PPP | Data Communication | Traffic Migration

Technology Reports

Seamless Traffic Migration between the Mobile and Fixed Networks

We have developed traffic migration technology for distributing communication traffic from mobile networks to fixed networks in a seamless manner. This technology using enhanced PPP makes it possible to switch communication traffic without interrupting application sessions between disparate networks.

Research Laboratories ***Takayuki Tamura***
Hosei Matsuoka
Minoru Takahata

1. Introduction

Due to the expansion of the mobile phone network (hereinafter referred to as "3GNW"), users now take it for granted that they can connect to the networks anytime and anywhere to access content they desire. This content is no longer limited to e-mail and Web surfing but has come to include multimedia content such as video and audio. This multimedia content requires large-capacity data communication and is consequently increasing the ratio of data communication dramatically. In other words, the content received and transmitted over 3GNW is becoming increasingly diverse generating a growing need for large-capacity data communication. Communication traffic on 3GNW is therefore expected to increase all the more in the years ahead. This increase in communication traffic can cause congestion and delay on the network thereby degrading the quality of communication. Against this background, one technique for reducing the load on 3GNW is to distribute the communication traffic on 3GNW to other available networks. Here, the other networks may be a home wireless Local Area Network (LAN) connected to the fixed network or a public wireless LAN (hotspot) that can be found at train stations, airports, and other public places and also cafes where people tend to gather as a type of mobile network. Having the 3GNW and the other networks cooperate in this way will provide users with a pleasant and convenient high-speed communication environment.

Cooperation between the mobile network and the fixed network through communication traffic migration technology should be an effective means of dealing with this increase in data communication on the 3GNW and, in particular, with the increase in multimedia content as in video and audio that require large-capacity data communication.

As described above, wireless LAN, which is becoming widely used at home and in public spaces, can be suitable as a destination for migrating communication traffic. In fact, mobile devices that come equipped with both a 3G interface and a wireless LAN interface are increasing in number giving users even more opportunities for using wireless LAN. Although wireless LAN has a small coverage area compared to 3GNW, it can be used for high-speed, large-capacity communication including large-capacity content such as video and audio.

However, 3GNW and wireless LAN are mutually independent networks, which means that the IP addresses assigned to the mobile terminal must be changed when the communication traffic migrates from 3GNW to wireless LAN. In real-time applications such as video streaming*1 and Voice over Internet Protocol (VoIP), which are types of video and audio content, the application session*2 will be interrupted by changing IP addresses resulting in the switching from one communication path to another. At this time, the application session must be reestablished to continue communication. In the case of streaming video, this may require that playback of the content in question be restarted from the beginning of the file, and in the case of VoIP, the call may have to be made again. Needless to say, interrupting the application session in this way does not make for a convenient service. It is vitally important to distribute traffic on 3GNW to another network without interrupting the application session.

In response to the above need, we propose technology for migrating communication traffic on 3GNW to disparate networks like wireless LAN while preserving the application session. In this proposal, we focus on Point to Point Protocol (PPP)*3 [1] as used for data communication on 3GNW generally and we achieve seamless migration of communication traffic without a change in IP address by migrating the PPP session. Environments for switching from the mobile network to the fixed network as in the Home U service are already being deployed, and our technique expands upon those systems enabling even more seamless switching between the mobile and fixed networks. With this technique, users will be able to enjoy an even better communication environment without being conscious of any switching between the mobile and fixed networks.

In this article, we describe the design and implementation of the proposed method and evaluate a prototype system.

2. Effects of Communication Traffic Migration Technology

This technology will not only be able to distribute communication traffic but will also allow users to enjoy video and audio content without interruption while moving between disparate networks. For example, when a user returns home while enjoying streaming video using 3GNW, current technology interrupts the application session and requires the session to be reestablished when switching from the mobile network of 3GNW to the home wireless LAN connected to the fixed network. With the proposed technology, however, the user can continue to enjoy content since the sessions are maintained regardless of how many times network switching occurs (**Figure 1**). Here, the user is oblivious to any network switching.

By switching communication traffic from 3GNW to a public wireless LAN, this technology also has the potential of reducing the energy required for communicating with a base station and other mobile terminals. Compared with 3GNW, wireless LAN has a small cell radius and low transmit power per bit, which means that positive use of wireless LAN can reduce the power consumed for transmitting the same amount of data.

