New Technology Report

Special Article on IMT-2000 Services (2)
– Launch of FOMA, the Pioneer of the New Mobile Age –

Gateway Technologies
– WPCG, TCPGW and ExGW –

Makoto Jinguji, Masaki Yamashina, Yasushi Kondo, Osamu Takahashi, Koji Tsurumaki and Hideharu Suzuki

This article reviews the development concepts of the gateway systems developed by NTT DoCoMo with the aim to introduce IMT-2000 packet-switched services in an efficient, flexible and prompt manner, and the role and characteristics of the three gateway systems developed based on these concepts.

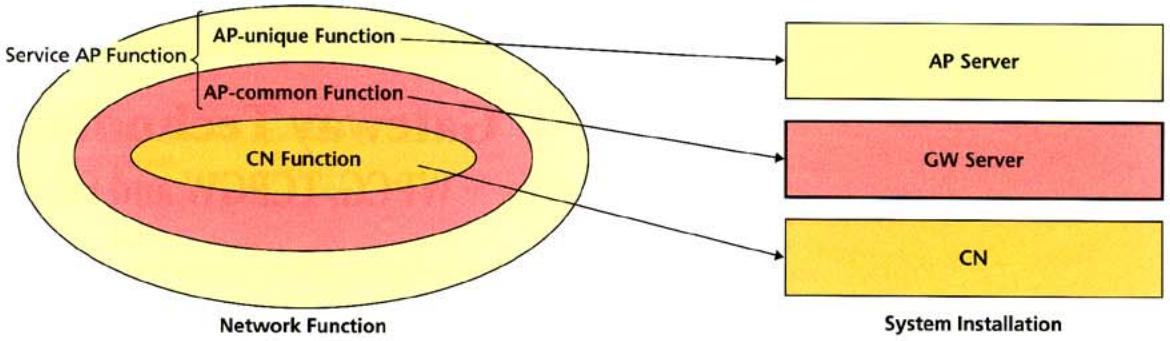
1. Introduction

For the development of large systems, it is important to categorize and stratify the functions, and clarify, disperse and modularize the interface in each layer. This enables efficient, flexible and prompt system development.

This article reviews gateway (GW) systems for packet-switched services based on International Mobile Telecommunications-2000 (IMT-2000). To begin with, the basic concepts of GW systems will be discussed, and the objective of gateway development will be clarified. This will be followed by the overview of the functions and technical characteristics of three GW systems developed based on these concepts, namely, the Wireless Protocol Conversion Gateway (WPCG), the TCP GateWay (TCPGW) and the packet Exchange GateWay (ExGW).

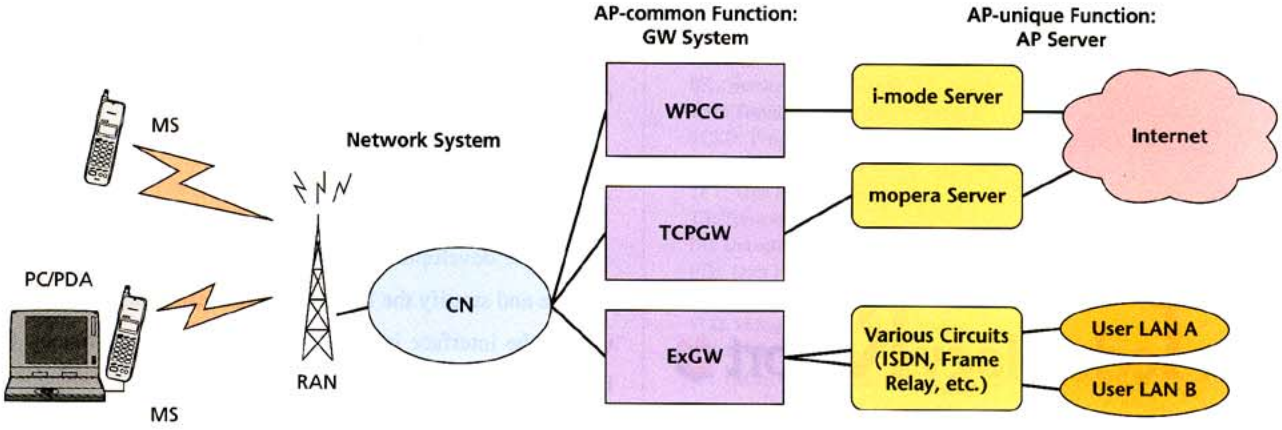
2. Development Concepts of GW Systems

An effective way to accelerate the introduction of new services based on the combination of mobile communications and the Internet and to improve the efficiency of system development is to divide service APplication (AP) functions into AP-common functions (GW system) and AP-unique functions (AP server) and mount them separately (**Figure 1**). GW systems developed by NTT DoCoMo are installed based on the AP-common function concept (**Figure 2**). Functions offered by GW systems include the conversion of the Internet Protocol into



AP: APplication
CN: Core Network
GW: GateWay

Figure 1 Development Concepts of GW System



AP: APplication
CN: Core Network
ExGW: packet Exchange GateWay
GW: GateWay
ISDN: Integrated Services Digital Network
LAN: Local Area Network

mopera: Mobile OPEration Radio Assistant
MS: Mobile Station
PDA: Personal Digital Assistant
RAN: Radio Access Network
TCPGW: TCP GateWay
WPCG: Wireless Protocol Conversion Gateway

Figure 2 Installation of GW System

a protocol that suits the mobile communications environment as well as address conversion. These functions are offered through three types of GW system separately, as the GW functions depend on the way in which the terminal is used (the mobile phone may be used alone, or it may be used in combination with a PC), and the network type of destination(the Internet, user Local Area Network (LAN)). GW systems have the following merits.

- They are configured based on architecture independent of the Core Network (CN). Development is simpler and more efficient, making it possible to develop new, additional functions in a short period.
- Optional data services from application servers and other AP-common functions can be offered by GW systems, ensuring a competitive advantage.
- Operation independent of CN is possible. In the event of any congestion or fault, it is easy to divert the traffic. Risks associated with the introduction of new functions and services can also be avoided.

The following sections review each GW system based on these development concepts.

3. WPCG

3.1 Function Overview

WPCG is a proxy-type gateway that connects CN with IMT-GRIMM (IMT Gateway service Representative Internet Market Mobile access exchange), which is a group of servers geared to the i-mode service for IMT-2000 packet-switched communica-

tions. It terminates, converts and relays the Control Plane (C-Plane) protocol, which is for controlling signals exchanged with CN, the Transmission Control Protocol (TCP), which is the User Plane (U-Plane) protocol for forwarding user data, the HyperText Transfer Protocol (HTTP) and the Domain Name System (DNS). One of the requirements in the development of WPCG was to make i-mode services applicable over standard Internet protocols (HTTP/TCP), and the issue was to improve the communication performance of TCP in an environment that suffers from longer transmission delay and higher error rate, as in the case of a mobile environment. Also, optional functions were required in the mail notification service, which is one of the noteworthy services in i-mode: triggered by the incoming mail notification message from IMT-GRIMM (C-Plane), WPCG had to order the establishment of packet communication sessions and shift the mail notification message to the U-Plane protocol, in order to deliver the mail notification message to the destination mobile phone immediately. Another important requirement with respect to IMT-GRIMM was to offer highly reliable packet communications equivalent to CN. Accordingly, NTT DoCoMo made development efforts concentrating on system configuration considering the loading balance of the connecting destination server, signal process communication sequence control in view of the conditions where the destination mobile phone is out of the range and the effect of system resources, and functions related to operation and maintenance.

