社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＱＡＩ－25（９）
2007／10／26

Overlay Private IP Address Networks over Wide Area Ethernet

Le Na BUI† Yoshihiro KAWAHARA‡ and Tohru ASAMI‡

† The University of Tokyo Hongo 7-3-1, Bunkyo-ku, Tokyo, 113-8656 Japan
E-mail: {builena, kawahara, asami}@akg.t.u-tokyo.ac.jp

Abstract With the development of Wide Area Ethernet, national scale Ethernet-based service networks have been provided. In this paper, we propose solutions to improve those Ethernet service for enterprise network which is believed to use mainly Ethernet-based network with private IP address. More specifically, we try to overlay enterprise networks with private IP addresses over the Wide Area Ethernet service network.

Keyword Mobile IP, Wide Area Ethernet, PPPoE, 3GPP2, Remote Access

プライベートネットワークを広域イーサネット上に重畳する方式に関する検討

ブイレーナ† 川原圭博‡ 浅見徹‡

†東京大学大学院 〒113--8656 東京都京区本郷 7-3-1
E-mail: {builena, kawahara, asami}@akg.t.u-tokyo.ac.jp

あらまし 広域 Ethernet サービスの普及により全国規模の Ethernet 接続サービスを前提にネットワーク設計ができるようになった．本稿では，企業の LAN 間接続に用いられることが多かったこの種のサービスの利用を一歩進め，企業網へのアクセス網として Ethernet をみなし，プライベート IP アドレスを持つことが多い企業網の一部，もしくは全部を Ethernet 上にオーバーレイする手法について検討する．

キーワード Mobile IP, Wide Area Ethernet, PPPoE, 3GPP2, Remote Access

1. Introduction

In corporations, people at branch offices, telecommuters, and people who are traveling may need access to the corporate network. Inside the corporation a user simply has to connect to the Ethernet and do the authentication to the corporate network under a single administrative management domain, where the management policy of the network is usually determined by the information system department (hereafter called the network management department). Outside of the corporation or at small-and-home-office the access is more complicated since they belong to two different management domains, ISP and their corporate network. The typical way from a mobile terminal such as a laptop (hereafter we refer to it as MN, mobile node) is using PPP software to access to the ISP service network through public access Ethernet services or cellular phone data communication services, then using a VPN tool to access to the corporate network. The first access is managed by ISP, and the second by the network management department.

There are two shortcomings in this architecture.

1) From a point of view of the network management department, they cannot monitor the communication activities of MN unless it is connected through VPN to their network. Thus they cannot prevent malicious activities such as information leaks by the use of MN. In this sense, MN physically located outside the company cannot be controlled by the management authority of the corresponding corporate network. Allowing such kind of MNs outside the network increases the operation overhead at the help desk.

2) From a point of view of a user outside the company, he has to solve his daily network problems by himself getting necessary information from the ISP's help desk as well as from his company's help desk. This requires him to have a level of network engineering technology, which restricts the remote access service to technically advanced users. Each user has to set up the configurations of his MN such that the firewall according to the instructions from

the network management department. Operation mistakes of the firewall setup by a lack of the engineering knowledge may introduce a security hole for the Internet, which is a cause of another type of information leaks. The most of the drawbacks come from the fact that the terminal belongs to two administrative domains. If it can be controlled under a single administration, the information system department in this case, many of the above problems will be solved.

On the other hand, wide area Ethernet services have become popular for the last few years, and cover most of the cities in Japan[1]. With this nation-wide Ethernet service, many of the Japanese companies connect branch offices to their head offices only using Ethernet protocol. This layer 2 based connection service for corporate networks reduces the demand for IP-VPN, a layer 3 based connection service. Such Ethernet services can be used as the layer 2 access media of MN. This combination of the wide area Ethernet services and public access Ethernet services has a potential to connect every class of users, from a single person to a large company office, with just Ethernet. This means a single administrative domain above IP layers can be realized for a set of users distributed in all over the country.

This paper presents the methods to overlay all these corporate networks on a single Ethernet service, where terminals may be located anywhere in the areas of these Ethernet services. What is different from conventional Ethernet access services is that many of corporate networks use private IP addresses such as 10.0.0.0/8. Address conflicts occur ordinarily on the same physical network. Under this condition, we design a network not to force location dependent network accesses on a user.

