Papers on UNIVERGE Hardware

Mobile IP System: UNIVERGE MB Series

By Hiroaki YOSHII,* Gen MOTOYOSHI,* Hiromi TAZAKI* and Hiroyuki NISHIMURA*

ABSTRACT This paper describes the UNIVERGE MB series among the UNIVERGE solution, which can offer IPsec for security and mobile IPv4 for seamless handover at the same time. With UNIVERGE MB, you can use groupware or shared servers from the outside and inside a corporate network in the same manner as you work at your own office desk.

KEYWORDS **Mobile IP, Seamless handover, Security, IP sec, NAT traversal**

1. INTRODUCTION

Security measures for preventing settlement information, transaction information, and confidential information on the Internet from leakage are becoming important as the Internet society gets into full swing these days. Increasing needs for seamless handover among different types of services, such as corporate networks, public wireless LANs and 3G mobile phone networks required to implement ubiquitous services, have been bringing mobile IPv4 technology to engineers' attention, because the mobile IPv4 technology which is capable of providing upper layer-independent mobility function and terminating IP calls at terminals is essential to the implementation of IP telephone systems.

The UNIVERGE MB series system can offer the IPsec function for security measure and the mobile IPv4 function for seamless handover service together. It was jointly developed in software alliance between NEC and ipUnplugged of Sweden. This paper details the UNIVERGE MB series.

2. UNIVERGE MB SERIES OVERVIEW

The current UNIVERGE MB series lineup includes the MB1500 series that has an IPsec hardware board and is suitable for integration into a large-scale network, and the MB1200 series that can be easily integrated into a medium- or small-size network because of its low cost attained by using software for IPsec processing and limiting the number of users that can be connected simultaneously to a low level. Its technical data is listed in **Table I**.

3. INTRODUCTION TO EACH UNIT AND SOFTWARE FUNCTION

Each unit and software function used with the MB series and their operations are briefly described below.

3.1 Roaming Gateway

The roaming gateway unit has home and foreign agent functions based on the mobile IP. As shown in **Fig. 1**, placing it on a corporate network causes it to run as a home agent for mobile terminals in which roaming client software is installed, thus realizing mobility.

If there is a foreign agent on a network to which a mobile terminal will move, the home agent of the mobile terminal is informed of the terminal's c/o address via the foreign agent. If there is no foreign agent on a network to which a mobile terminal will move, the home agent of the mobile terminal is informed of an IP address obtained by the mobile terminal, using the DHCP (Dynamic Host Configuration Protocol), as a coexisting c/o address (transmission of registration request message). If the address is authenticated by the home agent, the home agent memorizes the correspondence (mobility binding) between the unique IP address (called home address) assigned to the mobile terminal and the c/o address.

The home agent makes traffic reach the mobile terminal by receiving the traffic directed to the mobile terminal's home address on behalf of the terminal, adding an IP header to (capsulating) the traffic, and sending it to the c/o address. The home agent

*IP Networks Division

realizes proxy reception by broadcasting charge-free messages and making an ARP response to an ARP request to the home address (proxy ARP). Supporting reverse tunneling set out by RFC3024, the home agent receives packets capsulated by the mobile terminal and directed to a remote party, un-capsulates the packets, and sends them to the remote party.

Mobile terminals use a wide variety of communication media ranging from Ethernet to wireless LAN and dial-up lines. If the c/o address of a mobile terminal is changed because of its communication media or its connected wireless LAN base stations being switched, the mobile terminal informs the home agent of the newly obtained c/o address, and the home agent updates its mobility binding and sends traffic to the new c/o address. Even when a c/o address is changed, the communication session is not disconnected, because the home address is not changed.

Traffic transmitted between a mobile terminal and the home agent can be encrypted with respect to IPsec so as to implement a secure remote access solution by introducing a roaming gateway into a corporate system. **Figure 2** shows the remote access operation performed with the UNIVERGE MB series.

Table I Specifications of MB series.

Item	MB1500	MB1200
Protocol function	IPv4 (RFC791), IP-IP Tunneling (RFC2003)	
Mobility function	Mobile IP HA/FA (RFC3344), Reverse Tunneling (RFC3024) Mobile IP NAT traversal	
Firewall function	Ingress/Egress filtering function, SRC/DST port number, Filtering by the protocol, session state management function	
NAT function	NAT/NAPT (RFC3022)	
VPN function	IPsec transport mode / tunnel mode, IKE (RFC2409), IPsec (RFC2401 ~ RFC2408), DES (RFC1829) / 3DES (RFC1851)	
	IPsec hardware accelerator loading	–
Number of simultaneous connection	100/200/500/1,000 user	100/200 user
Throughput	200Mbps (max)	20Mbps (max)
Interface	10BASE-T/100BASE-TX/ 1000BASE-T (RJ45) : 4port	10BASE-T/100BASE-TX (RJ45) : 3port

