



# **Wireless LAN Switch**

## **WLS-1280**

### **User's Manual**

***Version 1.00***

## Copyright

Copyright © 2006 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

## Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

## FCC Caution

To assure continued compliance. (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: ( 1 ) This device may not cause harmful interference, and ( 2 ) this Device must accept any interference received, including interference that may cause undesired operation.

## Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm

(8 inches) during normal operation.

## Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

## EU Countries Not Intended for Use

The ETSI version of this device is intended for home and office use in Austria Belgium, Denmark, Finland, France (with Frequency channel restrictions). Germany, Greece, Ireland, Italy, Luxembourg .The Netherlands, Portugal, Spain, Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

## WEEE regulation



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

## Revision

User's Manual for PLANET Wireless LAN Switch

Model: WLS-1280

Rev: 1.0 (Oct, 2006)

Part No. EM-WLS1280

# Table of Contents

<b>1.</b>	<b><i>Before You Start</i></b> .....	<b>3</b>
1.1	Preface .....	3
1.2	Document Convention .....	3
<b>2.</b>	<b><i>System Overview</i></b> .....	<b>3</b>
2.1	Introduction of PLANET WLS-1280.....	3
2.2	System Concept .....	4
2.3	Specification .....	5
2.3.1	Hardware Specification.....	5
2.3.2	Technical Specification .....	5
<b>3.</b>	<b><i>Base Installation</i></b> .....	<b>8</b>
3.1	Hardware Installation.....	8
3.1.1	System Requirements.....	8
3.1.2	Package Contents .....	8
3.1.3	Panel Function Descriptions .....	9
3.1.4	Installation Steps .....	10
3.2	Software Configuration.....	12
3.2.1	Quick Configuration .....	12
3.2.2	User Login Portal Page .....	22
<b>4.</b>	<b><i>Web Interface Configuration</i></b> .....	<b>24</b>
4.1	System Configuration .....	26
4.1.1	Configuration Wizard.....	26
4.1.2	System Information.....	27
4.1.3	WAN1 Configuration .....	29
4.1.4	WAN2 & Failover .....	31
4.1.5	LAN Port Roles.....	33
4.1.6	Controlled Configuration .....	34
4.1.7	Uncontrolled Configuration .....	36
4.2	User Authentication .....	40
4.2.1	Authentication Configuration .....	40
4.2.2	Black List Configuration.....	57
4.2.3	Policy Configuration.....	60
4.2.4	Additional Configuration .....	64
4.3	AP Management.....	82
4.3.1	AP List .....	82
4.3.2	AP Discovery .....	94
4.3.3	Manual Configuration .....	95

4.3.4	Template Settings.....	95
4.3.5	Firmware Management .....	96
4.3.6	AP Upgrade.....	96
4.4	Network Configuration .....	96
4.4.1	Network Address Translation.....	97
4.4.2	Privilege List.....	100
4.4.3	Monitor IP List.....	101
4.4.4	Walled Garden List .....	102
4.4.5	Proxy Server Properties .....	103
4.4.6	Dynamic DNS .....	105
4.4.7	IP Mobility .....	105
4.4.8	VPN Termination .....	105
4.5	Utilities.....	107
4.5.1	Change Password .....	107
4.5.2	Backup/Restore Settings .....	109
4.5.3	Firmware Upgrade .....	109
4.5.4	Restart .....	110
4.6	Status.....	111
4.6.1	System Status .....	112
4.6.2	Interface Status.....	113
4.6.3	Current Users .....	115
4.6.4	Traffic History.....	116
4.6.5	Notification Configuration .....	117
4.7	Help.....	119
5.	<b><i>Appendix A – Console Interface .....</i></b>	<b>120</b>
6.	<b><i>Appendix B – Network Configuration on PC .....</i></b>	<b>123</b>
7.	<b><i>Appendix C – IPSec VPN .....</i></b>	<b>128</b>
8.	<b><i>Appendix D –Proxy Setting for Hotspot.....</i></b>	<b>133</b>
9.	<b><i>Appendix E –Proxy Setting for Enterprise .....</i></b>	<b>136</b>
10.	<b><i>Appendix F –Disclaimer for Users .....</i></b>	<b>141</b>

# 1. Before You Start

## 1.1 Preface

This manual is for Hotspot owners or administrators in enterprises to set up network environment using PLANET WLS-1280. It contains step by step procedures and graphic examples to guide MIS staff or individuals with slight network system knowledge to complete the installation.

## 1.2 Document Convention

- For any caution or warning that requires special attention of readers, a highlight box with the eye-catching italic font is used as below:

***Warning:*** For security purposes, you should immediately change the Administrator's password.



Indicates that clicking this button will return to the homepage of this section.



Indicates that clicking this button will return to the previous page..



Indicates that clicking this button will apply all of your settings.



Indicates that clicking this button will clear what you set before these settings are applied.

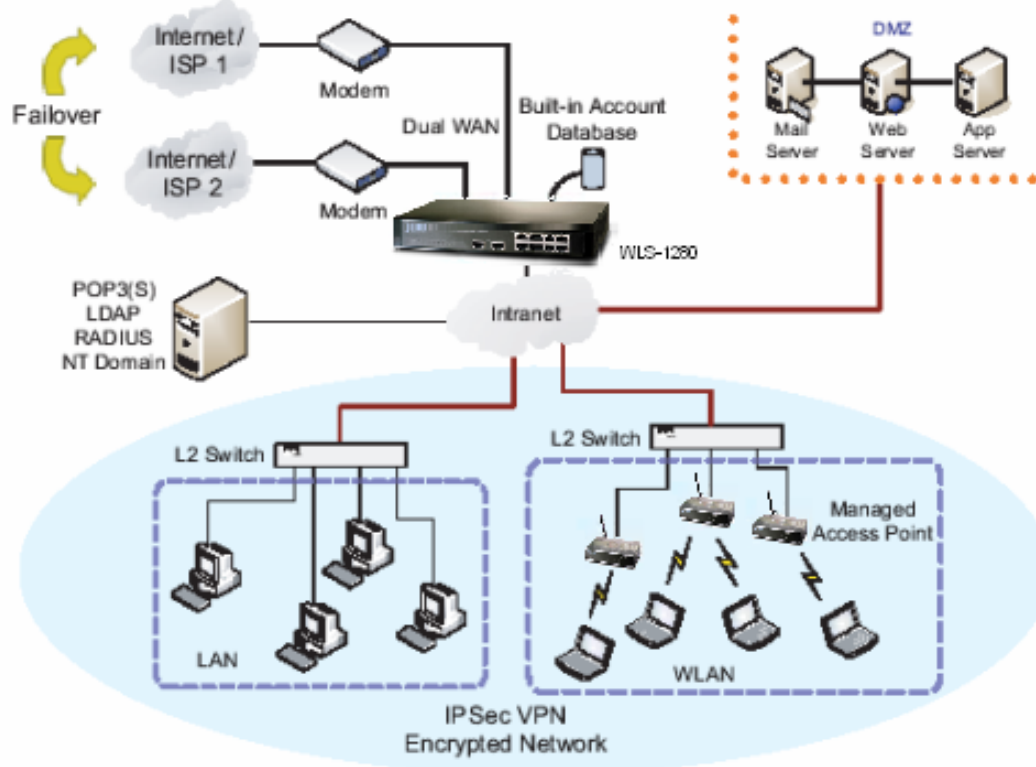
## 2. System Overview

### 2.1 Introduction of PLANET WLS-1280

PLANET WLS-1280 is an all-in-one product specially designed for Hotspot wireless network environment. It integrates “**Access Control**” and “**Wireless Network Access**” into one system to fulfill the needs in Hotspot environment.

## 2.2 System Concept

PLANET WLS-1280 is specially designed for user authentication, authorization and management. The user account information is stored in the local database or a specified external databases server. User authentication is processed via the SSL encrypted web interface. This interface is compatible to most desktop devices and palm computers. The following figure is an example of PLANET WLS-1280 set to control a part of the company's intranet. The whole managed network includes the cable network users and the wireless network users.



## 2.3 Specification

### 2.3.1 Hardware Specification

- **General**

Form Factor: Mini-desktop

Dimensions (W x D x H): 243 mm x 150 mm x 45.5 mm

Weight: 1.4 Kg

Operating Temperature: 0 ~ 45 oC

Storage Temperature: 0 ~ 65 oC

Power: 110~220 VAC, 50/60 Hz

Ethernet Interfaces: 10 x Fast Ethernet (10/100 Mbps)

- **Connectors & Display**

WAN Ports: 2 x 10BASE-T/100BASE-TX RJ-45

LAN Ports: 8 x 10BASE-T/100BASE-TX RJ-45

Console Port: 1 x RJ-11

LED Indicators: 1 x Power, 1 x Status, 2 x WAN, 8 x LAN

### 2.3.2 Technical Specification

- **Networking**

Supports Router, NAT mode

Supports Static IP, DHCP, PPPoE on WAN interface

Configurable LAN ports authentication

Supports IP Plug and Play (IP PnP)

Built-in DHCP server and supports DHCP relay

Supports NAT:

1. IP/Port Destination Redirection
2. DMZ Server Mapping
3. Virtual Server Mapping

Supports static route

Supports SMTP redirection

Supports Walled Garden (free surfing zone)

Supports MAC Address Pass-Through

Supports HTTP Proxy

- **Security**

Supports data encryption: WEP (64/128-bit), WPA, WPA2

Supports authentication: WPA-PSK, WPA2-PSK, IEEE 802.1x (EAP-MD5, EAP-TLS, CHAP, PEAP)

Supports VPN Pass-through (IPSec and PPTP)

Supports DoS attack protection

Supports user Black List

Allows user identity plus MAC address authentication for local accounts

- **User Management**

Supports up to 120 concurrent users

Provides 500 local accounts

Provides 2000 on-demand accounts

Simultaneous support for multiple authentication methods (Local and On-demand accounts, POP3(S), LDAP, RADIUS, NT Domain)

Role-based and policy-based access control (per-role assignments based on Firewall policies, Routing, Login Schedule, Bandwidth)

Customizable login and logout portal page

User Session Management:

1. SSL protected login portal page
2. Supports multiple logins with one single account
3. Session idle timer
4. Session/account expiration control
5. Friendly notification email to provide a hyperlink to login portal page
6. Windows domain transparent login
7. Configurable login time frame

- **AP Management**

Supports up to 12 manageable IEEE 802.11 compliant APs

Centralized remote management via HTTP/SNMP interface

Automatic discovery of managed APs and list of managed APs

Allows administrators to add and delete APs from the device list

Allows administrators to enable or disable managed APs

Provides MAC Access Control List of client stations for each managed AP

Locally maintained configuration profiles of managed APs

Single UI for upgrading and restoring managed APs' firmware

System status monitoring of managed APs and associated client stations

Automatic recovery of APs in case of system failure

System alarms and status reports on managed APs

- **Monitoring and Reporting**

Status monitoring of on-line users

IP-based monitoring of network devices

WAN connection failure alert

Syslog support for diagnosing and troubleshooting

User traffic history logging

- **Accounting and Billing**

Support for RADIUS accounting, RADIUS VSA (Vendor Specific Attributes)

Built-in billing profiles for on-demand accounts

Enables session expiration control for on-demand accounts by time (hour) and data volume (MB)

Provides billing report on screen for on-demand accounts

Detailed per-user traffic history based on time and data volume for both local and on-demand accounts

Traffic history report in an automatic email to administrator

- **System Administration**

Multi-lingual, web-based management UI

SSH remote management

Remote firmware upgrade

NTP time synchronization

Backup and restore of system configuration

## **3. Base Installation**

### **3.1 Hardware Installation**

#### **3.1.1 System Requirements**

- Standard 10/100BaseT including five network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

#### **3.1.2 Package Contents**

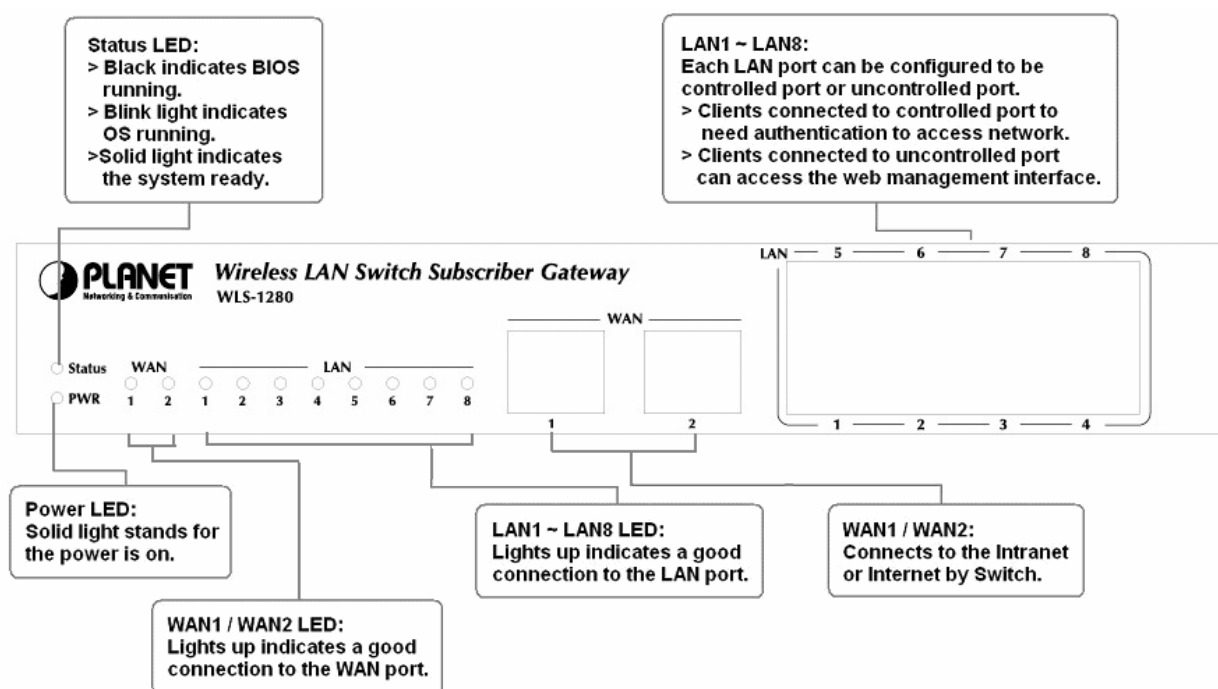
The standard package of PLANET WLS-1280 includes:

- PLANET WLS-1280 x 1
- CD-ROM x 1
- Quick Installation Guide x 1
- Power Adapter (DC 12V) x 1
- Cross Over Ethernet Cable x 1
- Console Cable x 1

**Warning:** *It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.*

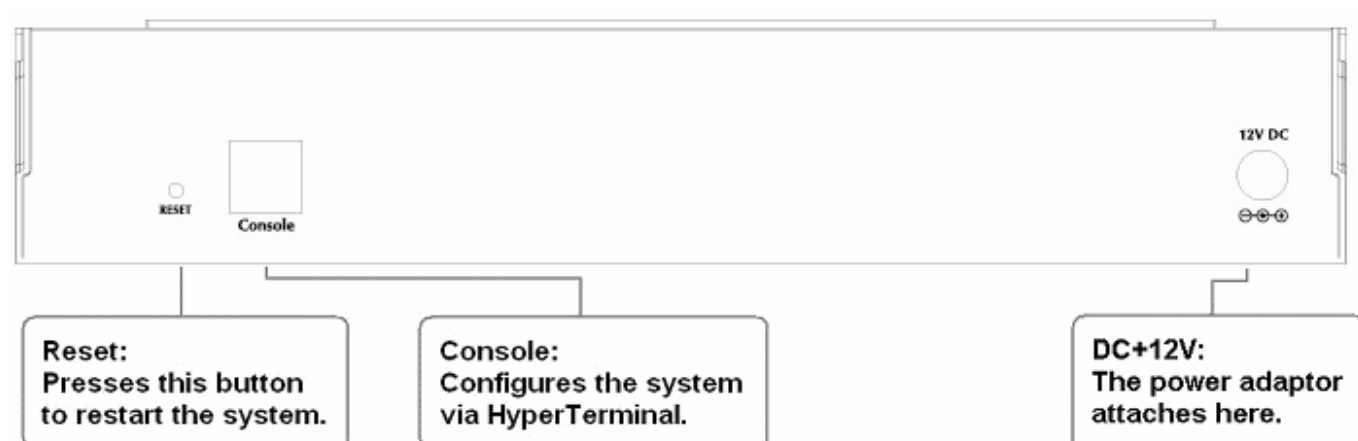
### 3.1.3 Panel Function Descriptions

#### Front Panel



- **LED:** There are four kinds of LED, PWR, Status, WAN and LAN LED, to indicate different status of the system.
- **WAN1/WAN2:** The two WAN ports are connected to a network which is not managed by PLANET WLS-1280 system, and this port can be used to connect the ATU-Router of ADSL, the port of Cable Modem, or the Switch or Hub on the LAN of a company. WAN2 doesn't support load balance with WAN1
- **LAN1~LAN8:** Client machines connect to PLANET WLS-1280 via LAN ports. Each LAN port can be configured to one of two roles, controlled or uncontrolled. The differences of these two roles for a client connected to are:
  - Clients connected to controlled port to need authentication to access network.
  - Clients connected to uncontrolled port can access the web management interface.

#### Rear Panel



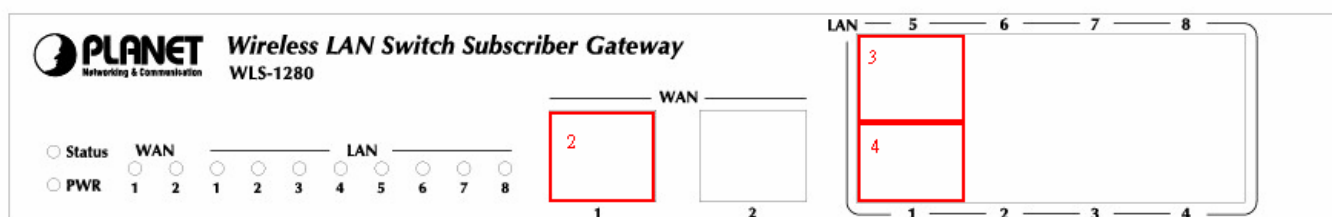
- **Reset:** Press this button to restart the system.
- **Console:** The system can be configured via serial console port. An administrator can use terminal emulation program such as Microsoft's HyperTerminal to login to the configuration console interface to change admin password or monitor system status, etc.
- **DC+12V:** The power adapter attaches here.

### 3.1.4 Installation Steps

Please follow the following steps to install PLANET WLS-1280:



1. Connect the 12V DC power adapter to the power connector socket on the rear panel. The Power LED should be on to indicate a proper connection.



2. Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to ADSL modem, cable modem or a switch/hub of the internal network. The LED of WAN1 port should be on to indicate a proper connection.
3. Connect an Ethernet cable to one of the LAN5~LAN8 Port on the front panel. Connect the other end of the Ethernet cable to a client's PC. The LED of the connected port should be on to indicate a proper connection. (Note: The default role of these four ports is **Uncontrolled Port**.)
4. Connect an Ethernet cable to one of the LAN1~LAN4 Port on the front panel. Connect the other end of the Ethernet cable to a client PC, AP or switch in managed network. The LED of the connected port should be on to indicate a proper connection. (Note: The default role of these four ports is **Controlled Port**.)

#### **Attention:**

1. PLANET WLS-1280 supports Auto Sensing MDI/MDIX. You may use either straight through or cross over cable to connect the Ethernet Port.
2. Usually a straight cable could be applied when PLANET WLS-1280 connects to an Access Point which supports

*automatic crossover. If after the AP hardware resets, PLANET WLS-1280 could not be able to connect to the AP while connecting with a straight cable, the user have to pull out and plug-in the straight cable again. This scenario does NOT occur while using a crossover cable.*

After the hardware of PLANET WLS-1280 is installed completely, the system is ready to be configured in the following sections.

## 3.2 Software Configuration

### 3.2.1 Quick Configuration

There are two ways to configure the system: using **Configuration Wizard** or change the setting by demands manually. The Configuration Wizard has 6 steps providing a simple and easy way to guide you through the setup of PLANET WLS-1280. Follow the procedures and instructions given by the Wizard to enter the required information step by step. After saving and restarting PLANET WLS-1280, it is ready to use. There will be 6 steps as listed below:

1. Change Admin's Password
2. Choose System's Time Zone
3. Set System Information
4. Select the Connection Type for WAN Port
5. Set Authentication Methods
6. Save and Restart PLANET WLS-1280

Please follow the following steps to complete the quick configuration.