3.2 Reliability-conscious System Configuration Technologies

WPCG is positioned between the Gateway Mobile Multimedia switching System (GMMS), which is the gateway switching system in the IMT-2000 core network, and the Neo Interface-Mobile Access eXchange (NI-MAX), which is the interface/server of IMT-GRIMM. **Figure 3** illustrates the configuration of the IMT-2000 packet-switched communication network for i-mode service. WPCG is based on a parallel configuration of (N+1) (N: natural number) units under one GMMS, and in order to ensure the capacity upon the fault of one unit, the subscriber capacity design requirement is set at N units. Between WPCG and NI-MAX, the configuration of connection is based on a N : M (M: natural number) ratio, achieving a flexible network configuration. For the purpose of dispersing the load of call connections, GMMS selects the destination of connection from X units of WPCG by the round robin, whereas WPCG selects the destination of connection from M units of NI-MAX by the round robin. Upon mail-reception, the NI-MAX selects the WPCG used for access just before at the destination mobile phone , and the WPCG directly notifies the mail-reception to the one-and-only GMMS above it.

The main unit of WPCG and peripheral equipment are based on a reliability-conscious redundant configuration, which is highly robust against faults. Middleware that constitute the software environment have functions that ensure high availability, including disk mirroring, internal resources management and LAN interface monitoring.

3.3 Communication Protocol Processing Technologies

The C-Plane protocol is responsible for the control sequence associated with call connection, release and call reception with the connecting destination node. It also offers operation and maintenance functions, including blocking, restriction and health-check. The U-Plane protocol relays HTTP requests and

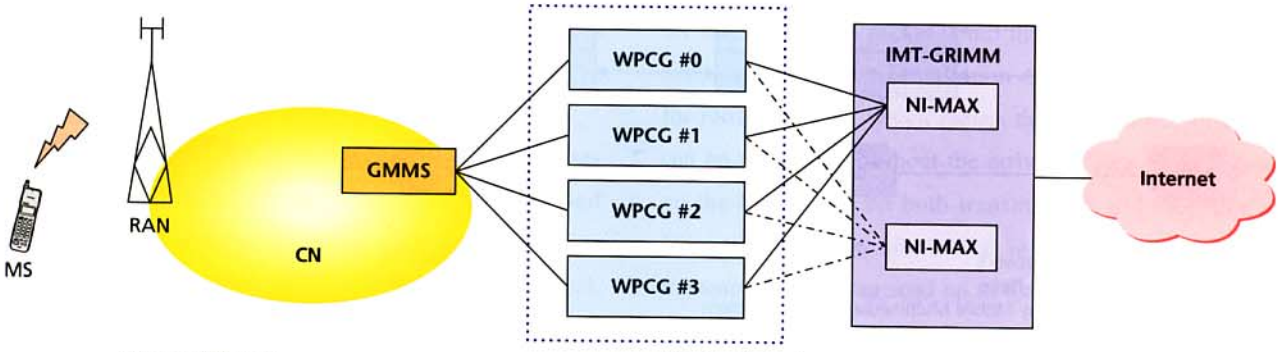


Figure 3 Configuration of IMT-2000 Packet-switched Communication Network for i-mode Service

responses, and enables the browsing of i-mode HTML (HyperText Markup Language) content published over Web servers, the transmission/reception of i-mode mail, the mail notification and messages to mobile phones. **Figure 4** shows the configuration of the C-Plane and U-Plane protocols supported by WPCG.

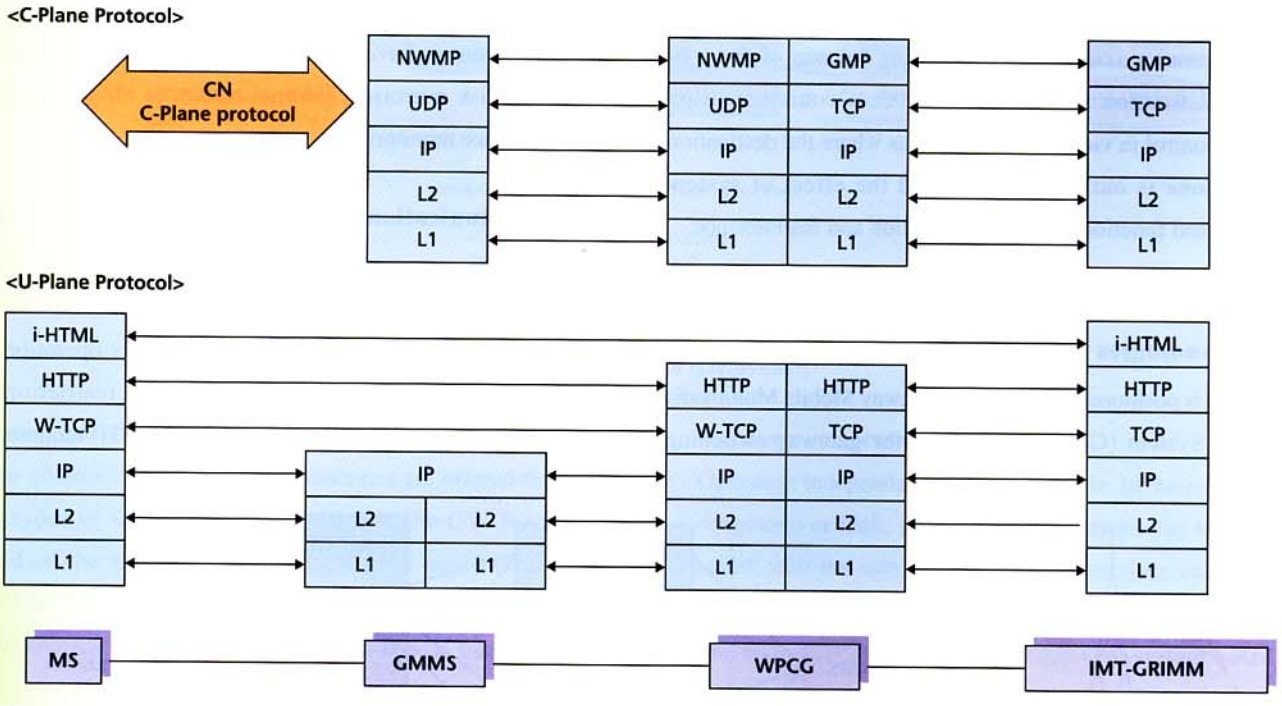
(1) C-Plane Protocol

The C-Plane protocol between GMMS and WPCG is referred to as the NetWork Management Protocol (NWMP), whereas the C-Plane protocol between WPCG and NI-MAX is referred to as the Grimm Management Protocol (GMP). WPCG converts the message and information elements notified by GMMS into GMP, and informs NI-MAX of the same. WPCG manages the access status of mobile phones, such as call connection notification and release notification by the termination of the C-Plane protocol. It also disposes the communication packets with abnormal communication sequences and invalid signal formats. Moreover, to enable IMT-GRIMM to identify the packet-communication originating mobile phone in origination sequence, WPCG extracts the information elements that help identify the mobile phone from the connection notification message given by GMMS, and inserts them into the HTTP request message addressed to IMT-GRIMM as an extension header.