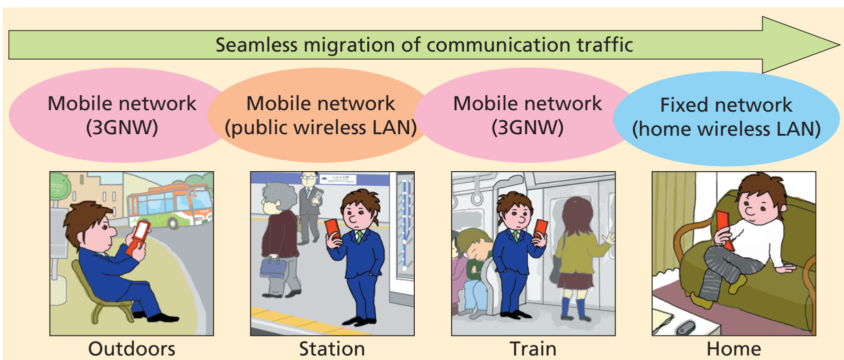

Figure 1 Migration of traffic with change in environment

*1 **Streaming**: A type of communication method for sending and receiving audio and video data over the network—data is received and played back simultaneously.

*2 **Session**: A virtual communication path for transmitting data or the transmission of data itself.

*3 **PPP**: A layer 2 protocol widely used for data communication in 3GNW. It enables two points on the network to be connected and data communication to be performed between those points.

3. Design of Proposed Method

The proposed method extends PPP, which is widely used for data communication on 3GNW, to enable the migration of communication traffic from 3GNW to disparate networks like wireless LAN without disconnecting the PPP session established on 3GNW, that is, to keep the established application session.

In present network systems, the switching of the communication path from 3GNW to wireless LAN involves the changing of the IP address and resulting disconnection of the application session. However, by changing the communication path on a layer lower than the IP layer (layer 3[*4]), it is possible to migrate communication traffic from 3GNW to disparate networks without inducing a change in IP address and while continuing the application session. In the proposed method, we focus on PPP, a protocol on layer 2[*5] used for data communication on 3GNW. By extending PPP, we have achieved seamless migration of communication traffic on layer 2 [3].

3.1 Network Configuration

The network configuration in the proposed method is shown in **Figure 2**. This network features an extended PPP client and PPP server that are equipped with multiple communication interfaces. In the figure, multiple PPP communication paths are simultaneously established between the PPP client and the PPP server via 3GNW and the Internet. The migration of communication traffic is performed between these PPP communication paths. The PPP server assigns an IP address to the PPP client when establishing a communication path. Using the IP address, the PPP client can communicate with a correspondent node[*6] via the PPP server. Here, an extension has been made to PPP so that a single IP address, which is assigned to the first PPP communication path, can be shared by multiple PPP communication paths that have been established between the PPP client and the PPP server. In this way, the IP address need not be changed when switching between communication paths and the application session can be kept.

3.2 PPP Extension

The PPP consists of several subprotocols. In the proposed method, we extend these subprotocols to enable IP address sharing and communication traffic migration. An ordinary PPP session is established on the basis of the following three subprotocols.

1) Link Control Protocol (LCP)[*7]

LCP sets up the link layer.

2) Authentication Protocol

Authentication protocols, such as Permission Authentication Protocol (PAP)[*8] or Challenge Handshake Authentication Protocol (CHAP)[*9], grant user permission for access.

3) Network Control Protocol (NCP)[*10]

