(2) MAPS

Motoyasu Takehara, Takao Komori,

Hideki Kinjo and Shigeki Kawabata

We developed MAPS in order to provide safe, secure and convenient Internet access from mobile environments, for the main purpose of expanding the FOMA data communication traffic. This made it possible to access the Internet via ADSL and FTTH from home or office environments or via wireless LAN from subway premises, coffee shops, public facilities, etc., depending on the usage location and environment of customers.

1. Introduction

DoCoMo has so far provided Mobile OPEration Radio Assistant (mopera) net surfing and mopera mail, which are mobile Internet access and e-mail services, respectively. These services do not require any provider subscription, i.e. they are charged based on communication volumes, and the main targets were Personal Handy-phone Systems (PHS). In the future, however, it will be necessary to aggressively shift all data communication traffic to FOMA and provide subscription-based Internet access from home and office environments as well as via public wireless Local Area Network (LAN) using the same ID.

The mopera U[*1] service was launched in June 2005; it is a subscription-based Internet access service whose main business purpose is to expand the data communication traffic of FOMA and others. The mopera U service uses FOMA data communication to provide safe, secure and comfortable Internet access environment, supporting fixed BroadBand (BB) connections such as Asymmetric Digital Subscriber Line (ADSL) and Fiber To The Home (FTTH) as well as Internet access via wireless LAN such as Mzone[*2] (**Figure 1**). This allows customers to select a suitable access line according to the service usage location. **Table 1** shows services provided for each access line.

This time, we developed Multi Access Platform System (MAPS), for providing mopera U services. This article explains the technologies utilized in MAPS.
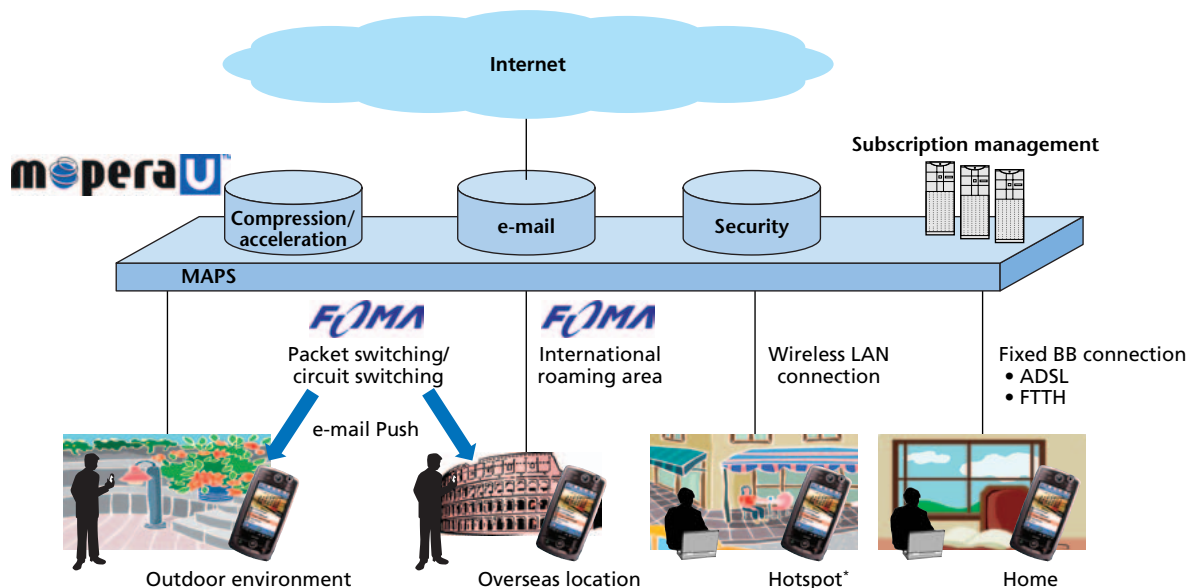
2. Network Control

MAPS, which is a dedicated system for providing mopera U services, blocks unnecessary packets and handles bandwidth control in order to provide the optimal network services according to the characteristics of each access line, such as bandwidth and always-on connection status.

