Yet another mobility support for the Internet

SHIN MIYAKAWA,[†,††] SATOSHI ONO,[††] TAKURO KUBO ,[†,†††]
KAZUYUKI TERAO [††] and KATSUYUKI HASEBE[†,†††]

In this paper, we describe a new way of mobility support for the Internet and Intranet called "Unified Access™ ". Different from other similar proposed technologies like mobile IP[1], our scheme is more easy to use, secure, and have the full backward compatibility with existing equipment which is already used.

1. Introduction

Today, there is no need to say more about the importance of the Internet. Also the development of the telecommunication media has become rapidly day by day so that we can use higher bandwidth communication lines at less expensive costs than before and we could not find ourselves without mobile communication systems such as cellar phones, wireless LANs, etc.

Consequently it is very natural that many people now wants to use the Internet and so called Intranet applications on various media. But if using standard Internet technologies, we still need to change settings of the operating systems of the terminal computer and/or pause the connection between it and servers to replace the communication media. In other words, mobile computing still is not fully compatible or not friendly with existing Internet. To satisfy these kinds of demand many researchers and developers have made many attempts in this decade.

Among them it seems that Mobile IP[1),2)]is the likely winner of this race and L2TP technology[3)] also suggests some clues to solve this kind of problem. However, we can still see some defects in these solutions.

Thus, in this paper, at first we summarize existing schemes, especially these two protocols and note their weaknesses. Then we will describe our new solution called Unified Access™ in the next section which is followed by discussion, future work and the conclusion.

† NTT Multimedia Communications Laboratories, Palo Alto, CA, USA
†† NTT Software Laboratories, Tokyo, Japan
††† NTT System Service Department, Tokyo, Japan

2. Analysis of existing schemes

Although there are so many proposals to support mobility for the Internet, we could classify these schemes into two kinds of categories shown as below according to our survey.

(1) new layer 3 protocol which supports mobility
ex: Mobile IP, VIP[4)], ···

(2) VLAN (Virtual LAN)
ex: L2TP, ATM LAN Emulation[5)], ···

We will pick up one representative scheme for each category namely Mobile IP as the former example and L2TP as the later, and summarize the characteristics of each category.

2.1 Mobile IP

Mobile IP, or just "mobility support for the Internet" as the standard of IETF efforts, is the protocol which enables a mobile terminal to communicate with other hosts in the Internet. By using this scheme, even if it is moving around but connecting with the Internet, it could communicate with other hosts.

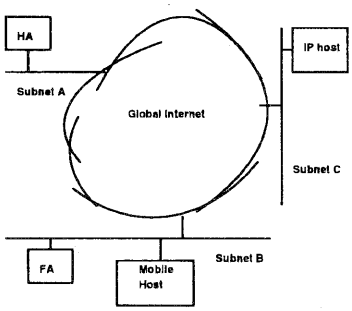

Fig. 1 Mobile IP

Mobile IP consists of four entities, mobile host(MH), home agent (HA), foreign agent (FA) and usual IP host, which are all connected with the global Internet (Fig.1). In this set-

tings, a MH has two addresses. One is the "care-of address" which is assigned by subnet B temporally and other is the fixed address which belongs to the subnet A permanently.

Communications between the IP host and the MH could be described as below. First, when the MH arrives at subnet B, it request a care-of address to subnet B (typically, it is provided by DHCP server, but there are many other possibilities). Then, it communicate with the FA to ask to establish an IP tunnel connection between that FA and its own HA. After this, a packet bound for the MH from an IP host is sent to subnet A according to the routing system of the global Internet. At the subnet A, instead of the MH, the HA receives that packet then resent to the FA through the tunnel and the FA delivers that packet to the MH. The case when packets travel from the MH to the IP host are different. The MH sends a packet to the FA which directly send to the IP host as a normal IP packet.

This mobile IP might looks simple and efficient way to realize the goal (supporting the mobile computing in the Internet world). But unfortunately we could see some numbers of defects of this scheme in the current Internet situation.

(1) *necessity of a new protocol stack within the terminal's OS*
For the sake of communication between a FA and a MH, it is required to introduce a new protocol stack within the terminal's OS, because of using two addresses at the same time. However, ordinary people do not like to change there terminal operating systems' software settings. (For example, a story is found in an article[6] which says at the point of January 1997, 51 percent of U.S. PCs are still running Windows 3.1 or 3.0, while 41 percent are running Windows 95.) This fact indicates that it is hard to let end-users install new protocol stack module or new version of OS, more over it is almost impossible to upgrade operating systems of PDAs which has protocol stacks inside its ROMs

(2) *not compatible with private (so called net-10) IP addresses and a firewall with NAT*
It is easy to see the fact that Mobile IP is not compatible with private IP addresses and NAT(network address translator)[7] Now, some efforts are under way, but basically, or in other words, PHILOSOPHICALLY, Mobile IP is against the concept of firewalls especially with NAT functions ☆1.