(2) U-Plane Protocol

Between the mobile phone and NI-MAX, HTTP is applied to Web access and i-mode mail; WPCG serves as the HTTP proxy between the mobile phone and NI-MAX. For TCP applied between the mobile phone and WPCG, the communication parameters have been tuned in consideration of the transmission properties of the IMT-2000 packet-switched communication network (referred to as "TCP Profile over W-CDMA" or "W-TCP") [1]. As the Internet standard TCP is directly applied between WPCG and NI-MAX, WPCG executes TCP protocol conversion.

In addition, WPCG has the function to respond to Domain Name System (DNS) queries, which are transmitted by the mobile phone to resolve the WPCG address upon packet communication origination, and supports the CONNECT method of



CN: Core Network
C-Plane: Control-Plane
GMMS: Gateway Mobile Multimedia switching System
GMP: GRIMM Management Protocol
IMT-GRIMM: IMT-Gateway service Representative Internet Market Mobile access exchange
HTML: Hyper Text Markup Language
HTTP: Hyper Text Transfer Protocol
IP: Internet Protocol
MS: Mobile Station
NWMP: NetWork Management Protocol
TCP: Transmission Control Protocol
U-Plane: User-Plane
UDP: User Datagram Protocol
W-TCP: TCP Profile over W-CDMA
WPCG: Wireless Protocol Conversion Gateway

Figure 4 Signal Control and User Data Protocol supported by WPCG

HTTP to carry out secure communications based on the Secure Sockets Layer (SSL).

(3) Protocol for Mail Notification

When IMT-GRIMM receives mail, etc., NI-MAX sends a GMP mail notification message to WPCG. In response, the WPCG informs GMMS by NWMP of the mail-reception and prompts it to establish a packet communication session with the destination mobile phone. In the process, WPCG determines whether the target mobile phone is engaged or not, and executes dynamic control as to whether it should prompt the establishment of a new session or use an existing session. Then, WPCG sends the mail notification message specified in the U-Plane to the mobile phone and in response to the session-involved mobile phone, sends a delivery confirmation message (GMP) to NI-MAX.

3.4 Operation and Maintenance Function

WPCG has operation and maintenance functions to assist the stable operation of the system. Some of the functions are as described below.

(1) File Updating

WPCG has a file updating function to absorb program faults and add new service functions. File updating may take two forms: complete file updating, which involves memory initialization and the replacement of all processes, and partial file updating, which involves the replacement of specific processes.

(2) Restart Process

Restart process is a function that eradicates the causes of problems in total or partial WPCG software failure and promptly restores the system to the normal state by rebooting.

For example, during file updating, if any problems occur in the course of monitoring file updating, the system will automatically detect it, execute the restart process and restore the files to their previous state.

(3) Congestion Control

Congestion control involves the detection of rapid increases in traffic by monitoring the Central Processing Unit (CPU) and the memory usage. It automatically imposes restrictions before the transmission or reception of packets goes out of control. Restriction includes primary restriction, which involves the transmission of a restriction request to the connection destination node, secondary restriction, which prevents the establishment of new calls, and overload restriction, which involves the disposal of signals other than release and reply messages and the gradual closure of the U-Plane paths.

(4) Monitoring Function

The monitoring function manages peripheral network equipment using the Simple Network Management Protocol (SNMP), and in the event of any faults in the equipment, it informs the maintenance terminal of the faults by trap signals (messages). Between WPCG and the connecting destination node, health-check signals are exchanged to detect any abnormalities in the other node. Also, the traffic data is monitored to check the normal operation status and to make use of it as basic reference data for designing equipment in the future.

(5) Subscriber Status Management

Subscriber status management is done based on the real-time displaying of mobile phone information being processed at WPCG by the input of commands from the maintenance terminal. There are also functions to gather communication logs and trace signals.

4. TCPGW

4.1 Function Overview

In IMT-2000 high-speed and packet-switched services (downlink 384kbit/s, uplink 64kbit/s), it is known that the latency within the network, including radio zones, may become significant in consideration of the bearer's bandwidth. As a result, the throughput might be insufficient in high-speed and packet-switched communication services when the TCP/IP protocol, which is adopted by WWW and many other Internet applications, is applied at the standard format or without changing the default settings.

TCP is a protocol designed to carry out data forwarding in a reliable manner, over connectionless IP networks. In principle, its basic operation is to wait for the Ack packet to be returned for each forwarded packet. Until the Ack packet is returned, it needs to store the communication data in the buffer to prepare for retransmission, which means that the volume of data that can be transmitted without the arrival of Ack packets depends on the buffer size on both transmission and reception side. Normally, the buffer size is 8kB in most TCP equipment. The transmission side can send up to 8kB of data at once, but until the Ack packet is returned, it cannot start operations to send the next set of data; as a result, the efficiency of circuit usage falls and the throughput is limited. To prevent this from happening, it is necessary to increase the volume of data that can be sent without waiting for the arrival of the Ack packets by increasing

the buffer size on both transmission side and reception side, so as to improve the efficiency of circuit usage and the throughput.

NTT DoCoMo advocates a technique that diminishes the reduction in throughput caused by long delays by tuning the parameters within the range of the existing TCP protocol [1]. As the parameter-optimized W-TCP is based only on technologies published by the Internet Engineering Task Force (IETF), a standardization body of Internet technologies, it can be applied to conventionally configured equipments without any problems. The aim of the TCP Gateway (TCPGW) is to improve the throughput of Internet applications by installing a W-TCP gateway within the network. In other words, the function of TCPGW is to improve the efficiency of circuit usage for customers accessing the Internet via NTT DoCoMo's mobile network (specifically, customers using the mopera Internet connection service) by installing a gateway that relays between the W-TCP and the existing TCP in the edge of NTT DoCoMo's network.

4.2 Reliability-Conscious System Configuration

Figure 5 shows the TCPGW network configuration and protocol stack. The TCPGW unit itself is based on a redundant configuration of 2 units, and switching is carried out by the Layer 4 SWitch (L4SW), which directs nothing but packets subject to TCPGW processing to the TCPGW unit. Packets which are not subject to TCPGW processing, such as the Internet Control Message Protocol (ICMP) and the User Datagram Protocol, are directed into the circuit directly connected to two L4SW units.

