UDC 621.398: 681.3

Network Applications for Mobile Computing

●Akiyoshi Ochi ●Toru Atsumi ●Keiji Michine

(Manuscript received March 26,1998)

Mobile computing, which enables real-time remote access to corporate networks from a notebook computer, is now being spotlighted as notebook computers become smaller and more complex, and ISDN, wireless networks, and cellular phones become more popular. Unlike conventional networks, many problems encountered when constructing mobile computing environments affect mobile computing users and network administrators. This paper discusses these problems and introduces three communications software products to help users overcome them.

1. Introduction

The current trend toward downsizing and greater complexity has enhanced the mobility of computers, thus affording convenient use anywhere at any time. The significant progress made in communications technology has facilitated the explosive growth of ISDN and wireless networks, in addition to the popularization of PHS and cellular phones. Such advanced technologies have thrust mobile computing, which enables the remote access of electronic information, into the public limelight.

Corporate information systems require a network environment for mobile computing so that employees can effectively use business information, promote the sharing of information, expand lines of communication, improve work efficiency, and enhance customer confidence and satisfaction. However, unlike conventional networks, many problems and inconveniences imposed by mobility are encountered when companies construct environments for mobile computing.

This paper identifies and discusses these problems then introduces communications software with which users can overcome them.

2. Problems of Mobile Computing

We first considered situations in which mobile computing is used to identify problems that occur when constructing a mobile computing environment based on existing network infrastructure.

As previously mentioned, mobile computing requires an environment in which anyone and any necessary information can be accessed at any time from any location. For mobile computing, "from any location" is the key consideration. Thus, the most pressing problem is how to construct a network environment that enables access from any location in the same way.

The use of mobile computing can be categorized by location as follows:

1) Inside the company

In this case, employees must go to other departments with portable computers to access information servers in the office, the Internet via LAN, or infrared communications environments. Otherwise, company employees must go to other companies to access information servers via LAN or infrared communications environments.

MICROSOFT CORP.
EXHIBIT 1010

2) Outside the company

In this case, employees access information servers in the corporate networks from outside the company (e.g., while on a train, in a hotel, or at home) using cellular or public phones to obtain information or send reports. This includes accessing corporate or WWW servers on the Internet through an Internet Service Provider (ISP).

2.1 Problems When Used Inside the Company

LAN or an infrared communications environment is generally used to access a server in our department or another department from a portable computer. In this case, the following needs must be addressed:

1) Constructing information outlets

Employees going to another department or company to access servers in their departments or on the Internet must connect their computers to the network there. This is why access points (information outlets) must be provided for mobile users in every department. Since conventional network environments are constructed based on access from fixed computers, there may be no access points for mobile users. Consequently, information outlets (i.e., access points for LAN or infrared communications) must be constructed for mobile computing.

2) Unified administration and automatic distribution of communications environments

Due to the growing prevalence of the Internet, TCP/IP is commonly used in corporate networks. Unfortunately, this protocol is based on access from fixed computers. New protocols like Mobile IP[1] are now being studied to apply TCP/IP to mobile computing in some prominent institutions and corporations, but this will take time to complete.

Even with information outlets provided, mobile users must obtain the following location-dependent information and configure their mobile machines to construct the same access environments as in their departments:

- Information required to communicate with TCP/IP(e.g., IP address, subnet mask, gateway address)
- Names of printers and information about printer drivers required to print documents
- Names and addresses of shared servers required to exchange information
- Information about the operating environments of application software

Some basic information described above (e.g., IP address, subnet mask, gateway address) can be automatically obtained from the Dynamic Host Configuration Protocol (DHCP)[2] server. The following problems are encountered, however, when applying DHCP to mobile computing.[3]

- Difficulty in pooling IP addresses for mobile users due to depleted IP addresses
- Mobile computer access of multiple IP addresses
- Unsecured network access due to IP address assignment upon request

Because information about printers, shared servers, and operating environments for application software is unique to each department's network, this information must be obtained from the network administrator of the department concerned. Thus, mobile users wishing to remotely access a conventional network environment must first obtain the information required from the network administrator then manually reconfigure their computers. These tasks impose a large burden on both administrators and mobile users.

To enhance the convenience of mobile computing environments and relieve the burden on network administrators, a mechanism is needed to enable the unified administration of information needed by mobile users, and to automatically obtain the information when required and reconfigure the mobile computers.