Also it might be needed to modify or recompile application programs running on the terminal computers in some case.☆2

In short, Mobile IP is not "backward compatible" with the existing Internet i.e. it is doubtful that mobile IP could be popular among the public, non-technical or ordinary end-users in the practical point of view.

2.2 L2TP

Purpose of the L2TP (Layer 2 Tunnelling Protocol[3]) is creating new advanced dial-up function called "virtual dial-up" to form a VPN (Virtual Private Network) which extends a LAN over the global Internet or other networks.

The system of L2TP is shown in the Fig.2.

A terminal computer with modem is connected with LAC (L2TP Access Concentrator) via the PSTN (Public Switched Telephone Network) ☆3 or the ISDN (Integrated Services Digital Network). In the LAN side (usually located in some office), there is a device called LNS (L2TP Network Server). LAC is a sort of existing NAS (Network Access Server) which accepts in-coming call from users to establish dial-up connection. LAC and LNS are connected with each other via the Internet, some TCP/IP networks, X.25 or the Frame Relay networks (but in this paper, we focus the case of IP only). More detailed argument can be trailed in the L2TP internet draft[3].

The story of the virtual dial-up like this; The terminal computer initiates a dial-up call to LAC in some ISP (Internet Service Provider) using PPP (Point to Point Protocol)[8] as usual. LAC may take part in the authentication procedure to distinguish the end user whether he/she is remote user or not. After LAC detects the fact that the user is remote, and decides which LNS is suitable to use ☆4, if there are no tunnel

☆1 Steve Deering told us this incompatibility with private addresses is the one of the most strong reasons why now he is working for IPv6 which enables huge number of global addresses.

☆2 We understand the fact that if the OS is carefully implemented, it could be fine without this kind of modifications on legacy applications.

☆3 In short, usual analog telephone system

☆4 There are many possibilities to do this. For example, structured username such as user-

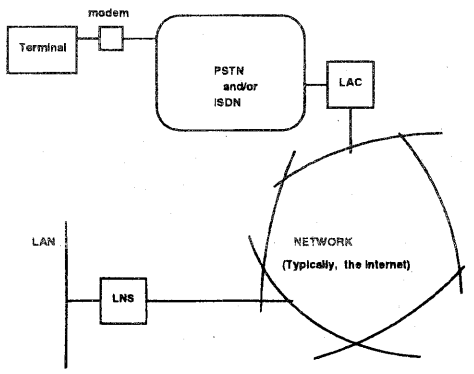

Fig. 2 L2TP

between the LAC and the LNS, it is initiated and one channel in the tunnel is assigned to carry that PPP connection. Then, LNS completes rest of authentication procedure and establish the PPP connection from/to the terminal computer through the tunnel between LNS and LAC.

L2TP provides some good new benefits for both end-users and LAN (or ISP) managers.

(1) *realize a cheap dial-up solution*
Original motivation of L2TP is to gain possibilities of dial-up more easily from more remotely than before, namely from outside the local call area or more, for example, from foreign countries. L2TP could realize a way to dial-up from far away at cheap cost (usually only local call tall).

(2) *utilize private IP addresses without NAT*
Today, due to shortage of IP address spaces, using private IP addresses is almost mandatory. Many organizations do not have enough global IP address spaces to assign to all the host they have so that the equipment called NAT which converts IP addresses inside a packet from/to private address to/from global one, is required. But unfortunately NAT restricts the usage of a TCP/IP connection through it and has some possibilities against securities.
Usually it is enough to read and send E-mails, access database on the LAN and check schedules of colleagues remotely, then by using L2TP, we could use private IP addresses without NAT.

(3) *backward compatibility*
L2TP does not require the terminal computer to change. Legacy system can be used. Only network side equipment is replaced by newer versions. This means that the deployment of this technology is very easy.

Although we could find more benefits of L2TP, now we'd like to point out the limits of this scheme.

(1) *lack of security*
L2TP itself does not provide network security. It requires to use other security technologies like IPsec[9] and OTP (One Time Password)[10], etc. to protect securities. But in many cases, these frameworks are hard to use for especially non-technical users.