4.3 Communication Protocol Processing Technologies

(1) Requirements

TCPGW terminates the TCP connection with two different profiles and forwards the user data. Unlike normal proxy servers, it needs to function as a transparent gateway: from the user PC's point of view, the destination of connection must look like an Internet Service Provider (ISP) server, whereas from the ISP server's viewpoint must look like the user PC. Also, in order to eliminate unnecessary packet billing, the TCP connection between TCPGW and the ISP server must be established before the TCP connection between the user PC and TCPGW. TCPGW meet these requirements by its address conversion and connection establishment.

(2) Software Configuration

Figure 6 illustrates the TCPGW software configuration and data flow. The TCPGW unit runs on a general-purpose Unix OS. The call processor consists of two processes: a transparent TCP-Agent and a ProxyAPL. The transparent TCP-Agent is a process that ensures the transparency of IP datagrams going through TCPGW between the ISP server and the PC connected

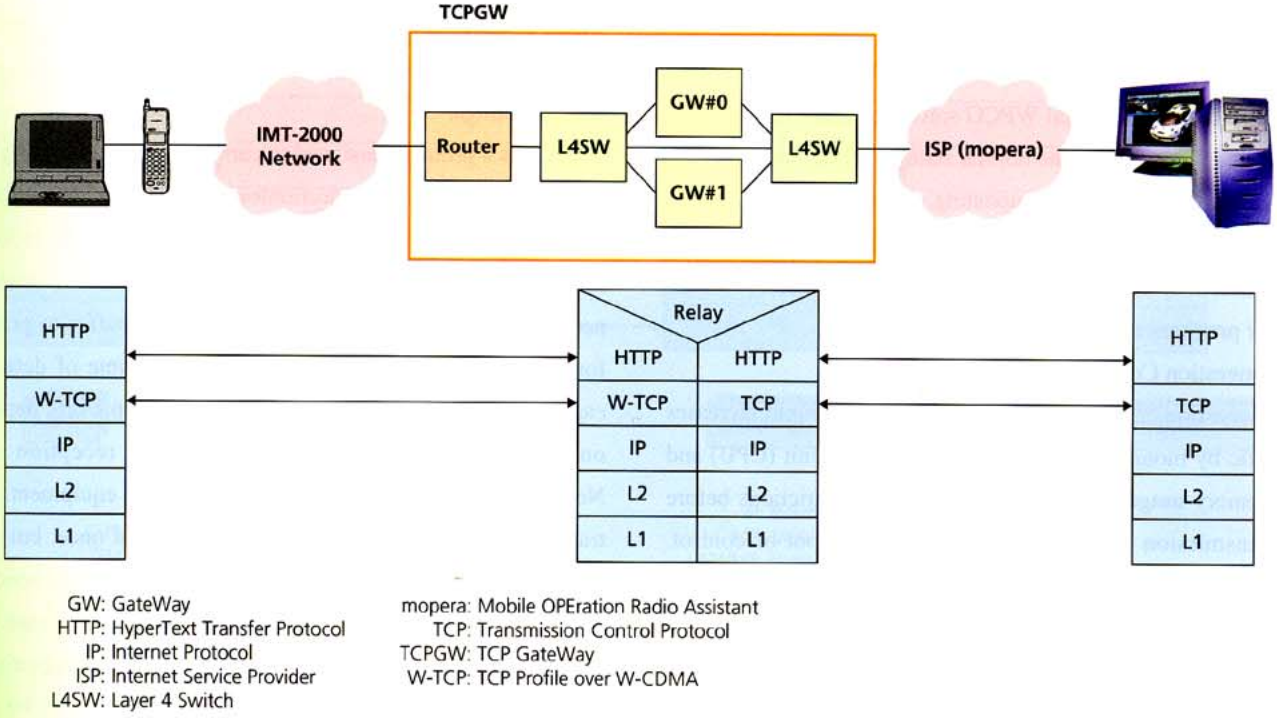


Figure 5 TCPGW Network Configuration and Protocol Stack

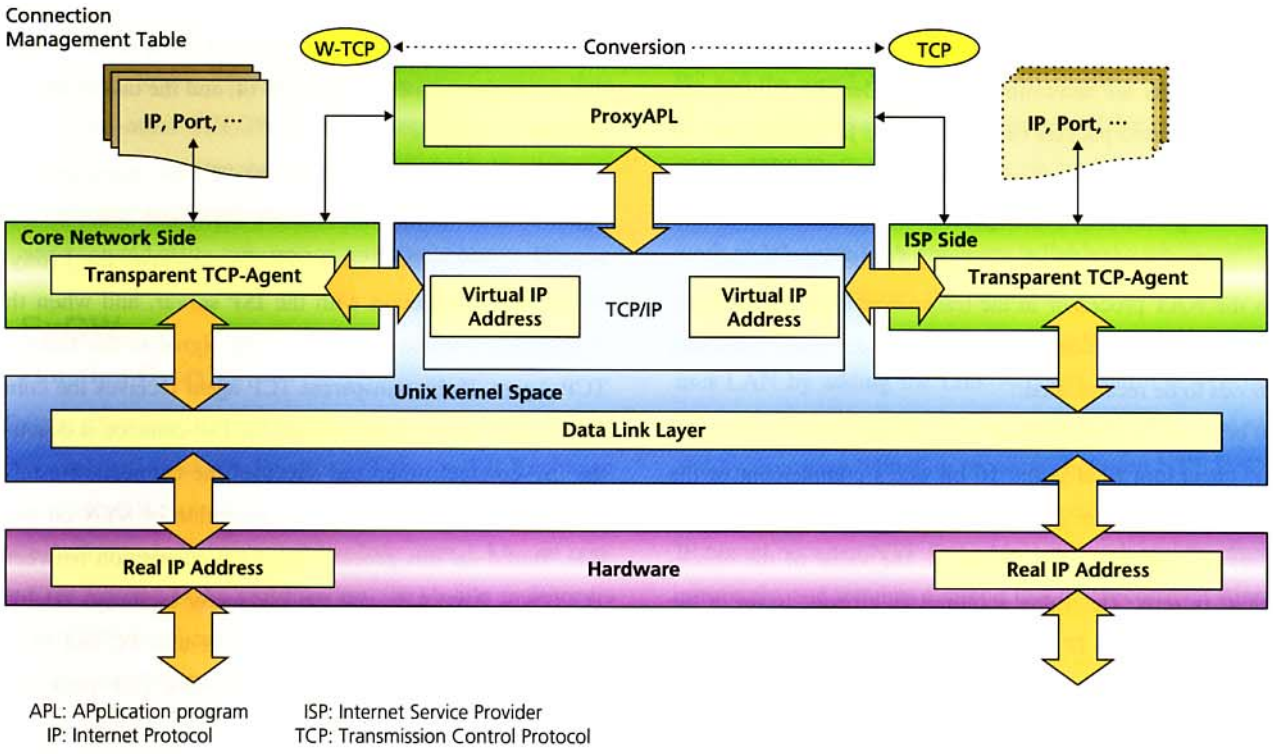


Figure 6 TCPGW Software Configuration and Dataflow

to an IMT-2000 mobile phone. ProxyAPL is a process that relays the TCP segment between the PC and the ISP server and converts W-TCP and TCP.