With such a network environment, once the IT system section of a company has already set up MN for a user, he doesn't have to change anything to access to the corporate network whenever he connects it to the home Ethernet or ones outside the company. Everyone who has or hasn't got knowledge about network can easily use it. In this case, MN is permanently under the security policy of the company and is set up always to access to the company's server, which is one step to protect from information leakage. Of cause there are still tons of other ways for information leakages that we cannot solve all here like MN robbery, using USB memory stick, peeping... These kinds of problems are outside of the scope of this paper.

In the next section, we review some related works. In section 3, we present 2 solutions using Mobile IP (MIP) to reach the main purpose: 1)MIP+PPPoE, 2)MIP+VLAN tag, and some new related problems. In section 4 we compare these solutions. In the last section we make some conclusions and figure out future works.

2. Overviews of Remote Network Accsess Technologies

Before discussing about the detailed remote network access method to a corporate network, we will summarize some conventional network access technologies, related to corporate network to be accessed from foreign networks.

2.1. Remote access methods through ISP networks

In an ordinary network environment for a person outside a corporate network, he has to accress an IPS's network through PPP or PPPoE at his first stage of communication. The former is used by sales workers through a dial up network such as PSTN, a celluar phone network, etc., while the latter is used by workers in SOHO or equivalents through ADSL, FTTH, etc. To access to the corporate network there is another stage: connecting his terminal to his corporate network with some VPN tools such as IPSec. This kind of two stage connection is corrently quite popular. A typical network configuration used in ADSL services is shown in figure 1.

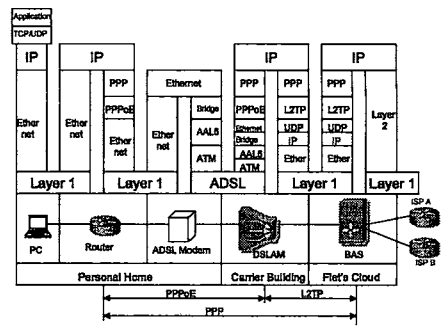

Figure 1 Typical network configurations for ADSL[2]

A PPPoE server in this figure is called as BAS (Broad band Access Server) serving usually tens of thousands of clients. The VPN configuration is based on the similar server-client system between a VPN server in a corporate network and each client. As a whole, the access network topology is a double star with a VPN server as a root node, PPPoE servers and client terminals.

With this method there must be 2 accesses belonging to two different management domains, ISP and the corporate network. As mentioned in section 1, this has weakness in security as well as usability. To increase usability, one solution is to connect each corporate network directly to BAS. Then each MN can be connected to its corresponding corporate network after inputting user id and password. The login overhead is reduced one half, and the usability problem seems to be solved to some extent.

Since BAS is a layer 2 switch, any network, whether or not it uses a private IP address space, can be connected. The role of PPPoE in ADSL is exactly the same as of PPP in PSTN. The difference is that a PPP server is physically located inside a corporate network and the management policy of this PPP server is determined by the network management department of that company, whereas a BAS in a provider's building shared among many corporate networks and the management of PPPoE server is done by ISP, not by each corporate network's network management department. A better method to keep the management privilege of each company for access control of terminals outside the corporate network should be investigated while increasing the usability of users.

2.2. 3G cellular architecture

The recent trend of the increasing number of cellular phones comes to the situation that most of internet access terminals are cellular phones.

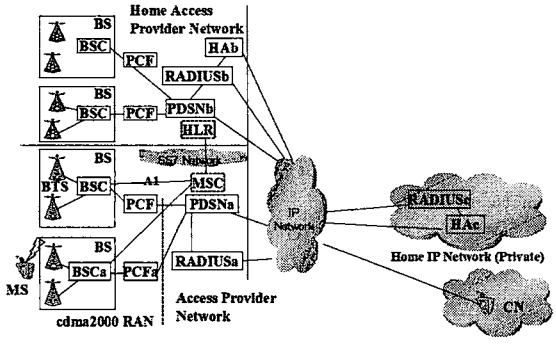

Figure 2. cdma2000 MIP4 architecture

Figure 2 shows cdma2000 wireless packet data network[3]. The network topology is a tree with PDSN as the root node. Between BTS and MN is cdma2000 radio access network, the other parts are connected by wire. The path from MN to PDSN in cdma2000 wireless packet data network is designed to be shared among MNs belonging to different home IP networks, possible with the same private IP address spaces. A specially configured version of Mobile IP is used for this purpose.