NCP sets up the network layer. The 3GNW uses the Internet Protocol Con-

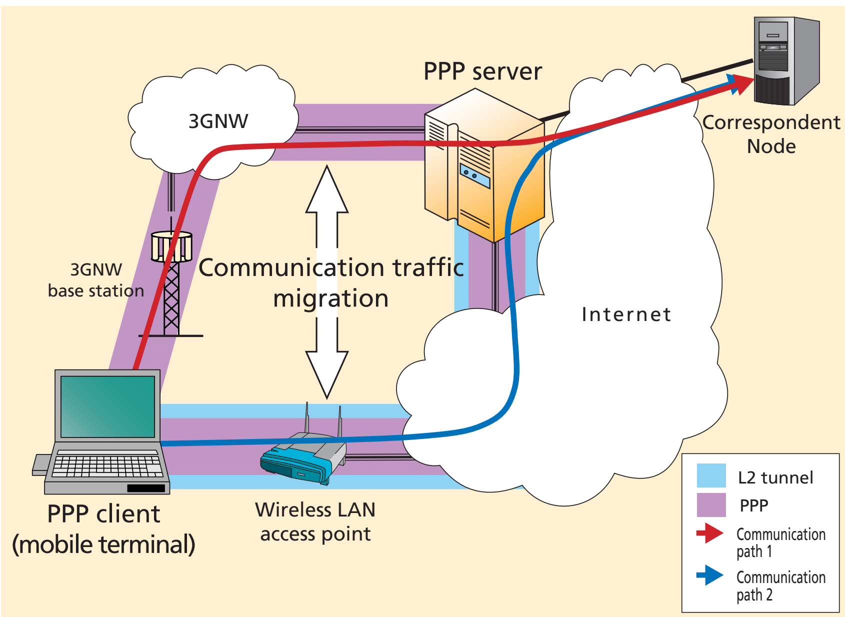

Figure 2 Network configuration in the proposed method

*4 **Layer 3**: The third layer (IP layer) in the OSI reference model.

*5 **Layer 2**: The second layer (data link layer) in the OSI reference model.

*6 **Correspondent node**: The node that the user is communicating with on the network.

*7 **LCP**: A protocol for setting up communication on the data link layer and for negotiating connections and disconnections.

*8 **PAP**: A type of protocol for authenticating users widely used by Internet providers and others.

*9 **CHAP**: A type of protocol for authenticating users. It enhances security by encapsulating authentication information.

*10 **NCP**: A protocol for setting up communication on the network layer. On 3GNW, IPCP (see*11) is used as the NCP.

trol Protocol (IPCP)[*11] as the NCP. The PPP client is assigned an IP address within IPCP.

Repeating the execution of these subprotocols several times can establish multiple PPP communication paths between the PPP client and the PPP server. In the sequence of existing PPP, however, the multiple execution of NCP allocates different IP addresses to each communication path for the same PPP client. Thus, in the event that communication traffic migrates from the first PPP communication path to the second one, the IP address used for communication will change preventing the application session from being preserved (**Figure 3**(a)).

In the proposed method, an extension is made so that NCP is not executed in the second PPP connection establishment and the IP address assigned in NCP of the first PPP connection establishment is shared with the second PPP communication path (Fig. 3(b)).

Thus, no change in the IP address occurs when the PPP client migrates communication traffic from 3GNW to wireless LAN and there is no application session interruption. To migrate the communication traffic, the communication path can be switched by simply selecting the interface allocated to each LCP of the migration destination.

3.3 Sequence of Communication Traffic Migration

Figure 4 shows the sequence for establishing a communication path on 3GNW and for migrating traffic to a disparate network while communication is in progress.

In this extension, the first PPP connection can be established by the same procedure as PPP without an extension. Then, when the opportunity arrives for the migration, communication traffic migration can be automatically performed by simply establishing a second PPP communication path.

Establishing the first communication path is performed in the order of LCP, authentication, and NCP the same as in existing PPP. In this extension, we have added sequences for identifying a PPP client within the LCP negotiation sequences (Fig. 4 (1), (2)). The proposed method performs communication traffic migration among multiple PPP communication paths established between the PPP client and the PPP server. Since the PPP server accepts PPP connections from multiple PPP clients, each PPP client must be identified so that traffic is not mistakenly transferred to the PPP communication path of another PPP client when communication traffic migration is performed. To identify the PPP client using an ID and password, the PPP server returns IDs and passwords to each PPP client as needed (Fig. 4 (1)).

Now, when making the second PPP connection, the PPP client sends the ID and password received from the PPP server at the first PPP connection establishment to the PPP server in the added sequence of LCP. The PPP server checks the ID and password so received

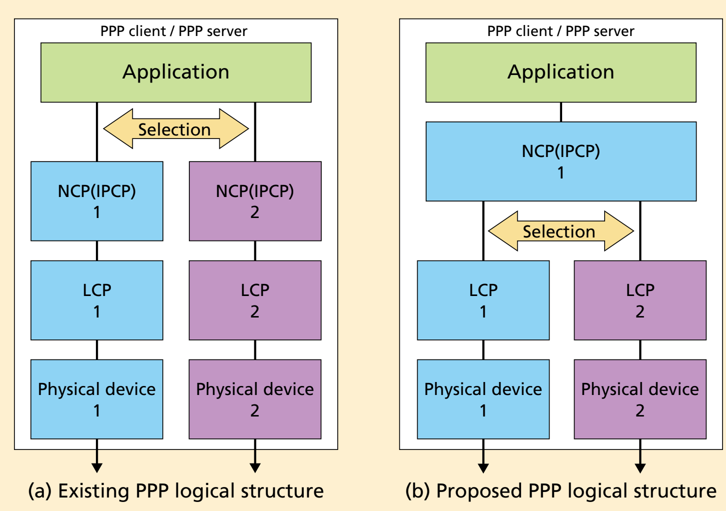

Figure 3 Subprotocol interrelationship

*11 **IPCP**: A type of NCP. IPCP sets up communication on the IP layer. An IP address is assigned during IPCP negotiations.