1. Use the network cable of the 10/100BaseT to connect a PC to the uncontrolled port, and then start a browser (such as Microsoft IE or Firefox). Next, enter the gateway IP address as the web management interface's URL, the default is <https://192.168.2.254>. In the opened webpage, you will see the login screen. Enter "**admin**", the default username and password, in the User Name and Password column. Click **Enter** to log in.



**Caution** :If you can't get the login screen, the reasons may be: 1. The PC is set incorrectly so that the PC can't obtain the IP address automatically from the LAN port; 2. The IP address and the default gateway are not under the same network segment. Please use default IP address such as 192.168.2.xx in your network and then try it again. For the PC configuration on PC, please refer to **6. Appendix B – Network Configuration on PC**.

PLANET WLS-1280 supports three kinds of account interface. You can log in as **admin**, **manager** or **operator**. The default username and password as follows.

**Admin:** The administrator can access all area of PLANET WLS-1280.

User Name: **admin**

Password: **admin**

**Manager:** The manager can access the area under **User Authentication** to manage the user account, but no permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

Password: **manager**

**Operator:** The operator can only access the area of **Create On-demand User** to create and print out the new on-demand user accounts.

User Name: **operator**

Password: **operator**

2. After successfully logging into PLANET WLS-1280, enter the web management interface and see the welcome screen. There is a **Logout** button on the upper right corner to log out the system when finished.



3. Then, run the configuration wizard to complete the configuration. Click **System Configuration** to the **System Configuration** homepage.

System Configuration	
<b>Configuration Wizard</b>	This wizard will guide you through basic system setup.
<b>System Information</b>	Configure system and network related parameters: system name, administrator information, SNMP, and time zone. Clients will be directed to URL entered in the 'Home Page' field after successful login. Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely. Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server.
<b>WAN1 Configuration</b>	Configure static IP, DHCP, PPTP or PPPoE client on WAN1 port.
<b>WAN2 &amp; Failover</b>	Configure static IP, DHCP, on WAN2 port. The "Internet Connection Detection" and "WAN Failover" are also configured here.
<b>LAN Port Roles</b>	The roles define two types of LAN ports: 'Controlled' Authentication is required for wireless clients to access the network through these LAN ports. 'Uncontrolled' No authentication is required for wireless clients to access the network through these LAN ports.
<b>Controlled Configuration</b>	Clients from Controlled port(s) must login before accessing network, except those devices listed on the IP/MAC Privilege List. The Controlled operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.
<b>Uncontrolled Configuration</b>	Clients from Uncontrolled port(s) will not be authenticated. The Uncontrolled operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.

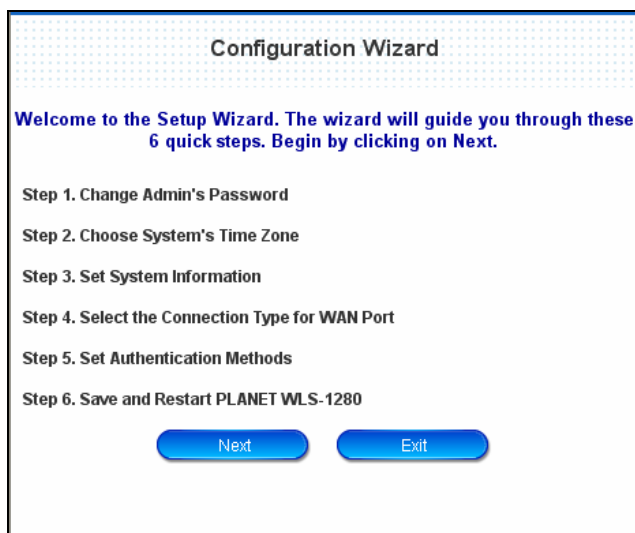
4. Click the **System Configuration** from the top menu and the homepage of **System Configuration** will appear. Then, click on **Configuration Wizard** and click the **Run Wizard** button to start the wizard.

**Configuration Wizard**

PLANET WLS-1280 is a Network Access Controller with access control features ideal for hotspot, small and medium business networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure PLANET WLS-1280.

**Run Wizard**

## 5. Configuration Wizard



The Configuration Wizard welcome screen features a title bar and a header section with a dotted background. Below the header, a blue text block provides a welcome message and instructions. A list of six steps follows, detailing the configuration process. At the bottom, there are two blue buttons labeled 'Next' and 'Exit'.

**Configuration Wizard**

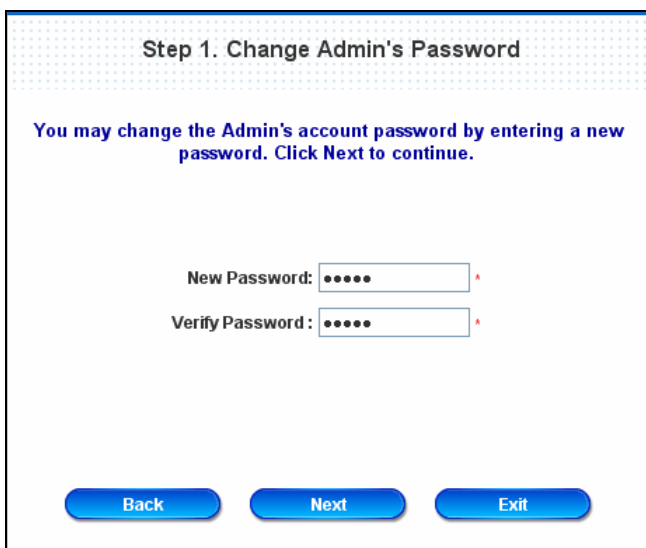
Welcome to the Setup Wizard. The wizard will guide you through these 6 quick steps. Begin by clicking on Next.

Step 1. Change Admin's Password  
Step 2. Choose System's Time Zone  
Step 3. Set System Information  
Step 4. Select the Connection Type for WAN Port  
Step 5. Set Authentication Methods  
Step 6. Save and Restart PLANET WLS-1280

Next Exit

A welcome screen that briefly introduces the 6 steps will appear. Click **Next** to begin.

- **Step 1. Change Admin's Password**



The Step 1 screen has a title bar and a header section with a dotted background. Below the header, a blue text block provides instructions. Two password input fields are present, each with a red asterisk indicating a required field. At the bottom, there are three blue buttons labeled 'Back', 'Next', and 'Exit'.

**Step 1. Change Admin's Password**

You may change the Admin's account password by entering a new password. Click Next to continue.

New Password:  \*

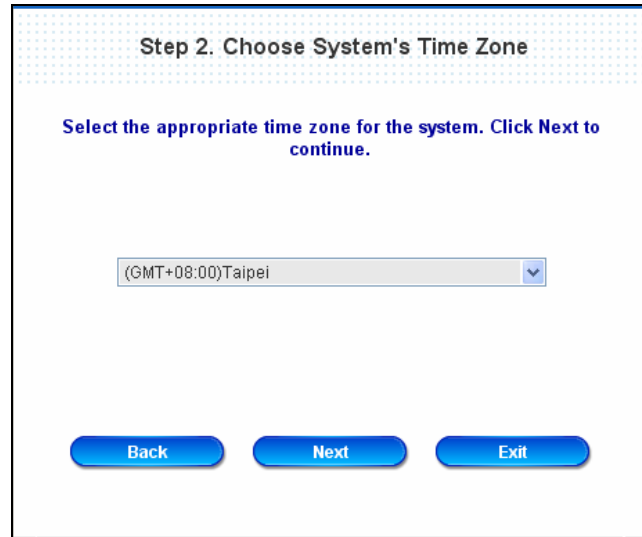
Verify Password:  \*

Back Next Exit

Enter a new password for the admin account and retype it in the verify password field (twenty-character maximum and no spaces).

Click **Next** to continue.

- **Step 2. Choose System's Time Zone**



Step 2. Choose System's Time Zone

Select the appropriate time zone for the system. Click Next to continue.

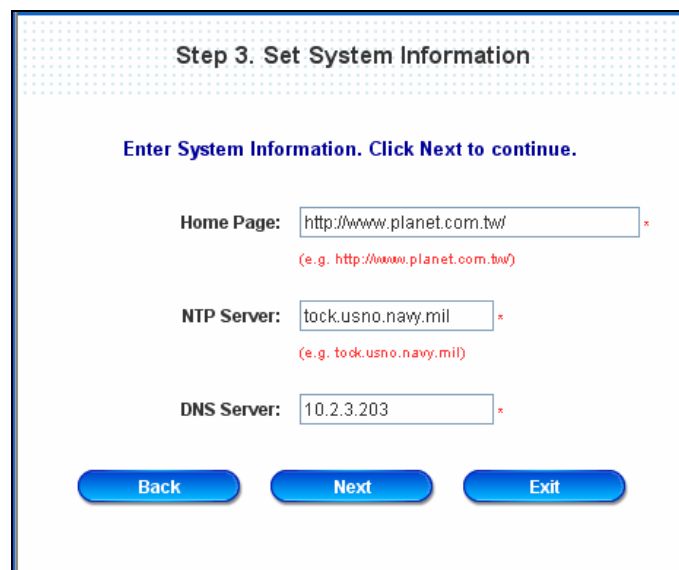
(GMT+08:00)Taipei

Back Next Exit

Select a proper time zone via the drop-down menu.

Click **Next** to continue.

- **Step 3. Set System Information**



Step 3. Set System Information

Enter System Information. Click Next to continue.

Home Page:  \*

(e.g. http://www.planet.com.tw/)

NTP Server:  \*

(e.g. tock.usno.navy.mil)

DNS Server:  \*

Back Next Exit

**Home Page:** Enter the URL to where the users should be directed when they are successfully authenticated.

**NTP Server:** Enter the IP address or domain name of external time server for PLANET WLS-1280 time synchronization or use the default.

**DNS Server:** Enter a DNS Server provided by the ISP (Internet Service Provider). Contact the ISP if the DNS IP Address is unknown.

Click **Next** to continue.

- **Step 4. Select the Connection Type for WAN Port**

Step 4. Select the Connection Type for WAN Port

Select the connection type for WAN port. Click Next to continue.

☒ **Static IP Address** Select it to set static IP address.

☐ **Dynamic IP Address** Select it to obtain an IP address automatically. (For most cable modem users.)

☐ **PPPoE Client** Enter the PPPoE Client's Username and Password. (For most DSL users.)

Back Next Exit

There are three types of WAN1 port to select in wizard: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**.

Select a proper Internet connection type and click **Next** to continue.

- **Static IP Address: Set WAN Port's Static IP Address**

Enter the **"IP Address"**, **"Subnet Mask"** and **"Default Gateway"** provided by your ISP or network administrator.

Click **Next** to continue.

Step 4 (Cont). Set WAN Port's Static IP Address

Click Next to continue.

IP Address: 10.30.1.252 \*

Subnet Mask: 255.255.255.0 \*

Default Gateway: 10.30.1.254 \*

Back Next Exit

- **Dynamic IP Address**

If this option is selected, PLANET WLS-1280 will obtain IP settings from external DHCP server on network connected by WAN1 automatically.

Click **Next** to continue.

➤ **PPPoE Client: Set PPPoE Client's Information**

Step 4 (Cont). Set PPPoE Client's Information

Enter the PPPoE Client's Username and Password. (For most DSL users.)

Username:

Password:

Back Next Exit

Enter the “**Username**” and “**Password**” provided by the ISP.  
Click **Next** to continue.

- **Step 5. Set Authentication Methods**

Step 5. Set Authentication Methods

Select a default User Authentication Method. Click Next to continue.

Postfix:   
(Its postfix name.)

Policy

☒ Local User ☐ LDAP

☐ POP3 ☐ NT Domain

☐ RADIUS

Back Next Exit

Set the user's information in advance. Enter an easily identified name as the postfix name in the **Postfix** field (e.g. Local), select a policy to assign to, and choose an authentication method.  
Click **Next** to continue. Different information has to be provided for each kind of authentication method:

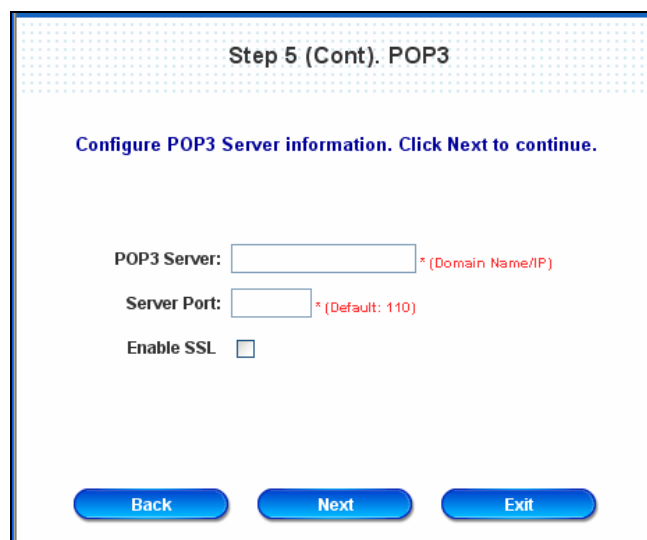
➤ **Local User: Add User**



A new user can be added to the local user data base. To add a user here, enter the **Username** (e.g. test), **Password** (e.g. test), **MAC** (optional, to specify the valid MAC address of this user) and assign it a policy (or use the default). Click the **ADD** button to add the user..

**Attention:** The policy selected in this step is applied to this user only.  
Per-user policy setting take over the group policy setting at precious step unless you select None here. Click **Next** to continue.

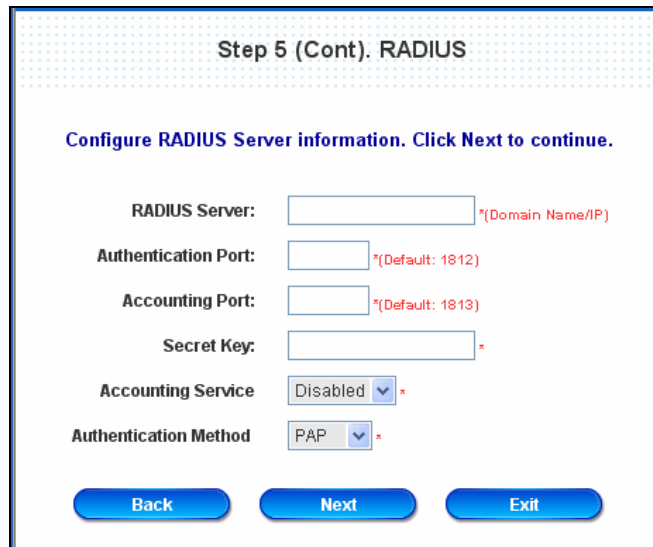
➤ **POP3 User: POP3**



Enter IP/Domain Name and server port of the POP3 server provided by the ISP, and then choose enable SSL or not.

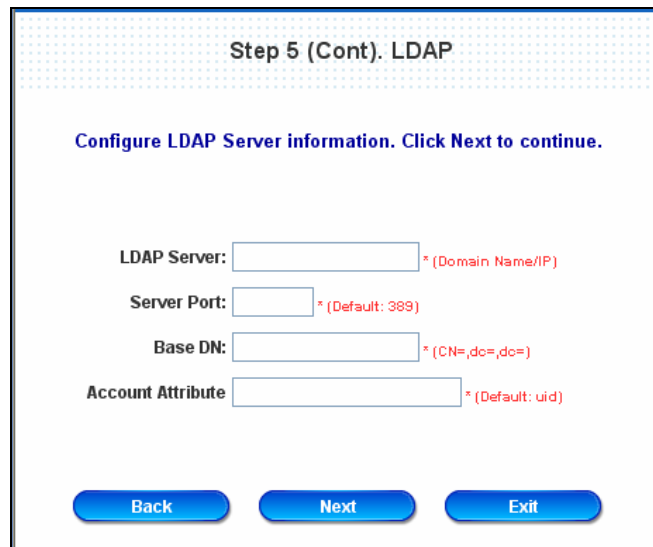
Click **Next** to continue.

➤ **RADIUS User: RADIUS**



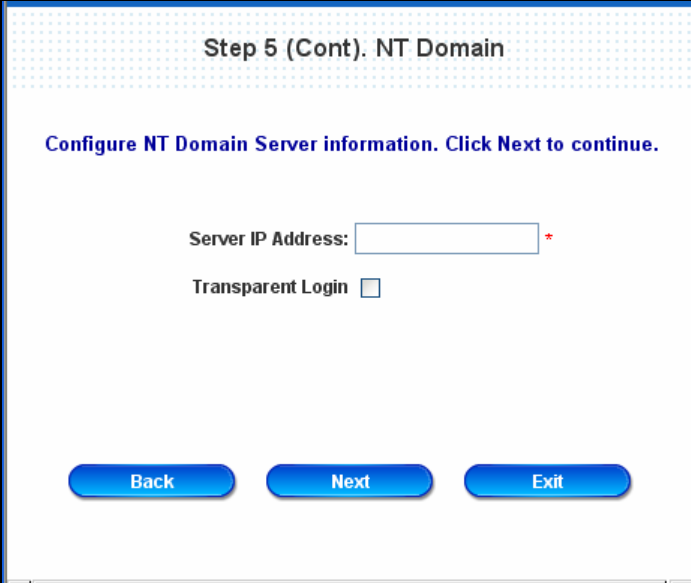
Enter RADIUS server IP/Domain Name, authentication port, accounting port and secret key. Then choose to enable accounting service or not, and choose the desired authentication method. Click **Next** to continue.

➤ **LDAP User: LDAP**



Configure external LDAP user data base here. Enter the “**LDAP Server**”, “**Server Port**”, “**Base DN**” and “**Account Attribute**”. Click **Next** to continue.

➤ **NT Domain User: NT Domain**



The screenshot shows a configuration window titled "Step 5 (Cont). NT Domain". Below the title bar, there is a header area with a dotted pattern containing the text "Step 5 (Cont). NT Domain". The main area contains the instruction "Configure NT Domain Server information. Click Next to continue." followed by a "Server IP Address:" label and a text input field with a red asterisk. Below this is a "Transparent Login" label and an unchecked checkbox. At the bottom, there are three blue buttons: "Back", "Next", and "Exit".

When NT Domain User is selected, enter the information for “**Server IP Address**”, and choose to enable/disable “**Transparent Login**”.

If “Transparent Login” is enabled, users are logged in PLANET WLS-1280’s NT Domain active directory and authenticated automatically when they log into their Windows OS domain.

Click **Next** to continue.

- **Step 6. Save and Restart PLANET WLS-1280**



The screenshot shows a completion window titled "Step 6. Save and Restart PLANET WLS-1280". Below the title bar, there is a header area with a dotted pattern containing the text "Step 6. Save and Restart PLANET WLS-1280". The main area contains the instruction "The Setup Wizard has completed. Click on Back to review or modify settings. Click Restart to save the settings and restart the system to have the current settings take effect." At the bottom, there are three blue buttons: "Back", "Restart", and "Exit".

Click **Restart** to save the current settings and restart PLANET WLS-1280. The Setup Wizard is now completed.

- **Setup Wizard.** During PLANET WLS-1280 restart, a “**Restarting now. Please wait for a while.**” message will appear on the screen. Please do not interrupt PLANET WLS-1280 until the message has disappeared. This indicates that a complete and successful restart process has finished.



**Caution:** During every step of the wizard, if you wish to go back to modify the settings, please click the **Back** button to go back to the previous step.

### 3.2.2 User Login Portal Page

To login from the login portal page via the controlled port, the user have to be identified the user name and password. The administrator also can verify the correctness of the configuration steps of PLANET WLS-1280.

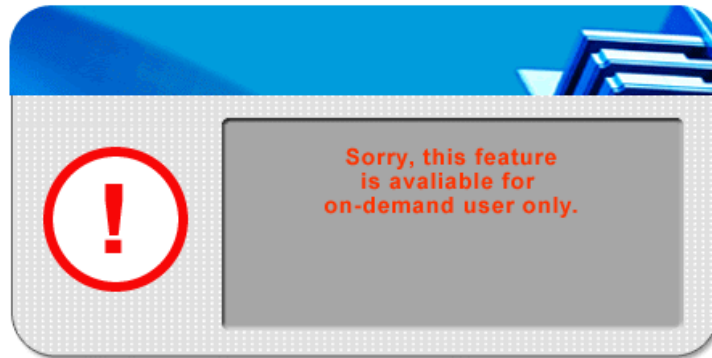
1. First, connect a user-end device (for example, a PC) to the controlled port of PLANET WLS-1280, and set the device to obtain IP address automatically. After the client obtains the network address, please open up an Internet browser and the default login webpage will appear on the Internet browser.  
Enter a valid user name and password. Assumeing local user database is chosen in the configuration wizard, enter the username and password created and then click **Submit** button (e.g. **test@Local** for the username and **test** for the password).