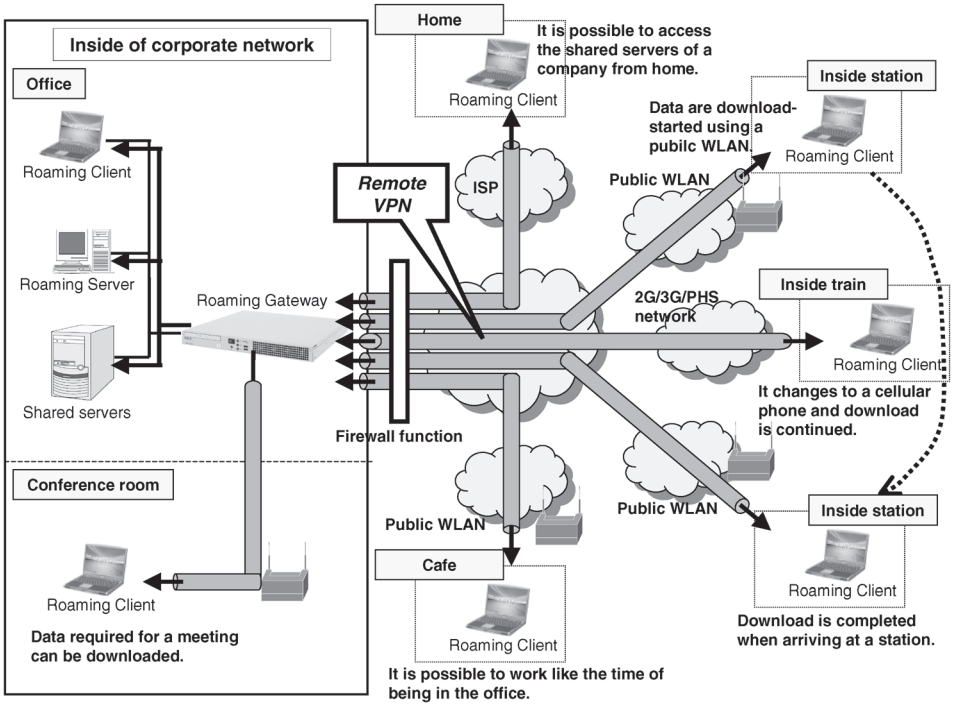

Fig. 1 Introduction case of MB series.

Other typical functions are described below.

(1) VLAN Function

This function supports IEEE802.1Q to enable up to 32 virtual interfaces to be generated on one physical interface.

(2) NAT Traversal

The conventional capsulation set forth in RFC2003 uses IP-IP tunneling. It poses a problem that the mobile IP cannot be used in an environment in which mobile terminals have acquired local addresses, because packets cannot pass through general NAPT routers. The UNIVERGE MB series enables roaming in this environment by supporting UDP-based packet tunneling.

3.2 Roaming Client

This software is installed in a mobile terminal to implement a mobile IP client function. Its Windows version is available. Its typical functions are explained below.

(1) Mobile IP-Based Seamless Communication

Using the mobile IP, the software enables a session to be continued even when the IP address is changed as the communication media change. In addition, the software has an Ethernet or wireless LAN link-down/-up function or an automatic dial-up/on-hook function triggered with a threshold to wireless LAN radio intensity in order to reinforce the convenience of seamless communication. The software can also automatically select an optimum connection mode according to whether there is a foreign agent or DHCP server, so it makes unnecessary the Windows network re-setting that may be needed when a shift occurs to a different network, hence improves user-friendliness.

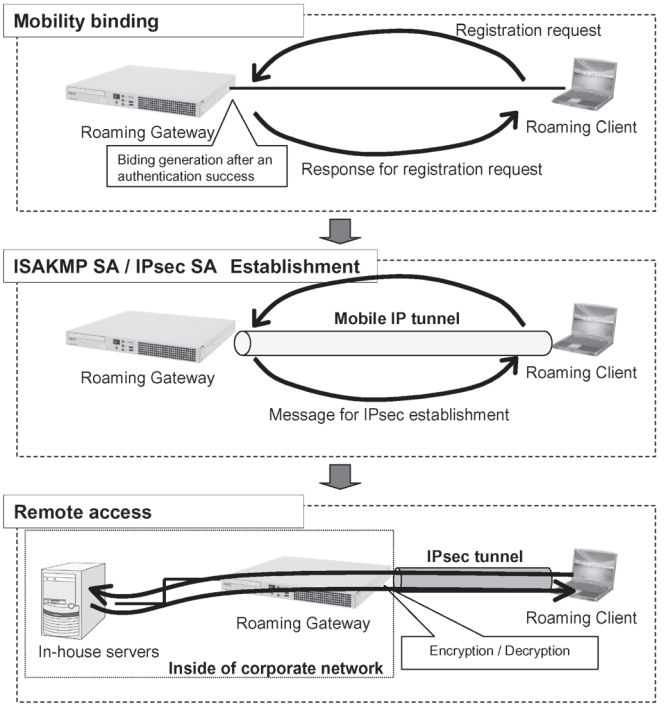

Fig. 2 Behavior in remote-access.