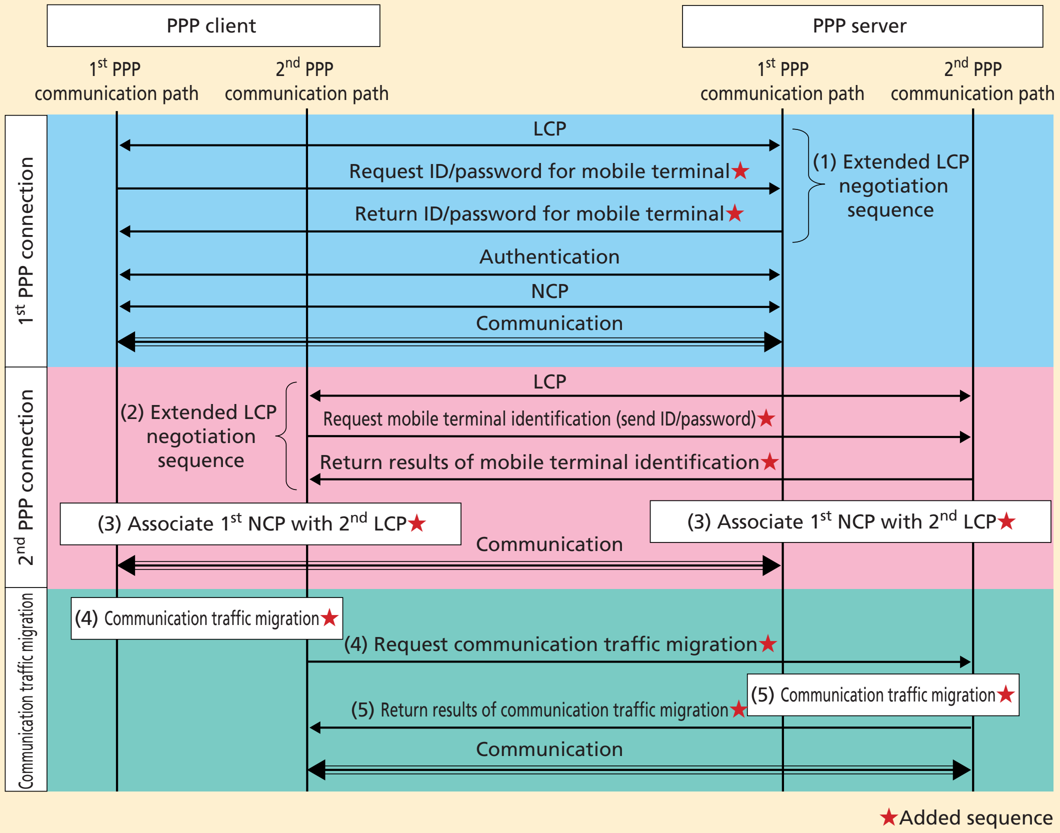

Figure 4 Communication traffic migration sequence

and identifies the PPP client accordingly (Fig. 4 (2)). On completing this identification process and the LCP for the second PPP connection, an association is made between the NCP established for the first PPP connection and the LCP established for the second PPP connection (Fig. 4(3)). This enables two PPP communication paths established by different interfaces to be associated with one IP address. Next, the PPP client sends a communication traffic migration request to the PPP server enabling the communication path switching process to be performed (Fig. 4 (4), (5)). In this way, communication traffic migration between any two PPP communication paths that have been established can be performed at any time.

In the sequence described above, communication traffic migration is initiated by the PPP client. It is also possible, however, to initiate communication traffic migration by a command triggered from the PPP server. For example, if the PPP server monitors network conditions, the PPP server can instruct a PPP client capable of using wireless LAN to migrate traffic from 3GNW to wireless LAN depending on those conditions. This makes for more efficient distribution of traffic in accordance with the current state of the network.

3.4 Adaptation to Disparate Networks

The proposed method performs communication traffic migration via PPP. It also uses an L2 tunnel to enable migration of traffic to disparate networks such as wireless LAN that do not normally use PPP.