The screenshot shows the 'User Login Page' with a blue header. Below the header, it says 'Welcome To User Login Page!' and 'Please Enter Your User Name and Password To Sign In.' There are two input fields: 'User Name:' with the value 'jennifer@local' and 'Password:' with masked characters. At the bottom, there are three buttons: 'Submit', 'Clear', and 'Remaining'.

2. Login succeed page will appear if PLANET WLS-1280 has been installed and configured successfully. Now, clients can browse the network or surf the Internet.

The screenshot shows the 'Login Success Page' with a blue header. It features a red sphere icon and a key icon. A message box says 'Hello, jennifer@local'. Below this, it says 'Please close this window or click this button to' followed by a 'Logout' button. At the bottom, it says 'Thank you.' and 'Login time: 2006-10-2 21:37:47'.

3. If the screen shows “**Sorry, this feature is available for on-demand user only**”, it means that the “**Remaining**” button has been clicked. This button is only for on-demand users only. For clients other than on-demand users, please click the **Submit** button.



4. An on-demand user can enter the username and password in the “**User Login Page**” and click the **Remaining** button to view the remaining time the account.

A screenshot of a web page titled "User Login Page". Below the title is a welcome message: "Welcome To User Login Page! Please Enter Your User Name and Password To Sign In." There are two input fields: "User Name:" with the value "KY6F@ondemand" and "Password:" with masked characters ".....". At the bottom are three buttons: "Submit", "Clear", and "Remaining".

5. When an on-demand user logs in successfully, the following **Login Successfully** screen will appear. There is an extra line showing “**Remaining usage**” and a “**Redeem**” button.



- **Remaining usage:** Show the remaining time or data volume that the on-demand user can use to surf Internet.



The image shows a web interface titled "Redeem Page". It has a blue header with the title. Below the header, it says "Welcome To Redeem Page!" and "Please Enter Your User Name and Password To Sign In.". There are two input fields: "User Name:" with a person icon and "Password:" with a key icon. At the bottom, there are two buttons: "Enter" and "Clear", both with checkmark icons.


- **Redeem:** When the remaining time or data size is insufficient, the client has to pay for adding credit at the counter, and then, the client will get a new username and password. After clicking the **Redeem** button, a login screen will appear. Please enter the new username and password obtained and click **Redeem** button. The total available use time and data size after adding credit will show up.

## 4. Web Interface Configuration

This chapter will guide you through further detailed settings. The following table is the UI and functions of PLANET WLS-1280.

OPTION	System Configuration	User Authentication	AP Management	Network Configuration	Utilities	Status
FUNCTION	Configuration Wizard	Authentication Configuration	AP List	Network Address Translation	Change Password	System Status
	System Information	Black List Configuration	AP Discovery	Privilege List	Backup/Restore Settings	Interface Status
	WAN1 Configuration	Policy Configuration	Manual Configuration	Monitor IP List	Firmware Upgrade	Current Users
	WAN2 & Failover	Additional Configuration	Template Settings	Walled Garden List	Restart	Traffic History
	LAN Port Roles		Firmware Management	Proxy Server Properties		Notification Configuration
	Controlled Configuration		AP Upgrade	Dynamic DNS		
	Uncontrolled Configuration			IP Mobility		

				VPN Termination		
--	--	--	--	--------------------	--	--

	<p><b>Caution:</b> After finishing the configuration of the settings, please click <b>Apply</b> and pay attention to see if a restart message appears on the screen. If such message appears, system must be restarted to allow the settings to take effect. All on-line users will be disconnected during restart.</p>
---	---

## 4.1 System Configuration

This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN1 Configuration**, **WAN2 & Failover**, **LAN Port Roles**, **Controlled Configuration** and **Uncontrolled Configuration**.

System Configuration	
Configuration Wizard	This wizard will guide you through basic system setup.
System Information	Configure system and network related parameters: system name, administrator information, SNMP, and time zone. Clients will be directed to URL entered in the 'Home Page' field after successful login. Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely. Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server.
WAN1 Configuration	Configure static IP, DHCP, PPTP or PPPoE client on WAN1 port.
WAN2 & Failover	Configure static IP, DHCP, on WAN2 port. The "Internet Connection Detection" and "WAN Failover" are also configured here.
LAN Port Roles	The roles define two types of LAN ports: 'Controlled' Authentication is required for wireless clients to access the network through these LAN ports. 'Uncontrolled' No authentication is required for wireless clients to access the network through these LAN ports.
Controlled Configuration	Clients from Controlled port(s) must login before accessing network, except those devices listed on the IP/MAC Privilege List. The Controlled operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.
Uncontrolled Configuration	Clients from Uncontrolled port(s) will not be authenticated. The Uncontrolled operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.

### 4.1.1 Configuration Wizard

There are two ways to configure the system: using **Configuration Wizard** or change the setting by demands manually. The Configuration Wizard has 6 steps providing a simple and easy way to go through the basic setups of PLANET WLS-1280 and is served as **Quick Configuration**. Please refer to **3.2.2 Quick Configuration** for the introduction and description of **Configuration Wizard**.

**Configuration Wizard**

PLANET WLS-1280 is a Network Access Controller with access control features ideal for hotspot, small and medium business networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure PLANET WLS-1280.

Run Wizard

## 4.1.2 System Information

Most of the major system information about PLANET WLS-1280 can be set here. Please refer to the following description for each field:

System Information	
System Name	PLANET WLS-1280
Device Name	<input type="text"/> (FQDN for this device)
Home Page	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <input type="text" value="http://www.planet.com.tw"/> * (e.g. http://www.planet.com.tw/)
Access History IP	<input type="text"/> (e.g. 192.168.2.1)
Remote Manage IP	<input type="text" value="0.0.0.0/0.0.0.0"/> (e.g. 192.168.3.1 or 192.168.3.0/24)
SNMP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
User Logon SSL	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Time	Device Time : 2006/09/27 14:35:12 Time Zone : <input type="text" value="(GMT+08:00)Taipei"/> <input checked="" type="radio"/> NTP Enable NTP Server 1: <input type="text" value="tock.usno.navy.mil"/> *(e.g. tock.usno.navy.mil) NTP Server 2: <input type="text" value="ntp1.fau.de"/> NTP Server 3: <input type="text" value="clock.cuhk.edu.hk"/> NTP Server 4: <input type="text" value="ntp1.pads.ufrj.br"/> NTP Server 5: <input type="text" value="ntp1.cs.mu.OZ.AU"/> <input type="radio"/> Set Device Date and Time

- **System Name:** Set the system's name or use the default.
- **Device Name:** Enter an identifiable name for this device.
- **Home Page:** Enter the website of a Web Server to be the homepage. When users log in successfully, they will be directed to the homepage set. Usually, the homepage is the company's website, such as <http://www.yahoo.com>. Regardless of the original webpage set in the users' computers, they will be redirect to this page after login.
- **Access History IP:** Specify an IP address of the administrator's computer or a billing system to get billing history information of PLANET WLS-1280 with fix format URLs.

Traffic History : <https://10.2.3.213/status/history/2005-02-17>

#Date	TYPE	Name	IP	MAC	Packets In	Bytes In	Packets Out	Bytes Out
2005-02-17 18:09:03 +0800	LOGIN	aaa@w1300.tw	192.168.30.189	00:0C:F1:28:BF:D8	0	0	0	0

On-demand History : [https://10.2.3.213/status/ondemand\\_history/2005-02-17](https://10.2.3.213/status/ondemand_history/2005-02-17)

#Date	System Name	Type	Name	IP	MAC	Packets In	Bytes In	Packets Out	Bytes Out	Expiretime	Valid
2005-02-17 16:44:19 +0800	QA-W1300-Casper-213	Create_OD_User	N7E9	0.0.0.0	00:00:00:00:00:00	0	0	0	0	0	0
2005-02-17 16:44:57 +0800	QA-W1300-Casper-213	OD_User_Login	N7E9	192.168.30.189	00:0C:F1:28:BF:D8	0	0	0	0	0	0
2005-02-17 16:45:22 +0800	QA-W1300-Casper-213	OD_User_Logout	N7E9	192.168.30.189	00:0C:F1:28:BF:D8	32	14499	30			

- **Remote Manage IP:** Set the IP range which is able to connect to the web management interface via WAN and/or controlled port. For example, 10.2.3.0/24 means that as long as you are within the IP address range of 10.2.3.0/24, you can reach the administration page of PLANET WLS-1280. If the IP range bit number is omitted, 32 is used to specify a single IP address.
- **SNMP:** PLANET WLS-1280 supports SNMPv2. If the function is enabled, it is able to assign the Manager IP address and the SNMP community name used to access the management information base (MIB) of the system.
- **User Logon SSL:** Enable to activate https (encryption) or disable to activate http (non encryption) login page.
- **Time:** PLANET WLS-1280 supports NTP communication protocol to synchronize the system time with remote time server. Please specify the local time zone and IP address of at least one server in the system configuration interface for adjusting the time automatically. (Universal Time is Greenwich Mean Time, GMT). Time can also be set manually when selecting “**Set Device Date and Time**”. Please enter the date and time for these fields.

Time	Device Time : 2006/10/02 17:42:07
	Time Zone :
	(GMT+08:00)Taipei
	<input checked="" type="radio"/> NTP Enable
	NTP Server 1: tock.usno.navy.mil <small>*(e.g. tock.usno.navy.mil)</small>
	NTP Server 2: ntp1.fau.de
	NTP Server 3: clock.cuhk.edu.hk
	NTP Server 4: ntps1.pads.ufrj.br
	NTP Server 5: ntp1.cs.mu.OZ.AU
	<input type="radio"/> Set Device Date and Time

Time	Device Time : 2006/10/02 17:42:07
	Time Zone :
	(GMT+08:00)Taipei
	<input type="radio"/> NTP Enable
	<input checked="" type="radio"/> Set Device Date and Time
	-- Year -- Month -- Day
	-- Hour -- Minute -- Second

### 4.1.3 WAN1 Configuration

There are 4 connection types for the WAN1 Port: **Static IP Address**, **Dynamic IP Address**, **PPPoE Client** and **PPTP Client**.

WAN1 Configuration	
WAN1 Port	<input checked="" type="radio"/> Static IP Address
	IP Address: 10.30.1.252 *
	Subnet Mask: 255.255.255.0 *
	Default Gateway: 10.30.1.254 *
	Preferred DNS Server: 10.2.3.203 *
	Alternate DNS Server: 168.95.1.1
	<input type="radio"/> Dynamic IP Address
	<input type="radio"/> PPPoE Client
	<input type="radio"/> PPTP Client

- **Static IP Address:** Manually specifying the IP address of the WAN1 Port is applicable for the network environment where the DHCP service is unavailable. The fields with red asterisks are required to be filled in.

**IP Address:** the IP address of the WAN1 port.

**Subnet Mask:** the subnet mask of the WAN1 port.

**Default Gateway:** the gateway of the WAN1 port.

**Preferred DNS Server:** The primary DNS Server of the WAN1 port.

**Alternate DNS Server:** The substitute DNS Server of the WAN1 port. This is not required.

- **Dynamic IP address:** It is only applicable for the network environment where the DHCP Server is available in the network. Click the **Renew** button to get an IP address.

WAN1 Configuration	
WAN1 Port	<input type="radio"/> Static IP Address
	<input checked="" type="radio"/> Dynamic IP Address <span>Renew</span>
	<input type="radio"/> PPPoE Client
	<input type="radio"/> PPTP Client

- **PPPoE Client:** Common ADSL connection type. When selecting PPPoE to connect to the network, please set the “**Username**”, “**Password**”, “**MTU**” and “**CLAMPMSS**”. There is a **Dial on Demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself

WAN1 Configuration	
WAN1 Port	<input type="radio"/> Static IP Address
	<input type="radio"/> Dynamic IP Address
	<input checked="" type="radio"/> PPPoE Client
	Username: <input type="text"/>
	Password: <input type="text"/>
	MTU: <input type="text"/> 1492 bytes (Range:1000~1492)
	CLAMPMSS: <input type="text"/> 1400 bytes (Range:980~1400)
	Maximum Idle Time: <input type="text"/> 0 minutes
	Dial on Demand <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
	<input type="radio"/> PPTP Client

- **PPTP Client:** Point to Point Tunneling Protocol is a service that applies to broadband connections used mainly in Europe and Israel. Select **STATIC** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red asterisks are required to be filled in. There is a **Dial on Demand** function under PPPTP. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself

WAN1 Configuration	
WAN1 Port	<input type="radio"/> Static IP Address <input type="radio"/> Dynamic IP Address <input type="radio"/> PPPoE Client <input checked="" type="radio"/> PPTP Client
	Type <input checked="" type="radio"/> Static <input type="radio"/> DHCP
	IP Address: <input type="text"/> *
	Subnet Mask: <input type="text"/> *
	Default Gateway: <input type="text"/> *
	PPTP Server IP: <input type="text"/> *
	Username: <input type="text"/> *
	Password: <input type="text"/> *
	PPTP Connection ID/Name: <input type="text"/>
	Maximum Idle Time: <input type="text"/> 0 minutes
Dial on Demand <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	

WAN1 Configuration	
WAN1 Port	<input type="radio"/> Static IP Address <input type="radio"/> Dynamic IP Address <input type="radio"/> PPPoE Client <input checked="" type="radio"/> PPTP Client
	Type <input type="radio"/> Static <input checked="" type="radio"/> DHCP
	PPTP Server IP: <input type="text"/> *
	Username: <input type="text"/> *
	Password: <input type="text"/> *
	PPTP Connection ID/Name: <input type="text"/>
	Maximum Idle Time: <input type="text"/> 0 minutes
	Dial on Demand <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

#### 4.1.4 WAN2 & Failover

Except selecting **None** to disable this function, there are 2 connection types for the WAN2 port: **Static IP Address** and **Dynamic IP Address**. Up to three URLs can be entered. Check “**Warning of Internet Disconnection**” to work with the WAN **Failover** function. When **Warning of Internet Disconnection** is enabled, the system will check the three URLs to detect the WAN ports connection status.

- **None:** The WAN2 Port is disabled. Up to three URLs can still be entered. Check “**Warning of Internet Disconnection**” to detect the WAN1 port connection status.

WAN2 & Failover	
<b>WAN2 Port</b>	<input checked="" type="radio"/> None <input type="radio"/> Static IP Address <input type="radio"/> Dynamic IP Address
<b>Failover</b>	<b>Probe Target</b> URL1: http:// <input type="text" value="www.google.com"/> URL2: http:// <input type="text"/> URL3: http:// <input type="text"/> <input checked="" type="checkbox"/> <b>Warning of Internet Disconnection</b> When Internet Connection is down, the system will display the warning messages as: <input type="text" value="Sorry! The service is temporarily unavailable."/> *

- **Static IP Address:** Specify the IP Address, Subnet Mask and Default Gateway of WAN2 Port, which should be applicable for the network environment. Up to three URLs can be entered. Check “**Warning of Internet Disconnection**” to work with the **WAN Failover** function.

WAN2 & Failover	
<b>WAN2 Port</b>	<input type="radio"/> None <input checked="" type="radio"/> Static IP Address IP Address: <input type="text"/> * Subnet Mask: <input type="text"/> * Default Gateway: <input type="text"/> * Preferred DNS Server: <input type="text"/> * Alternate DNS Server: <input type="text"/> <input type="radio"/> Dynamic IP Address
<b>Failover</b>	<b>Probe Target</b> URL1: http:// <input type="text" value="www.google.com"/> URL2: http:// <input type="text"/> URL3: http:// <input type="text"/> <input checked="" type="checkbox"/> <b>WAN Failover</b> <input type="checkbox"/> Fallback to WAN1 when possible <input checked="" type="checkbox"/> <b>Warning of Internet Disconnection</b> When Internet Connection is down, the system will display the warning messages as: <input type="text" value="Sorry! The service is temporarily unavailable."/> *

If **WAN Failover** function is enabled, when WAN1 connection fails, the traffic will be routed to WAN2

automatically. If **Fallback to WAN1 when possible** function is enabled, when WAN1 connection is recovered, the routed traffic will be back to WAN1.

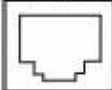
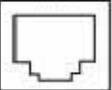




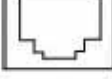



- **Dynamic IP Address:** Select this when WAN2 Port can obtain IP address automatically, such as a DHCP Server available from WAN2 Port. Up to three URLs can be entered. Check “**Warning of Internet Disconnection**” to work with the **WAN Failover** function.

WAN2 & Failover	
<b>WAN2 Port</b>	<input type="radio"/> None <input type="radio"/> Static IP Address <input checked="" type="radio"/> Dynamic IP Address <span>Renew</span>
<b>Failover</b>	Probe Target URL1: http:// <input type="text" value="www.google.com"/> URL2: http:// <input type="text"/> URL3: http:// <input type="text"/> <input checked="" type="checkbox"/> WAN Failover <input type="checkbox"/> Fallback to WAN1 when possible <input checked="" type="checkbox"/> Warning of Internet Disconnection When Internet Connection is down, the system will display the warning messages as: <input type="text" value="Sorry! The service is temporarily unavailable."/> *

For Dynamic IP Address, **WAN Failover** and **Fallback to WAN1 when possible** also can be enabled like as the function for **Static IP Address**. If **Warning of Internet Disconnection** is enabled, a warning message can be entered to indicate what the system should display when Internet connection is down.

## 4.1.5 LAN Port Roles

Client machines connect to PLANET WLS-1280 via LAN ports. Each LAN port can be configured to one of two roles, controlled or uncontrolled. The differences of these two roles for a client connected to are: Clients connected to controlled port to need authentication to access network; Clients connected to uncontrolled port can access the web management interface.

LAN Port Role Setting	
Check the box if the LAN ports need to be controlled.	
<div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div style="text-align: center;"> <input type="checkbox"/> WAN 1    <input checked="" type="checkbox"/> </div> <div style="text-align: center;"> <input type="checkbox"/> WAN 2    <input checked="" type="checkbox"/> </div> <div style="text-align: center;"> <input type="checkbox"/> LAN 5    <input type="checkbox"/> </div> <div style="text-align: center;"> <input type="checkbox"/> LAN 6    <input type="checkbox"/> </div> <div style="text-align: center;"> <input type="checkbox"/> LAN 7    <input type="checkbox"/> </div> <div style="text-align: center;"> <input type="checkbox"/> LAN 8    <input type="checkbox"/> </div> </div> <div style="display: flex; justify-content: space-around; align-items: flex-start; margin-top: 10px;"> <div style="text-align: center;">   <input checked="" type="checkbox"/> LAN 1         </div> <div style="text-align: center;">   <input checked="" type="checkbox"/> LAN 2         </div> <div style="text-align: center;">   <input checked="" type="checkbox"/> LAN 3         </div> <div style="text-align: center;">   <input checked="" type="checkbox"/> LAN 4         </div> </div>	

## 4.1.6 Controlled Configuration

The controlled port has the user authentication function which can be enabled or disabled.

Controlled Configuration	
Controlled	Operation Mode <input type="text" value="NAT"/>
	IP Address: <input type="text" value="192.168.1.254"/> *
	Subnet Mask: <input type="text" value="255.255.255.0"/> *
DHCP Server Configuration	<input checked="" type="radio"/> Disable DHCP Server
	<input type="radio"/> Enable DHCP Server
	<input type="radio"/> Enable DHCP Relay

- Controlled

Controlled Configuration	
Controlled	Operation Mode <input type="text" value="NAT"/>
	IP Address: <input type="text" value="192.168.1.254"/> *
	Subnet Mask: <input type="text" value="255.255.255.0"/> *

**Operation Mode:** Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

**IP Address:** Enter the desired IP address for the controlled port.

**Subnet Mask:** Enter the desired subnet mask for the controlled port.

- DHCP Server Configuration

There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

1. **Disable DHCP Server:** Disable DHCP Server function.

DHCP Server Configuration	<input checked="" type="radio"/> Disable DHCP Server
	<input type="radio"/> Enable DHCP Server
	<input type="radio"/> Enable DHCP Relay

2. **Enable DHCP Server:** Choose “**Enable DHCP Server**” function and set the appropriate configuration for the DHCP server. The fields with red mark are required. Please fill in these fields.

<b>DHCP Server Configuration</b>	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server	
	DHCP Scope	
	Start IP Address:	192.168.1.1 *
	End IP Address:	192.168.1.100 *
	Preferred DNS Server:	192.203.230.10 *
	Alternate DNS Server:	
	Domain Name:	domain *
	WINS Server IP:	
	Lease Time	1 Day ▼
	<a href="#">Reserved IP Address List</a>	
<input type="radio"/> Enable DHCP Relay		

**DHCP Scope:** Enter the “**Start IP Address**” and the “**End IP Address**” of this DHCP block. These fields define the IP address range that will be assigned to the Control Port clients.

