary to connect a mesh of VPN tunnels between entities. Due to the limitation in the number of tunnels, the VPN scalability is limited. For instance, the maximum number of IPSec tunnels (number of SAs) is restricted to the available memory or system resources of the connected nodes.

Based on the above examination, Architectures 2-3-4 and 2-2-3 excel most in VPN scalability.

Entity Scalability Entity scalability in MAVPN is determined by UNL scalability. These are considered below for each of the MAVPN architecture types.

- Architecture 2-3-4
  Architecture 2-3-4 uses network layer 4 and higher information. In this case, since entity identification is based on network layer 4 or higher information, there is no restriction on the number of entities inherited from the physical or LNL. Therefore, for entity scalability, this architecture excels most when compared with the other MAVPN architecture types.
- Architecture 2-2-3
  Since Architecture 2-2-3 uses network layer 3 information in the UNL, the number of entities is restricted by logical address limitations in network layer 3. For example, if using a typical layer 3 protocol like IPv4, the entity limit is determined by the IP address limit (2^{32}). However, as IPv6 is adopted, this entity limitation is resolved. For this reason, excellent scalability is expected for the near future.
- Architecture 3-3-3
  Architecture 3-3-3, like Architecture 2-2-3, uses network layer 3 information for the UNL and therefore is restricted by layer 3 logical address limitations.

However, like Architecture 2-2-3, in the near future the entity limitation is expected to be resolved. For this reason, excellent scalability is expected for the near future.

Based on the above examination, any of the architecture types are expected to enjoy good entity scalability for the future.

5.2 Transmission Speed

We evaluate the three MAVPN Architectures 2-3-4, 2-2-3, and 3-3-3 from the viewpoint of transmission speed. Since the most complex operations are performed at the UNL, it is necessary to consider the transmission speed scalability within this level. These are considered below for each of the architecture types.

- Architecture 2-3-4
  At the UNL, it is necessary to process information from network layer 4 and higher. Therefore, compared to the other two architectures, performance at the UNL is expected to be poor. Therefore, when compared to the other two architecture types, we expect Architecture 2-3-4 performance to suffer the most.
- Archtecture 2-2-3
  At the UNL, it is necessary to process information from network layer 3. Therefore, compared to Architecture 2-3-4, which processes layer 4 and higher data, faster processing speeds in the UNL are expected. Therefore, we expect performance to be better than Architecture 2-3-4.
- Archtecture 3-3-3
  At the UNL it is necessary to process data from network layer 3. Therefore, compared to Architecture 2-3-4, which processes layer 4 and higher data, faster processing speeds in the UNL are expected. Performance is expected to be similar to Architecture 2-2-3 which also processes information from network layer 3.

Based on the above examination, Architectures 2-2-3 and 3-3-3 excel the most in link speed scalability.

Usable Service Scalability We evaluate the three MAVPN Architectures 2-3-4, 2-2-3, and 3-3-3 from the viewpoint of usable service scalability. Since usable services are dependent on the protocols available to the user, it is necessary to consider the protocols used in forming the UNL. These are considered below for each of the architecture types.

- Architecture 2-3-4
  Since the UNL handles information from network layer 4 and higher, compared to MAVPN architectures which handle layer 3 information, there are fewer protocols available to users. Therefore, as compared to other MAVPN architectures, Architecture 2-3-4 suffers from lack of usable protocols.

– Architecture 2-2-3
  Since the UNL handles information from network layer 3, there are more usable protocols available to users than MAVPN Architecture 2-3-4, which handles information from layer 4. Therefore, this architecture excels over Architecture 2-3-4 in the number of available protocols for users.
– Architecture 3-3-3
  In Architecture 3-3-3, the UNL handles information from network layer 3. When compared with Architecture 2-3-4 which handles network layer 4 and higher information, Architecture 3-3-3 excels in the number of available protocols for users. However, depending on the tunneling technology that Architecture 3-3-3 uses, the number of protocols available to users may be limited. For example, when using a currently common tunneling technology like IPSec, the number of protocols available to users is limited. For this reason, when compared with Architecture 2-2-3 which handles information from network layer 3, the number of usable services available to Architecture 3-3-3 users is worse.

