Public Wireless LAN | Web Login (Cookies) | IEEE 802.1X

Technology Reports

Improving Usability of Public Wireless LAN Services

Until now, it has been necessary to either login using connectivity software, or to enter an ID and password on a Web page in order to use the public wireless LAN services provided by NTT DOCOMO. In order to make these public wireless LAN services easier to use, we have improved their usability by simplifying these connection procedures.

Ubiquitous Services Department

Atsushi Kobayashi[†1]
Hidekazu Sato[†2]
Yosuke Hirasawa
Kenji Hirata

1. Introduction

Public wireless LAN services are services which allow high-speed, high-capacity Internet access of up to 54 Mbit/s in places such as train stations, airports, cafes and fast-food restaurants for devices such as PCs, smart phones, PDAs and game machines that support IEEE 802.11a/b/g[*1] wireless protocols (**Table 1**). As of September, 2008, NTT DOCOMO's public wireless LAN service provided approximately 6,500 Access Points (AP) and several monthly and daily payment plans (moperaU + U "Public Wireless LAN" course, Mzone (monthly), and Mzone (daily)). For the user security, two stages of authentication are performed when using the public wireless LAN service (**Figure 1**).

1) AP Authentication

Authentication between the AP and mobile terminal is performed and the Service Set IDentifier (SSID)[*2] is used to differentiate between service providers. As a further security measure, communication between the AP and the mobile terminal is encrypted.

Two encryption methods are provided: Wired Equivalent Privacy (WEP)[*3], for which all users share the same encryption key, and IEEE 802.1X[*4] authentication, for which encryption keys are generated and can be periodically updated for each user, providing a high level of security.

2) User Authentication

Authentication is performed by entering an ID and password in a browser window to distinguish between users. The user must first connect to the Internet through the AP, performing AP authentication, and then perform user authentication by entering their ID and password on a Web login screen. In order to perform user authentication and login using devices such a smart phone, the user must enter the ID and password each time, which can require difficult and time-consuming text entry.

Table 1 Comparison of IEEE 802.11a/b/g

	Frequency band	Maximum throughput	Modulation
IEEE 802.11b	2.4 GHz	11 Mbit/s	DSSS
IEEE 802.11g	2.4 GHz	54 Mbit/s	OFDM
IEEE 802.11a	5.2 GHz	54 Mbit/s	OFDM(CCK)

CCK: Complementary Code Keying
DSSS: Direct Sequence Spread Spectrum
OFDM: Orthogonal Frequency Division Multiplexing

†1 Currently Core Network Engineering Department
†2 Currently Frontier Services Department

*1 **IEEE 802.11a/b/g**: Wireless LAN standards regulated by IEEE using the 5.2 GHz and 2.4 GHz frequency bands and supporting a maximum bit rate of 54 Mbit/s.
*2 **SSID**: An identifier for wireless LAN AP.
*3 **WEP**: Encryption technology specified by IEEE 802.11 in which mobile terminal and AP share an encryption key.