The transparent TCP-Agent is divided into two sides: the CN side which executes W-TCP communications with the PC; and the ISP side which executes TCP communications with the ISP server. Both sides recognize the real IP address and the virtual IP address. The CN side consists of the IP Network Address Translator (NAT) processor, which imports and transmits the PC's IP datagrams from the Network Interface Card (NIC), and the W-TCP processor, which carries out communications via a W-TCP stream socket. The ISP side consists of the NAT processor, which imports and transmits the ISP server's IP datagrams from NIC, and the TCP processor, which carries out communications via a TCP stream socket.

The W-TCP processor and the TCP processor in the transparent TCP-Agent hands over the TCP segment based on stream socket using the virtual IP address and the ProxyAPL positioned above the transparent TCP-Agent.

(3) Address Conversion

The NAT processor in the transparent TCP-Agent captures all packets going into NIC on the CN side, based on the Data Link Program Interface (DLPI) function. The following items are converted with respect to packets that meet the import requirements so that TCPGW fulfills the transparent relay function.

- Source address of the IP header
- Destination address of the IP header
- Source port of the TCP header
- Destination port of the TCP header

Packets that do not meet the import requirements are disposed without being relayed. The import requirements are as follows:

① The protocol number must be 6 (TCP);

② The destination IP address is not the real IP address of TCPGW; and

③ There must be a corresponding connection management table.

Even if there is no connection management table corresponded, the packets are imported in the following circumstances:

④ Upon the reception of the confirmation request packet (SYN) for the first time, the connection management table is acquired and the packets are imported accordingly.

⑤ Due to the half-open connection upon the reception of data packets, the packets are imported rather than being disposed of, to prepare for RST return.

Packets that satisfy the import requirements come from two

directions: from the PC (or the ISP server) or the ProxyAPL. The source IP address and the destination IP address of the imported packets are determined so as to identify the direction which the imported packets came from. The IP address and the port number of each packet are converted with reference to the corresponding connection management table.

(4) Recalculation of IP Header and TCP Header Checksum

As the NAT processor in the transparent TCP-Agent resets the fields in the IP header and the TCP header, each checksum field needs to be recalculated.

To begin with, the checksum is recalculated for the IP header. The checksum field is the 16 bit one's complement of the one's complement sum of all 16 bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero. The value acquired as a result is set in the checksum field of the IP header. Also, the 96-bit TCP pseudo-header is placed in front of the segment to recalculate the checksum for the TCP header and the TCP data. The checksum is calculated in the same manner as in the case of the IP header.

The transparent TCP-Agent assigns one virtual port number to a pair of virtual IP addresses (the CN side and the ISP side). A virtual port number is acquired with respect to each connection request, and each number is kept unique in TCPGW as it must serve as the key that associates the received packet with the connection management table. The virtual port number is allocated within the range of numbers defined in SG data, and the recycling of the allocated virtual port number is prohibited until the connection is released. The range of numbers is defined in consideration of the maximum number of simultaneous connections.

(5) Connection Establishment

In some cases, the user PC might not be able to establish TCP connection: for example, the destination IP address could be missing from the TCP connection SYN sent from the user PC, or the ISP server might temporarily be out of service. If TCP connection is established between the user PC and the proxy first, as in the case of normal proxy servers, the user PC might send an HTTP request packet, which could lead to unnecessary packet billing. In order to avoid this, TCPGW establishes the connection to the ISP side first, subsequent to the reception of the TCP connection SYN from the PC. Meanwhile, the connection-establishment process goes into standby mode on the CN side. After the connection is established on the ISP side, the connection-establishment process on the CN side (process after the reception of SYN) is performed. When connection cannot be established on the ISP side, no SYN.ACK is sent to the PC, the connection request is disposed of, and the task is abandoned until the PC retries.

After receiving SYN from the PC, the transparent TCP-Agent sets the timer (ISP-connect timer) and sends a connect-request signal to the ProxyAPL. In response, the ProxyAPL establishes connection with the ISP server, and when this is completed, it sends a connect-reply signal to the transparent TCP-Agent. If the transparent TCP agent receives the connect-reply signal before time runs out for ISP-connect, it deactivates the ISP-connect timer and executes the connection-establishment process subsequent to the reception of SYN on the CN side. Based on this process, the TCP connection between the TCPGW's ProxyAPL and the ISP server is always established before the TCP connection between the user PC and TCPGW, which prevents the PC from transmitting TCP packets with unidentified addressees.

The ISP-connect timer monitors the time taken between the transmission of the connect-request signal by the TCP-Agent, and the reception of the connect-reply signal from the ProxyAPL. There is a time limit for connection establishment + α, considering the maximum time taken for the connection establishment request to be retried on the ISP side.

For connection established on the ISP side subsequent to the reception of SYN and prior to the transmission of SYN.ACK by the PC, the PC might retransmit SYN depending on network delays over the Internet and delays in processing by the ISP server. The ISP-connect timer will not be reset in the event of the reception of a retransmitted SYN in connect-reply signal standby mode; the retransmitted SYN will be ignored, as the reply for the first connect-request signal is expected to arrive. In the event of the reception of a retransmitted SYN following a connect-reply signal, it will be ignored because the connection will already have been established on the ISP side and SYN.ACK will have been sent.

If the server is out of service on the ISP side, ProxyAPL connection will be regarded abnormal (ETIMEDOUT), and the connect-reply signal (ETIMEDOUT) will be returned from the transparent TCP-Agent before ISP-connect timeout.

After the reception of the connect-reply signal, ProxyAPL deactivates the ISP-connect timer and disposes of the connection request without sending SYN.ACK to the PC.

4.4 Operation and Maintenance Functions

TCPGW is connected with a maintenance terminal via a LAN interface. Status monitoring, file updating, station data alteration and other TCPGW maintenance tasks can be performed from the maintenance terminal. TCPGW is also connected with the integrated operation system via the LAN interface, and can send alarm information to the operation center.

5. ExGW

5.1 Function Overview

(1) Existing Services

An explanation of the functions of the packet Exchange Gateway (ExGW) requires reference to the way in which mobile packet-switched terminals and the user LAN are connected for existing DoPa★ and Freedom Of Mobile multimedia Access (FOMA) services.