(2) *lack of mobility support*
Therefore L2TP is not intended to do so basically, it might not fair to claim this, but we'd like to just mention about the fact that L2TP itself is not enough to provide mobility support for TCP/IP networks.

3. Unified Access™

We introduce our system Unified Access™ as a new way to provide mobility support, virtual dial-up and dial-out with security but without any difficulties to use even if for non-technical users.

The concept could be said as "secure / mobile PPP using high-functional modem". It provides users virtual circuits which

- transport PPP streams,
- could roam over various communication media without disconnecting the communication,
- could be initiated from both sides of the system, i.e. from the terminal computer and/or from the access server too,
- and have the ability to authenticate who use themselves by using advanced security techniques.

To describe the entire system, we define some terms as below.

***e*-modem** An *e*-modem is the high-functional modem which terminates a PPP tunnel from/to an *N*-unit. This handles the authentication procedure and also might have various kinds of media interfaces and functions regarding the "media hand-over" which is described later.

---

name@ispname.com can be used or just using pre-configured settings is of course OK.

e-unit An *e*-unit is defined as an ordinary IP equipment which is connected with a TCP/IP network by a PPP interface[☆] and an *e*-modem. Or, an *e*-unit could be implemented as a host which could terminate the PPP tunnel over the *UA protocol* by itself using a protocol stack of its operating system.

***N*-unit** An *N*-unit is a sort of NAS and similar concept of LNS of L2TP. An *N*-unit terminates multiple PPP tunnels from/to it and could be implemented as an standard NAS with special interface card which can handle *UA protocol*.

Be-unit, BN-unit An Be-unit is the equipment which is connected with *e*-units via some communication media, and other backbone facilities on the UA backbone network. In other hand, an BN-unit is the partner of *N*-units.

AUTH AUTH provides key information needed for authentication.

LPR LPR is the database which provides information about *e*-units' locations and so on.

UA-protocol UA-protocol is the protocol which transport the PPP stream between an *e*-unit and Be-unit and between an *N*-unit and BN-unit.

UA-relay-protocol UA-relay-protocol is the protocol which is used inside the backbone network.

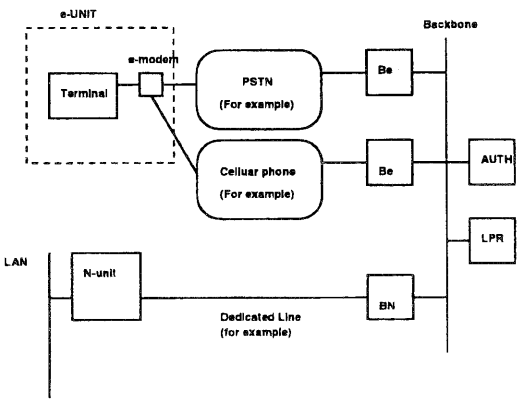

Fig. 3 Unified Access™

[☆] You can imagine just as a normal, standard Windows 95 terminal as an example of *e*-unit, but it is not restricted to it. It could be a router or anything that satisfies this definition.

First, the terminal computer initiates a PPP connection as usual. *e*-modem decides which media is suitable to use according to its settings and situations, then establishes an UA-protocol connection over the physical media with a Be-unit. With helps from AUTH and LPR database, *e*-unit and Be-unit identify each other. Then, Be-unit starts negotiation with suitable BN-unit by using the UA-relay-protocol over the backbone network. After authentication between Be and BN, Be asks BN to establish an UA-protocol connection between BN and *N*-unit which completes by the same way of the *e*-Be connection. As a result, a PPP virtual circuit is established between *e*, Be, BN and *N*.

Of course, this could be done by initiating from the *N*-unit. Logically, dial-up (from *e* to *N*) and dial-out (from *N* to *e*) are the same.

If the terminal want to change its connection media, *e*-modem could initiate other channel to the *N* in the same way, then the PPP virtual circuit can roam from the old path to the new path without disconnecting of logical connection between *e* and *N*.

Since authentication of the mobile terminal is done by using the identification which is stored in the *e*-modem, human users may not required to ask any information to login to the home LAN. This is very similar situation like ATM card of banking system or a credit card, i.e. the hardware of *e*-modem is the identification. Of course, easy password could be used for supplementary protection but this is not too painful to use even for a non-technical end-user.

4. Discussion

To make a comparison with our system and existing schemes, we summarize them again.