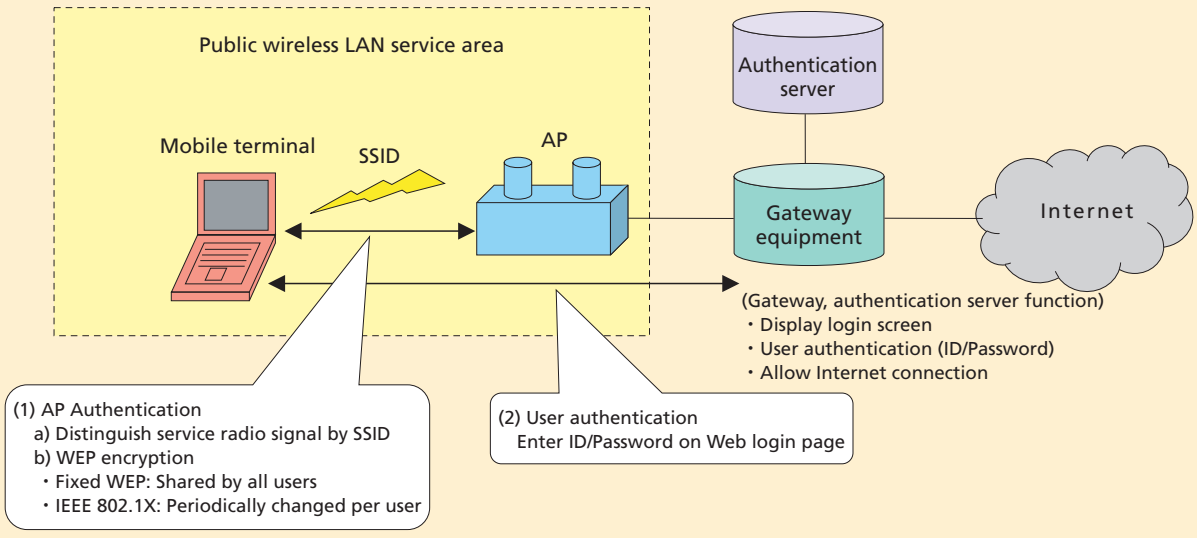

Figure 1 Overview of connection methods for public wireless LAN services

To address this and improve usability, NTT DOCOMO introduced two new functions within its public wireless LAN service area from July 1, 2008.

- Automatic login

  For mobile terminals supporting the high-security IEEE 802.1X protocol, user authentication is performed automatically when making a wireless connection within the coverage area.
- Simple login

  For mobile terminals not supporting IEEE 802.1X, the ID and password used for user authentication are stored temporarily in the browser, so that user authentication is easier for the second and later attempts.

This article describes these two functions.

2. Automatic Login Function

2.1 Description

Earlier, it was possible to perform one-click Web login using client software, but using this new function, the wireless connection using IEEE 802.1X and user authentication are completed at the same time, with no need to install client software. Automatic login using IEEE 802.1X is shown in **Figure 2**.

1) Previous Login Function

When the user starts the mobile terminal within the wireless LAN area, the terminal attempts to connect to an AP using IEEE 802.1X authentication (Step 1: AP authentication(1)). The AP communicates with the authentication server to authenticate the terminal according to the terminal's request (Step 1 (2)). The terminal acquires an IP address (Step 1 (3)). The user logs in by entering an ID and password on a Web login screen (Step 2: User authentication (1)). The gateway performs ID/password authentication, and if successful, allows a connection to the Internet (Step2: (2)). Application-level communication is now possible (Step 3: Internet connection).

2) New Login Function

When the user starts the mobile terminal within the wireless LAN area, the process is the same as before up until acquiring an IP address (Step 1: AP authentication and User authentication (1) to (3)). User authentication is per-

*4 **IEEE 802.1X**: User authentication method for wireless LAN as regulated by the IEEE. NTT DOCOMO provides for both EAP-TTLS (see *5) and PEAP (see *6) authentication methods. IEEE 802.1X provides improved security by having the AP perform re-authentication periodically, and by updating the encryption key between mobile terminal and AP.

formed at the gateway using the ID and password used during AP authentication, and an Internet connection is provided to the mobile terminal (Step 1: AP authentication, User authentication (4)). This allows application-level communication (Step 2: Internet connection).

Using this function, users can connect to the Internet by simply turning on their mobile terminal within the NTT DOCOMO public wireless LAN service area.

2.2 Improvements with the New Functions

1) Connection-denied Cases are Eliminated by Providing Two IEEE 802.1X Methods

In addition to EAP Tunneled Transport Layer Security (EAP-TTLS[*5], hereinafter reffered to as "TTLS") from IEEE 802.1X, which was also provided for automatic login earlier, we now also support Protected EAP (PEAP)[*6], which is supported by Windows XP®[*7] and Windows Vista®[*8]. Now, by simply configuring the mobile terminal, and without installing additional client software, automatic login can be enabled. This means two methods IEEE 802.1X authentication methods are supported