2.1 Control of Unnecessary Packets

Currently, new worms such as Blaster and Sasser are generated on an everyday basis all over the Internet, and many of

---

*1 mopera U: A trademark of NTT DoCoMo, Inc.
*2 Mzone: Public wireless LAN service provided by NTT DoCoMo, Inc.

* Areas corresponding to Mzone (including roaming inside and outside Japan).

Figure 1 Service overview

Table 1 Services provided by each access line

Access line		FOMA packet switching	FOMA circuit switching	ADSL*	FTTH*	Mzone*
Network control	Control of unnecessary packet					
	Bandwidth control					
	International roaming					
Web browsing	Web compression					
	Website block*					
e-mail	Automatic reception	(M1000 only)				
	POP/IMAP simultaneous use					
	e-mail virus check*					
User support	Welcome message					
	Automatic terminal setting					

* Requires optional subscription.

these flood the networks with junk packets to which the infected terminals are connected. Since FOMA adopts packet billing, it is essential to provide a safe and secure Internet access environment by protecting customers from unnecessary packets sent by such worms and, to protect other terminals from junk packets sent from the infected terminals when customers' terminals are infected.

MAPS incorporates an Intrusion Prevention System (IPS) for the FOMA and fixed BB access lines in order to block such junk packets and adopts a mechanism to detect packet patterns (signatures) sent by worms from packets transmitted on the network and block corresponding packets.

In communication among customers using the FOMA network, packets were bounced by the FOMA core router in the past, and it was thus not possible to block junk packets. As part of this development, we designed and changed the core router settings such that all connection calls using the FOMA network are sent via MAPS, making it possible to block junk packets (**Figure 2**).

2.2 Bandwidth Control for Each Access Line

MAPS is not only able to handle connections via FOMA, but also connection via fixed BB lines and Mzone. The maximum packet communication speed of FOMA is 384 kbit/s, whereas the corresponding value is 11 Mbit/s for Mzone, 50 Mbit/s for ADSL and 100 Mbit/s for FTTH, each of which are considerably faster than FOMA. If these various access lines with highly different bandwidths are connected without any restriction to the Internet via FOMA lines whose bandwidths are limited, the customers connected via FOMA may be drowned out due to the heavy traffic of fixed BB lines. Moreover,

always-on connections are common among fixed BB line users and it is not rare that customers generate large amounts of continuous traffic, which increases the risk that a few customers may occupy the MAPS line resources.

For this reason, MAPS uses a system where the bandwidth is controlled independently for each line and, if the traffic of customers in general increases in busy hours, causing line resources to become scarce, bandwidth is assigned to FOMA users with higher priority to let our core FOMA customers maintain comfortable communication. Moreover, this function can easily be applied to other access lines as well; it can, for instance, support introduction of services with different throughput such as High-Speed Downlink Packet Access (HSDPA) to FOMA.

Furthermore, MAPS is equipped with functions for controlling the total throughput of each customer. If a customer uses applications that consume large amounts of network resources, such as Winny[*3], it is possible to suppress the traffic generated by this customer.

2.3 International Roaming

In order to support international roaming with FOMA packet communication as well, MAPS allows to use two different methods for authorizing packet connection to the Internet, PDP TYPE=PPP[*4] [1], which is the mainstream in Japan, as well as PDP TYPE=IP[*4] [1], which is the mainstream in overseas locations.