2.2.1. FA-mode Mobile IP (MIP)

MIP lets users keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP subnets or networks. Suppose there exists a correspondent Node (CN), which wants to have a communication with MN, the communication is started as follows. In FA-mode MIP, every Mobile Node (MN) has a Home Network (HN) with a Home Agent (HA) which will act as a proxy sever when MN moves to a Foreign Network (FN). In FA-mode Mobile IP, there is a Foreign Agent (FA) in FN which manages a session with every MN by 3 parameters: Home IP Address of MN (HoA), IP address of HA, Care-of Address (CoA) which is a temporary address of MN in FN and is issued dynamically to MN by an auto-configuration protocol[4].

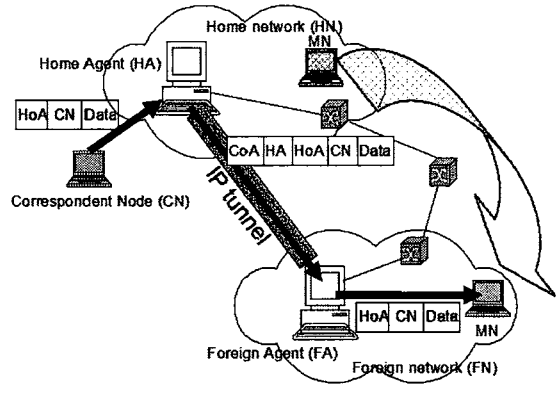

Figure 3 FA-mode Mobile IP architechture

FA advertises its presence by periodically broadcasting Agent Advertisement (AA) messages. An AA message lists one or more care-of addresses. A MN which moved to FN gets CoA from AA and reply with a Registration Reply (RR) message. RR contains HoA and IP address of HA. FA confirms that information by another RR to HA. If the authentication is successful, FA then establishes an IP Tunnel with HA, and the communication between CN and MN is started as depicted in figure 3.

2.2.2. 3GPP2 Mobile IP architecture

In 3GPP2 Mobile IP, PDSN acts as FA as well as PPP server. There is a HA in every private network. MN uses PPP to connect to FA over cdma2000 data link layer.

The reasons why we mention 3GPP2 Mobile IP here are: (1) This architecture allows MN in access provider networks to connect to its home IP network in 3GPP2 Mobile IP terminologies. (2) MNs belonging to different home IP networks share the same access provider network. (3) Most of home IP networks have private IP network addresses such as 10.0.0.0/8. In this sense, it's quite similar to a remote access technology to a corporate network from more general public access networks, which want to design in this paper..

2.3. Wide Area Ethernet and VLAN

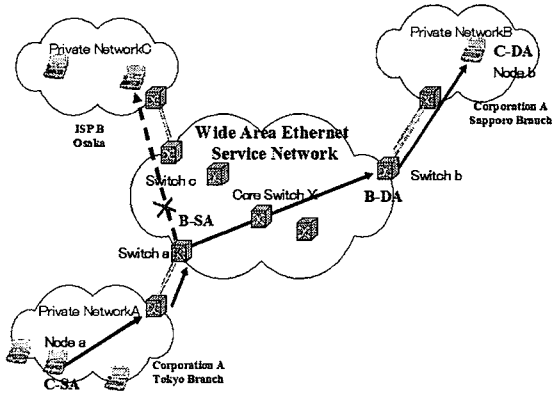

Figure 4 Wide Area Ethernet

Wide Area Ethernet, as depicted in figure 4, includes number of user private network connected to the Wide Area Ethernet service network which covers a large geographical area. Wide Area Ethernet is constructed by switches therefore can supply a high-speed, high-security and low cost Ethernet-based access service.

VLAN technology is used in Wide Area Ethernet to develop a mechanism to allow multiple bridged networks to transparently share the same physical network link without leakage of information between networks. Frames in IEEE802.1Q, 802.1ad and 802.1ah are depicted in figure 8. As for the operation of IEEE802.1ad, when node a with MAC address C-SA sends a frame to node b with address C-DA, switch a finds the corresponding VID of node a, according to the input port number of switch a. After tagging S-TAG with VID to the frame, switch a transfer it to switch b through core switch X. Receiving this frame, switch b checks if this VID corresponds to VLAN calculated from the port to which node b belongs. If it is the case, then switch b removes the S-TAG and transmits the frame to node b.

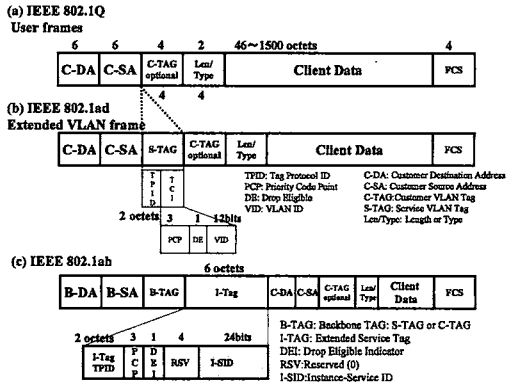

Figure 5 VLAN tagged Ethernet frame format[1]

In figure 5(b) C-TAG is determined by some corporation's network policies and is tagged by switches inside the corporation. S-TAG as well as B-TAG and I-TAG of IEEE802.1ah is tagged by switches of the Wide Area Ethernet service network.