**Preferred DNS Server:** The primary DNS server for the DHCP.

**Alternate DNS Server:** The substitute DNS server for the DHCP.

**Domain Name:** Enter the domain name.

**WINS Server IP:** Enter the IP address of WINS

**Lease Time:** Choose the time to change the DHCP.

**Reserved IP Address List:** For reserved IP address settings in detail, please click the hyperlink of **Reserved IP Address**. Click on the **Reserved IP Address List** on the management interface to use the **Reserved IP Address List** function. Reserved IP Address List as shown in the following figure will appear. Enter the related Reserved IP Address, MAC, and some description (not compulsory). When finished, click **Apply** to complete the setup.

Reserved IP Address List - Controlled			
Item	Reserved IP Address	MAC	Description
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>
(Total:40) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a>			

3. **Enable DHCP Relay:** Another DHCP Server IP address must be specified to enable this function. See the following figure.


DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input checked="" type="radio"/> Enable DHCP Relay
	DHCP Server IP <input type="text"/> *

### 4.1.7 Uncontrolled Configuration

The uncontrolled port doesn't have to authenticate clients before they can access the network. In this section, you can set the related configuration for uncontrolled port and DHCP server.

Uncontrolled Configuration	
Uncontrolled	Operation Mode <input type="text" value="NAT"/> ▼
	IP Address: <input type="text" value="192.168.2.254"/> *
	Subnet Mask: <input type="text" value="255.255.255.0"/> *
DHCP Server Configuration	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay

- **Uncontrolled**

Uncontrolled Configuration	
<b>Uncontrolled</b>	Operation Mode: <span>NAT</span> 
	IP Address: <span>192.168.2.254</span> *
	Subnet Mask: <span>255.255.255.0</span> *

**Operation Mode:** Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

**IP Address:** Enter the desired IP address for the uncontrolled port.

**Subnet Mask:** Enter the desired subnet mask for the uncontrolled port.

- **DHCP Server Configuration**

There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

1. **Disable DHCP Server:** Disable DHCP Server function.

<b>DHCP Server Configuration</b>	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay
----------------------------------	---

2. **Enable DHCP Server:** Choose “**Enable DHCP Server**” function and set the appropriate configuration for the DHCP server. The fields with red mark are required. Please fill in these fields.

Uncontrolled Configuration	
Uncontrolled	Operation Mode: <span>NAT</span>
	IP Address: <span>192.168.2.254</span> *
	Subnet Mask: <span>255.255.255.0</span> *
DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server
	DHCP Scope
	Start IP Address: <span>192.168.2.1</span> *
	End IP Address: <span>192.168.2.100</span> *
	Preferred DNS Server: <span>192.203.230.10</span> *
	Alternate DNS Server: <span></span>
	Domain Name: <span>domain</span> *
	WINS Server IP: <span></span>
	Lease Time: <span>1 Day</span>
	<a href="#">Reserved IP Address List</a>
	<input type="radio"/> Enable DHCP Relay

**DHCP Scope:** Enter the “**Start IP Address**” and the “**End IP Address**” of this DHCP block. These fields define the IP address range that will be assigned to the Private LAN clients.

**Preferred DNS Server:** The primary DNS server for the DHCP.

**Alternate DNS Server:** The substitute DNS server for the DHCP.

**Domain Name:** Enter the domain name.

**WINS Server IP:** Enter the IP address of WINS.

**Lease Time:** Choose the time to change the DHCP.

**Reserved IP Address List:** For reserved IP address settings in detail, please click the hyperlink of **Reserved IP Address**. If using the **Reserved IP Address List** function is desired, click on the **Reserved IP Address List** on the management interface. Then, the setup of the Reserved IP Address List as shown in the following figure will appear. Enter the related Reserved IP Address, MAC, and some description (not compulsory). When finished, click **Apply** to complete the setup.

Reserved IP Address List - Uncontrolled			
Item	Reserved IP Address	MAC	Description
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>
(Total:40) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a>			

3. **Enable DHCP Relay:** If you want to enable this function, you must specify other DHCP Server IP address.  
See the following figure.

DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input checked="" type="radio"/> Enable DHCP Relay
	DHCP Server IP <input type="text"/> *

## 4.2 User Authentication

This section includes the following functions: **Authentication Configuration**, **Black List Configuration**, **Policy Configuration**, and **Additional Configuration**.



User Authentication	
<b>Authentication Configuration</b>	System provides 3 authentication servers. Each server allows only one type of authentication method and one Black List Profile. An authentication policy may be assigned to any policy. System supports the following external authentication servers: POP3(S), RADIUS, LDAP and NT Domain. System also has embedded user database storing 2500 user accounts for local user group (500) and On-demand user group (2000). System may print out On-demand user accounts information using an external printer. By default, the On-demand user database is empty.
<b>Black List Configuration</b>	System supports 5 Black List profiles for used within the authentication server. On-demand users are NOT bounded by the Black List.
<b>Policy Configuration</b>	System provides 8 policies, each policy can apply independent firewall profile, specific route profile, login schedule profile and bandwidth policy.
<b>Additional Configuration</b>	Users will be logged out automatically after being idle for a specified period of time. Multiple login of the same user account could be enabled or disabled (not available to On-demand users). System provides Friendly Logout options, Login Page and Logout Page customization, and login notification email to client. When MAC Access Control is enabled, system will only provide login page to those devices listed.

### 4.2.1 Authentication Configuration

This function is used to configure the settings for authentication server and on-demand user authentication. Click on the server name to set the related configurations for that particular server. Users can log into the default server without the postfix to allow faster login process.

Authentication Server Configuration					
Server Name	Auth Method	Postfix	Policy	Default	Enabled
<a href="#">Server 1</a>	LOCAL	Postfix1	Policy 1	<input type="radio"/>	<input type="checkbox"/>
<a href="#">Server 2</a>	POP3	Postfix2	Policy 2	<input type="radio"/>	<input type="checkbox"/>
<a href="#">Server 3</a>	LDAP	Postfix3	Policy 3	<input type="radio"/>	<input type="checkbox"/>
<a href="#">On-demand User</a>	ONDEMAND	ondemand	Policy 1	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>

- **Server 1~3:** There are 5 kinds of authentication methods, Local User, POP3, RADIUS, LDAP and NTDomain to setup from.

Authentication Server - Server 1	
Server Name	Server 1 <small>*(Its server name)</small>
Server Status	Disabled
Postfix	Postfix1 <small>*(Its postfix name)</small>
Black List	None ▼
Authentication Method	Local User ▼ <a href="#">Local User Setting</a>
Policy	Policy 1 ▼

**Server Name:** Set a name for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (\_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

**Sever Status:** The status shows that the server is enabled or disabled.

**Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (\_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

**Black List:** There are 5 sets of black lists. Select one of them or choose “None”. Please refer to **4.2.2 Black List Configuration** for more information.

**Authentication Method:** There are 5 authentication methods, **Local**, **POP3**, **RADIUS**, **LDAP** and **NT Domain** to configure from. Select the desired method and then click the link besides the pull-down menu for more advanced configuration. For more details, please refer to **4.2.1.1~5 Authentication Method**.

**Notice:** Enabling two or more servers of the same authentication method is not allowed.

**Policy:** There are 3 policies to choose from to apply to this particular server.

- **On-demand User:** When the customers need to use wireless Internet in the store, they have to get a printed receipt with username and password from the store to log in the system for wireless access. There are 2000 On-demand User accounts available.

On-demand User Server Configuration	
Server Status	Enabled
Postfix	<input type="text" value="ondemand"/> *(e.g. ondemand. Max: 40 char)
Receipt Header 1	<input type="text" value="Welcome!"/> (e.g. Welcome!)
Receipt Header 2	<input type="text"/>
Receipt Footer	<input type="text" value="Thank You!"/> (e.g. Thank You!)
Monetary Unit	<input checked="" type="radio"/> none <input type="radio"/> \$ USD <input type="radio"/> £ GBP <input type="radio"/> € EUR <input type="radio"/> <input type="text"/> (Input other desired monetary unit, e.g. AU)
Policy Name	Policy 1 <input type="button" value="v"/>
WLAN ESSID	<input type="text" value="default"/> (e.g. ondemand)
Wireless Key	<input type="text"/>
Remark	<input type="text"/> (for customer)
Billing Notice Interval	<input checked="" type="radio"/> 10mins <input type="radio"/> 15mins <input type="radio"/> 20mins
<a href="#">Users List</a> <a href="#">Billing Configuration</a> <a href="#">Create On-demand User</a> <a href="#">Billing Report</a>	

**Server Status:** The status shows that the server is enabled or disabled.

**Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (\_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

**Receipt Header:** There are two fields, **Receipt Header 1** and **Receipt Header 2**, for the receipt's header. Enter receipt header message or use the default.

**Receipt Footer:** Enter receipt footer message here or use the default.

**Monetary Unit:** Select or enter the desired monetary unit.

**Policy Name:** Select a policy for the on-demand user.

**WLAN ESSID:** Enter the ESSID of the AP.

**Wireless Key:** Enter the Wireless key of the AP.

**Remark:** Enter any additional information that will appear at the bottom of the receipt.

**Billing Notice Interval:** While a volume type on-demand user is still logged in, the system will update the billing notice of the login successful page by the time interval defined here.

**User List:** Click to enter the **On-demand User List** screen. In the **On-demand User List**, detailed information will be documented here.

On-demand Users List					
Username	Password	Remain Time/Volume	Status	Expire Time	<input type="button" value="Delete All"/>
DH3P	ER4843FE	2 hour	2 hour	2005/06/02-17:23:39	<a href="#">Delete</a>
97UU	V7B23947	2 hour	2 hour	2005/06/05-11:45:26	<a href="#">Delete</a>

(Total:2)
 [First](#)
[Previous](#)
[Next](#)
[Last](#)

- **Search:** Enter a keyword of a username to be searched in the text field and click this button to perform the search. All usernames matching the keyword will be listed.
- **Username:** The login name of the on-demand user.
- **Password:** The login password of the on-demand user.
- **Remain Time/Volume:** The total time/Volume that the user can use currently.
- **Status:** The status of the account. Normal indicates that the account is not in-use and not overdue. Online indicates that the account is in-use and not overdue. Expire indicates that the account is overdue and cannot be used.
- **Expire Time:** The expiration time of the account.
- **Delete All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.

**Billing Configuration:** Click this to enter the **Billing Configuration** page. In the **Billing Configuration** screen, Administrator may configure up to 10 billing plans.


Billing Configuration						
Plan	Status	Type	Expired info	Valid Duration	Price	
1	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	<input type="radio"/> Volume <input type="text"/> Mbyte <input checked="" type="radio"/> Time <input type="text"/> hours <input type="text"/> mins	<input type="text"/> days <input type="text"/> hours	<input type="text"/> days	<input type="text"/>	
2	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	<input type="radio"/> Volume <input type="text"/> Mbyte <input type="radio"/> Time <input type="text"/> hours <input type="text"/> mins	<input type="text"/> days <input type="text"/> hours	<input type="text"/> days	<input type="text"/>	
3	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	<input type="radio"/> Volume <input type="text"/> Mbyte <input type="radio"/> Time <input type="text"/> hours <input type="text"/> mins	<input type="text"/> days <input type="text"/> hours	<input type="text"/> days	<input type="text"/>	
4	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	<input type="radio"/> Volume <input type="text"/> Mbyte <input type="radio"/> Time <input type="text"/> hours <input type="text"/> mins	<input type="text"/> days <input type="text"/> hours	<input type="text"/> days	<input type="text"/>	
5	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	<input type="radio"/> Volume <input type="text"/> Mbyte <input type="radio"/> Time <input type="text"/> hours <input type="text"/> mins	<input type="text"/> days <input type="text"/> hours	<input type="text"/> days	<input type="text"/>	

- **Status:** Select to enable or disable this billing plan.
- **Type:** Set the billing plan by **“Volume”** (the maximum volume allowed is 9999999 Mbyte) or **“Time”** (the maximum time allowed is 999 hours and 59 minutes).
- **Expired info:** This is the duration of time that the user needs to activate the account after the generation of the account. If the account is not activated during this duration, the account will self-expire.
- **Valid Duration:** This is the duration of time that the user can use the account after the activation of the account. After this duration, the account will self-expires.
- **Price:** The price charged for this billing plan.

**Create On-demand User:** Click this to enter the **On-demand User Generate** page.

Create On-demand User				
Plan	Type	Price	Status	Function
1	2 hrs 0 mins	20	Enabled	Create
2	N/A	N/A	Disabled	Create
3	N/A	N/A	Disabled	Create
4	N/A	N/A	Disabled	Create
5	N/A	N/A	Disabled	Create
6	N/A	N/A	Disabled	Create
7	N/A	N/A	Disabled	Create
8	N/A	N/A	Disabled	Create
9	N/A	N/A	Disabled	Create
0	N/A	N/A	Disabled	Create

Pressing the **Create** button for the desired rule, an On-demand user will be created, then click **Printout** to print a receipt which will contain this on-demand user's information. There are 2000 On-demand user accounts available.

 **Welcome!**

<b>Username</b>	<b>Z5F6@ondemand</b>
<b>Password</b>	<b>ZFQ9M6C2</b>
<b>Price</b>	<b>20</b>
<b>Usage</b>	<b>2 hrs 0 mins</b>

ESSID : default

Valid to use until: 2006/10/05 18:18:27

**Thank You!**

Printout

Close

**Billing Report:** Click this to enter the **On-demand users Summary report** page. In **On-demand users Summary report** page, Administrator can get a complete report or a report of a particular period.

From year: -- month: -- day: --  
To year: -- month: -- day: --

- **Report All:** Click this to get a complete report including all the on-demand records. This report shows the total expenses and individual accounting of each plan for all plans available.

Report All	
Accounts sold in total	2
Plan1	2
Plan2	0
Plan3	0
Plan4	0
Plan5	0
Plan6	0
Plan7	0
Plan8	0
Plan9	0
Plan10	0
Total income	40
Income from tickets sold for time users	40
Income from tickets sold for volume users	0

- **Search:** Select a time period to get a periodical report. The report tells the total expenses and individual accounting of each plan for all plans available for that period of time.

Report from 2005/06/25 ~ 2005/06/28	
Accounts sold in total	2
Plan1	2
Plan2	0
Plan3	0
Plan4	0
Plan5	0
Plan6	0
Plan7	0
Plan8	0
Plan9	0
Plan10	0
Total income	40
Income from tickets sold for time users	40
Income from tickets sold for volume users	0

#### 4.2.1.1 Authentication Method – Local User Setting

Choose “**Local User**” in the **Authentication Method** field, the hyperlink besides the pull-down menu will become “**Local User Setting**”.

Authentication Server - Server 1	
Server Name	<input type="text" value="Server 1"/> <small>*(Its server name)</small>
Server Status	Disabled
Postfix	<input type="text" value="Postfix1"/> <small>*(Its postfix name)</small>
Black List	<input type="text" value="None"/>
Authentication Method	<div>Local User <a href="#">Local User Setting</a></div>
Policy	<div>Local User POP3 Radius LDAP NTDomain</div>

✓ Apply ← Clear

Click the hyperlink to get in for further configuration.

Local User Setting	
<a href="#">Edit Local User List</a>	
Radius Roaming Out	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
802.1x Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

- **Edit Local User List:** Click this to enter the “**Local User List**” page.

Users List				
Username	Password	MAC	Policy	<input type="button" value="Del All"/>
			Remark	
			VPN Termination Enabled	
(Total:0) <a href="#">First</a> <a href="#">Previous</a> <a href="#">Next</a> <a href="#">Last</a>				

- **Add User:** Click this to enter the **Add User** interface. Fill in the necessary information such as “**Username**”, “**Password**”, “**MAC**” (optional) and “**Remark**” (optional). Select a desired **Policy**, check whether to enable **VPN Termination**.

Add User						
Item	Username	Password	MAC (xx:xx:xx:xx:xx:xx)	Policy	Remark	VPN Termination
1	Alice	.....		Policy 1 ▾	in land	<input checked="" type="checkbox"/>
2	Bob	...	04:03:11:1b:2d:3a	Policy 6 ▾		<input type="checkbox"/>
3	Cathy	.....		Policy 4 ▾		<input checked="" type="checkbox"/>
4				None ▾		<input type="checkbox"/>
5				None ▾		<input type="checkbox"/>
6				None ▾		<input type="checkbox"/>
7				None ▾		<input type="checkbox"/>
8				None ▾		<input type="checkbox"/>
9				None ▾		<input type="checkbox"/>
10				None ▾		<input type="checkbox"/>

Click Apply to save all the settings after finishing to add users.

User 'Alice' has been added!

User 'Bob' has been added!

User 'Cathy' has been added!

Add User						
Item	Username	Password	MAC (xx:xx:xx:xx:xx:xx)	Policy	Remark	VPN Termination
1				None ▾		<input type="checkbox"/>
2				None ▾		<input type="checkbox"/>
3				None ▾		<input type="checkbox"/>
4				None ▾		<input type="checkbox"/>

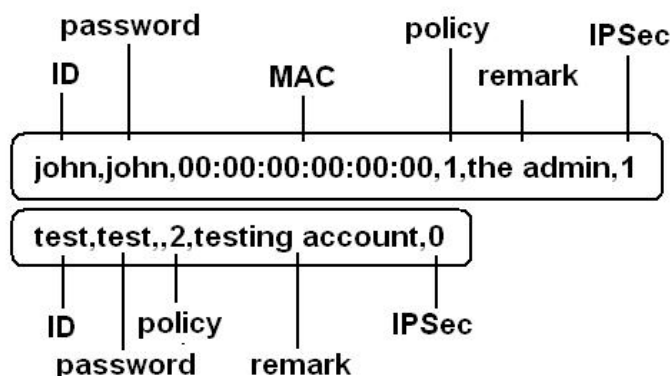
**Upload User:** Click this to enter the **Upload User** interface. Click the **Browse** button to select the text file for the user account upload. Then click **Submit** to complete the upload process.

Note: The format of each line is "ID, Password, MAC, Policy, Remark, IPSec" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.

Note: If you want user Enabled VPN Termination, please set IPSec field to 1, or 0 would disable.

Upload User Account	
File Name	<input type="text"/> Browse...
Submit	

The uploading file should be a text file and the format of each line is "**ID, Password, MAC, Policy, Remark, IPSec**" without the quotes. There must be no spaces between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. The Group field indicates policy number to use. When adding user accounts by uploading a file, the existing accounts in the embedded database will not be replaced by new ones. If you want user Enable VPN Termination, please set **IPSec** field to 1 to enable VPN, or 0 to disable VPN.



**Download User:** Click this to enter the **Users List** page and the system will directly show a list of all created user accounts. Click **Download** to create a .txt file and then save it on disk.

Users List			
Username	Password	MAC	Policy
			Remark
			VPN Termination Enabled
Alice	alice		1
			in land
			1
Bob	123	04:03:11:1b:2d:3a	6
			0
Cathy	asdfasdaf		4
			0

[Download](#)

**Refresh:** Click this to renew the **User List** page.

<a href="#">Add User</a> <a href="#">Upload User</a> <a href="#">Download User</a> <a href="#">Refresh</a>				
<input type="text"/> <a href="#">Search</a>				
Users List				
Username	Password	MAC	Policy	<a href="#">Del All</a>
			Remark	
			VPN Termination Enabled	
<a href="#">Alice</a>	alice		Policy 1	<a href="#">Delete</a>
			in land	
			Yes	
<a href="#">Bob</a>	123	04:03:11:1b:2d:3a	Policy 6	<a href="#">Delete</a>
			No	
<a href="#">Cathy</a>	asdfasdasd f		Policy 4	<a href="#">Delete</a>
			No	
<a href="#">Allen</a>	al135		Policy 2	<a href="#">Delete</a>
			Yes	

**Search:** Enter a keyword of a username that you wish to search in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.

Add User

Upload User

Download User

Refresh

Search

Users List				
Username	Password	MAC	Policy	<div>Del All</div>
			Remark	
			VPN Termination Enabled	
<a href="#">Bob</a>	123	04:03:11:1b:2d:3a	Policy 6	<a href="#">Delete</a>
			No	

(Total:1)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

**Del All:** This will delete all the users at once.

**Delete:** This will delete the users individually.

**Edit User:** If you want to edit the content of individual user account, click the username of the desired user account to enter the **User Profile** Interface for that particular user, and then modify or add any desired information such as “**Username**”, “**Password**”, “**MAC**” (optional) and “**Remark**” (optional). Then check “**VPN Termination**” to enable this function or not. Click **Apply** to complete the modification.

User Profile	
Username	Bob *
Password	...
MAC	04:03:11:1b:2d:3a
Policy	Policy 6 ▼
Enable VPN Termination	<input type="checkbox"/>
Remark	

- **Radius Roaming Out / 802.1x Authentication:** These 2 functions can be enabled or disabled by checking the correct button. Checking either of them makes the hyperlink called **Radius Client List** show up.