In addition, a function that notifies calling country information from the FOMA network to the MAPS side has been implemented, to make it possible to determine the networks that the

*3 Winny: Commonly used Peer to Peer (P2P) software.
*4 One of the authentication methods defined by the 3rd Generation Partnership Project (3GPP).
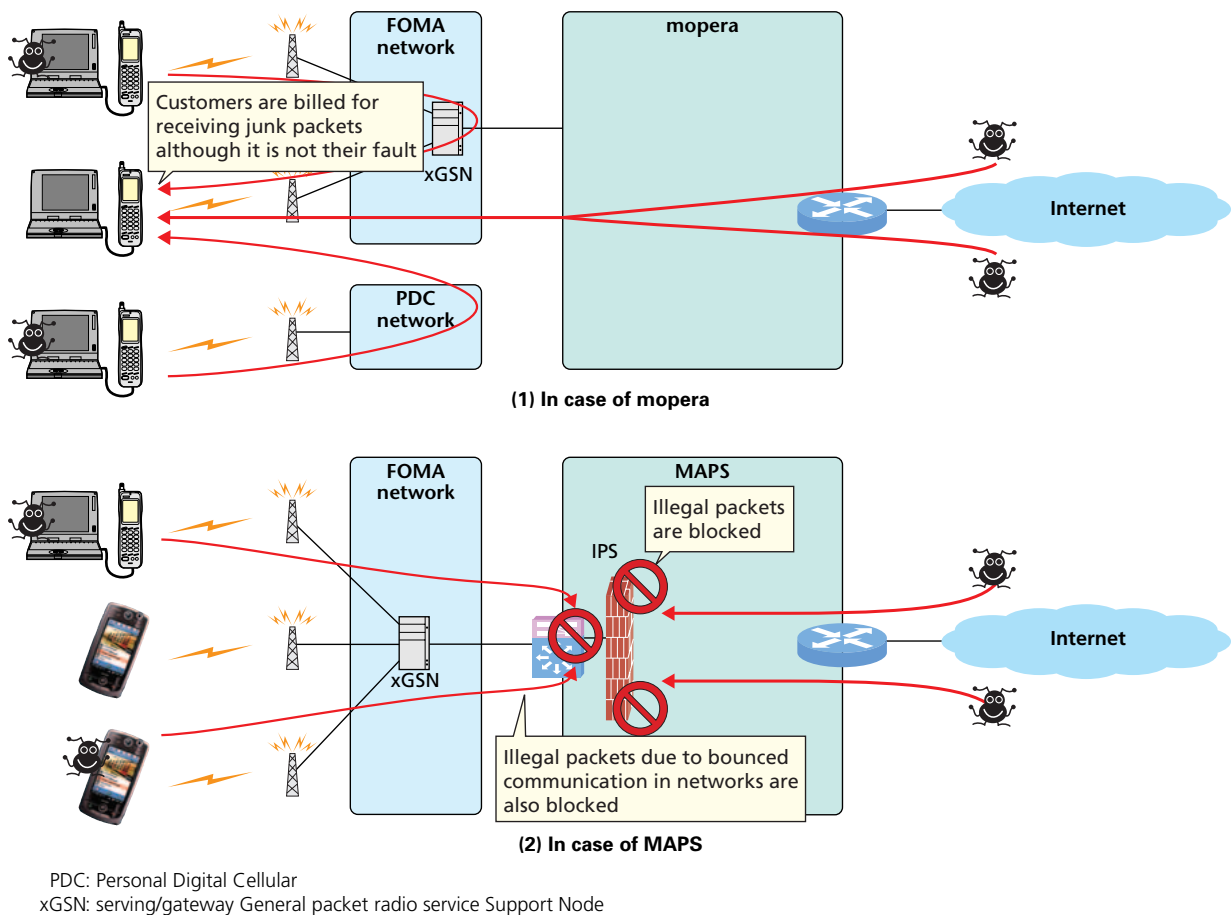
(1) In case of mopera

Customers are billed for receiving junk packets although it is not their fault

FOMA network

mopera

Internet

xGSN

PDC network

(2) In case of MAPS

FOMA network

MAPS

Illegal packets are blocked

IPS

xGSN

Illegal packets due to bounced communication in networks are also blocked

Internet

PDC: Personal Digital Cellular
xGSN: serving/gateway General packet radio service Support Node

Figure 2 Blocking unnecessary packets

user is in range of to control access for the purpose of contents delivery to outbound roaming users. This function will control the limitation of contents delivery for each outbound roaming destination country in the future.