3. Proposed methods

After all written in Section 1 and 2, the purpose of this research: To make a network environment that an enterprise's MN is always under the security policy of the corporation network, the user access is unchanged at outside or inside of the corporation. To reach that purpose we have to unify the ISP access and home network access authentication through the Ethernet service from the usability point of view and also to clearly divide the overall network management policy into two parts: a carrier or ISP domain and a corporate network domain. This is also the first step to design a Wide Area Ethernet-based service network which can offer a more convenient method for remote access to corporation networks.

Learning from the 3G cellular network, we think of using MIP to unify the 2 access authentication and also to divide the management policy between FA and HA. FA manages layer 2 sessions with all MNs by 3 parameters HoA, HA and CoA and executes layer 2 switching between FN and a tunnel to HA. In this sense, the management policy at FA is based on the access privileges of each MN on layer 2 of the provider network. As for HA, it takes care the policies on layer 3 as well as layer 2 of the corporate network.

The single authentication controlled by HA can be done as follows. When MN sends an access request to the

PPPoE server of FN, i.e. FA, FA then automatically transfers this request to HA. If the authentication by HA is successful, FA will send MN the access permission to FN. Therefore the 2 authentication accesses can be unified using this scheme.

Using Mobile IP we have to face other problems:

(1) Multicast can be used in HN. Wide Area Ethernet service also should support this efficient delivery method to a group of MNs from the same HN. PPPoE-based architecture is not suitable to transfer multicast packets.

(2) If we adopt the architecture, similar to ARP, there might be some nodes with a same IP address connected to the Wide Area Ethernet service since MNs use private IP addresses in their HN. If MN uses ARP or equivalents, there would be a conflict over IP address.

(3) IF MN uses ARP or equivalents outside the corporate network, it will reveal its IP and MAC address to other terminals, which must be avoided from the security reasons.

(4) Stronger security is required in the wireless transmission protocol of the Wide Area Ethernet Service and some different techniques from the wired part will be necessary.

In this paper, as the first step, we concentrate on solving problems in the wired part of the Wide Area Ethernet (or assume that all MNs connect to the Wide Area Ethernet by LAN cables). The easy extension from the current access network configurations will be porting 3GPP2 Mobile IP to the Wide Area Ethernet.

3.1. MIP+PPPoE

MIP+PPPoE[5] is similar to 3GPP2's implementation, which uses PPP to connect MN and FA over cdma2000 data link layer. The diffrence here is that a mobile phone or mobile station (MS) uses PPP at both HN and FN. When moves to a new FN, MN receives AA which is encapsulated in a PPP frame, then makes the PPP connection with the PPP server. If we do exactly the same for MN in the Wide Area Ethernet, MN has to use PPP at HN which means that multicast among the corporate network cannot be effectively transferred. Furthermore if FA has to unicast AA to thousands of MN through PPPoE, it would need a very large bandwidth.

We propose a protocol to change between PPPoE and ARP. MN uses ARP at HN as normal and uses PPPoE at FN. After connecting to FN, MN awares of that event by receiving a broadcast frame AA sent by FA via the Wide Area Ethernet. After knowing the MAC address of FA, which is also that of the PPPoE server, MN starts the PPP session with FA without any PPPoE discovery. From then MN doesn't use ARP, so doesn't reveal its IP and MAC address. This reduces the traditional two step discovery procedure for FA and PPPoE server to one step for FA. The more frequent AA broadcasting means the faster handover.

Since AA is not encapsulated in PPPoE frame, MN receives it once before the PPPoE session. When MN leaves FN, after a specified time of PPPoE connection idle, MN terminates PPPoE and change to normal ARP. If MN moves to other FN, another AA will come.