(2) Encryption

In addition to the aforementioned mobile IP function, the software implements secure access from the Internet to a corporate resource by establishing an IPsec connection with the roaming gateway, using ISAKMP, encrypting traffic, and transmitting packets by the mobile IP protocol. The software can also reduce troublesome settings by downloading key information used by the mobile IP and ISAKMP in a form of profile from a roaming server described later. In addition, the software supports holding of multiple profiles, which can be switched easily. Using the previously registered foreign agent or DHCP domain as a trigger, the software may be able to perform non-encrypted communication depending on the network connected.

3.3 Roaming Server

Employing a server in which the roaming server software (both Windows and RedHat Linux versions are available) supplied together with this product is installed on a network makes it possible to set up and manage the roaming gateway and distribute mobile terminal profiles on a GUI basis. It is also possible for one roaming server to control more than one roaming gateway, so it is easy to introduce the product to a large-scale network. Other functions are described below.

(1) RADIUS Authentication and Accounting Function

When the home agent receives a mobile IP registration request message, it is possible to make the roaming server take charge of authenticating the message. The roaming gateway can send information about the connection time and communication amount of mobile terminals, using the RADIUS accounting protocol. The roaming server supports reception of this information.

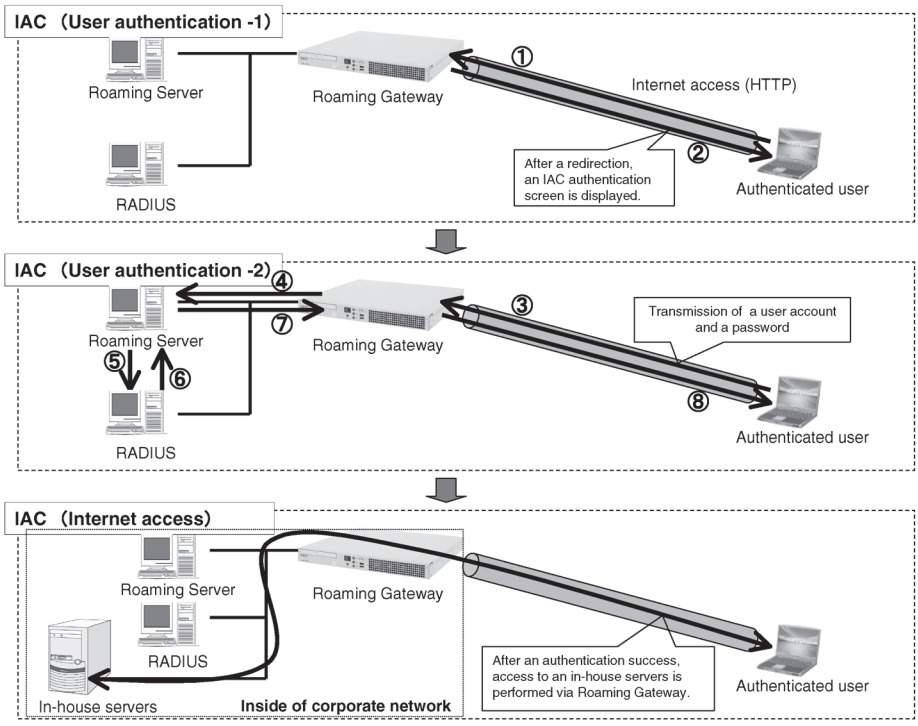

Fig. 3 Behavior in cooperation between MIP and IAC.

(2) IAC (Internet Access Control) Function

The UNIVERGE MB series has an IAC function independent of the mobile IP. The IAC function enables access via the roaming gateway for authenticated users by dynamically changing the firewall rules of the roaming gateway according to web authentication. In this process, the roaming server offers web server functions and controls the firewall of the roaming gateway. It also supports local database-based authentication and external RADIUS server-based authentication for users.

Traffic for users for which mobile IP registration requests are authenticated is redirected to display an IAC authentication window on a browser by combining this function with the mobile IP (see **Fig. 3**). Linkage with other authentication servers supporting RADIUS is realized by building an environment in which access to a corporate network is allowed upon completion of Web authentication.

4. CONCLUSION

This paper has introduced the UNIVERGE MB series.

We assume that seamless roaming based on the mobile IPv4 technology of the UNIVERGE MB series is important to build ubiquitous networks. We will continue to enrich the security functions designed around the mobile IP technology in order to develop products that can offer more powerful ubiquitous services.

Received September 21, 2004

* * * * * * * * * * * * * * * *

*Ethernet is a trademark of XEROX Corporation.

†Windows is a trademark or a registered trademark of Microsoft Corporation and used in the USA and other countries.

‡RedHat is a registered trademark of RedHat software, Inc.

§Linux is a trademark or a registered trademark of Linus Torvalds and used in the USA and other countries.

Hiroaki YOSHII joined NEC Corporation in 1987. He is currently Manager of IP Networks Division.

Hiromi TAZAKI joined NEC Corporation in 1991. She is currently staff member of IP Networks Division.

Gen MOTOYOSHI joined NEC Corporation in 1995. He is currently senior staff member of IP Networks Division.

Hiroyuki NISHIMURA joined NEC Corporation in 2002. He is currently staff member of IP Networks Division.

* * * * * * * * * * * * * * * * *