3) Assurance of network security

Constructing mobile computing environments in corporate departments or subsidiaries may incur the risk of unauthorized network access from outside the company. Since confiden-

tial information within a department or company may be leaked, adequate provisions should be made for security when constructing mobile computing environments.

For example, the conventional mechanism of DHCP allows anyone to obtain an IP address from the DHCP server in the network and then access the network. A mechanism is required to verify users attempting to access the network, but which does not assign IP addresses to unauthenticated users for network access. A means to prevent mobile users from accessing particular servers that keep highly confidential information is also needed.

Since mobile users connected to LAN can view information flowing through the network, important information should be transmitted with data encryption, or LAN segments for mobile users should be kept separate in the department.

2.2 Problems When Used Outside the Company

Remotely accessing a corporate server with a portable computer generally requires connection through a wireless network using cellular phones, or through a dial-up network or ISDN using public phones or hotel telephones. Therefore, the problems posed by using a wireless network or accessing a corporate network through ISP should be addressed as follows:

1) Reducing communication costs

The remote access of corporate networks poses accounting problems since most communication is performed through a Wide Area Network (WAN) like a dial-up network. Therefore, a more cost-effective means of communications, such as one that applies mobile agent technology, is urgently needed.

This technology allows mobile agents arranged in the corporate network to perform tasks as instructed and report the results via notebook computers. In this way, connection need not be maintained while the mobile agents actually perform the jobs, and communication costs can be significantly reduced.

Such compression technologies as data compression and IP header compression also help reduce communication costs. Other technologies are also being studied to reduce costs. The most important considerations for mobile computing are reducing the amount of data transferred and the connection time.

2) Automatic recovery from line errors

During communication using cellular phones through a wireless network, radio waves may be obstructed and the computer disconnected. In such case, the call must be made again. This takes time and is an inefficient means of communicating.

Therefore, a means of automatically reconnecting notebook and other computers, and resuming data transfer from the point of interruption must be devised so that disconnection is transparent to the application software.

3) Countermeasures against wiretapping of data and illegal access of corporate networks

There may be other means of accessing a corporate network via the nearest ISP to reduce communication costs. However, a high-risk factor exists since confidential information may pass through the Internet and be illegally accessed. Therefore, a means to enable cryptographic communications must be devised.

Another means to protect access points in corporate networks is needed. Anyone who knows the phone number of an access point and the password can access a corporate network through a mobile computing environment. This is why the illegal access of networks is relatively easy. More importantly, a system could actually be destroyed by the leaking of confidential information. Therefore, firewalls should be installed at the access points of corporate networks with strict authentication to prevent illegal access.

We have identified and discussed existing problems when constructing mobile computing environments. The next chapter introduces some communications software products with which

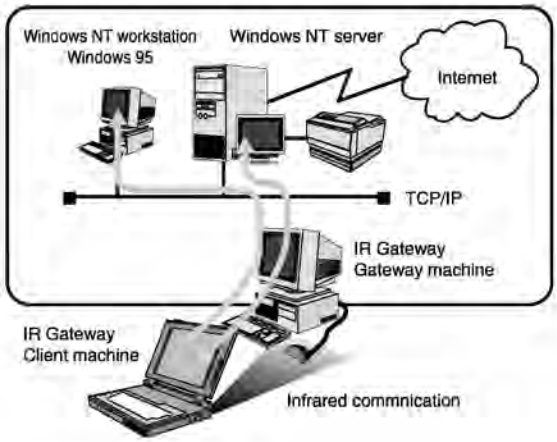

Figure.1
IR Gateway.

users can overcome these problems.

3. Mobile Computing Software

To solve the problems mentioned above, we developed the following products :

- IR Gateway
- Network AccessDirector (tentative name)
- WebCross

3.1 IR Gateway

IR Gateway is a software product that enables the wireless access of TCP/IP-based intranets by employing standard infrared ports implemented in notebook computers and INTERTop[note1] (**Figure 1**).

IR Gateway allows mobile computers (e.g., notebook computers, INTERTop) used in the company to easily access LAN without having to consider each network's environment. This solves the problem of having to reconfigure network settings for every site visited (as described in Chapter 2). This software also eliminates the need for such hardware options as a LAN card and direct cable connection for mobile computers, and enables LAN environment access without sacrificing the portability of mobile computers. IR Gateway features the following :

1) Easier mobile computer setup

IR Gateway provides a simplified DHCP function that allows client mobile computers to communicate without having to consider the environment (IP address).

Simplified DHCP runs on gateway machines and automatically sets the information necessary for TCP/IP communication, such as the IP address, default gateway, and Windows Internet Name Service (WINS).[4] This simplifies mobile computer setup.