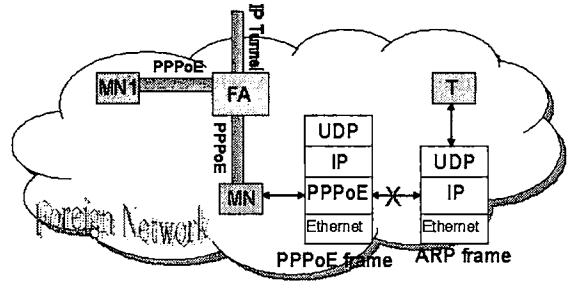

Figure 6 MIP+PPPoE implementation

3.2. MIP+VLAN

In the above method FA has to unicast frames to each MN. When there are a number of MNs from a same HN connected to FN, it's more efficient if FA can group them as a logical network that can use multicast. For example when there is a multicast frame from or to HN, instead of unicasting it to each MN of the group, FA can multicast the frame to the group. Or MNs from a same HN can send frames to the other members without transferring it to HA. We think of VLAN tag since it is a useful tool to make a virtual LAN in Wide Area Ethernet[6].

Assume a simple case like figure 7. We consider that MN and FA are VLAN-aware which can tag VLAN-tag. Have a look at the VLAN-tagged Ethernet frame format in figure 5. There are 2 tasks here:

1)Frames sent by MN to its corporate network have to be tagged C-TAG to specify its corporate network managed by switch A.

2)Switch A has to give all frames, sent by MN with the above C-TAG, VLAN1 as I-TAG.

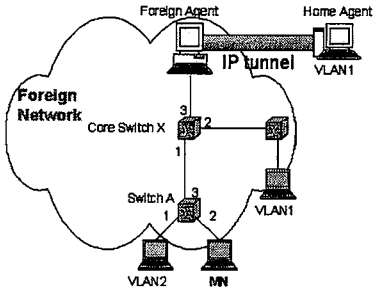

Figure 7 Sample Ethernet

We propose a method by making a new function for switches: automatic VLAN-tag learning. FA broadcasts AA via the Wide Area Ethernet without any VLAN-tag at MN. Switches forward broadcast frames to every port in the Ethernet (but multicast frames are forwarded to only nodes in the indicated VLAN). After moving to FN, MN is aware of that by receiving AA with available C-TAGs generated by switch A. MN then unicast RR to switch A. Switch A resends it to FA with the reserved I-TAG. After knowing the HN of MN and doing the authentication with HA, FA gets VLAN1 used to serve MNs of this HN and lets switch set up a mapping between the previously selected C-TAG and this I-TAG(VLAN1). FA then tags the I-TAG (=VLAN1) to the Registration Reply message and unicast to MN using this tag VLAN1. The Ethernet frame of this message is like in figure 5(c) with C-DA is the MAC address of MN and C-SA is the MAC address of FA. Switch A then generates MN's C-TAG from VLAN1 according the mapping table. Switch A then removes the I-TAG, adds C-TAG and forward the frame to MN. From then, every time MN sends a frame, switch A will tag it with VLAN1 and send to core switch X.

4. Discussion about proposed methods

MIP+PPPoE: Since this method has been applied successfully in 3G cellular network, we think of it first to reach our goal. The advantage of this method is that we don't have to change any protocol of MN or function of switches. Imitating 3GPP2 MIP, we can execute this method immediately with low implementation cost. PPP supplies a connection-oriented network media and stronger security to malicious users than the other method. But there are many disadvantages, and the most serious one is that multicast cannot be efficiently used in FN.

MIP+VLAN: This method further solves the above problem. Multicast can be used among the group of MNs from the same HN, which can reduce a great deal of network traffics. But this method is most difficult to execute since we have to make new function for switches to reconfigure VLAN automatically.

5. Conclusions and future work

Until now we studied methods to reach our purpose. But after listing all advantages and disadvantages of each method, we decide to concentrate on MIP+VLAN method since it can solve most of the problems (1) through (4) mentioned in section 3. Even though it makes us face a big challenge of interacting with switches. An important future work is to design the scalability of the Wide Area Ethernet-based access service.

References

[1] Tohru Asami, "Nation-wide Ethernet Service: The History of Commercial Services and the Direction of Protocol Developments," Journal of IEICE, Vol.90, No.6, pp.470-475, 2007.6.

[2] http://www.infraexpert.com/info/6adsl.htm.

[3] Tohru Asami, "Mobile IP as Service Construction in Cellular Phone Networks," IPSJ Magazine, Vol.47, No.10, pp.1137-1143, 2006.10.

[4] W. Richard Stevens, "TCP/IP Illustrated, Volume 1, The Protocols," Addison-Wesley, 1994.

[5] Le Na BUI, "Overlay Private IP address Network over Ethernet," Procs. of 2007 IEICE Society Conference, B-7-82, 2007.9.

[6] Rich Seifert, "The Switch Book," John Willey & Sons, 2000.