Local User Setting	
<a href="#">Edit Local User List</a>	
Radius Roaming Out	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
802.1x Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<a href="#">Radius Client List</a>	

Click the hyperlink of **Radius Client List** to enter the **Radius Client Configuration** page. Choose the desired type, **Disable**, **Roaming Out** or **802.1x** and key in the related data and then click **Apply** to complete the settings.

Radius Client Configuration				
No.	Type	IP Address	Segment	Secret
1	Roaming Out ▼	10.0.0.0	255.0.0.0 (/8) ▼	12345678
2	Disable ▼		255.255.255.255 (/32) ▼	
3	Disable ▼		255.255.255.255 (/32) ▼	
4	Disable ▼		255.255.255.255 (/32) ▼	
5	Disable ▼		255.255.255.255 (/32) ▼	

**Radius Roaming Out:** When “**Radius Roaming Out**” is selected, local users can login from other domains by using their original accounts.

**802.1x Authentication:** 802.1x is a security standard for wired and wireless LANs. It encapsulates EAP (Extensible Authentication Protocol) processes into Ethernet packets instead of using the protocol's native PPP (Point-to-Point Protocol) environment, thus reducing some network overhead. It also puts the bulk of the processing burden upon the client (called a supplicant in 802.1x parlance) and the authentication server (such as a RADIUS), letting the "authenticator" middleman simply pass the packets back and forth.

### 4.2.1.2 Authentication Method – POP3

Choose “**POP3**” in the **Authentication Method** field, the hyperlink beside the pull-down menu will become “**POP3 Setting**”.

Authentication Server - Server 1	
Server Name	<input type="text" value="Server 1"/> <small>*(Its server name)</small>
Server Status	Disabled
Postfix	<input type="text" value="Postfix1"/> <small>*(Its postfix name)</small>
Black List	<input type="text" value="None"/>
Authentication Method	<div> <input type="text" value="POP3"/> </div> <a href="#">POP3 Setting</a>
Policy	<div> Local User  <b>POP3</b>  Radius  LDAP  NTDomain </div>
Enable VPN Termination	

When **POP3**, **Radius**, **LDAP** or **NTDomain** is selected from the drop-down menu, “**Enable VPN Termination**” will show up. Check “**Enable VPN Termination**” to enable this function. Click the hyperlink for further configuration. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red star are necessary information. These settings will become effective immediately after clicking the **Apply** button.

Primary POP3 Server	
Server IP	<input type="text"/> <small>*(Domain Name/IP)</small>
Port	<input type="text"/> <small>*(Default: 110)</small>
SSL Setting	<input type="checkbox"/> Enable SSL Connection
Secondary POP3 Server	
Server IP	<input type="text"/>
Port	<input type="text"/>
SSL Setting	<input type="checkbox"/> Enable SSL Connection

- **Server IP:** Enter the IP address/domain name given by the ISP.
- **Port:** Enter the Port given by the ISP. The default value is 100.
- **Enable SSL Connection:** If this option is enabled, the POP3s protocol will be used to encrypt the

authentication.

#### 4.2.1.3 Authentication Method – Radius

Choose “**Radius**” in the **Authentication Method** field, the hyperlink beside the pull-down menu will become “**Radius Setting**”.

Authentication Server - Server 3	
Server Name	<input type="text" value="Server 3"/> <small>*(Its server name)</small>
Server Status	Enabled
Postfix	<input type="text" value="Postfix3"/> <small>*(Its postfix name)</small>
Black List	<input type="text" value="None"/> ▼
Authentication Method	<input type="text" value="Radius"/> ▼ <a href="#">Radius Setting</a>
Policy	<input type="text" value="Policy 1"/> ▼ <a href="#">Edit Policy Mapping</a>
Enable VPN Termination	<input type="checkbox"/>

When **POP3**, **Radius**, **LDAP** or **NTDomain** is selected from the drop-down menu, “**Enable VPN Termination**” will show up. Check “**Enable VPN Termination**” to enable this function or not. Click the hyperlink for further configuration. The Radius server sets the external authentication for user accounts. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red star are necessary information. These settings will become effective immediately after clicking the **Apply** button.

Radius Setting	
802.1x Authentication	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Trans Full Name	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
NASID	<input type="text"/>
Primary RADIUS Server	
Server IP	<input type="text"/> *
Authentication Port	<input type="text"/> *(Default: 1812)
Accounting Port	<input type="text"/> *(Default: 1813)
Secret Key	<input type="text"/> *
Accounting Service	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Authentication Protocol	PAP <input type="button" value="v"/>
Secondary RADIUS Server	
Server IP	<input type="text"/>
Authentication Port	<input type="text"/>
Accounting Port	<input type="text"/>
Secret Key	<input type="text"/>
Accounting Service	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Authentication Protocol	CHAP <input type="button" value="v"/>

- 802.1X Authentication:** Enable this function and the hyperlink of **Radius Client List** will appear. Click the hyperlink to get into the Radius Client Configuration list for further configuration. In the **Radius Client Configuration** page, the clients, which are using 802.1X as the authentication method, shall be put into this table. PLANET WLS-1280 will forward the authentication request from these clients to the configured Radius Servers.

Radius Client Configuration				
No.	Type	IP Address	Segment	Secret
1	Disable		255.255.255.255 (/32)	
2	Disable		255.255.255.255 (/32)	
3	Disable		255.255.255.255 (/32)	
4	Disable		255.255.255.255 (/32)	
5	Disable		255.255.255.255 (/32)	
6	Disable		255.255.255.255 (/32)	
7	Disable		255.255.255.255 (/32)	
8	Disable		255.255.255.255 (/32)	
9	Disable		255.255.255.255 (/32)	
10	Disable		255.255.255.255 (/32)	

- **Trans Full Name:** When enabled, the ID and postfix will be transferred to the RADIUS server for authentication. When disabled, only the ID will be transferred to RADIUS server for authentication.
- **NASID:** Enter the NASID of PLANET WLS-1280 for the RADIUS server.
- **Server IP:** Enter the IP address/domain name of the RADIUS server.
- **Authentication Port:** Enter the authentication port of the RADIUS server and the default value is 1812.
- **Accounting Port:** Enter the accounting port of the RADIUS server and the default value is 1813.
- **Secret Key:** Enter the key for encryption and decryption.
- **Accounting Service:** Select this to enable or disable the “**Accounting Service**” for accounting capabilities.
- **Authentication Protocol:** There are two methods, CHAP and PAP for selection.
- **Policy Mapping:** Enable or disable policy mapping by RADIUS class attributes.
- 

Policy Mapping - Server 3			
<input checked="" type="radio"/> Enable		<input type="radio"/> Disable	
No.	Class Attribute	Policy	Remark
1		Policy 1	
2		Policy 1	
3		Policy 1	
4		Policy 1	
5		Policy 1	
6		Policy 1	
7		Policy 1	
8		Policy 1	

- **Class Attribute:** Class attribute sent from the RADIUS server.
- **Policy:** Select the mapping policy of this class attribute.
- **Remark:** Add some description if needed.

#### 4.2.1.4 Authentication Method – LDAP

Choose “**LDAP**” in the **Authentication Method** field, the hyperlink beside the pull-down menu will become “**LDAP Setting**”.

Authentication Server - Server 1	
Server Name	Server 1 <small>*(Its server name)</small>
Server Status	Disabled
Postfix	Postfix1 <small>*(Its postfix name)</small>
Black List	None
Authentication Method	LDAP <a href="#">LDAP Setting</a>
Policy	Local User POP3 Radius LDAP NTDomain
Enable VPN Termination	

When **POP3**, **Radius**, **LDAP** or **NTDomain** is selected from the drop-down menu, “**Enable VPN Termination**” will show up. Check “**Enable VPN Termination**” to enable this function or not. Click the hyperlink for further configuration. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red star are necessary information. These settings will become effective immediately after clicking the **Apply** button.

Primary LDAP Server	
Server IP	<input type="text"/> <small>*(Domain Name/IP)</small>
Port	<input type="text"/> <small>*(Default: 389)</small>
Base DN	<input type="text"/> <small>*(CN=,dc=,dc=)</small>
Account Attribute	<input type="text"/> <small>(Default: uid)</small>
Secondary LDAP Server	
Server IP	<input type="text"/>
Port	<input type="text"/>
Base DN	<input type="text"/>
Account Attribute	<input type="text"/>

- **Server IP:** Enter the IP address or domain name of the LDAP server.
- **Port:** Enter the Port of the LDAP server, and the default value is 389.
- **Base DN:** Enter the distinguished name of the LDAP server.
- **Account Attribute:** Enter the account attribute of the LDAP server.

#### 4.2.1.5 Authentication Method – NTDomain

Choose “**NTDomain**” in the **Authentication Method** field, the hyperlink beside the pull-down menu will become “**NTDomain Setting**”.

Authentication Server - Server 1	
Server Name	Server 1 <small>*(its server name)</small>
Server Status	Disabled
Postfix	Postfix1 <small>*(its postfix name)</small>
Black List	None ▼
Authentication Method	NTDomain <a href="#">NT Domain Setting</a>
Policy	<div> Local User  POP3  Radius  LDAP  <b>NTDomain</b> </div>
Enable VPN Termination	

When **POP3**, **Radius**, **LDAP** or **NTDomain**, is selected from the drop-down menu “**Enable VPN Termination**” will show up. Check “**Enable VPN Termination**” to enable this function or not. Click the hyperlink for further configuration. Enter the server IP address and enable/disable the transparent login function. These settings will become effective immediately after clicking the **Apply** button.

Domain Controller	
Server IP address	<input type="text"/> *
Transparent Login	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

- **Server IP address:** Enter the server IP address of the domain controller.
- **Transparent Login:** If the function is enabled, when users log into the Windows domain, they will log into PLANET WLS-1280 automatically

## 4.2.2 Black List Configuration

The administrator can add, delete, or edit the black list for user access control. Each black list can include 40 users at most. If a user in the black list wants to log into the system, the user’s access will be denied. The administrator

can use the pull-down menu to select the desired black list.

Black List Configuration		
Select Black List: 1:Blacklist1 ▼		
Name	Blacklist1	
User	Remark	<input type="button" value="Delete"/>

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#)

[Add User to List](#)

- **Select Black List:** There are 5 lists to select from for the desired black list.
- **Name:** Set the black list name and it will show on the pull-down menu above.
- **Add User to List:** Click the hyperlink to add users to the selected black list.

Add Users to Blacklist Blacklist1		
No	Username	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

After entering the usernames in the “**Username**” blanks and the related information in the “**Remark**” blank (not required).

Add Users to Blacklist Blacklist1		
Item	Username	Remark
1	<input type="text" value="James"/>	<input type="text" value="fraud"/>
2	<input type="text" value="Junior"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Click **Apply** to save the settings.

User 'James' has been added!

User 'Junior' has been added!



**Add Users to Blacklist**

Add Users to Blacklist Blacklist1		
Item	Username	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>

If the administrator wants to remove a user from the black list, just select the user's “**Delete**” check box and then click the **Delete** button to remove that user from the black list.

Black List Configuration		
Select Black List: 1:Blacklist1 ▼		
Name	Blacklist1	
User	Remark	Delete
James	fraud	<input type="checkbox"/>
Junior		<input checked="" type="checkbox"/>

(Total:2) [First](#) [Prev](#) [Next](#) [Last](#)

[Add User to List](#)

### 4.2.3 Policy Configuration

Each policy has three profiles, **Firewall Profile**, **Specific Route Profile**, and **Schedule Profile** as well as **Bandwidth** settings for that policy.

Policy Configuration	
Select Policy:	Policy A ▼
Firewall Profile	<a href="#">Setting</a>
Specific Route Profile	<a href="#">Setting</a>
Schedule Profile	<a href="#">Setting</a>
Total Bandwidth	Unlimited ▼
Individual Maximum Bandwidth	Unlimited ▼
Individual Request Bandwidth	None ▼

- **Firewall Profile**

Click the hyperlink of **Setting** for **Firewall Profile**, the **Firewall Profile** page will appear. Click the numbers of **Filter Rule Item** to edit individual rules and click **Apply** to save the settings. The rule status will show on the list. Check “**Active**” to enable that rule.

**Attention:** Filter Rule Item 1 is the highest priority, Filter Rule Item 2 is the second priority, and so on.

**Profile Name:**

Firewall Profiles						
Filter Rule Item	Active	Action	Name	Source Destination	Protocol	MAC
<a href="#">1</a>	<input type="checkbox"/>	Block		ANY	ALL	
<a href="#">2</a>	<input type="checkbox"/>	Block		ANY	ALL	
<a href="#">3</a>	<input type="checkbox"/>	Block		ANY	ALL	
<a href="#">4</a>	<input type="checkbox"/>	Block		ANY	ALL	
<a href="#">5</a>	<input type="checkbox"/>	Block		ANY	ALL	

Edit Filter Rule					
<b>Rule Item: 1</b>					
<b>Rule Name:</b> <input type="text"/>			<input type="checkbox"/> <b>Enable this Rule</b>		
<b>Action :</b> <input type="text" value="Block"/>			<b>Protocol</b> <input type="text" value="ALL"/>		
<b>Source MAC Address:</b> <input type="text"/>			<b>(For Specific MAC Address Filter)</b>		
	Interface	IP	Subnet Mask	Start Port	End Port
Source	<input type="text" value="ALL"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>
Destination	<input type="text" value="ALL"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>

**Rule Item:** This is the rule selected.

**Rule Name:** The rule name can be changed here. The rule name can be set to easily identify, for example: *“from file server”, “HTTP request”* or *“to web”*, etc.

**Enable this Rule:** After checking this function, the rule will be enabled.

**Action:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.

**Protocol:** There are three protocols to select, **TCP**, **UDP** and **ICMP**, or choose **ALL** to use all three protocols.

**Source MAC Address:** The MAC address of the source IP address. This is for specific MAC address filter.

**Source/Destination Interface:** There are four interfaces to choose, **ALL**, **WAN1**, **WAN2**, **Controlled Port** and **Uncontrolled Port**.

**Source/Destination IP:** Enter the source and destination IP addresses.

**Source/Destination Subnet Mask:** Enter the source and destination subnet masks.

**Source/Destination Start/End Port:** Enter the range of source and destination ports.

- **Specific Route Profile**

Click the hyperlink of **Setting** for **Specific Route Profile**, the **Specific Default Route** and **Specific Route Profile** page will appear.

**Profile Name:**

Specific Default Route			
Enable <input type="checkbox"/>	Default Gateway: <input type="text" value="IP Address"/> <input type="button" value="v"/>		
Specific Route Profile			
Route Item	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> <input type="button" value="v"/>	<input type="text"/>
2	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> <input type="button" value="v"/>	<input type="text"/>
3	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> <input type="button" value="v"/>	<input type="text"/>
4	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> <input type="button" value="v"/>	<input type="text"/>
5	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> <input type="button" value="v"/>	<input type="text"/>
6	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> <input type="button" value="v"/>	<input type="text"/>
7	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> <input type="button" value="v"/>	<input type="text"/>
8	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> <input type="button" value="v"/>	<input type="text"/>
9	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> <input type="button" value="v"/>	<input type="text"/>
10	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> <input type="button" value="v"/>	<input type="text"/>

### Specific Default Route

**Enable:** Click to enable the setting of specific default route.

**Default Gateway:** There are 3 methods of the default gateway that **Specific Default Route** supports. Select **WAN1 Default Gateway** to set WAN1 as the default gateway. Select **WAN2 Default Gateway** to set WAN2 as the default gateway. Select **IP Address** and enter the IP address of the specific router.

### Specific Route Profile

**Profile Name:** The profile name can be changed here.

**Destination IP Address:** The destination IP address of the host or the network.

**Destination Subnet Netmask:** Select a destination subnet netmask of the host or the network.

**Gateway IP Address:** The IP address of the gateway or the router to the destination.

- **Schedule Profile**

Click the hyperlink of **Setting** for **Schedule Profile** to enter the Schedule Profile list. Select “**Enable**” to show the list. This function is used to restrict the time the users can log in. Please enable/disable the desired time slot and click **Apply** to save the settings. These settings will become effective immediately after clicking the **Apply** button.

**Profile Name:** 
☒ Enabled ☐ Disabled

Login Schedule Profile							
HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
00:00~00:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
01:00~01:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
02:00~02:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
03:00~03:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
04:00~04:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
05:00~05:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
06:00~06:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
07:00~07:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
08:00~08:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
09:00~09:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10:00~10:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11:00~11:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12:00~12:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13:00~13:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14:00~14:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15:00~15:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16:00~16:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17:00~17:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18:00~18:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19:00~19:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20:00~20:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21:00~21:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22:00~22:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23:00~23:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- **Total Bandwidth**

Select the bandwidth from the drop-down menu. It's the total bandwidth the users under this particular policy need to share.

- **Individual Maximum Bandwidth**

Select the bandwidth from the drop-down menu. It's the most bandwidth an individual user can obtain under this particular policy, which cannot exceed the value for **Total Bandwidth**.

- **Individual Request Bandwidth**

Select the bandwidth from the drop-down menu. It's the requested bandwidth for an user under this particular policy, which cannot exceed the value for **Individual Maximum Bandwidth**.

## 4.2.4 Additional Configuration

Additional Configuration	
<b>User Control</b>	Idle Timer: <input type="text" value="10"/> minutes <small>*(Range: 1-1440)</small> Multiple Login <input type="checkbox"/> <small>(On-demand and RADIUS authentication do NOT support multiple login.)</small> Friendly Logout <input checked="" type="checkbox"/>
<b>Roaming Out Timer</b>	Session Timeout: <input type="text" value="120"/> <small>*(Range: 5-1440)</small> Idle Timeout: <input type="text" value="10"/> <small>*(Range: 1-120)</small> Interim Update: <input type="text" value="5"/> <small>*(Range: 1-120)</small>
<b>Upload File</b>	<a href="#">Certificate</a> <a href="#">Login Page</a> <a href="#">Logout Page</a> <a href="#">Login Success Page</a> <a href="#">Login Success Page for On-Demand</a> <a href="#">Logout Success Page</a>
<b>Credit Reminder</b>	Volume <input type="radio"/> Enable <input checked="" type="radio"/> Disable Time <input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>POP3 Message</b>	<a href="#">Edit Mail Message</a>
<b>Enhance User Authentication</b>	<a href="#">Permit MAC Address List</a>

- **User Control:** Functions under this section applies for all general users.

**Idle Timer:** If a user has been idled with no network activities, the system will automatically kick out the user. The logout timer can be set in the range of 1~1440 minutes, and the default logout time is 10 minutes.

**Multiple Login:** When enabled, the same account can be logged in by different clients at the same time. (This function doesn't support On-demand users and RADIUS server)

**Friendly Logout:** When a user logs into the network, a small window will appear to show the user's information and there is a logout button for the logout. If enabled. When the users try to close the small window, there will be

a new popup window to confirm the logout in case the users click the logout button by accident.

- **Roaming Out Timer**

**Session Timeout:** The time that the user can access the network while roaming. When the time is up, the user will be kicked out automatically.

**Idle Timeout:** If a user has been idled with no network activities, the system will automatically kick out the user.

**Interim Update:** The system will update the users' current status and usage according to this time periodically.

- **Upload File**

1. **Certificate:** The administrator can upload new private key and customer certification. Click the **Browse** button to select the file for the certificate upload. Then click **Submit** to complete the upload process.

The screenshot shows two stacked form sections. The top section is titled 'Upload Private Key' and contains a 'File Name' label, an empty text input field, and a '浏览...' (Browse...) button. The bottom section is titled 'Upload Customer Certificate' and also contains a 'File Name' label, an empty text input field, and a '浏览...' (Browse...) button. Below these two sections is a single button labeled 'Use Default Certificate'.

Click **Use Default Certificate** to use the default certificate and key.

**You just overwrote the setting with default KEY & default CA file**

2. **Login Page:** The administrator can use the default login page or get the customized login page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, you can click **Preview** to see the login page.

a. Choose **Default Page** to use the default login page.

The screenshot shows two stacked form sections. The top section is titled 'Login Page Selection for Users' and contains four radio button options: 'Default Page' (selected), 'Template Page', 'Uploaded Page', and 'External Page'. The bottom section is titled 'Default Page Setting' and contains the text: 'This is default login page for users. You could click preview link to preview the default login page. Thanks.' Below this text is a 'Preview' link.

- b. Choose **Template Page** to make a customized login page here. Click **Select** to pick up a color and then fill in all of the blanks. Click **Preview** to see the result first.