Based on the above examination, in terms of number of services available to users, the suitability of the architectures is ranked from best to worst as: Architecture 2-2-3, 3-3-3, 2-3-4.

5.3 VPN Management

Evaluation of the ease of management of Architectures 2-3-4, 2-2-3, and 3-3-3 will be the topic of a future discussion.

5.4 Overall Evaluation Result

Table 2 shows the overall evaluation result as discussed in the previous sections. With regards to the evaluated criteria, of the three architectures (2-3-4, 2-2-3, 3-3-3), Architecture 2-2-3 excels most overall. Based on these results, we plan to further direct our attention to Architecture 2-2-3, including development of a prototype.

Table 2. Evaluation of each architecture

Viewpoints		2-3-4	2-2-3	3-3-3
Scalability	Number of Nodes	△	△	◯
	Number of VPNs	◯	◯	×
	Number of Entities	◯	△	△
Transmission Speed		×	◯	◯
Usable Service		×	◯	△
Total		×	◯	△

◯: good △: no good ×: bad

6 Conclusion and Topic for Future Discussion

In this paper we have proposed a new VPN architecture which would allow users to be multiply associated with several VPNs simultaneously. First, we proposed a VPN architecture which would allow users to multiply associated with multiple VPNs. We also discussed the required functionality. The VPN architectures proposed in this paper are layered in configuration, with three network levels (PNL, UNL, and UNL). After determining the functional requirements and evaluating how each representative architecture type's utilized network layer 2, 3, and 4 in realizing each of the network levels, we were able to conclude that that Architecture 2-2-3 was superior. Topics for future discussion include evaluating a wider range of criteria such as manageability, security, reliability, and building an MAVPN prototype to run with existing network technology.

Acknowledgement

This study was performed through Special Coordination Funds for Promoting Science and Technology from the Ministry of Education, Culture, Sports, Science and Technology of the Japanese Government.

References

1. Hara, Y., Ohsaki, H., Imase, M., Tajima, Y., Maruyoshi, M., Murayama, J., Matsuda, K.: VPN architecture enabling users to be associated with multiple VPNs. Technical Report of IEICE (IN2003-50) (2003) 47–52
2. Carugi, M., et al.: Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks. Internet Draft `<draft-ietf-l3vpn-requirements-00.txt>` (2003)
3. Nagarajan, A.: Generic Requirements for Provider Provisioned VPN. Internet Draft `<draft-ietf-l3vpn-generic-reqts-01.txt>` (2003)
4. Callon, R., et al.: A Framework for Layer 3 Provider Provisioned Virtual Private Networks. Internet Draft `<draft-ietf-l3vpn-framework-00.txt>` (2003)
5. Hara, H., Murayama, J., Isagai, K., Imaida, I.: IP-VPN Architecture for Policy-Based Networking. IEICE Technical Report IN2000-101 **100** (2000) 39–46 (in Japanese).
6. Miyoshi, J., Imaida, I., Isagai, K., Murayama, J., Kuribayashi, S.: A Mechanism of Policy-Based Service Control in Communication between VPNs. IEICE Technical Report SSE99-171 **99** (2000) 61–66 (in Japanese).
7. Rosen, E., Viswanathan, A., Callon, R.: Multiprotocol label switching architecture. Request for Comments (RFC) 3031 (2001)
8. Rosen, E., Rekhter, Y.: BGP/MPLS VPNs. Request for Comments (RFC) 2547 (1999)
9. IEEE Standards for Local and Metropolitan Area Networks: Virtual bridged local area networks. IEEE Standard 802.1Q-1998 (1998)
10. Townsley, W., et al.: Layer two tunneling protocol "L2TP". Request for Comments (RFC) 2661 (1999)
11. Kent, S., Atkinson, R.: Security architecture for the internet protocol. Request for Comments (RFC) 2401 (1998)