In general, wireless LAN need not establish PPP communication and therefore cannot migrate communication traffic via PPP. Hence we focus on a tunneling protocol. The tunneling protocol on layer 2 creates a virtual tunnel between any two points on the network enabling the use of PPP between those points. The tunneling protocol on layer-2 enables wireless LAN to use PPP communication.

The protocol stack of the proposed method is shown in **Figure 5**. In this case, we use Layer-2 Tunneling Protocol (L2TP)[*12] [2] as the tunneling protocol. First, an L2 tunnel is created between the PPP client and the PPP server using the IP address obtained from a wireless LAN access point. Next, a PPP connection is made on the L2 tunnel enabling a PPP communication path to be established on wireless LAN. Using an L2 tunnel enables communication traffic migration among disparate networks as long as the networks can obtain an IP address.

4. Implementation

In this chapter, we describe an implementation of the proposed method using FreeBSD[*13] -4.11 as the PPP device driver and PPPd-2.3 as the PPP daemon (PPPd).

4.1 Extension of PPPd

The PPPd is a user daemon that manages the sequence for establishing PPP communication including LCP, authentication, and NCP. Using negotiation messages decided on beforehand, PPPd negotiates PPP communication parameters and processes connections and disconnections. The content of negotiation messages are identified on the basis of individually assigned ID numbers. In this implementation of the proposed method, new negotiation messages are added to PPPd to process the migration of PPP traffic.

4.2 Extension of PPP Driver

Many operating systems create pseudo devices when establishing a PPP communication path and associate those pseudo devices with physical devices. A pseudo device manages one IP address normally, and a mobile terminal performs communication through the pseudo device. The relationship between PPP pseudo and physical devices in existing PPP and in this implementation is shown in **Figure 6**. In the existing PPP device driver, a pseudo device is created for each physical device. As a result, an IP address is assigned to each pseudo device, which means that the IP address will change when switching from one communication path to another thereby interrupting the application session. In contrast, the implementation presented here associates one pseudo device with multiple physical devices. Thus, a single IP address managed by the pseudo device can be shared by multiple physical devices, and as a result, no change in IP address will occur when switching communication paths enabling the application session to be preserved.

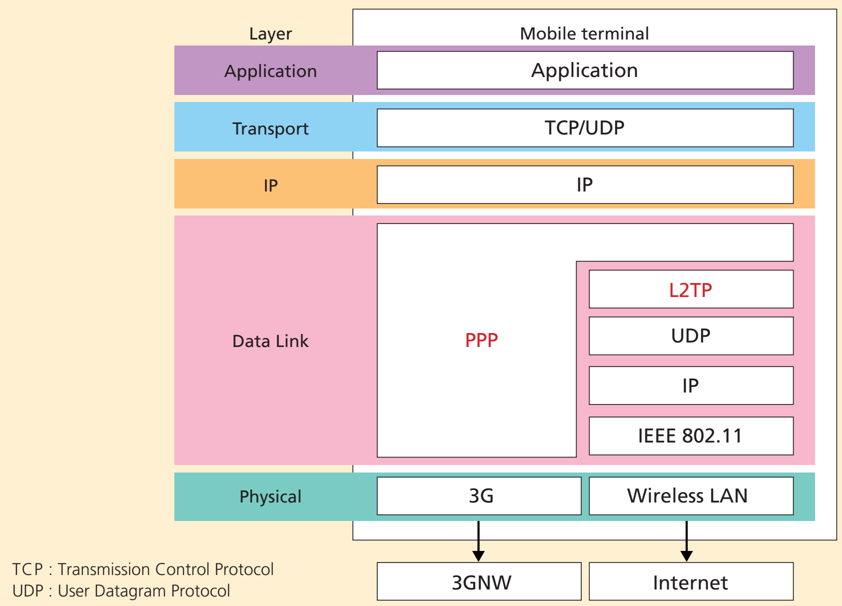

Figure 5 Protocol stack of proposed method (mobile terminal side)

*12 **L2TP**: Protocol for creating an L2 tunnel between any two points on the network. The interval between these two points connected by the tunnel can be virtually viewed as one hop.

*13 **FreeBSD**: A kind of UNIX OS.