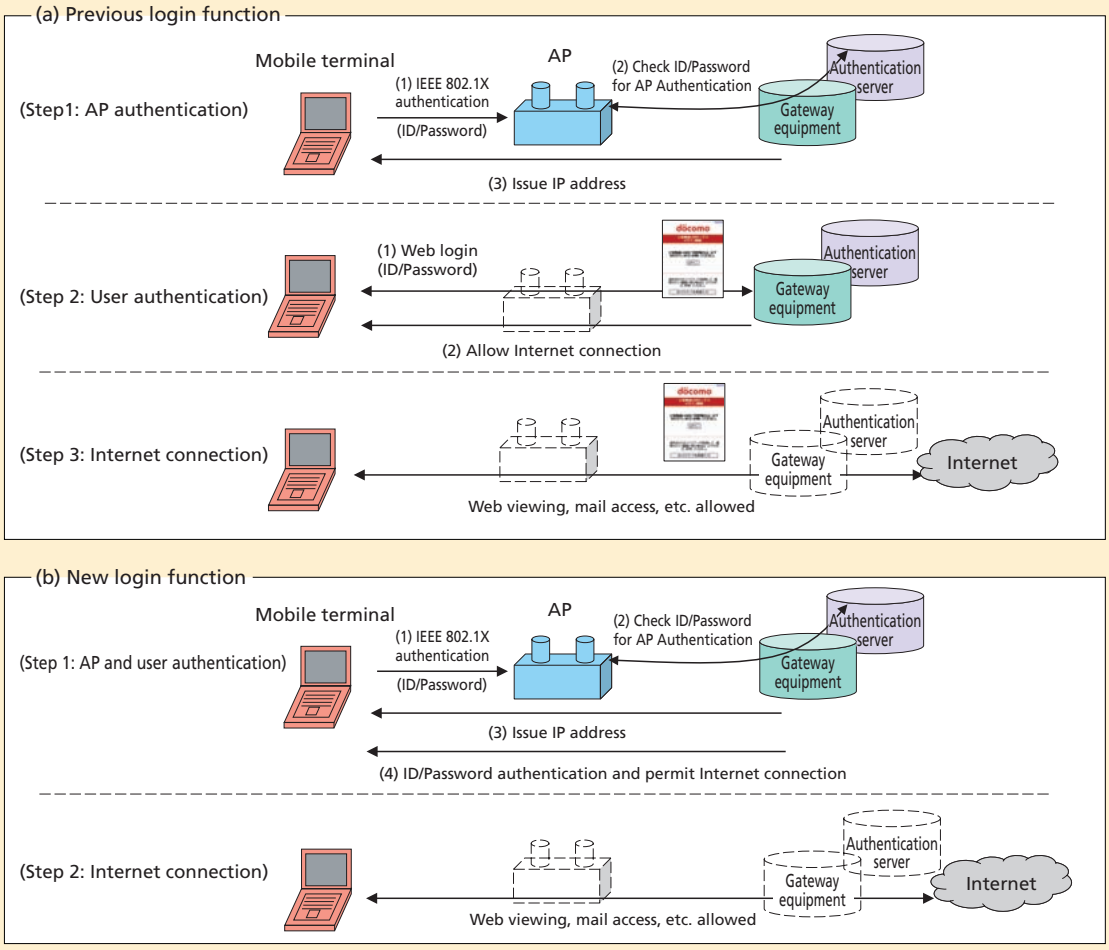

Figure 2 Automatic login using IEEE 802.1X authentication

*5 **EAP-TTLS**: A method for setting the ID and password on the mobile terminal.

*6 **PEAP**: PEAP is a standard developed by Microsoft Corp., which is used to set the ID and password of a mobile terminal, similar to EAP-TTLS. It is included as standard in Windows XP, and Windows Vista.

*7 **Windows XP®**: A registered trademark of Microsoft Corp. in the United States.

*8 **Windows Vista®**: A registered trademark of Microsoft Corp. in the United States.

(TTLS and PEAP), but we discovered that under particular conditions certain mobile terminals could not connect (terminals that use the user ID, "anonymous"[*9] during phase 1 of PEAP authentication).

- Issue

The client software provided by NTT DOCOMO uses "anonymous" as the ID in phase 1 of the TTLS authentication, but PEAP authentication assumes that anonymous will not be used in that case. Nevertheless, there are such cases with PEAP authentication, and in these cases, the authentication server assumes that the user is requesting TTLS authentication. The terminal receives a TTLS-Start notification, but then sends a request for PEAP authentication back to the authentication server. We found that the authentication server then denies a connection because it has already settled on TTLS as the method (**Figure 3** (a)).