3. Web Browsing Support Functions

MAPS is based on Internet access using FOMA lines. In order to browse Web contents that are becoming bloated with the increasing diffusion of BB lines comfortably via FOMA lines, we implemented various Web contents compression functions to improve the effective throughput and reduce the associated packet communication fees.

Furthermore, in the Internet world, there are Websites that may adversely affect adolescents and those that inflict harm on young people simply by being accessed. Thus, specific site block functions have also been furnished to improve security at home.

3.1 Web Contents Compression Function

Normally, a method where a compression server is installed

in the Web browser of a terminal as a proxy is used to compress Web contents. In MAPS, on the other hand, a server on the MAPS side checks the compression settings set by a customer when he/she accesses a Webpage and only performs compression processing based on the specified setting values if the function is turned on, so that the user will have to make as few setting operations as possible (**Figure 3**).

The file format determines which Web contents will be compressed (**Table 2**). The effect of compression depends on the contents and file format, but it has been found to be possible to reduce the packet communication volume up to approximately 70% in this way.

MAPS also supports conversion functions for Microsoft Office documents (Word, Excel, PowerPoint)[*5], which are increasingly being placed on Websites; it is possible to convert each page of an Office document, whose file size tends be large, into either Graphic Interchange Format (GIF) or Scalable Vector Graphics (SVG) format before displaying it in the

---

(2) Check of the user's compression settings
(on/off, images to be compressed, compression level
and Office document conversion method)

DB...Database

Customer DB

(1) HTTP request

(3) HTTP request

Internet

Website on the Internet

M1000

Compression server

Compression

(6) HTTP response
(respond with data after
compression processing)

(4) HTTP response
(the Website responds
with the Web contents
as usual)

(5) Compression processing
(the Web contents received from the
Website is compressed based on the
setting information acquired in step (2))