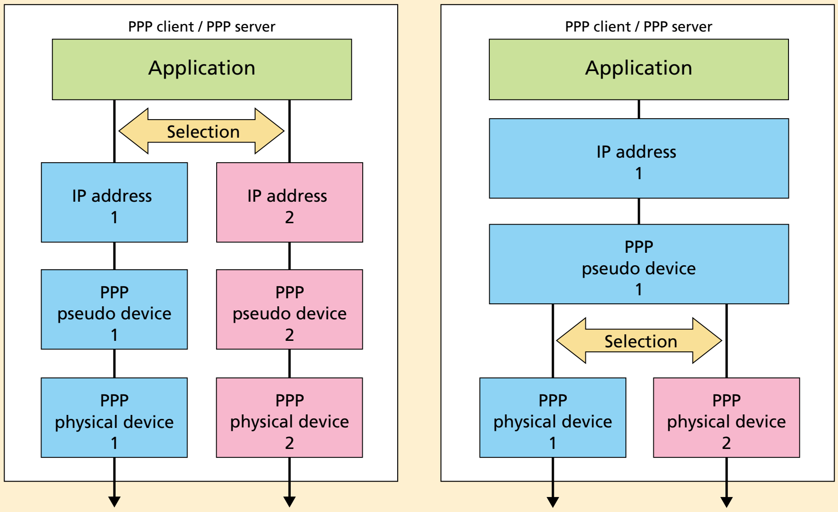

Figure 6 PPP driver extension

5. Evaluation of Prototype System

We constructed a prototype system to evaluate the effectiveness of the proposed method.

5.1 System Configuration

The prototype system consists of an extended PPP client and an extended PPP server. The PPP client is equipped with a FOMA data communication card (FOMA P2402) and a wireless LAN communication card (IEEE 802.11b). The PPP server is equipped with an Ethernet interface and an ISDN modem connected to a telephone line. The PPP client communicates with the correspondent node via the PPP server.

5.2 System Evaluation

We examined the communication traffic migration of the proposed method on the prototype system. To examine the effects of migrating communication traffic between two networks having different communication quality, we observed packet behavior at the time of migration. For examining the proposed method, we used a VoIP application, which requires that the session be maintained during communication. We performed VoIP communication between the PPP client and the correspondent node and evaluated VoIP packet behavior. Here, packets were assigned sequence numbers and their receive times at the correspondent node were recorded. In the examination, the communication path is changed from FOMA to wireless LAN. Measurement results revealed that about a dozen packets arrived out of order immediately after migration. The packet receive times also showed that the one-way delay time between the PPP client and the correspondent node in the prototype system was several hundred ms when communicating by FOMA and several tens of ms when communicating by wireless LAN. These results indicate that the occurrence of out-of-order packets can be attributed to the overtaking of packets submitted on the FOMA circuit switching network by packets submitted on the wireless LAN path.

5.3 Discussion

Based on the above test results, we concluded that packet overtaking occurs at the time of migration due to a difference in quality between the two networks involving, for example, delay times. Such packet overtaking can affect the quality of the current application by distorting the audio or video stream. One method for solving this issue is to modify the application buffer depending on the networks or their communication traffic conditions.

At the same time, the difference in communication quality between two networks can provide a positive effect since an improvement in communication quality as a result of migration will automatically improve the quality of audio or video as received by the user.

6. Conclusion

We proposed a new method for using the mobile network and the fixed network in a seamless manner.

The communication traffic migration technology proposed here can transfer 3GNW traffic to disparate networks like wireless LAN while preserving the application session. Through the use of PPP, it has achieved a convergence between the mobile network and the fixed network while maintaining high backward compatibility with the existing 3GNW.

In addition to coordinating with the current application as described above, the ability to search for available networks and to determine optimal timing for migration are considered to be important capabilities for making this technology even more useful. Techniques that use wireless LAN signal strength are now being implemented to achieve such capabilities.

To enable users to enjoy a better communication environment at any time and any place without being conscious of any switching between the mobile and fixed networks, our plan is to make a mechanism for autonomously selecting a communication path with even better communication conditions from networks that are available to mobile devices and a mechanism for migrating communication traffic at a time optimal for the application and for releasing communication paths that are no longer needed.

References

[1] W. Simpson: "The Point-to-Point Protocol (PPP)," IETF, Request for Comments 1661, Jul. 1994.

[2] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter: "Layer Two Tunneling Protocol "L2TP"," IETF, RFC 2661, Aug. 1999.

[3] T. Tamura, H. Matsuoka and M. Takahata: "Seamless PPP Migration between Disparate Wireless Networks," Internet Conference 2008 Proceedings, pp. 25-31, Oct. 2008.