(1) new layer 3 protocol supporting mobility

(2) VLAN

The former, the way of creating new layer 3 protocol stack which enables a computer to be mobile, is represented by Mobile IP today. VIP (Virtual Internet Protocol) is also included in this category. This type of solution is fundamental and efficient solution. Therefore, if the IPv6[11] world which has the ability to support mobile computing naturally, this is an ideal way and should be used. But in the legacy IPv4 world, it is not realistic to change all the mobile computers' protocol stacks to enable users could fully functional mobile computing over the Internet. Backward compatibility must be

satisfied.

VLAN is the way of simulating legacy networking technology by using other communication media. L2TP is one of the dial-up types of VLAN technologies and there are so many kind of technologies to simulate the virtual Ethernet type of network. By definition, this will satisfy good backward compatibility with legacy implementations, but we could not find a version of this category which intend to support mobile communication over the various media only with small equipment in the mobile computer side.

Unified Access™is one of the versions of VLAN technologies which intended to support fully functional mobile computing with security and easy to use the scheme. In this context, Unified Access™has every good points which VLAN solutions have, but Mobile IP's weak points.

Way of this secure / mobile PPP way allows us to be free from bunch of IP address space problems and also it gives us the full backward compatibility with existing network protocol implementations which already has the de facto standard protocol for transporting an IP packet or PPP.

We believe Unified Access™is the best way and recent hardware technologies allows us to implement an *e*-modem into a PCMCIA size of card which can be fitted with a notebook computer or small size of PDAs.

5. Future work

Now, we're implementing whole system to demonstrate and prove all the benefits of this scheme. We have a sample demonstration system using emulation software running on the Unix systems and already confirm of the efficiency of the UA and UA-relay protocols. Also more detailed version of the paper will be submitted to some international meetings and magazines in near future.

6. Conclusion

In this paper, we summarized existing schemes which supports mobility for the Internet and pointed out their shortcomings. Then, we described a new way of mobility support for the Internet called Unified Access™which is more easy to use, secure, and fully backward compatible with legacy systems which means that it's easy to be deployed to the public.

Acknowledgments

Special thanks to Dr. Steve Deering of Cisco Systems, Inc., a chairman of the IETF IPng WG, for giving us good suggestions and advises which make us confident about this research. Also thanks to Dr. Mary Baker of Stanford University and her students (and her baby) for making discussion with about this topic which were very helpful, too. We wish to keep these good relationships with all of them. And we would like to thank Dr. Masaki Itoh and other NTT MCL members, also Dr. Haruhisa Ichikawa and colleagues of Global Computing Lab. in NTT Software Laboratories for their support for our activities.

References

1) Perkins, C. (ed.):IP Mobility Support, RFC2002, Standard Track RFC, IETF, Oct. 1996.
2) Perkins, C. : Mobile IP - Design Principles and Practices, Addison-Wesley, 1997. ISBN 0-201-63469-4
3) Valencia,A., Hamzeh,K., Rubens,A., Kolar,T., Littlewood,M., Townsley,W.M., Taarud,J., Pall,G.S., Palter,B. and Verthein,W. : Layer Two Tunneling Protocol "L2TP", draft-ietf-pppext-l2tp-11.txt, Internet Draft, IETF, May. 1998.
4) Fumio Teraoka : VIP: A Protocol Providing Host Migration Transparency, SCSL-TR093-019, Sony Computer Science Laboratory Inc. Technical Report, 1993.
5) Held, Gilbert : Virtual LANs - Construction, Implementation, and Management, John Wiley & Sons, Inc., 1997. ISBN 0-471-17732-6
6) Bradley J. Fikes : Road to Memphis has a few bumps, http://techweb.cmp.com/crw/newsite/172softw040.html, Jul. 1997
7) Egevang,K. and Francis, P. :The IP Network Address Translator (NAT), RFC1631, Informatial RFC, IETF, May. 1994
8) Simpson, W. (ed.) :The Point-to-Point Protocol (PPP), STD51, Internet Standard, IETF, July. 1994
9) Stephen, K. and Randall, A. :Security Architecture for the Internet Protocol, draft-ietf-ipsec-arch-sec-07.txt, Internet Draft, IETF, July 1998.
10) Haller, N. : The S/KEY One-Time Password System, RFC1760, Informatial RFC, IETF, Feb. 1995
11) Deering, S. and Hinden, R. :Internet Protocol, Version 6 (IPv6) Specification draft-ietf-ipngwg-ipv6-spec-v2-02.txt, Internet Draft, IETF, Aug. 1998