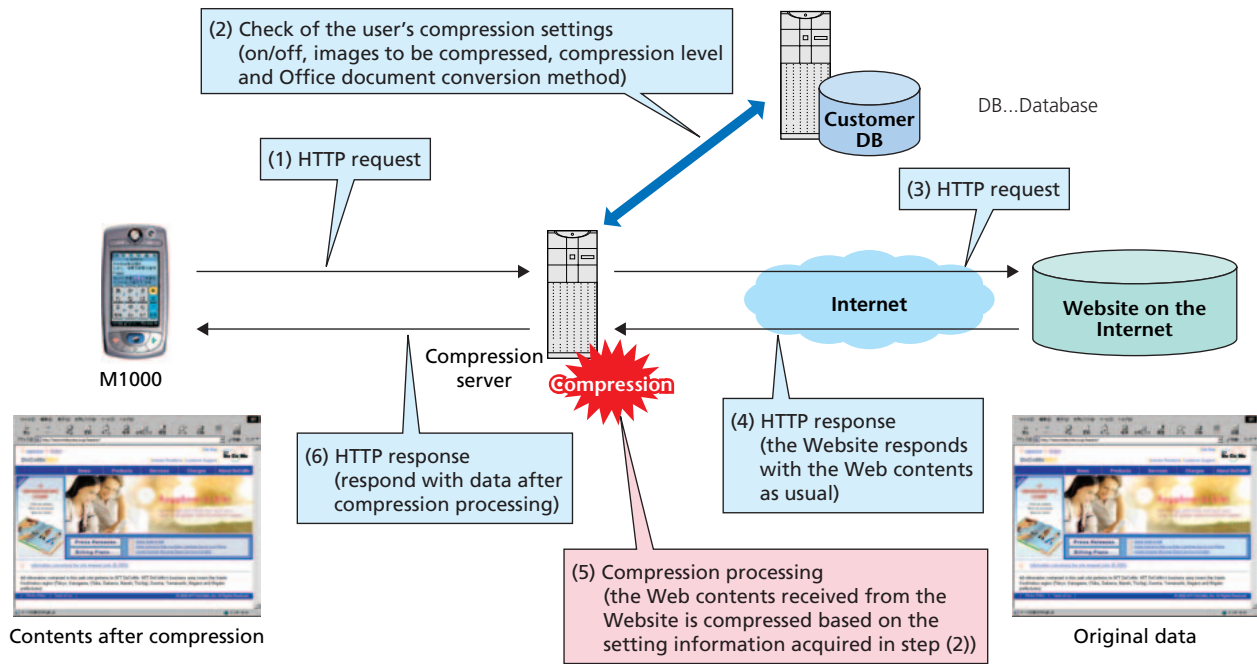Contents after compression

Original data

Figure 3 Overview of compression processing

browser. This function also works when displaying e-mails with MAPS' Web mail program, making it feasible to display Office documents attached to e-mails.

In case of file formats that are not compressed (e.g. Flash[*6]), the original data is displayed as is even if the compression function is turned on.

The compression function has the following functional options, which can be used via settings from the Web setting screen provided by MAPS.

- Turning the compression function on/off
- Image format to be compressed
- Compression level (five different levels can be chosen)
- Conversion method for Microsoft Office documents (SVG/GIF)

If the compression function is applied for images, the Web browser displays image contents with reduced resolution and fewer colors. If it is desired to acquire the original contents (i.e. the uncompressed Web contents), it is possible with a few sim-

Table 2 Targets of compression

Target file	Format (extension)	Compression method
Text	txt	Compression using the GZIP method prescribed by RFC1952
	htm	
	html	
	jsp	
	asp	
	cgi	
Image	gif	Compression by subtractive color process
	png	
	jpg	Compression by data thinning-out
	jpeg	
Office document	doc	Reduction of data size by converting to SVG/GIF format (equivalent to compression)
	xls	
	ppt	

ple operations by incorporating plug-in software that DoCoMo plans to provide in browsers.

3.2 Website Block Function

MAPS is designed with cases where not only the FOMA terminal subscribers themselves, but also their family members use the terminals via fixed BB lines in mind, and is thus equipped with a function to restrict access to specific sites that can be registered in advance.

This Website block function can generally be set either on the mobile terminal side or on the server side. However, in the same way as for the Web compression function above, MAPS

*6 Flash is a trademark or registered trademark of Macromedia, Inc. in the US and other countries.

only allows the user to turn the function on or off by making settings on the server side. This not only eliminates complicated settings on the terminal side, but also prevents unauthorized users (people other than the subscribers themselves) from changing the function setting in MAPS; this is because if the function settings are made on the mobile terminal, the setting may easily be cancelled with some knowledge even when a parent (subscriber) does not wish to allow access to sites that may adversely affect children. This function allows the setting of restrictions independently for Internet access via FOMA (mobile environment) and fixed networks (assuming home use); it is thus possible to switch the blocking off when a subscriber performs mobile communication and switch them on when the children access the Internet at home.

The method to register blocked sites is as follows: DoCoMo classifies candidate Websites to be blocked into several categories, and customers specify which of these categories of sites they wish to block. With this method, it is possible to address the constant addition of specific sites to be blocked without causing additional burdens on the users.

4. Internet e-mail Function

In addition to functions similar to "e-mail virus check services" and "additional account management" provided by fixed system providers, MAPS provides the following functions specifically targeted for Internet e-mail usage via mobile environments and various access lines.