- Resolution and improvements

We resolved this issue by not determining the authentication method based on the phase-1 ID, making unifying the first notification from the authentication server to be PEAP-Start, and having the

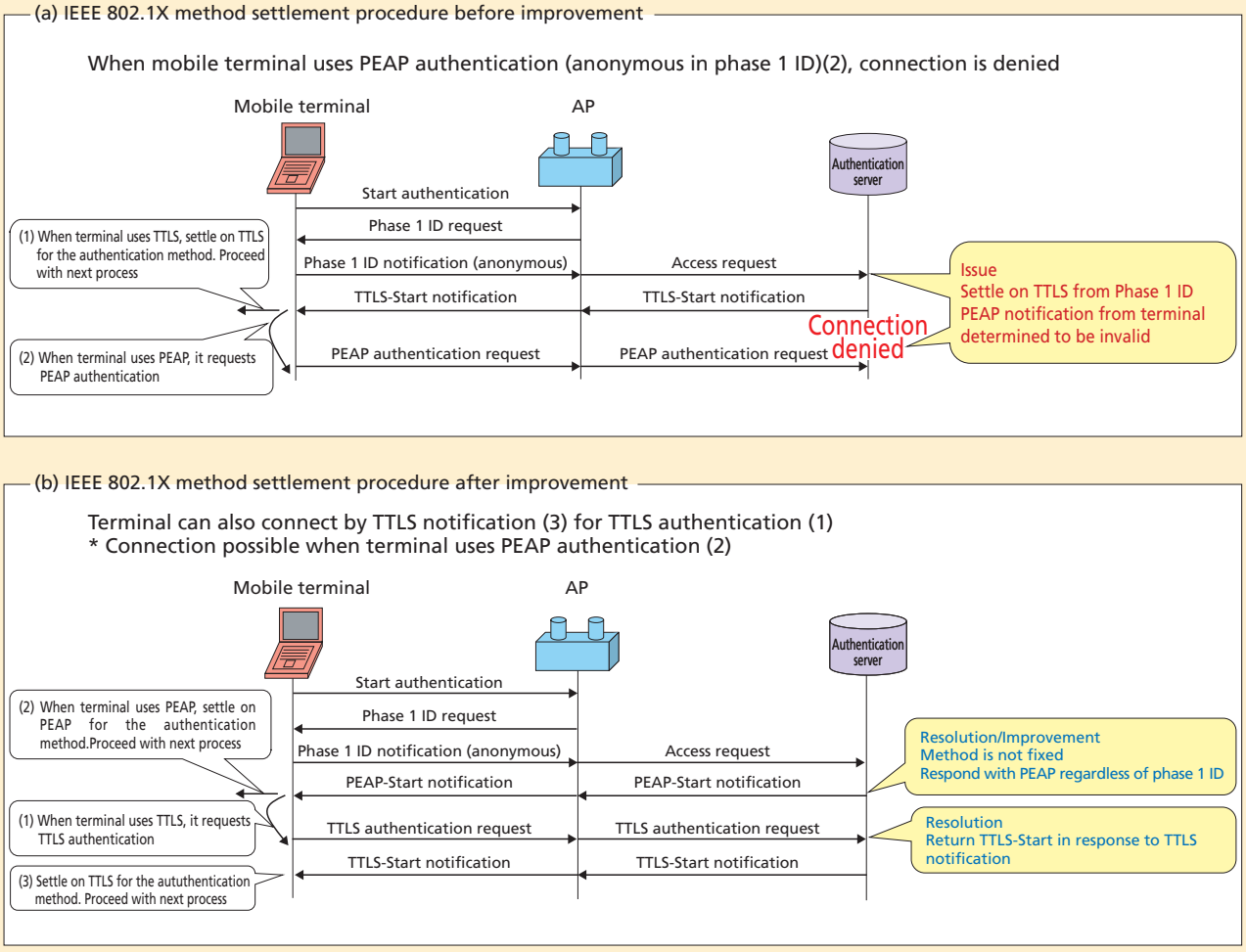

Figure 3 Settling on authentication method for IEEE 802.1X

*9 **anonymous**: A user ID used when not disclosing the real user ID.

server respond appropriately whether it receives a response or a request for a different type of authentication. If the mobile terminal requests TTLS authentication, it can send a TTLS authentication request even though the authentication server has sent it a PEAP-Start notification. The authentication request differs from the expected response, but the authentication server can respond to the TTLS-Start and continue with the authentication (Fig.3 (b)).