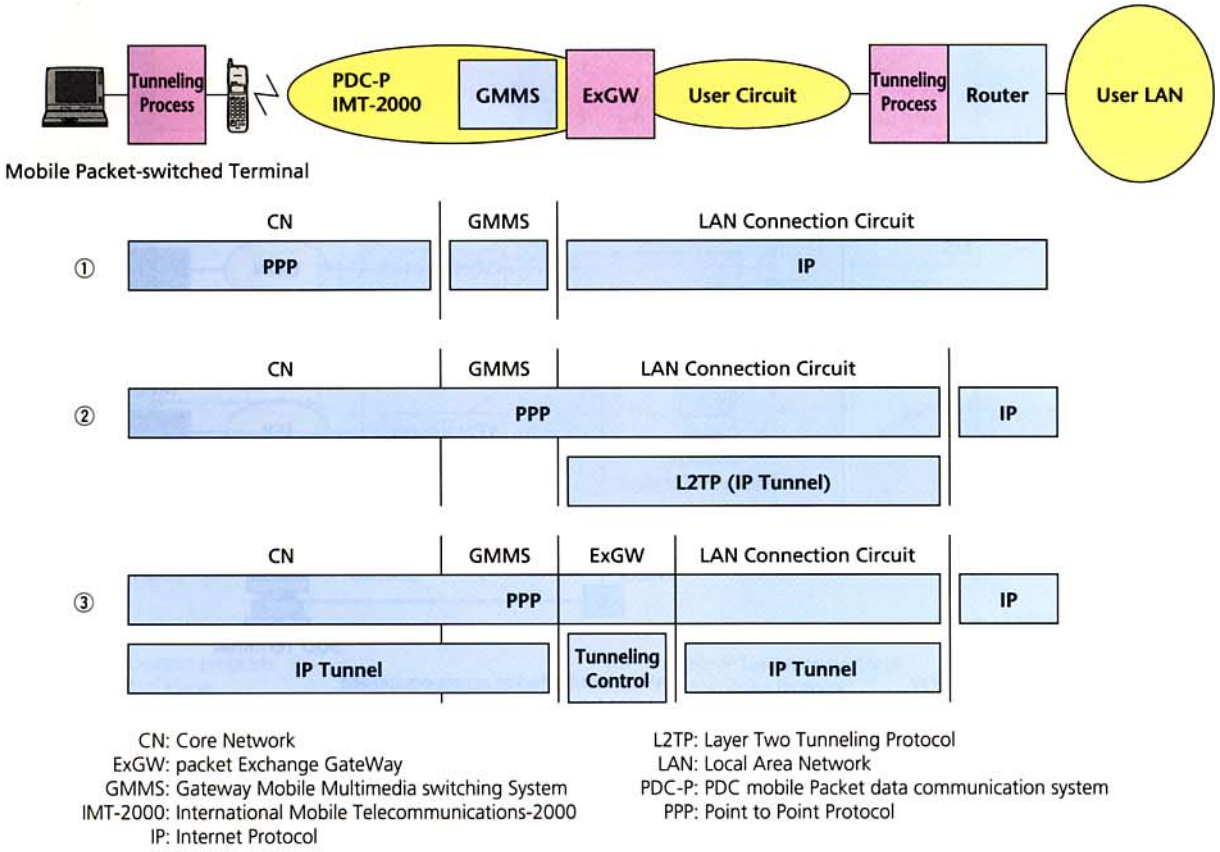
As shown in **Figure 7** ①, the mobile PC side is connected with the network based on PPP (Point to Point Protocol) authentication procedures. An IP address registered with the network in advance (the subnet address of the user LAN) is issued to the mobile PC, and NTT DoCoMo's network is interconnected with the user LAN to enable IP communication between the mobile PC and the user LAN. This process requires the authentication of the mobile PC and the management of the user's IP address within NTT DoCoMo's network, as well as a dedicated Wide Area Network (WAN) circuit between NTT DoCoMo's network and the user LAN for every individual user.

Figure 7 ② shows the enhanced version of this service. DoPa enables authentication between the mobile PC and the user LAN by adding the Link Access Control (LAC) function [2] of the Layer Two Tunneling Protocol (L2TP) in the network and by executing tunneling processes between NTT DoCoMo's network and the user LAN. This system also has to sustain the IP tunnel between NTT DoCoMo's network and the user LAN constantly, and requires a circuit that offers constant connection between them for the user to occupy.

(2) Functions of ExGW

Services offered by ExGW are as shown in Figure 7 ③, which focus on users who do not generate enough traffic to justify the installation of constant-connection circuits between NTT DoCoMo's network and the user LAN, such as lines dedicated to connecting mobile packet-switched terminals. This type

★ DoPa: NTT DoCoMo's service launched in March 1997, which connects data terminals to the PDC-P network to enable them to access the Internet, corporate LAN and other external networks.



CN: Core Network
ExGW: packet Exchange GateWay
GMMS: Gateway Mobile Multimedia switching System
IMT-2000: International Mobile Telecommunications-2000
IP: Internet Protocol
L2TP: Layer Two Tunneling Protocol
LAN: Local Area Network
PDC-P: PDC mobile Packet data communication system
PPP: Point to Point Protocol

Figure 7 Comparison of Methods of Connecting ExGW with Mobile Packet-switched

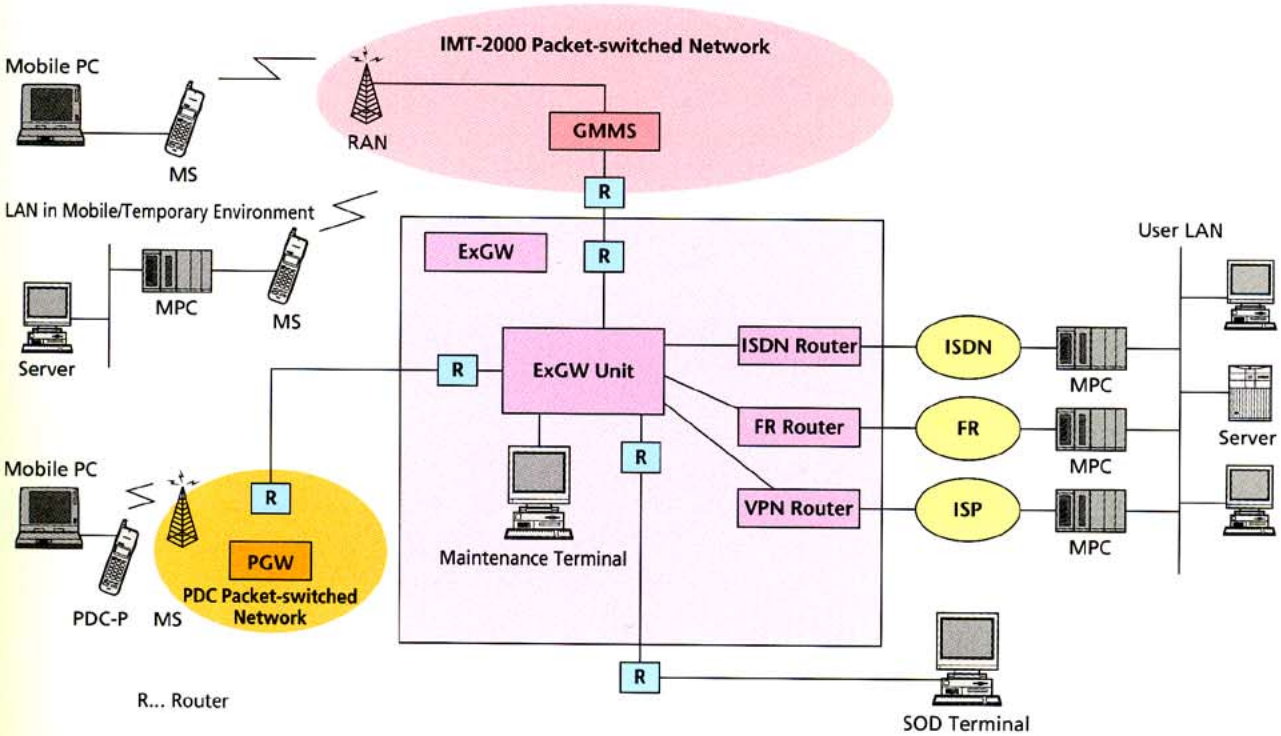
of connection establishes an IP tunnel suitable for mobile communications between ExGW and the mobile PC, and between ExGW and the user LAN, to enable PPP authentication between the mobile PC and the user LAN through the tunnel, and to enable the user to issue an IP address. It also authenticates the mobile packet-switched terminal by PPP through Integrated Services Digital Network (ISDN) and other dial-up circuits, and enables connection in the same manner as PHS and other circuit-switched terminals, in order to reduce the load incurred by circuits on the user side.