Login Page Selection for Users	
<input type="radio"/> Default Page	<input checked="" type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Template Page Setting	
Color for Title Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Title	<input type="text" value="User Login Page"/>
Welcome	<input type="text" value="Welcome To User Login Page"/>
Information	<input type="text" value="Please Enter Your Name and Password to Sign In"/>
Username	<input type="text" value="Username"/>
Password	<input type="text" value="Password"/>
Submit	<input type="text" value="Submit"/>
Clear	<input type="text" value="Clear"/>
Remaining	<input type="text" value="Remaining"/>
Copyright	<input type="text" value="Copyright (c)"/>
<input type="button" value="Preview"/>	

- c. Choose **Uploaded Page** and upload a login page. Click the **Browse** button to select the file to upload. Then click **Submit** to complete the upload process.

Login Page Selection for Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input checked="" type="radio"/> Uploaded Page	<input type="radio"/> External Page

Uploaded Page Setting	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

Existing Image Files:

**Total Capacity:** 512 K  
**Now Used:** 0 K

Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
<a href="#">Preview</a>	

After the upload process is completed, the new login page can be previewed by clicking **Preview** button at the bottom.



The image shows a preview of a user login page. It has a blue header with the text "User Login Page". Below the header, it says "Welcome To User Login Page!" and "Please Enter Your User Name and Password To Sign In.". There are two input fields: "User Name:" and "Password:". Below the input fields, there are three buttons: "Submit", "Clear", and "Remaining".

The user-defined login page must include the following HTML codes to provide the necessary fields for username and password.

```

<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>

```

If the user-defined login page includes an image file, the image file path in the HTML code must be the image file you will upload.

```

```

Then, enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click **Submit**. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login page, click the **Use Default Page** button to restore it to default.

<b>Total Capacity:</b> 512 K <b>Now Used:</b> 0 K	
Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click **Delete** to delete the file.

<b>Existing Image Files :</b> 1102474548_732cn.gif <input type="checkbox"/>
<input type="button" value="Delete"/>

In PLANET WLS-1280, the end user first gets a login page when she/he opens its web browser right after associating with an access point. However, in some situations, the hotspot owners or MIS staff may want to display "terms of use" or announcement information before the login page. Hotspot owners or MIS staff can design a new disclaimer/announcement page and save the page in their local server. After the agreement shown on the page is read, users are asked whether they agree or disagree with the disclaimer. By clicking I agree, users are able to log in. If users choose to decline, they will get a popup window saying they are unable to log in. The basic design is to have the disclaimer and login function in the same page but with the login function hidden until users agree with the disclaimer.

**For more details about the codes of the disclaimer, please refer to Appendix F.**

If the page is successfully loaded, an **upload success** page will show up.

Successful!

You just uploaded page:[default\\_login\\_with\\_disclaimer.html](#)

[Preview](#)

“Preview” can be clicked to see the uploaded page.



The image shows a web form titled "Service Disclaimer". It contains two paragraphs of text. The first paragraph states that personal information (e-mail address, physical contact information, credit card numbers, and transactional information) may be collected and stored based on internet service activities. The second paragraph states that if the information cannot be verified, additional information (driver license, credit card statement, utility bill, etc.) or answers to questions may be requested. Below the text are two radio buttons: "I agree." and "I disagree.". At the bottom is a "Next" button.

Service Disclaimer

We may collect and store the following personal information:  
e-mail address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)

☐ I agree.  
☐ I disagree.

Next

If user checks “I agree” and clicks **Next**, then he/she is prompted to fill in the login name and password.



The image shows a web form titled "User Login Page". It has a welcome message and a prompt to enter user name and password. There are two input fields: "User Name:" and "Password:". Below the fields are three buttons: "Submit", "Clear", and "Remaining".

User Login Page

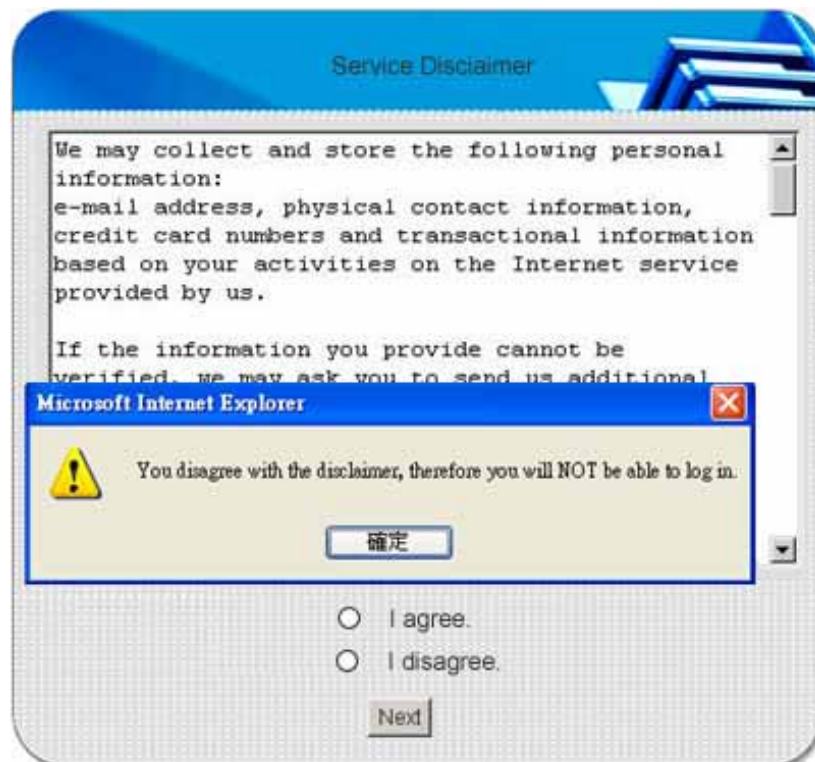
Welcome To User Login Page!  
Please Enter Your User Name and Password To Sign In.

User Name:

Password:

Submit Clear Remaining

If user checks “I disagree” and clicks **Next**, a window will pop up to tell user that he/she cannot log in



- d. Choose the **External Page** selection and get the login page from the specific website. Enter the website address in the “**External Page Setting**” field and then click **Apply**.

Login Page Selection for Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input checked="" type="radio"/> External Page

External Page Setting	
External URL :	<input type="text" value="http://"/>
<input type="button" value="Preview"/>	

After applying the setting, the new login page can be previewed by clicking **Preview** button at the bottom of this page.



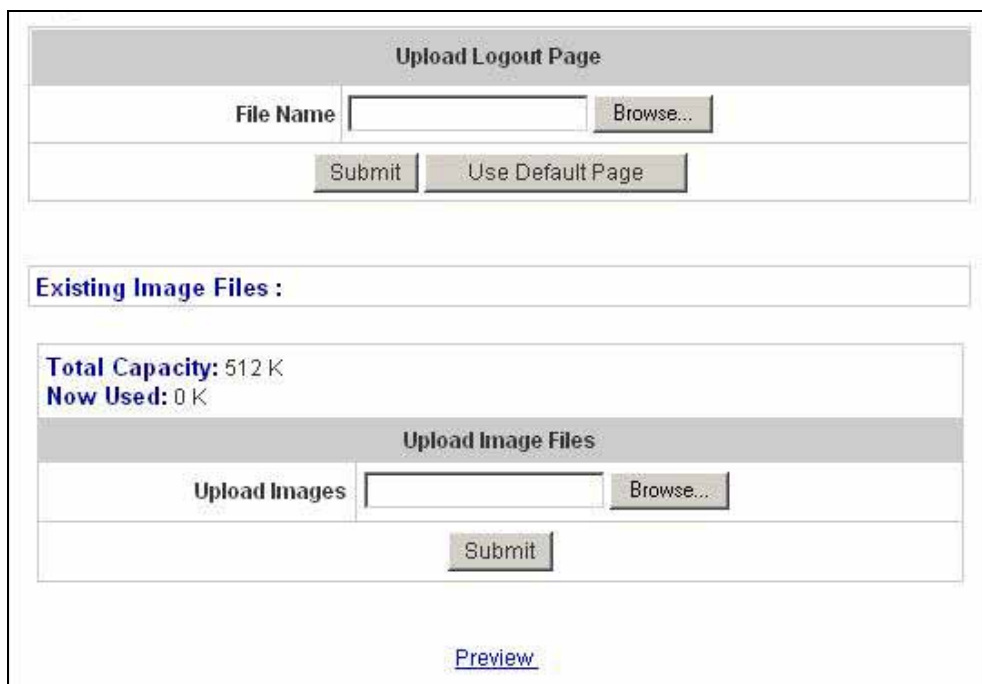
**User Login Page**

Welcome To User Login Page!  
Please Enter Your User Name and Password To Sign In.

User Name:

Password:

3. **Logout Page:** The users can apply their own logout page here. The process is similar to that of Logout Page.



**Upload Logout Page**

File Name

**Existing Image Files :**

**Total Capacity:** 512 K  
**Now Used:** 0 K

**Upload Image Files**

Upload Images

[Preview](#)

The different part is the HTML code of the user-defined logout interface must include the following HTML code that the user can enter the username and password. After the upload is completed, the user-defined login user interface can be previewed by clicking **Preview** at the bottom of this page. If want to restore the factory default setting of the logout interface, click the **"Use Default Page"** button.

```
<form action="userlogout.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Logout">
<input type="reset" name="clear" value="Clear">
</form>
```

4. **Login Success Page:** The administrator can use the default login success page or get the customized login success page by setting the template page, uploading the page or using the external website. After finishing the setting, you can click **Preview** to see the login success page.
- a. Choose **Default Page** to use the default login success page.

Login Success Page Selection for Users	
<input checked="" type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Default Page Setting
<p><b>This is default login success page for users.</b></p> <p><b>You could click preview link to preview the default login success page.</b></p> <p><b>Thanks.</b></p> <p><a href="#">Preview</a></p>

- b. Choose **Template Page** to make a customized login success page here. Click **Select** to pick up a color and then fill in all of the blanks. You can click **Preview** to see the result first.

Login Success Page Selection for Users	
<input type="radio"/> Default Page	<input checked="" type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Template Page Setting	
Color for Title Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Title	<input type="text" value="Login Succeed Page"/>
Welcome	<input type="text" value="Hello"/>
Information	<input type="text" value="Please click this button to"/>
Logout	<input type="text" value="Logout"/>
Information2	<input type="text" value="Thank you"/>
Login Time	<input type="text" value="Login Time"/>
<input type="button" value="Preview"/>	

- c. Choose **Uploaded Page** and you can get the login success page by uploading. Click the **Browse** button to select the file for the login success page upload. Then click **Submit** to complete the upload process.

Login Success Page Selection for Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input checked="" type="radio"/> Uploaded Page	<input type="radio"/> External Page

Uploaded Page Setting	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

Existing Image Files:

**Total Capacity:** 512 K  
**Now Used:** 0 K

Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
<a href="#">Preview</a>	

After the upload process is completed, the new login success page can be previewed by clicking **Preview** button at the bottom.

If the user-defined login success page includes an image file, the image file path in the HTML code must be the image file you will upload.

****

Then, enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click **Submit**. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login success page, click the **Use Default Page** button to restore it to default.

<b>Total Capacity:</b> 512 K <b>Now Used:</b> 0 K	
Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

After the image file is uploaded, the file name will show on the “**Existing Image Files**” field. Check the file and click **Delete** to delete the file.

<b>Existing Image Files :</b>	
1102474548_732cn.gif <input type="checkbox"/>	<input type="button" value="Delete"/>

- d. Choose the **External Page** selection and you can get the login success page e from the specific website. Enter the website address in the “**External Page Setting**” field and then click **Apply**. After applying the setting, the new login success page can be previewed by clicking **Preview** button at the bottom of this page.

Login Success Page Selection for Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input checked="" type="radio"/> External Page

External Page Setting	
External URL :	<input type="text" value="http://"/>
<input type="button" value="Preview"/>	

5. **Login Success Page for On-Demand:** The administrator can use the default login success page for On-Demand or get the customized login success page for On-Demand by setting the template page, uploading the page or using the external website. After finishing the setting, you can click **Preview** to see the login success page for On-Demand.
- a. Choose **Default Page** to use the default login success page for On-Demand.

Login Success Page Selection for on-demand Users	
<input checked="" type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Default Page Setting	
<p><b>This is default login success page for on-demand users.</b> <b>You could click preview link to preview the default login success page.</b> <b>Thanks.</b></p>	
<p><a href="#">Preview</a></p>	

- b. Choose **Template Page** to make a customized login success page for On-Demand here. Click **Select** to pick up a color and then fill in all of the blanks. You can click **Preview** to see the result first.

Login Success Page Selection for on-demand Users	
<input type="radio"/> Default Page	<input checked="" type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Template Page Setting	
Color for Title Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Title	<input type="text" value="Login Succeed Page for on-demand"/>
Welcome	<input type="text" value="Welcome"/>
Information	<input type="text" value="Please click this button to"/>
Logout	<input type="text" value="Logout"/>
Information2	<input type="text" value="Thank you"/>
Remaining Usage	<input type="text" value="Remaining Usage"/>
Day	<input type="text" value="Day"/>
Hour	<input type="text" value="Hour"/>
Min	<input type="text" value="Min"/>
Sec	<input type="text" value="Sec"/>
Login Time	<input type="text" value="Login Time"/>
Redeem	<input type="text" value="Redeem"/>
<input type="button" value="Preview"/>	

- c. Choose **Uploaded Page** and you can get the **Login Success Page Section for On-Demand Users**. Click the **Browse** button to select the file for the login success page for On-Demand. Then click **Submit** to complete the upload process.

Login Success Page Selection for on-demand Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input checked="" type="radio"/> Uploaded Page	<input type="radio"/> External Page

Upload Login Success Page for on-demand	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

Existing Image Files:

**Total Capacity:** 512 K  
**Now Used:** 0 K

Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
<a href="#">Preview</a>	

After the upload process is completed, the new login success page for On-Demand can be previewed by clicking **Preview** button at the bottom.

If the user-defined login success page for On-Demand includes an image file, the image file path in the HTML code must be the image file you will upload.

****

Then, enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click **Submit**. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login success page for On-Demand, click the **Use Default Page** button to restore it to default.

<b>Total Capacity:</b> 512 K <b>Now Used:</b> 0 K	
Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file

and click **Delete** to delete the file.

<b>Existing Image Files :</b>	
1102474548_732cn.gif <input type="checkbox"/>	<input type="button" value="Delete"/>

- d. Choose the **External Page** selection and you can get the login success page for On-Demand from the specific website. Enter the website address in the “**External Page Setting**” field and then click **Apply**. After applying the setting, the new login success page for On-Demand can be previewed by clicking **Preview** button at the bottom of this page.

Login Success Page Selection for Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input checked="" type="radio"/> External Page

External Page Setting	
External URL :	<input type="text" value="http://"/>
<input type="button" value="Preview"/>	

6. **Logout Success Page:** The administrator can use the default logout success page or get the customized logout success page by setting the template page, uploading the page or using the external website. After finishing the setting, you can click **Preview** to see the logout success page.

- a. Choose **Default Page** to use the default logout success page.

Logout Success Page Selection for Users	
<input checked="" type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Default Page Setting	
This is default logout success page for users. You could click preview link to preview the default logout success page. Thanks.	
<a href="#">Preview</a>	

- b. Choose **Template Page** to make a customized logout success page here. Click **Select** to pick up a color and then fill in all of the blanks. You can click **Preview** to see the result first.

Logout Success Page Selection for Users	
<input type="radio"/> Default Page	<input checked="" type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Template Page Setting	
Color for Title Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Title	<input type="text" value="Logout Succeed Page"/>
Information	<input type="text" value="Logout successfully"/>
<input type="button" value="Preview"/>	

- c. Choose **Uploaded Page** and you can get the logout success page by uploading. Click the **Browse** button to select the file for the logout success page upload. Then click **Submit** to complete the upload process.

Logout Success Page Selection for Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input checked="" type="radio"/> Uploaded Page	<input type="radio"/> External Page

Upload Logout Success Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

Existing Image Files:

<b>Total Capacity:</b> 512 K <b>Now Used:</b> 0 K	
Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
<a href="#">Preview</a>	

After the upload process is completed, the new logout success page can be previewed by clicking **Preview** button at the bottom.

If the user-defined logout success page includes an image file, the image file path in the HTML code must be the image file you will upload.

****

Then, enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click **Submit**. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login success page, click the **Use Default Page** button to restore it to default.

<b>Total Capacity:</b> 512 K <b>Now Used:</b> 0 K	
Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

After the image file is uploaded, the file name will show on the “**Existing Image Files**” field. Check the file and click **Delete** to delete the file.

<b>Existing Image Files :</b> 1102474548_732cn.gif <input type="checkbox"/>
<input type="button" value="Delete"/>

- d. Choose the **External Page** selection and you can get the logout success page from the specific website. Enter the website address in the “**External Page Setting**” field and then click **Apply**. After applying the setting, the new logout success page can be previewed by clicking **Preview** button at the bottom of this page.

Logout Success Page Selection for Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input checked="" type="radio"/> External Page

External Page Setting	
External URL :	<input type="text" value="http://"/>
<input type="button" value="Preview"/>	

- **Credit Reminder:** The administrator can enable this function to remind the on-demand users before their credit run out. There are two kinds of reminder, **Volume** and **Time**. The default reminding trigger level for **Volume** is 1Mbyte and the level for **Time** is 5 minutes.

Credit Reminder	Volume	<input checked="" type="radio"/> Enabled <input type="radio"/> Disable
	<input type="text" value="1"/> Mbyte	*(Range: 1-10; Default: 1)
	Time	<input checked="" type="radio"/> Enabled <input type="radio"/> Disable
	<input type="text" value="5"/> minutes	*(Range: 1-30; Default: 5)

- **POP3 Message:** If a user tries to retrieve mail from POP3 mail server before login, the users will receive a welcome mail from PLANET WLS-1280. The administrator can edit the content of this welcome mail.

Edit Mail Message	
Text	<pre>&lt;!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"&gt; &lt;HTML&gt;&lt;HEAD&gt; &lt;META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=us-ascii"&gt; &lt;/HEAD&gt; &lt;BODY&gt; &lt;DIV&gt; &lt;DIV&gt; &lt;FONT face="Times New Roman" size=6&gt; &lt;STRONG&gt;Welcome!&lt;/STRONG&gt; &lt;/FONT&gt; &lt;/DIV&gt; &lt;DIV&gt; &lt;FONT size=4&gt;&lt;STRONG&gt;&lt;/STRONG&gt; &lt;/FONT&gt;</pre>

- **Enhance User Authentication:** With this function enabled, only the users with their MAC addresses in this list can log into PLANET WLS-1280. There will only be 40 users allowed in this MAC address list. User authentication is still required for these users. Please click the **Permit MAC Address List** to fill in these MAC addresses, select **Enable**, and then click **Apply**.

MAC Address Control			
<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled			
Item	MAC Address	Item	MAC Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

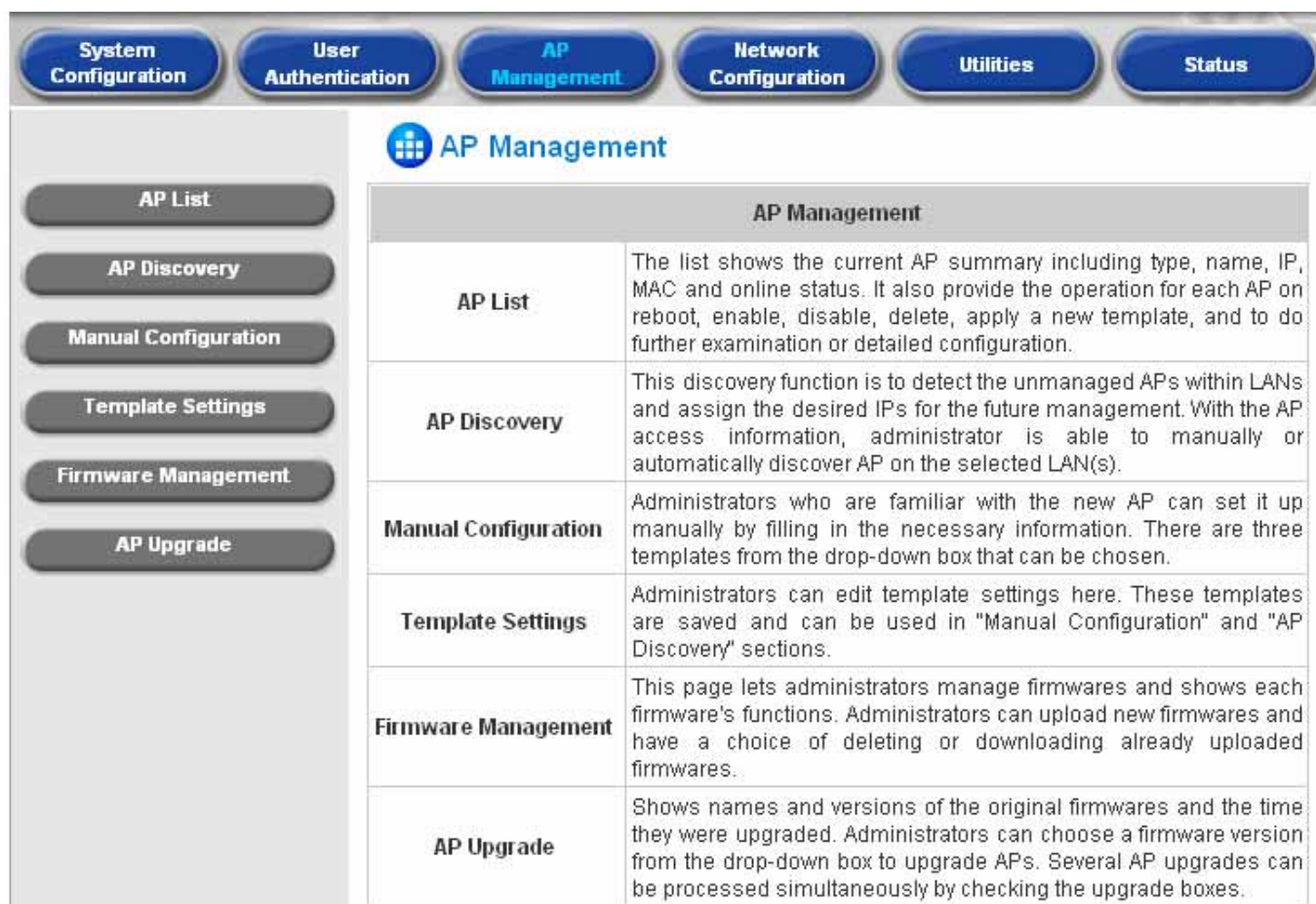
(Total:40) [First](#) [Prev](#) [Next](#) [Last](#)



**Caution:** The format of the MAC address is: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

## 4.3 AP Management

This section includes the following functions: **AP List**, **AP Discovery**, **Manual Configuration**, **Template Settings**, **Firmware Management** and **AP Upgrade**.