2) Executing Double-login Control and Display on the Web Screen

Since the public wireless LAN service can be used from multiple mobile terminals using the same ID and password, it is necessary to prevent double-login so that multiple mobile terminals cannot login using the same ID at the same time. However, re-authentication is done periodically, with IEEE 802.1X AP authentication, so it was necessary to allow double logins (use of the same user ID and password) for AP authentication because of cases such as when nearby public wireless LAN service areas overlap, resulting in movement from one AP to another. It was possible to disallow multiple logins at the user level, however, preventing use by multiple mobile terminals at the same time.

However, there are cases under certain conditions when the user has a wireless connection, intending to login automatically, but cannot connect to the Internet due to a double-login state. In order to prevent this sort of occurrence during automatic login, instead of the login screen, a double-login error screen indicating that the user's ID and password are already in use is displayed upon the first HTTP request. This screen also allows the user to logout one of the sessions if desired.

3) Preventing Erroneous Charges

Because it is possible to connect to the Internet by simply turning on the mobile terminal while in the public wireless LAN service area, users with daily-use contracts or roaming-in users[*10] could incur charges without being aware of it. To prevent this from occurring, the automatic login function can be enabled based on the type of subscriber contract, and it is only enabled for users with a monthly or flat-rate plan.

4) URL Logout

Previously, a screen was displayed after login with a logout button that the user could click to stop using the service, but with automatic login, this logout screen is no longer displayed. Instead, we have provided a URL that the user can simply enter in the address field of the browser in order to log out.

5) Reminder upon Logout

When automatic login is enabled, the wireless connection continues and IEEE 802.1X re-authentication is performed even after logging out, so unless the wireless connection is also terminated, the user will be logged in again automatically. To prevent this we place a reminder to also terminate the wireless connection on the logout screen.

3. Simple Login Function

3.1 Description

On the Web login screen, we provide a function to enable one-click login, storing the user's ID and password for up to 30 days (**Figure 4**).

1) Previous Function

Previously, the login screen was displayed for user authentication, and the login operation was required each time the service was used.

- Display of login screen.

  When the user launches the Web browser, the gateway determines whether connection to the Internet is allowed and redirects to the Web login screen if not.

- Login operation.

  The user enters an ID and password on the login screen and clicks the login button. The gateway evaluates the ID and password and if authentication completes successfully, allows a connection to the Internet.

2) New Login Function

With the new function, the user enters an ID and password once, and if saved, they can login by simply clicking a login button, without entering ID and password (for 30 days from when they are saved). Note that for one-click login to work, the mobile terminal must

*10 **Roaming-in user**: A user contracted to another operator that is using the NTT DOCOMO public wireless LAN area.