5.2 System Configuration

Figure 8 illustrates the system configuration of ExGW that achieves the functions explained in 5.1 (2). As shown in the figure, ExGW is connected not only with the IMT-2000 network but also with the PDC-mobile Packet data communication system (PDC-P) network. It has the function to connect FOMA terminals and DoPa terminals to the user LAN via ISDN (dialup), Frame Relay (FR) network and ISP. In addition, it has the function to connect LANs in a mobile or temporary environment with LANs connected via FR, ISP, etc. by using Mobile Packet aCcess equipment (MPC) attached to FOMA terminals.

ExGW consists of a GW unit based on a UNIX server, WAN router including ISDN and FR, maintenance terminals, etc. Circuits between ExGW and ISDN, FR network and ISP are shared by multiple users. The router for ISP connection has a Virtual Private Network (VPN) function based on Internet Protocol Security (IPSec) [3]. To terminate the PPP frame sent and received by the mobile PC at the MPC set on the WAN side of the user LAN, an IP tunnel is set between ExGW and the mobile PC as well as between ExGW and MPC. The tunnel is used for forwarding the PPP frame transparently. In the process, ExGW terminates the Mobile IP Tunneling protocol (MPT) used in the system, hands over the PPP frame from the IP tunnel on the mobile network side to the IP tunnel on the WAN side, and forwards it to the MPC via the router facing the designated transmission medium (ISDN, FR, Internet, etc.).

The Service Order Discharge (SOD) terminal connected with ExGW has the function to inject information required for the operation of the GW from a remote site every time when a



ExGW: packet Exchange GateWay
FR: Frame Relay
GMMS: Gateway Mobile Multimedia switching System
IMT-2000: International Mobile Telecommunications-2000
ISDN: Integrated Services Digital Network
ISP: Internet Service Provider
LAN: Local Area Network

MPC: Mobile Packet access equipment
MS: Mobile Station
PDC-P: PDC mobile Packet data communication system
PGW: Packet GateWay module
RAN: Radio Access Network
SOD: Service OrDer from operation terminal
VPN: Virtual Private Network

Figure 8 ExGW System Configuration

user is added. The terminal is able to inject routing information, etc. into the GW unit and the WAN router. In the case of mobile packet-switched terminals accommodated in the user LAN, their registration with the GW via ISDN requires to inject (a) the number of the mobile phones to be connected, and (b) the ISDN number for connection with MPC and the IP address for the tunnel using SOD terminal. The mobile PC and the MPC require a function to terminate the IP tunnel established with ExGW; the function for the former is fulfilled in the form of a tunnel driver installed in the PC, whereas the function for latter is offered by a dedicated device based on a dialup router.

5.3 Communication Protocol Processing Technologies

(1) Protocol Stack

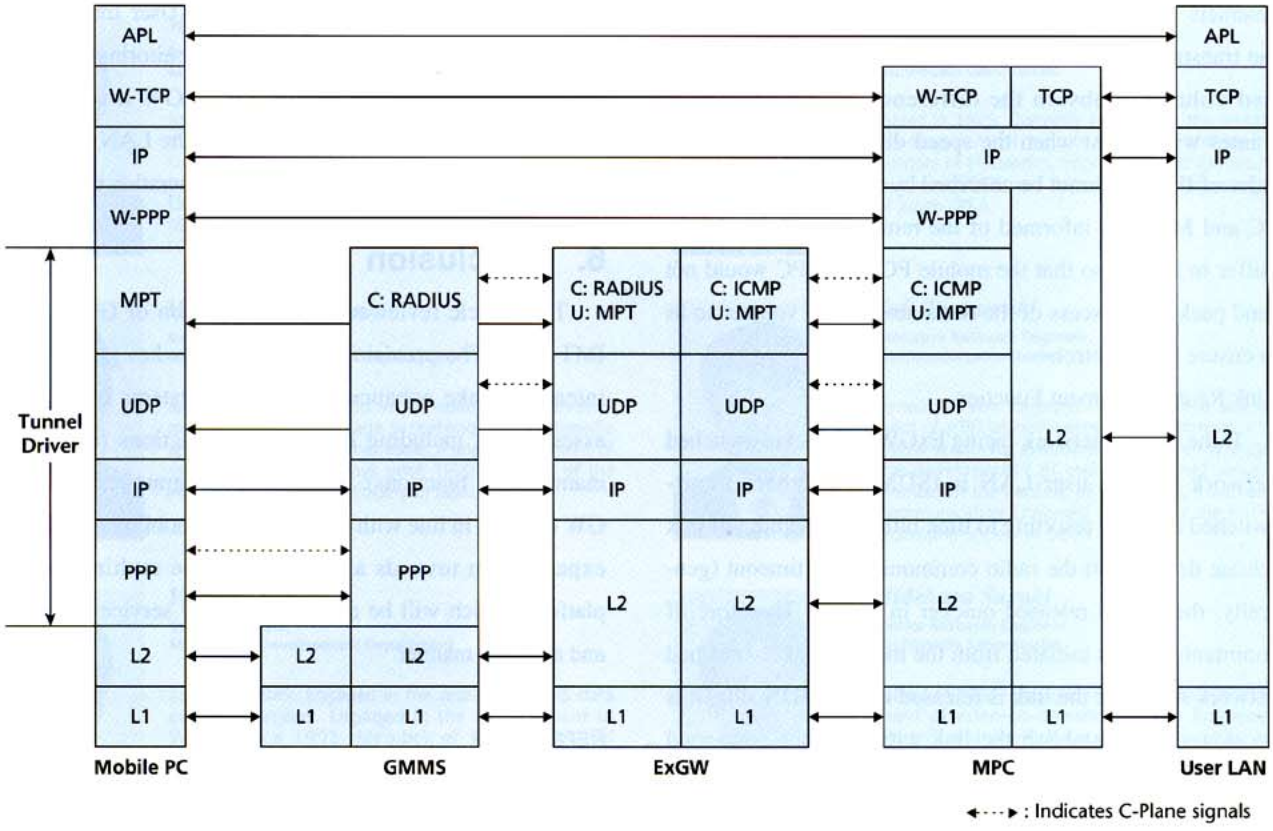
Figure 9 shows the system's protocol stack. The following explains the communication operations when a call is originated from the mobile PC.