2) Network Address Translation (NAT)[5] function

The existing IP network requires an IP address for each host. The number of usable IP addresses is limited, however, and the depletion of IP addresses becomes a problem as the number of hosts increases. IR Gateway provides the NAT function, which eliminates the need for a new IP address when a mobile computer is connected via a gateway machine.

This function makes it possible to share IP addresses previously assigned to a gateway machine. For communication between a gateway machine and mobile computer, IR Gateway uses a private IP address. This address is created automatically on the gateway machine and set up in the mobile computer by the simplified DHCP function above.

3) Routing function between a mobile computer and LAN

With IR Gateway, a mobile computer usually uses the IP address of a subnet (network number) other than the network to which the gateway machine belongs. Therefore, a mobile computer sends all packets to the gateway machine as the default gateway. To route these packets, IR Gateway queues the packets once on the gateway machine. Once the destination address of each packet is determined by ARP,[6] the packets are routed to LAN.

---

note1) INTERTop is a mobile terminal developed by FUJITSU LIMITED.
INTERTop is a registered trademark of FUJITSU LIMITED.

4) Improved performance

The maximum transfer speed of IrDA is 115.2 kbps or 4 Mbps. Though communication speed is much faster than that of serial transfer or a WAN network, it is much slower than the 10 Mbps or 100 Mbps of LAN media. To improve performance, IR Gateway compresses data for communication between a gateway machine and mobile computer. By compressing data, transfer speed is increased 3 or 4 times.

5) Compliance with WINS protocol

When multiple gateway machines equipped with IR Gateway run on LAN and a mobile computer is moved between each machine, the IP address of the mobile computer on LAN will change dynamically. The IP address of the mobile computer does not change, however, and registration in WINS is not updated. Consequently, the contents of registration in WINS may differ from the actual IP address from the standpoint of LAN. To solve this problem, the gateway machine checks the contents of WINS registration upon detecting a connection by IR. If the IP addresses do not match, the gateway machine updates the registration instead of the mobile computer.

3.2 Network AccessDirector

Network AccessDirector is a product now being developed. It allows employees who use notebook computers or handheld PCs to access an intranet more easily, while reducing the administrator's intranet workload.

Network AccessDirector provides all the necessary functions mentioned in Chapter 2 (e.g., automatic configuration of network environment information, network security function) for workers dispatched to company offices or other companies.

1) Automatic configuration of network environment

Mobile users wishing to access the intranet must first configure the address and other information for each application (e.g., browser, mailer) in addition to various network settings about the TCP/IP stack. Such users often ask the intranet administrator for help in completing their work. For instance, to print something, these users ask about which printer (and printer driver) to use, or to pass files to someone, they ask about which network drive of which server should be shared. The growing workload placed on intranet administrators can no longer be ignored. To resolve such problems, we will implement the three features described below.

Table.1 List of configuration items.

Function	Item
Browser	Homepage, Security, Connection, Proxy server
Mailer	Server information (SMTP, POP3 server address), User information (User name, Password, E-mail address)
6680 emulator	Connection (Procedure, Information name), Local information, Relay device, Device type, Session, Extended function
Others	Files configured by administrators in advance, Registry key and value

- Automatic configuration of the application environment

This feature allows Network AccessDirector servers to configure mobile computers automatically according to the environment information set by the administrator in advance so that mobile users can use applications like browsers when accessing the intranet in the field. **Table 1** lists examples of configuration items.

- Automatic sharing of network drives

When mobile users access the intranet in the field using shared resources on the Network AccessDirector servers set by the administrator in advance, this feature maps network drives and creates shortcuts on the desktop.

When a mobile computer is connected to the network, files, Web pages and display notices for network users, as well as floor plans (showing the location of printers, etc.) can be opened as the need arises.