The screenshot shows the 'AP Management' section of a web interface. At the top, there are navigation tabs: System Configuration, User Authentication, **AP Management**, Network Configuration, Utilities, and Status. On the left, a sidebar contains buttons for AP List, AP Discovery, Manual Configuration, Template Settings, Firmware Management, and AP Upgrade. The main content area is titled 'AP Management' and contains a table with the following functions:

AP Management	
<b>AP List</b>	The list shows the current AP summary including type, name, IP, MAC and online status. It also provide the operation for each AP on reboot, enable, disable, delete, apply a new template, and to do further examination or detailed configuration.
<b>AP Discovery</b>	This discovery function is to detect the unmanaged APs within LANs and assign the desired IPs for the future management. With the AP access information, administrator is able to manually or automatically discover AP on the selected LAN(s).
<b>Manual Configuration</b>	Administrators who are familiar with the new AP can set it up manually by filling in the necessary information. There are three templates from the drop-down box that can be chosen.
<b>Template Settings</b>	Administrators can edit template settings here. These templates are saved and can be used in "Manual Configuration" and "AP Discovery" sections.
<b>Firmware Management</b>	This page lets administrators manage firmwares and shows each firmware's functions. Administrators can upload new firmwares and have a choice of deleting or downloading already uploaded firmwares.
<b>AP Upgrade</b>	Shows names and versions of the original firmwares and the time they were upgraded. Administrators can choose a firmware version from the drop-down box to upgrade APs. Several AP upgrades can be processed simultaneously by checking the upgrade boxes.

### 4.3.1 AP List

All of the APs under the management of PLANET WLS-1280 will be shown in the list. At first the list is empty; administrators can add APs from AP Discovery page (see **4.3.2. AP Discovery** for details) or Manual Configuration page (see **4.3.3. Manual Configuration** for details)

AP List				
<input type="checkbox"/>	AP Type	AP Name	IP	Status
			MAC	
<div>RebootEnableDisableDeleteApply Template</div> <div>(Total: 0) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a></div>				

After adding 2 APs:

AP List				
<input type="checkbox"/>	AP Type	AP Name	IP	Status
			MAC	
<input type="checkbox"/>	WAP-4060PE	<a href="#">NEWDEV-00003</a>	192.168.1.13	<a href="#">Offline</a>
			00:30:4F:42:B0:0C	
<input type="checkbox"/>	WAP-4033	<a href="#">NEWDEV-00004</a>	192.168.1.5	<a href="#">Online (Enabled)</a>
			00:30:4F:4C:DA:FF	
<div>RebootEnableDisableDeleteApply Template</div>				
(Total: 2) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a>				

- **Status**

After clicking the hyperlink of Status, the basic information of the AP including **AP Name**, **AP Type**, **LAN MAC**, **Wireless LAN MAC**, **Up Time**, **Report Time**, **SSID**, **Number of Associated Clients** and **Remark**. In the bottom of this page, there are other hyperlinks for further related information: **System Status**, **LAN Status**, **Wireless LAN Status**, **Access Control Status**, and **Associated Client Status**.

AP Status Summary	
AP Name	NEWDEV-00004
AP Type	WAP-4033
LAN MAC	00:30:4f:4c:da:ff
Wireless LAN MAC	00:30:4f:4c:da:ff
Up Time	0day:0h:12m:22s
Report Time	2006-09-29 11:52:45
SSID	default
Number of Associated Clients	0
Remark	

AP Status Detail
<a href="#">System Status</a>
<a href="#">LAN Status</a>
<a href="#">Wireless LAN Status</a>
<a href="#">Access Control Status</a>
<a href="#">Associated Client Status</a>

- **System Status:** The table shows the information about **AP Name**, **AP Status** and **Last Reporting Time**.

System Information	
AP Name	NEWDEV-00004
AP Status	Online
Last Reporting Time	2006-09-29 11:54:46

- **LAN Status:** The table shows the information about **IP Address**, **Subnet Mask** and **Gateway**.

LAN Interface	
IP Address	192.168.1.5
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

- **Wireless LAN Status:** The table shows all of the related wireless information.

Wireless Interface	
Up Time	0day:0h:20m:29s
SSID	default
Beacon Interval (ms)	100
RTS Threshold	2347
Channel	11
Transmission Rate	Auto
Preamble Type	Long Preamble
IAPP	Enabled
Security	Disable

- **Access Control Status:** The table shows the status of MAC under the control of the AP, which may appear to be “Disabled” or “Enabled” according to the settings.

Access Control	
Status	Disabled

Access Control	
Status	Enabled

Control List	
00:30:4F:28:BF:D8	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00

- **Associated Client Status:** The table shows the clients connected to the AP and the related information of the client.

Client List							
No.	MAC	User ID	TX Packet(s)	RX Packet(s)	Rate	Power Saving	Expiration countdown

- **AP Name**

Click **AP Name** and configure the settings of the AP.

General Settings		
<a href="#">Setting</a>	<b>Name</b>	NEWDEV-00004
	<b>Remark</b>	None
	<b>Firmware</b>	1.24

LAN Interface Setting		
<a href="#">LAN</a>	<b>IP</b>	192.168.1.5
	<b>Mode</b>	Static IP

Wireless Interface Setting		
<a href="#">Wireless LAN</a>	<b>SSID</b>	default
	<b>Channel</b>	11
	<b>Security Type</b>	Disabled

Access Control Setting		
<a href="#">Access Control</a>	<b>Status</b>	Disabled
	<b>Mode</b>	Allowed
	<b>Number of MAC Addresses</b>	0

Please note that since there are 2 types of APs that can associate with PLANET WLS-1280—WAP-4033 and WAP-4060—the interfaces for these 2 types of APs are different due to their functionalities.

When the **Setting** hyperlink is clicked:

**For WAP-4033:**

Administrators can input name of the AP, password, and remark.

General Settings	
<b>Name</b>	<input type="text" value="NEWDEV-00004"/>
<b>Admin Password</b>	<input type="text" value="admin"/>
<b>Remark</b>	<input type="text"/>
<b>Firmware</b>	1.24

**For WAP-4060:**

Administrator must specify a country or domain from the drop-down menu. Also the description field can be filled in

for later reference. Syslog can be disabled or enabled, and a minimum severity level can be selected to note on the Syslog report. Check to enable Rogue AP Detection or leave it as a blank to disable it.

General Settings	
<b>Name</b>	NEWDEV-00003 *
<b>Admin Password</b>	password *
<b>Country or Domain</b>	Taiwan *
<b>Description</b>	
<b>Syslog</b>	Disabled Minimum Severity Level: Error
<b>Rogue AP Detection</b>	<input type="checkbox"/> Enable Rogue AP Detection
<b>Firmware</b>	Version 2.3 Release 04
<b>Remark</b>	

When the **LAN** hyperlink is clicked:

**For WAP-4033:**

Enter the IP address, subnet mask, default gateway for LAN.

LAN Settings	
<b>IP Address</b>	192.168.1.5 *
<b>Subnet Mask</b>	255.255.255.0 *
<b>Default Gateway</b>	192.168.1.254 *

**For WAP-4060:**

Enter all the information including a DNS server IP address.

LAN Settings	
<b>IP Address</b>	192.168.1.13 *
<b>Subnet Mask</b>	255.255.255.0 *
<b>Default Gateway</b>	192.168.1.254 *
<b>DNS</b>	192.203.230.10 *

When the **Wireless LAN** hyperlink is clicked:

**For WAP-4033:**

## Properties

- **SSID:** The SSID is the unique name shared among all devices in a wireless network. The SSID must be the same for all devices in the wireless network. It is case sensitive and has a maximum length of 32 bytes.
- **SSID Broadcast:** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from being seen on networked.
- **Channel:** Select the appropriate channel from the list to correspond with the network settings; for example, 1 to 11 channels are suitable for the North America area.
- **Transmission Mode:** There are 3 modes to select, **802.11b** (2.4G, 1~11Mbps), **802.11g** (2.4G, 54Mbps) and **Mix mode** (b and g).
- **Transmission Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **CTS Protection:** The default value is **Disable**. When select "**Enable**", a protection mechanism will decrease collision probability when many 802.11g devices exist simultaneously. However, performance of your 802.11g devices may decrease.
- **Fragment Threshold:** Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.
- **RTS Threshold:** Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the access point and the wireless network.
- **Preamble Type:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select either Short Preamble or Long Preamble.
- **IAPP:** Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during handoff period.
- **Block Relay:** Select whether to enable this function.
- **Tx Power Level:** Choose which Tx power level desired from the drop-down menu.

## Security:

- **Security Type:** Choose one security type from the drop-down menu.
- **WEP:** Choose WEP authentication type here.

Wireless		
Properties	SSID	default
	SSID Broadcast	Enable <input type="button" value="v"/>
	Channel	11 <input type="button" value="v"/>
	Transmission Mode	Mixed <input type="button" value="v"/>
	Transmission Rate	Auto <input type="button" value="v"/> (Default: Auto; Range: from 1 to 54 Mbps)
	CTS Protection	Disable <input type="button" value="v"/> (Default: Disable)
	Fragment Threshold	2346 (Default: 2346; Range: from 256 to 2346)
	RTS Threshold	2347 (Default: 2347; Range: from 0 to 2347)
	Beacon Interval (ms)	100 (Default: 100; Range: from 20 to 1024 msec)
	Preamble Type	Long <input type="button" value="v"/> (Default: Long)
	IAPP	Enable <input type="button" value="v"/> (Default: Enable)
	Block Relay	Disable <input type="button" value="v"/>
	Tx Power Level	100% <input type="button" value="v"/>
Security	Security Type	Disable <input type="button" value="v"/> <input type="checkbox"/> 802.1x Authentication
	WEP	Authentication Type Both <input type="button" value="v"/>

#### For WAP-4060:

##### Properties

- **SSID Broadcast:** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from being seen on networked.
- **SSID Isolation:** Choose to isolate SSID or not.
- **Channel:** Select the appropriate channel from the list to correspond with your network settings; for example, 1 to 11 channels are suitable for the North America area.
- **Wireless Mode:** Choose a suitable wireless mode from the drop-down menu.
- **Transmission Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speed or you can keep the default setting, **Auto**, to make the Access Point

automatically use the fastest rate possible.

#### Parameters

- **Disassociated Timeout:** The AP will be disassociated after idling for the minutes specified.
- **Fragment Threshold:** Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.
- **CTS/RTS Threshold:** Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the access point and the wireless network.
- **Preamble Type:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select either Short Preamble or Long Preamble.
- **Tx Power Level:** Choose which Tx power level desired from the drop-down menu.

#### 802.11b

- **Protection Type:** Select a protection type from the drop-down menu.
- **Short Slot Time:** Choose to enable or disable.
- **Protection Mode:** Select a protection mode from the drop-down menu.
- **Protection Rate:** Choose a suitable protection rate.

#### Options:

- **Wireless Separation:** Choose to enable or disable.
- **Worldwide Mode (802.11d):** Choose to enable or disable.
- **XR(eXtended Range):** Choose to enable or disable.
- **WMM Support (Wi-Fi Multimedia):** Choose to enable or disable.

**Profile Configuration:** Click “**Configure**” to set each individual profile.

Wireless		
Properties	SSID Broadcast	Enable <input type="button" value="v"/>
	SSID Isolation	None <input type="button" value="v"/>
	Channel	Auto <input type="button" value="v"/>
	Wireless Mode	802.11b and 802.11g <input type="button" value="v"/>
	Transmission Rate	802.11b (1, 2, 5.5, 11 Mbps) <input type="button" value="v"/>
Parameters	Disassociated Timeout	5 <input type="text"/> Minutes <small>(Default: 5; Range: from 1 to 99)</small>
	Fragment Threshold	2346 <input type="text"/> <small>(Default: 2346; Range: from 256 to 2346)</small>
	CTS/RTS Threshold	2346 <input type="text"/> <small>(Default: 2346; Range: from 256 to 2346)</small>
	Beacon Interval (ms)	100 <input type="text"/> <small>(Default: 100; Range: from 20 to 1000 msec)</small>
	Preamble Type	Short <input type="button" value="v"/>
	Tx Power Level	Full <input type="button" value="v"/>
802.11b	Protection Type	CTS-only <input type="button" value="v"/>
	Short Slot Time	Enabled <input type="button" value="v"/>
	Protection Mode	Auto <input type="button" value="v"/>
	Protection Rate	11 Mbps <input type="button" value="v"/>

Options	Wireless Separation	Disabled <input type="button" value="v"/>
	Worldwide Mode (802.11d)	Disabled <input type="button" value="v"/>
	XR (eXtended Range)	Disabled <input type="button" value="v"/>
	WMM Support (Wi-Fi Multimedia)	Disabled <input type="button" value="v"/> <input type="checkbox"/> No Acknowledgement

Profile Configuration						
No.	Profile Name	SSID	Security Type	Mode	Primary	Config Profile
1	wireless	default	None	Enable <input type="button" value="v"/>	<input checked="" type="radio"/>	<input type="button" value="Config"/>
2		default	None	Disable <input type="button" value="v"/>	<input type="radio"/>	<input type="button" value="Config"/>
3		default	None	Disable <input type="button" value="v"/>	<input type="radio"/>	<input type="button" value="Config"/>
4		default	None	Disable <input type="button" value="v"/>	<input type="radio"/>	<input type="button" value="Config"/>
5		default	None	Disable <input type="button" value="v"/>	<input type="radio"/>	<input type="button" value="Config"/>
6		default	None	Disable <input type="button" value="v"/>	<input type="radio"/>	<input type="button" value="Config"/>
7		default	None	Disable <input type="button" value="v"/>	<input type="radio"/>	<input type="button" value="Config"/>
8		default	None	Disable <input type="button" value="v"/>	<input type="radio"/>	<input type="button" value="Config"/>

When **Access Control** hyperlink is clicked:

**Access Control:** In this function, when the status is “**Enabled**”, only the APs which MAC addresses are listed in the list can be allowed to connect PLANET WLS-1280. When “**Disabled**” is selected, all APs can connect PLANET WLS-1280.

**For WAP-4033:**

Access Control			
Status		Disabled ▼	

MAC Address List			
1	<input type="text" value="00:00:00:00:00:00"/>	2	<input type="text" value="00:00:00:00:00:00"/>
3	<input type="text" value="00:00:00:00:00:00"/>	4	<input type="text" value="00:00:00:00:00:00"/>
5	<input type="text" value="00:00:00:00:00:00"/>	6	<input type="text" value="00:00:00:00:00:00"/>
7	<input type="text" value="00:00:00:00:00:00"/>	8	<input type="text" value="00:00:00:00:00:00"/>
9	<input type="text" value="00:00:00:00:00:00"/>	10	<input type="text" value="00:00:00:00:00:00"/>
11	<input type="text" value="00:00:00:00:00:00"/>	12	<input type="text" value="00:00:00:00:00:00"/>
13	<input type="text" value="00:00:00:00:00:00"/>	14	<input type="text" value="00:00:00:00:00:00"/>
15	<input type="text" value="00:00:00:00:00:00"/>	16	<input type="text" value="00:00:00:00:00:00"/>
17	<input type="text" value="00:00:00:00:00:00"/>	18	<input type="text" value="00:00:00:00:00:00"/>
19	<input type="text" value="00:00:00:00:00:00"/>	20	<input type="text" value="00:00:00:00:00:00"/>

**For WAP-4060:**

The interface for WAP-4060 is generally the same as for WAP-4033, but with total of 128 sets of MAC Address that can be filled in.

## 4.3.2 AP Discovery

Use this function to find out all the APs in the network segments.

AP Discovery						
Interface	Uncontrolled <input type="checkbox"/>		Base IP	192.168.2.1	Pool Size	12
	Controlled <input type="checkbox"/>		Base IP	192.168.1.1	Pool Size	12
AP Access	AP Type		WAP-4033		<div>Discover</div>	
	IP Address Range	Start IP	192.168.0.1			
		End IP	192.168.0.1			
	ID		admin			
	Password		admin			
Auto-Discovery	Status	Disabled			<div>Configure</div>	

Discovered AP List					
AP Type	IP Address	Name	Password	Template	<div>Add</div>
	MAC Address				
<p>(Total: 0) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a></p> <p>Last discovery was done at <b>2006 September 29, 11:39:48</b>.</p>					

- **Interface:** Check the Controlled LAN or/and the Uncontrolled LAN and the IP address and Pool Size (the discovered APs will be configured to use IP address in this IP pool).
- **AP Access:** Input the **IP Address**, **ID** and **Password** of the AP.

Then click the **Discover** button and the devices match the given settings will show in the list below. For the desired device, input the desired Name and IP address, select one template, check it and then click **Add** to add it under the managed list. (About the template, please see 4.3.4 Template).

If the any IP address within the assigned **Base IP** and the **Pool Size** has been used, the used IP address will be listed and a warning message will show up. Please change the settings of Base IP or Pool Size.

### 4.3.3 Manual Configuration

The device also can be added manually. Choose which type of AP to configure, input the related data of the AP, and select a Template. Then click **ADD**, the AP will be added to the AP List.

Manual Configuration	
AP Type	WAP-4033 ▼
AP Name	<input type="text"/>
Admin Password	<input type="text" value="admin"/>
AP IP	<input type="text"/>
AP MAC	<input type="text"/>
Remark	<input type="text"/>
Template	TEMPLATE1 ▼

### 4.3.4 Template Settings

Template is a model that can be applied to every device and is not required to configure the device individually. There are three templates provided for each AP model. Click **Edit** to configure each Template.

Template Settings		
AP Type	WAP-4033 ▼	<input type="button" value="Edit"/>
Template Settings	TEMPLATE1 ▼	

Before configuring the template, copy the configuration mode of a device to the template by selecting a **Template Source**, and a template does not need to be designed from scratch. If this option is not desired, please select **NONE**. Input the **Template Name** and **Template Remark** and click the hyperlink of **Template ID** to proceed to configuration.

Template Edit	
Template ID	<a href="#">1</a>
Template Name	<input type="text" value="TEMPLATE1"/>
Template Source	None ▼
Template Remark	<input type="text" value="Template 1"/>

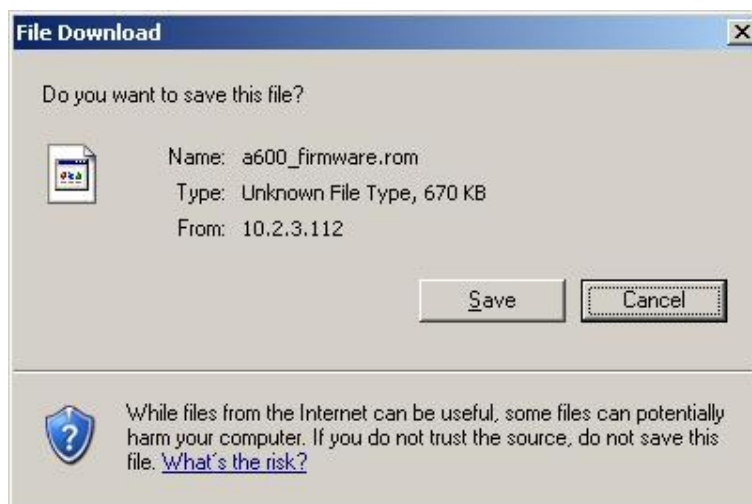
After entering the interface, revise the configuration and change administrator's password is desired. About other function settings, please refer to **4.3.1 AP List**.