4.1 Automatic e-mail Reception

As a special service provided for the business-oriented FOMA terminals (M1000), MAPS is equipped with an automatic e-mail reception function. According to the normal procedure used in Internet e-mail software, received e-mails are stored in a mailbox and the contents cannot be checked until a user accesses the server. When M1000 is used with MAPS, however, the e-mail is automatically received by the terminal in the same way as for i-mode terminals, i.e. a server sends a "Push notification" to the mobile terminal side as soon as an e-mail arrives, and the M1000 terminal inquires about and receives the e-mail from the server automatically (**Figure 4**). This automatic reception function was developed using Short Message Service (SMS) as prescribed in the 3G standards.

In addition, the function to activate a specified application on a mobile terminal with "Push notification" as a trigger can easily be expanded to applications other than e-mail software. This allows the Push service to be applied to various applications depending on the functions a given mobile terminal supports.

4.2 Simultaneous Use of POP and IMAP

The two main e-mail protocols used on the Internet, Post Office Protocol (POP) and Internet Message Access Protocol (IMAP), do not allow several e-mail programs to access the same mailbox simultaneously. MAPS, on the other hand, assumes that the same mailbox may be accessed from always-on connections using fixed BB lines at the office or at home as well as from mobile environments via FOMA, and thus permits simultaneous use of POP and IMAP. For this reason, the MAPS e-mail system is equipped with functions to cancel exclusive access control for the same mailbox and prevent conditions where the mailbox cannot be used from other lines when it is used from a certain access line.

5. User Support Functions

MAPS provides various optional functions and is designed such that these functions are made available by making settings
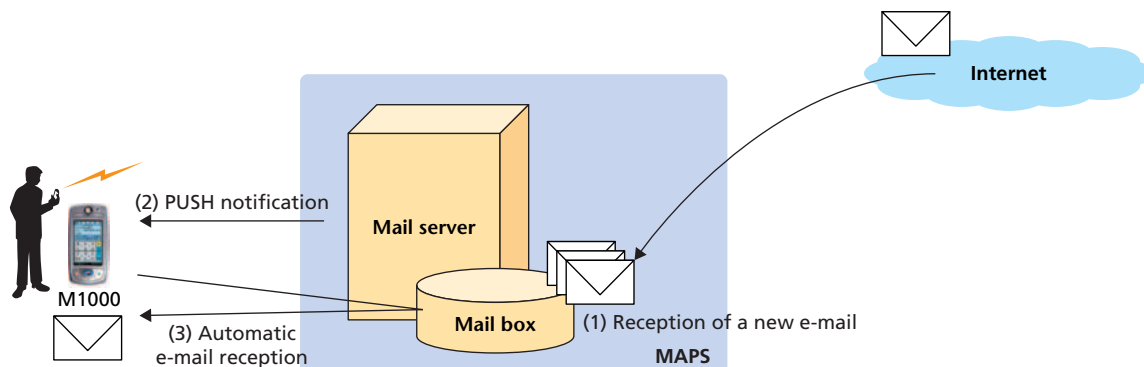

Figure 4 Automatic e-mail reception

on the server side without having to download any dedicated clients to the customers' terminals. The settings include the Web compression function, e-mail address change/acquisition, automatic e-mail reception, e-mail virus check, which requires additional subscription, turning the Website block function on/off, etc. Once set, the functions can be used with ease without having to worry further about the settings.

However, to perform the initial settings themselves may represent a tangled task for the customers. To aid the user in these tasks, MAPS adopts a system where a welcome message is sent via SMS when a subscription is started or changed, which guides the user to the initial setting screen. Since MAPS is based on FOMA subscriptions, reception of SMS is possible by default and provided to the users free of charge.

On the initial setting screen, it is not only possible to perform basic settings required to use the mopera U service via interactive forms, but also perform initial settings using a screen size suited for PCs, Personal Digital Assistants (PDA) or mobile terminals, respectively, after the initial setting screen recognizes the user agent of the connected terminal.