- Automatic sharing of printers

When mobile users access the intranet in the field using shared resources on the Network AccessDirector servers set by the administrator in advance, this feature automatically configures the

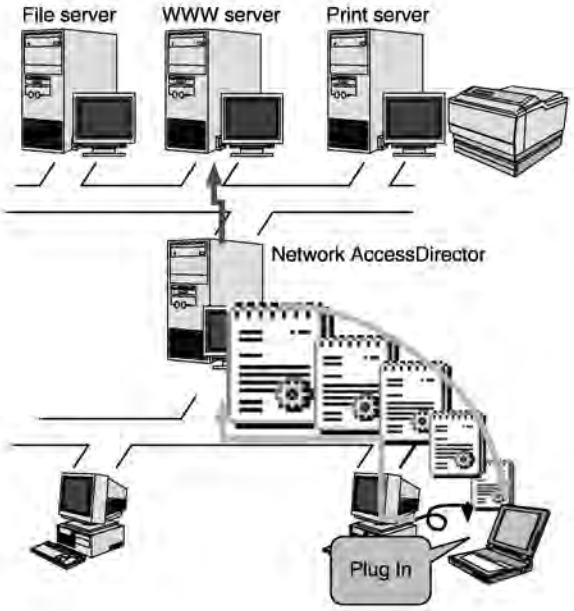

Figure 2.
Automatic configuration of network environment.

computer environment (for sharing network printers and selecting printer drivers) and allows users to print.

2) Automatic reconfiguration of the network environment

Thanks to this feature, a mobile computer is automatically reconfigured and restored to the previous network settings made in the field. Automatic configuration and this automatic reconfiguration allow mobile users to switch the configurations of mobile PCs automatically in different network environments and access the network without having to consider location (**Figure 2**).

3) User authentication and restricted access

The risk of internal information being leaked exists whenever a mobile user uses another section's LAN environment. Network AccessDirector provides a function that authenticates users for access to the LAN environment and prevents unauthenticated users from making such an access. Network AccessDirector provides another function that blocks packets other than those of specified services and addresses. This function

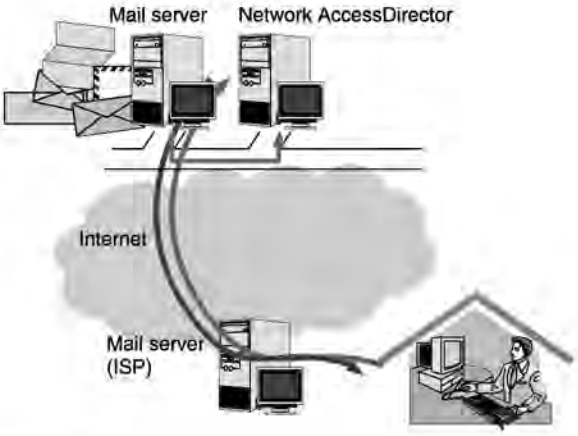

Figure 3.
Mail transmitter.

restricts access to critical information and protects against leakage of internal information.

4) Mail transmitter

As a means of communication, e-mail is an essential feature for mobile users. To receive mail in the field, users must access the POP3 server in their HOME LAN (in the office) or transfer received mail to an account that can be accessed in the field. Accessing the server poses the problems of cost and security. To transfer mail, users must ask the mail server administrator to change the configuration in advance, which increases administrative costs and may prove impossible in the event of a sudden business trip.

To resolve such problems, Network AccessDirector provides the mail transmitter feature. The mail transmitter allows users in the field to transfer mail addressed to the POP3 server in the HOME LAN (in the office) to their home (ISP) or mail account in the network without having to change the current configuration (of the POP3 server) and network settings of the home environment (**Figure 3**).

Mail transmitter works as a POP3 client. It operates as follows:

1) Mobile users e-mail transmission requests to the mail transmitter. The following information must be included: Authentication information, HOME LAN account, destination

Figure 4.
WebCross.

address, and attribute of transmitted mail (e.g., enable/disable file attachment). Transmission requests are encrypted with authentication information attached to protect against intrusion.

2) Upon receiving a transmission request, the mail transmitter decrypts the message, authenticates the client, then reads mail from the account (alternative reception) according to the transmission request.

3) The mail transmitter transfers mail according to the reported conditions.

3.3 WebCross

WebCross[note2] is a software product that enables mobile users to access a mainframe computer based on Internet/intranet infrastructure and its access environment (**Figure 4**).

1) Using existing infrastructure

Communicating with a mainframe computer from a personal computer conventionally requires special software with a terminal emulation function, such as WSMGR.[note3] In many cases, however, such terminal emulation software is not installed at mobile terminals (e.g., PDA, HPC, INTERTop) due to limited resources and OS support. When considering the means of access, access from a mobile computer poses many problems. A mobile computer requires special hardware (e.g., a communication card for the communication protocols), entails problems of communication cost and security due to the limited number of access points served by the mainframe computer or Fujitsu Network Architecture (FNA)[note4] gateway server, and requires registration in the mainframe computer beforehand. To overcome these problems, we developed the following functions:

- Host data conversion into HTML

WebCross employs a method of converting F6680/I3270[note5] format data into HTML-based text data for display on a client machine's WWW browser in conjunction with the FNA gateway server and WWW server. Consequently, mobile users can use the F6680/I3270 display terminal function without needing to change their existing mobile computers (hardware and software) on the network environment. WebCross also supports the display of F6680/I3270 screen input fields in the same format as used by the WWW browser.