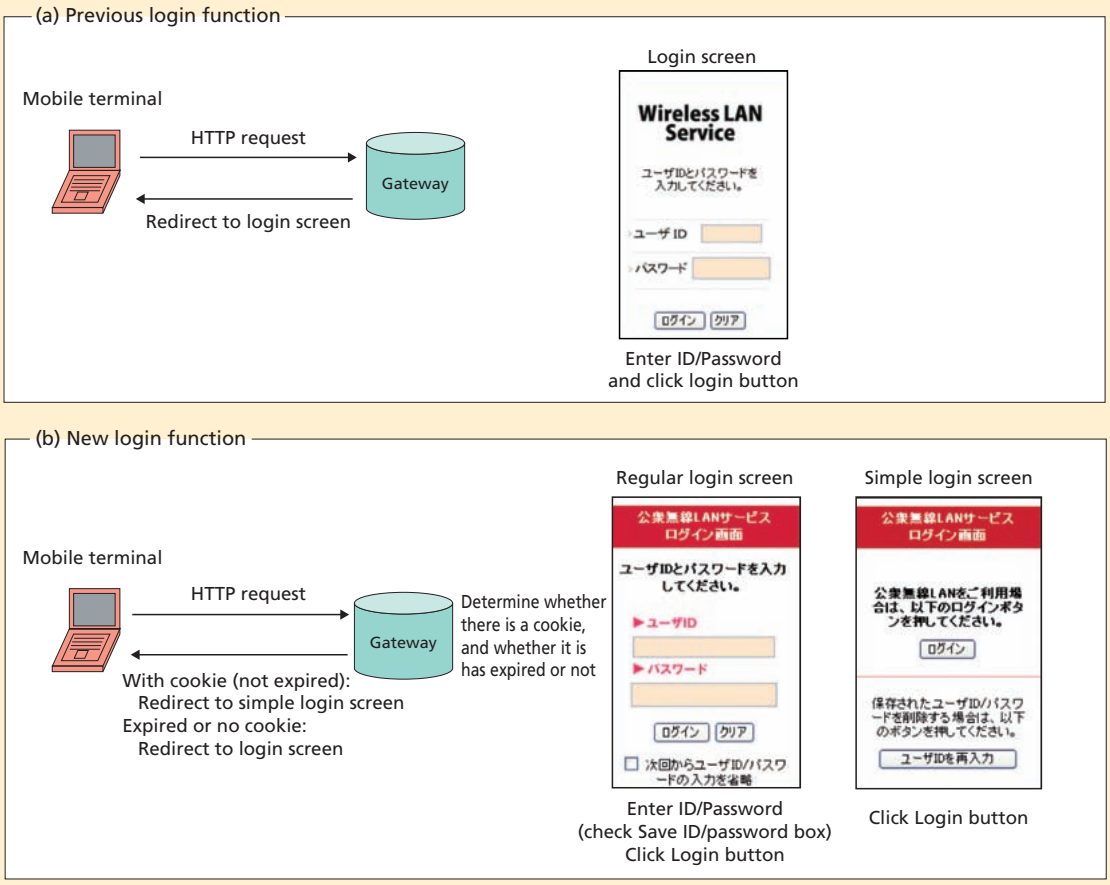

Figure 4 Comparison with Web login function (Simple login function)

be able to store cookies[*11], and this function must be enabled.

- Initial login screen and login operation.

  The user enters their ID and password on the login screen as with the earlier login method and also checks the "Save ID and password" checkbox before clicking the login button. The gateway evaluates the ID and password and allows a connection to the Internet if the authentication completes successfully, while passing a cookie to the mobile terminal, which the terminal saves.
- Login screen for the second and later login attempts.

  The gateway evaluates whether a connection to the Internet is permitted and whether the cookie has expired. If the cookie is 30 or fewer days old, it displays the simple login screen. If the cookie is more than 30 days old, the regular login screen is displayed.
- Login operation for second and later logins.

  If the cookie is 30 or fewer days old, the user simply clicks the login button. If it is more than 30 days old, login proceeds as with the initial login.

*11 **Cookie**: A function which stores information about the user, the time and number of visits to a site on the terminal, as a convenience for the user.

3.2 Improvements for the New Function

There are three main improvements arising from provision of simple login by saving the ID and password.

1) Security

- The ID and password are not displayed on the simple login screen

  Since the ID and password are not displayed, they cannot be seen from nearby when using the mobile terminal in public places.

- Cookie expiry settings

  By setting an expiry period for the cookie, even in the unlikely case that the cookie is leaked, unauthorized use is reduced because it cannot be used indefinitely. As well, the system is designed to allow flexible changes to the cookie expiry period as conditions require.

2) Improved Usability

A "Re-enter ID and password" button is provided on the login screen in case the user ID and/or password have changed, allowing this to be handled with one-click. By simply clicking this button, the previous cookie is invalidated and a login screen allowing entry of the new ID and password is displayed (the old cookie need not be deleted through the browser, etc.).

3) Display of Login Screens According to Simple-login State

As shown in Fig. 4, one of two login screens is displayed, depending on the circumstances. If the login screen is cached in the browser, there may be cases when the regular login screen is displayed when it should not, before the cookie has expired. This is handled by sending an HTTP header indicating that the page should not be cached (Cache-Control: no-cache). However, certain browsers use the cache for all pages during a given session (while the browser is still running), causing incorrect pages to be displayed. For this reason, the Web server is configured to also send the "Cache-Control: no-store" HTTP header to prevent caching of the page during a session and allow display of the login pages as expected.

4. Conclusion

In this article, we have described two new functions (automatic login and simple login) which make it easier to use the NTT DOCOMO public wireless LAN services. Through these functions and enhancing the service area, we have provided an environment that is even easier to use for users than before. We also plan to continue to develop wireless broadband services by further expanding the service area and adding more functionality.