① C-Plane Operation

When the mobile PC sends a connection request by PPP in the tunnel driver, GMMS requests authentication to ExGW based on the Remote Authentication Dial in Service (RADIUS) protocol. Here, ExGW returns the connection authentication to GMMS after establishing a WAN communication channel towards the target MPC, to prevent the mobile phone from being billed when the WAN circuit is busy and cannot be connected, including ISDN. In cases where the IP tunnel is already established between ExGW and MPC, if a connection request is sent from a new mobile phone to the MPC, ExGW will return a connection authentication to GMMS immediately.

② U-Plane Operation

After GMMS issues an IP address to the mobile PC, an IP tunnel is established with ExGW based on this IP address, and at the same time, an IP tunnel is established



APL: APpLication program
C-Plane: Control-Plane
ExGW: packet Exchange GateWay
GMMS: Gateway Mobile Multimedia switching System
ICMP: Internet Control Message Protocol
IP: Internet Protocol
LAN: Local Area Network
MPC: Mobile Packet access equipment
MPT: Mobile IP Tunneling protocol
PPP: Point to Point Protocol
RADIUS: Remote Authentication Dial in Service
TCP: Transmission Control Protocol
UDP: User Datagram Protocol
W-PPP: Wireless-PPP
W-TCP: TCP Profile over W-CDMA

Figure 9 ExGW Protocol Stack

between ExGW and MPC. MPT is a protocol for controlling the IP tunnel over the UDP. HTTP, SNMP and other application protocols are in a protocol stack above MPT. The protocol stack below MPT are hidden from applications in the form of a tunnel driver.

(2) MPT

MPT has a control packet for managing the IP tunnel via ExGW and a protocol header when forwarding data. Its functions are as follows:

① 2-link Tunnel Management

As multiple mobile PCs establish links with MPC, link management is required to determine which mobile PC should be the recipient of the IP packet sent to ExGW from LAN. To meet this requirement, the MPT protocol header has an ID for link management, which is used by ExGW to manage connection links.

② Flow Control

Both ends of ExGW are best-effort type transmission channels excluding ISDN, which may lead to variations in the transmission band. ExGW therefore has a buffer of limited volume to absorb the difference in speed. As user frames will be lost when the speed difference between two sides of ExGW cannot be absorbed by the buffer, the mobile PC and MPC are informed of the remaining volume of the buffer in ExGW so that the mobile PC and MPC would not send packets in excess of the remaining buffer volume so as to ensure flow control.

③ Link Re-establishment Function

If the mobile network facing ExGW is a packet-switched network and the user-LAN is ISDN or another circuit-switched network resorting to time billing, the timing of link release depends on the radio communications timeout (generally, the link is released quicker in ISDN). Therefore, if communication is initiated from the mobile packet-switched network side after the link is released on the ISDN side, it is necessary to re-establish the link with the once-connected MPC. As it takes time to establish the link with the circuit-switched network, this link is managed until the link is released from the mobile network side by ExGW, and at the same time, the data forwarded during link re-establishment is buffered by ExGW. Also, the unused circuit on the ISDN side is secured so that reconnection with MPC can be assured after link re-establishment.

(3) W-PPP and W-TCP

Wireless-PPP (W-PPP), which is a protocol based on PPP (RFC1661), has been uniquely enhanced under PPP Vendor Extensions (RFC2153) with the aim to shorten the connection time, etc. Normally, PPP negotiation requires three repetitions for link establishment, authentication and network protocol establishment. W-PPP reduces the connection time by completing the task with one repetition of an establishment request. TCP Profile over W-CDMA (W-TCP) tunes the TCP parameters so that the transmission band can be used effectively even in fast but delay-prone transmission channels. In this service, these protocols are terminated between the mobile PC and MPC. Refer to **4. TCPGW** for further information on W-TCP.

5.4 Operation and Maintenance Functions

ExGW is connected with the on-site and remote maintenance terminal via a LAN interface, and is able to carry out status monitoring, station data updating and gathering, and other maintenance tasks based on a Graphical User Interface (GUI). The basic operation, maintenance and monitoring functions are the same as explained in section **3.4**. ExGW is also connected with the integrated operation system via the LAN interface, and is able to send alarm information to the operation center.

6. Conclusion

This article reviewed the configuration of GW systems in IMT-2000. The provision of GW systems has just started. We intend to make enhancements to the systems based on field assessments, including management functions (operation and maintenance functions). We plan to integrate and advance the GW systems in line with the progress in mobile multimedia, and expand them towards a common mobile multimedia service platform which will be able to offer new services in a flexible and efficient manner.

REFERENCES

[1] Ishikawa, et al: "Protocol Technologies of Next-generation WAP (WAP 2.0)", NTT DoCoMo Technical Journal , Vol.9, No.3, pp71-78, Oct. 2001 [Japanese Version].

[2] W. Townsley, etc., RFC 2661 Layer Two Tunneling Protocol "L2TP", 1999.

[3] "Internet RFC Dictionary", edited by Multimedia Research Group, published by ASCII Corp. (1998).

GLOSSARY

AP: APplication
APL: APpLication program
C-Plane: Control-Plane
CN: Core Network
CPU: Central Processing Unit
DLPI: Data Link Program Interface
DNS: Domain Name System
ExGW: packet Exchange GateWay
FOMA: Freedom Of Mobile multimedia Access
FR: Frame Relay
GMMS: Gateway Mobile Multimedia switching System
GMP: GRIMM Management Protocol
GUI: Graphical User Interface
HTML: HyperText Markup Language
HTTP: HyperText Transfer Protocol
ICMP: Internet Control Message Protocol
IETF: Internet Engineering Task Force
IMT-2000: International Mobile Telecommunications-2000
IMT-GRIMM: IMT-Gateway service Representative Internet Market Mobile access exchange
IP: Internet Protocol
IPSec: Internet Protocol Security
ISDN: Integrated Services Digital Network
ISP: Internet Service Provider
L2TP: Layer 2 Tunneling Protocol
LAC: Link Access Control
LAN: Local Area Network
mopera: Mobile OPEration Radio Assistant
MPC: Mobile Packet access equipment
MPT: Mobile IP Tunneling protocol
MS: Mobile Station
NAT: the ip Network Address Translator
NI-MAX: Neo Interface-Mobile Access eXchange
NIC: Network Interface Card
NWMP: NetWork Management Protocol
PDA: Personal Digital Assistant
PDC-P: PDC mobile Packet data communication system
PGW: Packet GateWay module
PPP: Point to Point Protocol
RADIUS: Remote Authentication Dial in Service
SG: Study Group
SNMP: Simple Network Management Protocol
SOD: Service OrDer from operation terminal
SSL: Secure Sockets Layer
TCP: Transmission Control Protocol
TCPGW: TCP GateWay
U-Plane: User-Plane
UDP: User Datagram Protocol
VPN: Virtual Private Network
W-PPP: Wireless-PPP
W-TCP: TCP Profile over W-CDMA
WAN: Wide Area Network
WPCG: Wireless Protocol Conversion Gateway