- Code conversion

WebCross offers a function to automatically convert Japanese (2-byte) code and one-byte code (which differ between the mainframe computer and WWW browser) by preparing conversion tables on the server machine beforehand. User-defined code other than standard codes is converted the same way.

- Emulator private key

F6680/I3270 terminals have special keys such as program function (PF) keys and program access (PA) keys that are not supported by WWW browsers. The keypad function provides a method of entering these keys from a WWW browser screen.

---

note2) WebCross is a registered trademark of FUJITSU LIMITED.
note3) WSMGR is a registered trademark of FUJITSU LIMITED.
note4) FNA is the generic name of protocols used to access Fujitsu mainframe computers.
note5) F6680/I3270 is the name of a device used to access mainframe computers.

2) Support of PDAs

In addition to the functions described in 1) above, the following functions were developed for use on PDAs.

- Adjustable display size

The display size of PDAs is much smaller than that of notebook PCs, and the host screen is poorly displayed when converted as is. WebCross solves this problem by providing a function to thin out the display so that blank lines are not displayed.

- Improved response

WebCross operation with a PDA is performed via a dial-up connection. The built-in modems of existing PDAs offer relatively low speed and normally communicate at about 14.4 to 33.6 kbps. When using a digital mobile phone, the maximum transfer speed is 9,600 bps. Response had to be improved to reduce the stress of waiting. This was achieved by minimizing the data required for display and reducing traffic. In addition to the thinning out of blank lines mentioned above, we converted bitmap data into buttons to reduce the amount of data. We also employed the user template function described below to display only the information necessary for the user, and thereby minimize traffic.

- Support of built-in browsers

The built-in browsers of PDAs offer fewer functions than general-purpose ones (like Internet Explorer and Netscape Navigator [note6]). Thus, we ensured compliance with HTML 2.0 for converting F6680/I3270 format data and enabling display on most existing browsers. For browsers that support HTML versions after 2.0, we implemented a user template function that enables users to describe custom templates and use the latest browser functions.

note6) Netscape Navigator is a registered trademark of Netscape Communications Corporation.

4. Conclusion

This paper discussed specific problems that should be considered when constructing a mobile computing environment, and introduced communications software products developed to overcome these problems.

Unfortunately, these products cannot resolve all aspects of these problems. To construct better environments for mobile computing, many remaining problems involving hardware, protocols, application software, and other considerations must be addressed.

We should approach these problems not only from a technological standpoint, but also with regard to the prevailing characteristics of mobile computing at a given time.

References

1) C. Perkins : "IP Mobility Support. RFC 2002, Oct. 1996.
2) R. Droms : Dynamic Host Configuration Protocol. RFC 1541, Oct. 1993.
3) F. Teraoka : Protocols Providing Seamless Mobility. J. Inst. Elec. Engrs. ,Jpn., **80**, 4, pp.344-349 (1997).
4) John D. Ruley, David. Dix, David W. Methvin, Martin Heller, Arthur H. Germain III, James E. Powell, Jeffrey Sloman, and Eric Hall : Networking Windows NT. 1st ed., New York, John Wiley & Sons, Inc., 1994, p.538.
5) K. Egevang, and P. Francis : "The IP Network Address Translator (NAT)." RFC 1631, May 1994.
6) Douglas E. Comer : Internetworking With TCP/IP Volume I: Principles, Protocols, and Architecture. 3rd ed., New Jersey, Prentice-Hall, Inc., 1995, p.613.

Akiyoshi Ochi received a B.S. degree in Electrical Engineering from Ehime University in 1987.
He joined PFU Ltd., Machida in 1987 and has been engaged in the research and development of software for Integrated Services Digital Network (ISDN) and infrared (IR) communication.

Toru Atsumi received an M.S. degree in Applied Physics and Chemistry from the University of Electro-Communications in Tokyo in 1990.
He joined Fujitsu Ltd., Kawasaki in 1990 and has been engaged in the development of communication software for personal computers.

Keiji Michine received an M.S. degree in Mathematics from Ehime University in 1983.
He joined PFU Ltd., Machida in 1983 and has been engaged in the research and development of mainframe connectivity software for personal computers.