Moreover, an automatic terminal setting function that simplifies troublesome setting tasks by using the automatic terminal setting software for the mopera U service, is also provided.

6. Operation Monitoring Control Function

So far, the article focused on services for customers. In the following, functions for MAPS operators are explained.
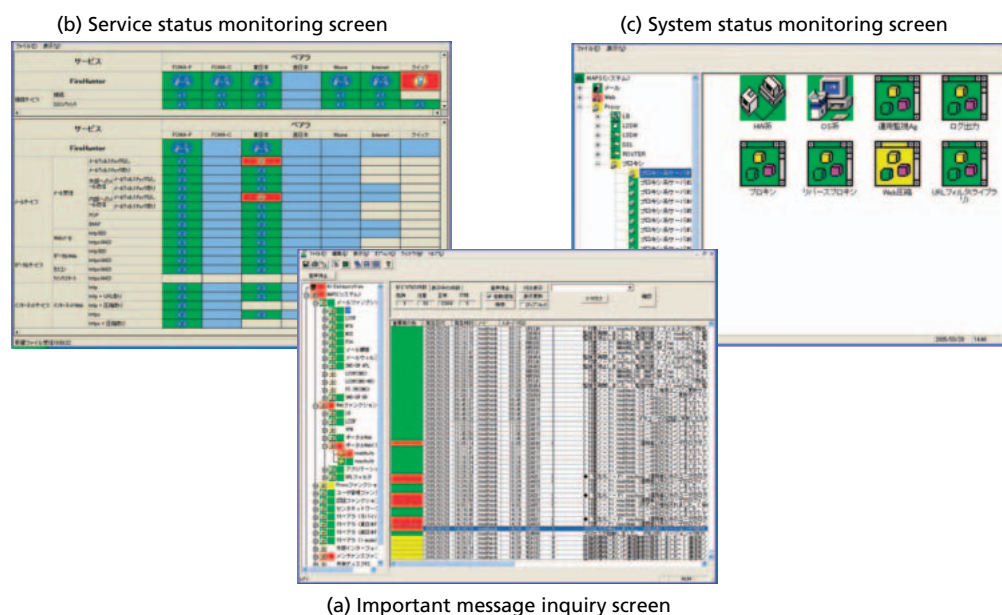
The goal of MAPS in terms of operation monitoring is to provide uninterrupted services. In other words, the issue is how to recover quickly from out of service that may occur due to system failures. To facilitate this quick recovery, it is required that the operators can obtain the necessary information as accurately as possible, so that they can narrow down the points of failure and determine the status of systems and services easily and that they can conduct appropriate recovery tasks promptly.

In order to satisfy these requirements, MAPS provides an important message inquiry screen that notifies about failure events etc., as well as two status monitoring screens that present the system and service states to the operators (**Figure 5**). In addition, the system control operations were integrated at the same time.

6.1 Important Message Inquiry Screen

1) Suppression of Redundant Messages

Identical messages generated in a certain period can be suppressed according to specific rules to prevent an increase of load on the monitoring function due to message rush (a phenomenon where identical messages are generated continuously), which may also adversely affect the monitoring of other nodes. Furthermore, we analyzed all messages notified by applications etc., their importance levels and their message contents, defined new rules for generation of such messages in advance to eliminate redundancy and improve the accuracy of the messages themselves and implemented the mechanism where systems can

(b) Service status monitoring screen

(c) System status monitoring screen

(a) Important message inquiry screen

* This function is provided in Japanese only.

Figure 5 The three monitoring screens providing information to operators

suppress messages according to the specified rules.

2) Generation of New Important Messages

MAPS is not only equipped with the aforementioned function for suppressing messages but also a message correlation function that generates new messages based on Simple Network Management Protocol (SNMP) traps and messages generated at failure. The message correlation function executes the following tasks according to the pre-defined specific rules, thereby allowing the operators to perform their work in an exact and prompt manner:

- The message importance level is changed from low to high
- The operator instruction statement in a message is changed into concrete contents
- The message is classified into various categories based on message ID and generation node

The message generation rules include threshold values related to how often and how many messages are generated and can be applied to multiple messages as well as single messages. Moreover, these rules and threshold values have been defined and set based on phenomena that were observed in failure tests and field tests conducted so far. The function can be tuned to operate more efficiently by defining new rules, modifying existing rules and tuning threshold values continuously during future operation. Note that the system status monitoring screen and the service status monitoring screen below have been implemented based on the use of this message correlation function as well.

6.2 System Status Monitoring Screen

We developed a system status monitoring function that displays information related to system status, such as system failure conditions, package active/standby status, load distribution conditions, etc., visually and in real time in an easy-to-understand manner, based on generated messages and system configuration information so that device failures can be identified and recovered in a prompt manner.

All the devices in MAPS are dual-redundant. In case a failure occurs, it is easy to judge whether or not the various services are being provided normally from the colors of icons on the screen. It is also possible to judge which device in which service category has a failure immediately after it occurs by classifying servers and network devices according to their service categories and displaying them graphically. This makes it possible to narrow down points of failure and judge the system status promptly.

6.3 Service Status Monitoring Screen

In order to detect problems such as service failures and take actions against them at the earliest stage possible, we developed a service status monitoring function that automatically checks end-to-end service status and displays the result graphically at all times.

This function monitors both FOMA and fixed BB lines in MAPS and can always monitor the normality of service functions such as net surfing, e-mail communication, e-mail virus check, specific Website block, Web compression and other services, not to mention authentication functions such as those of connection and applications. With this function, the operator can not only identify the status of each service immediately upon a failure, he/she can get a comprehensive overview of the situation, taking the results of the other two monitoring screens into consideration and quickly identifying whether the failure is on the network side or the MAPS side.

6.4 OS and Model-Independent System Control Operations

We developed a function that allows the operator to take basic countermeasures entirely using a Graphical User Interface (GUI) screen without having to be aware of OS and hardware models, so that the system operators can react promptly to the detected phenomena.

For example, menus are provided for tasks that must be performed frequently or promptly at normal operation and failure, such as starting/stopping services in MAPS, switching packages, connecting and disconnecting servers to/from load distributors and so forth, so that operators can perform these tasks without having to be aware of the particular OS and models. Moreover, various functions that are essential for prompt failure recovery, such as calling up failure countermeasure procedure manuals online directly from monitoring messages etc., are also incorporated.

7. Conclusion

MAPS was developed for the purpose of achieving a system that provides comfortable services "anytime and anywhere" by selecting optimal communication means from a wide range of options. MAPS provides a wide range of services, including bandwidth control for each type of access line, compression ser-

vices, setting support and operation monitoring control. In the future, we plan to provide further services to accommodate the users' needs for the further development of new mopera U services.

REFERENCES

[1] 3rd Generation Partnership Project: "3G TS 23.060 v3.3.0 (technical Specification)," 2000-04.

ABBREVIATIONS

3GPP: 3rd Generation Partnership Project
ADSL: Asymmetric Digital Subscriber Line
BB: BroadBand
FTTH: Fiber To The Home
GIF: Graphic Interchange Format
GUI: Graphical User Interface
HSDPA: High-Speed Downlink Packet Access
IMAP: Internet Message Access Protocol
IPS: Intrusion Prevention System
LAN: Local Area Network
MAPS: Multi Access Platform System
mopera: Mobile OPEration Radio Assistant

P2P: Peer to Peer
PDA: Personal Digital Assistant
PDC: Personal Digital Cellular
PDP: Packet Data Protocol
PHS: Personal Handy-phone System
POP: Post Office Protocol
PPP: Point to Point Protocol
SMS: Short Message Service
SNMP: Simple Network Management Protocol
SVG: Scalable Vector Graphics
xGSN: serving/gateway General packet radio service Support Node