## 4.3.5 Firmware Management

Upload the AP's firmware and download the present firmware from here.

Firmware Upload		
File Name	<input type="text"/>	<input type="button" value="瀏覽..."/>
		<input type="button" value="Upload"/>

Firmware List				
File Name	AP Type	Version	Size	Download
Checksum				Delete



## 4.3.6 AP Upgrade

Check the AP which needs to be upgraded and select the upgrade version of firmware. Click **Apply** to upgrade firmware.

AP List					
AP Name	AP Type	Current Version	Last Upgrading Time	Upgrade Version	Upgrade
NEWDEV-00004	WAP-4033	1.24	N/A	N/A	<input type="checkbox"/>

## 4.4 Network Configuration

This section includes the following functions: **Network Address Translation**, **Privilege List**, **Monitor IP List**, **Walled Garden List**, **Proxy Server Properties** and **Dynamic DNS**, **IP Mobility** and **VPN Termination**.

System Configuration
User Authentication
AP Management
Network Configuration
Utilities
Status

Network Address Translation

Privilege List

Monitor IP List

Walled Garden List

Proxy Server Properties

Dynamic DNS

IP Mobility

VPN Termination

### Network Configuration

Network Configuration	
<b>Network Address Translation</b>	PLANET WLS-1280 provides 3 types of network address translation: DMZ (Demilitarized Zone), Public Accessible Server and IP/Port Redirect.
<b>Privilege List</b>	System provides Privilege IP Address List and Privilege MAC Address List. System will NOT authenticate those listed devices.
<b>Monitor IP List</b>	System can monitor up to 40 network devices online status with an option to add them as public access servers via HTTP or HTTPS. Even under NAT mode, after added the devices as public access servers, the devices can be accessed by clicking the hypertext.
<b>Walled Garden List</b>	Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication.
<b>Proxy Server Properties</b>	PLANET WLS-1280 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
<b>Dynamic DNS</b>	PLANET WLS-1280 supports dynamic DNS (DDNS) feature.
<b>IP Mobility</b>	System supports IP PNP Configuration.
<b>VPN Termination</b>	VPN tunnels using IPsec can be terminated locally on PLANET WLS-1280.

#### 4.4.1 Network Address Translation











There are three parts, **DMZ**, **Public Accessible Server** and **Port and Redirect**, need to be set.

Network Address Translation
<a href="#">DMZ (Demilitarized Zone)</a>
<a href="#">Public Accessible Server</a>
<a href="#">Port and IP Redirect</a>

- DMZ**

DMZ allows administrators to define mandatory external to internal IP mapping, hence a user on WAN side network can access the private machine via the external IP. Choose to enable Automatic WAN IP Assignment by checkint the Enable box and enter the Internal IP address. For Static Assignment, enter Internal and External IP Addresses as a set and choose to use WAN1 or WAN2 for External Interface from the drop-down menu. These settings will become effective immediately after clicking the **Apply** button.

Automatic WAN IP Assignment			
Enable	Internal IP Address	External IP Address	External Interface
<input type="checkbox"/>	<input type="text"/>	10.30.1.252	WAN1

Static Assignments			
Item	Internal IP Address	External IP Address	External Interface
1	<input type="text"/>	<input type="text"/>	WAN1 
2	<input type="text"/>	<input type="text"/>	WAN1 
3	<input type="text"/>	<input type="text"/>	WAN1 
4	<input type="text"/>	<input type="text"/>	WAN1 
5	<input type="text"/>	<input type="text"/>	WAN1 
6	<input type="text"/>	<input type="text"/>	WAN1 
7	<input type="text"/>	<input type="text"/>	WAN1 
8	<input type="text"/>	<input type="text"/>	WAN1 
9	<input type="text"/>	<input type="text"/>	WAN1 
10	<input type="text"/>	<input type="text"/>	WAN1 

(Total:40) [First](#) [Prev](#) [Next](#) [Last](#)

- Public Accessible Server**

This function allows the administrator to set 40 virtual servers at most, so that the computers not belonging to the managed network can access the servers in the managed network via WAN port IP of PLANET WLS-1280. Please enter the “**External Service Port**”, “**Local Server IP Address**” and “**Local Server Port**”. According to the different services provided, the network service can use the **TCP** protocol or the **UDP** protocol. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the **Apply** button.

Public Accessible Server					
Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

(Total: 40) [First](#) [Prev](#) [Next](#) [Last](#)

- **Port and IP Redirect**

This function allows the administrator to set 40 sets of the IP addresses at most for redirection purpose. When the user attempts to connect to a destination IP address listed here, the connection packet will be converted and redirected to the corresponding destination. Please enter the **“IP Address”** and **“Port”** of **Destination**, and the **“IP Address”** and **“Port”** of **Translated to Destination**. According to the different services provided, choose the **“TCP”** protocol or the **“UDP”** protocol. These settings will become effective immediately after clicking **Apply**.

Item	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP

(Total:40) [First](#) [Prev](#) [Next](#) [Last](#)

## 4.4.2 Privilege List

There are two parts, **Privilege IP Address List** and **Privilege MAC Address List**, need to be set.

Privilege List
<a href="#">Privilege IP Address List</a>
<a href="#">Privilege MAC Address List</a>

- Privilege IP Address List**

If there are some workstations belonging to the managed server that need to access the network without authentication, enter the IP addresses of these workstations in this list. The “**Remark**” blank is not necessary but is useful to keep track. PLANET WLS-1280 allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking **Apply**.

Privilege IP Address List		
Item	Privilege IP Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>

**Warning:** Permitting specific IP addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems.

- **Privilege MAC Address List**

In addition to the IP address, you can also set the MAC address of the workstations that need to access the network without authentication in this list. PLANET WLS-1280 allows 100 privilege MAC addresses at most. If you want to manually create the list, enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (not necessary). These settings will become effective immediately after clicking **Apply**.

Privilege MAC Address List		
Item	MAC Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>

**Warning:** Permitting specific MAC addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems.



### 4.4.3 Monitor IP List

PLANET WLS-1280 will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the related information, click **Apply** and these settings will become effective immediately.

When the monitored devices have built-in Web servers and connect to NAT-enabled LAN interfaces, they can be easily added into public accessible servers by clicking the "Add" buttons.

Monitor IP List							
Item	Protocol	IP Address	Link	Item	Protocol	IP Address	Link
1	http ▼	<input type="text"/>	Add	2	http ▼	<input type="text"/>	Add
3	http ▼	<input type="text"/>	Add	4	http ▼	<input type="text"/>	Add
5	http ▼	<input type="text"/>	Add	6	http ▼	<input type="text"/>	Add
7	http ▼	<input type="text"/>	Add	8	http ▼	<input type="text"/>	Add
9	http ▼	<input type="text"/>	Add	10	http ▼	<input type="text"/>	Add
11	http ▼	<input type="text"/>	Add	12	http ▼	<input type="text"/>	Add
13	http ▼	<input type="text"/>	Add	14	http ▼	<input type="text"/>	Add
15	http ▼	<input type="text"/>	Add	16	http ▼	<input type="text"/>	Add
17	http ▼	<input type="text"/>	Add	18	http ▼	<input type="text"/>	Add
19	http ▼	<input type="text"/>	Add	20	http ▼	<input type="text"/>	Add


When "Monitor" button is clicked, Monitor IP Result page will show up. If the entered IP address is unreachable, a red dot under Result field will appear. A green dot indicates that the IP address is reachable and alive..

Monitor IP result		
No	IP Address	Result
1	192.168.1.200	
2	192.168.1.100	

#### 4.4.4 Walled Garden List

This function provides some free services to the users to access before login and authentication. Up to 20 addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Please enter the website **IP Address** or **Domain Name** in the list and these settings will become effective immediately after clicking **Apply**.

Walled Garden List			
Item	Address	Item	Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

	<p><b>Caution:</b> To use the domain name, PLANET WLS-1280 has to connect to DNS server first or this function will not work.</p>
---	---

### 4.4.5 Proxy Server Properties

PLANET WLS-1280 supports Internal Proxy Server and External Proxy Server functions.

External Proxy Server		
Item	Server IP	Port
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Internal Proxy Server	
Built-in Proxy Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

- **External Proxy Server:** Under PLANET WLS-1280 security management, the system will match the External Proxy Server list to the end-users' proxy setting. If there isn't a matching, then the end-users will no be able to reach the login page and thus unable to access the network. If there is a matching, then the end-users will be directed to the system first for authentication. After a successful authentication, the end-users will be redirected back to the desired proxy servers depending on various situations.
- **Internal Proxy Server:** PLANET WLS-1280 has a built-in proxy server. If this function is enabled, the end users will be forced to treat PLANET WLS-1280 as the proxy server regardless of the end-users' original proxy settings.

**For more details about how to set up the proxy servers, please refer to Appendix D and Appendix E.**

## 4.4.6 Dynamic DNS

PLANET WLS-1280 provides a convenient DNS function to translate a domain name to the IP address of WAN port that helps the administrator memorize and connect to WAN port. If the DHCP is activated at WAN port, this function will also update the newest IP address regularly to the DNS server. These settings will become effective immediately after clicking **Apply**.

Dynamic DNS	
DDNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Provider	<input type="text" value="DynDNS.org(Dynamic)"/>
Host name	<input type="text"/>
Username/E-mail	<input type="text"/>
Password/Key	<input type="text"/>

- **DDNS:** Enabling or disabling of this function.
- **Provider:** Select the DNS provider.
- **Host name:** The IP address/domain name of the WAN port.
- **Username/E-mail:** The register ID (username or e-mail) for the DNS provider.
- **Password/Key:** The register password for the DNS provider.

## 4.4.7 IP Mobility

PLANET WLS-1280 supports IP PNP function.

IP Mobility	
IP PNP	<input type="checkbox"/> Enable

If this function is enabled, a client can use any reasonable IP address to connect to the system. Regardless of what the IP address at the user end is, the client can still be authenticated through PLANET WLS-1280 and access the network.

## 4.4.8 VPN Termination

**Virtual Private Network**, or **VPN**, a type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POPS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

VPN Termination Setting	
Enable VPN Termination	<input checked="" type="checkbox"/>

VPN Parameters	
Encryption	<input type="radio"/> DES <input checked="" type="radio"/> 3-DES
Integrity	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA-1
Diffie-Hellman	<input checked="" type="radio"/> Group 1 <input type="radio"/> Group 2

VPN has several kinds of protocols and PLANET WLS-1280 supports **IPSec**. IPSec is a technology provided by Windows 2000 that allows you to create encrypted channels between two servers. IPSec can be used to filter IP traffic and to authenticate servers. If you need to use this function, check **Enable VPN Termination** and choose the desired parameters. Then click **Apply** to enable VPN Termination.

In PLANET WLS-1280, there are several functions with **VPN** or **IPSec** selection. When you enable them, they will apply the VPN settings you configured here.

For the details of IPSec VPN, please see **Appendix C -- IPSec VPN**.

## 4.5 Utilities

This section provides four utilities to customize and maintain the system including **Change Password**, **Backup/Restore Setting**, **Firmware Upgrade** and **Restart**.

The screenshot displays the PLANET WLS-1280 web interface. At the top, there is a navigation bar with buttons for System Configuration, User Authentication, AP Management, Network Configuration, Utilities (highlighted), and Status. On the left side, there is a sidebar with buttons for Change Password, Backup/Restore Settings, Firmware Upgrade, and Restart. The main content area is titled 'Utilities' and contains a table with the following information:

Utilities	
Change Password	Change the administration password.
Backup/Restore Settings	Backup and restore system settings. Administrator may also reset system settings to factory default.
Firmware Upgrade	Update PLANET WLS-1280 firmware.
Restart	Restart the system.

At the bottom of the main content area, there are two icons: a home icon and a back icon.

### 4.5.1 Change Password

PLANET WLS-1280 supports three kinds of account interface. You can log in as **admin**, **manager** or **operator**. The default usernames and passwords are as follow:

**Admin:** The administrator can access all configuration pages of PLANET WLS-1280.

User Name: **admin**

Password: **admin**

**Manager:** The manager can only access the configuration pages under **User Authentication** to manage the user accounts, but has no permission to change the settings of the profiles for Firewall, Specific Route and Schedule.

User Name: **manager**

Password: **manager**

**Operator:** The operator can only access the configuration page of **Create On-demand User** to create and print out the new on-demand user accounts.

User Name: **operator**

Password: **operator**

The administrator can change the passwords here. Please enter all the required fields with red asterisks if changing the password is desired. Click **Apply** to activate this new password.

Change Admin Password	
Old Password	<input type="password"/>
New Password	<input type="password"/>
Verify Password	<input type="password"/>
<div> <input type="button" value="✓ Apply"/> <input type="button" value="✗ Clear"/> </div>	

Change Manager Password	
New Password	<input type="password"/>
Verify Password	<input type="password"/>
<div> <input type="button" value="✓ Apply"/> <input type="button" value="✗ Clear"/> </div>	

Change Operator Password	
New Password	<input type="password"/>
Verify Password	<input type="password"/>



**Caution:** If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface on the serial port, console/printer port.

## 4.5.2 Backup/Restore Settings

This function is used to backup/restore PLANET WLS-1280 settings. Also, PLANET WLS-1280 can be reset to the factory default settings here.

Backup current system settings	
<div>Backup</div>	

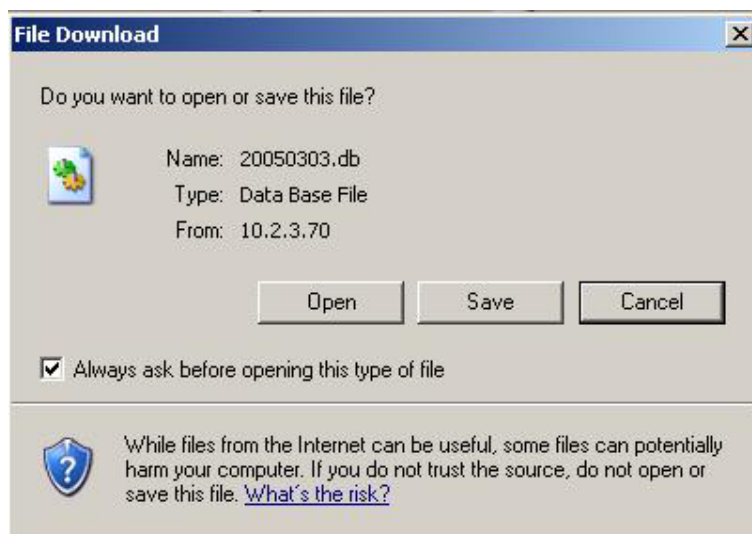
  

Restore system settings	
File Name	<input type="text"/> <div>瀏覽...</div>
<div>Restore</div>	

Reset to the factory-default settings	
<div>Reset</div>	

- **Backup current system settings:** Click **Backup** to create a .db database backup file and save it on disk.



- **Restore system settings:** Click **Browse** to search for a .db database backup file created by PLANET WLS-1280 and click **Restore** to restore to the same settings at the time the backup file was created.
- **Reset to the factory-default settings:** Click **Reset** to load the factory default settings of PLANET WLS-1280.

## 4.5.3 Firmware Upgrade

The administrator can download the latest firmware from website and upgrade the system here. Click **Browse** to

search for the firmware file and click **Apply** to go on with the firmware upgrade process. It might take a few minutes before the upgrade process completes and the system needs to be restarted afterwards to make the new firmware effective.

**Note: For maintenance issues, we strongly recommend you backup system settings before upgrading firmware.**

Firmware Upgrade	
Current Version	1.00.B1
File Name	<input type="text"/> <input data-bbox="1050 488 1166 528" type="button" value="Browse..."/>

**Warning:** 1. Firmware upgrade may cause the loss of some of the data. Please refer to the release notes for the limitation before upgrading the firmware. 2. Please restart the system after upgrading the firmware. Do not power on/off the system during the upgrade or the restart process. It may damage the system and cause it to malfunction.

#### 4.5.4 Restart

This function allows the administrator to safely restart PLANET WLS-1280 and the process should take about 100 seconds. Click **YES** to restart PLANET WLS-1280; click **NO** to go back to the previous screen. If you need to turn off the power, we recommend you to restart PLANET WLS-1280 first and then turn off the power after completing the restart process.

Do you want to **Restart** PLANET WLS-1280?



**Caution:** The connection of all online users of the system will be disconnected when system is in the process of restarting.

## 4.6 Status

This section includes **System Status**, **Interface Status**, **Current Users**, **Traffic History**, and **Notification Configuration** to provide system status information and online user status.



The screenshot shows a web-based network management interface. At the top, there is a horizontal navigation bar with six buttons: "System Configuration", "User Authentication", "AP Management", "Network Configuration", "Utilities", and "Status". The "Status" button is highlighted in blue. Below this bar, on the left side, is a vertical sidebar with five buttons: "System Status", "Interface Status", "Current Users", "Traffic History", and "Notification Configuration". The "System Status" button is highlighted. The main content area on the right is titled "Status" with a blue icon. It contains a table with five rows, each representing a status category and its description. At the bottom of the main content area, there are two blue circular icons: a home icon and an up arrow icon.

Status	
<b>System Status</b>	Display current system settings.
<b>Interface Status</b>	Display WAN 1, WAN 2, Controlled, Uncontrolled configurations and status.
<b>Current Users</b>	Display online user information including: Username, IP, MAC, packet count, byte count and idle time. Administrator may also kick out any on-line user from here.
<b>Traffic History</b>	Display detail usage information by day. A minimum of 3 days of history can be logged in the system volatile memory.
<b>Notification Configuration</b>	There are three email accounts available to be set for receiving Monitor IP report, Traffic History, On-demand User Log, and AP status change. External SYSLOG server can be configured here.

## 4.6.1 System Status

This section provides an overview of the system for the administrator.

System Status		
Current Firmware Version		1.00.B1
System Name		PLANET WLS-1280
Admin info		Sorry! The service is temporarily unavailable
Home Page		<a href="http://www.planet.com.tw">http://www.planet.com.tw</a>
Syslog server-Traffic History		N/A/N/A
Syslog server-On demand User log		N/A/N/A
Proxy Server		Disabled
Friendly Logout		Enabled
Internet Connection Detection		Disabled
Management	Remote Management IP	0.0.0.0/0.0.0.0
	SNMP	Disabled
History	Retained Days	3 days
	Traffic log Email To	N/A
	On-demand log Email To	N/A
Time	NTP Server	(tock.usno.navy.mil)
	Date Time	2007/01/05 15:22:58 +0800
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
	Guest Account	Disabled
DNS	Preferred DNS Server	192.203.230.10
	Alternate DNS Server	N/A

The description of the table is as follows:

<u>Item</u>	<u>Description</u>
<b>Current Firmware Version</b>	The present firmware version of PLANET WLS-1280
<b>System Name</b>	The system name. The default is PLANET WLS-1280
<b>Home Page</b>	The page to which the users are directed after initial login success.

<b>Syslog server-Traffic History</b>		The IP address and port number of the external Syslog Server. <b>N/A</b> means that it is not configured.
<b>Syslog server-On demand User log</b>		The IP address and port number of the external Syslog Server. <b>N/A</b> means that it is not configured.
<b>Proxy Server</b>		Enabled/disabled stands for that the system is currently using the proxy server or not.
<b>Friendly Logout</b>		Enabled/disabled stands for the setting of hiding/displaying an extra confirmation window when users try to close the login successful window .
<b>Warning of Internet Disconnection</b>		Enabled/Disabled stands for the connection at WAN is normal or abnormal and all online users are allowed/disallowed to log in the network.
<b>Management</b>	<b>Remote Management IP</b>	The IP or IPs that is allowed for accessing the management interface.
	<b>SNMP</b>	Enabled/disabled stands for the current status of the SNMP management function.
<b>History</b>	<b>Retained Days</b>	The maximum number of days for the system to retain the users' information.
	<b>Email To</b>	The email address that the traffic history information will be sent to.
<b>Time</b>	<b>NTP Server</b>	The network time server that the system is set to align.
	<b>Date Time</b>	The system time is shown as the local time.
<b>User</b>	<b>Idle Timer</b>	The number of minutes allowed for the users to be inactive.
	<b>Multiple Login</b>	Enabled/disabled stands for the current setting to allow/disallow multiple logins form the same account.
<b>DNS</b>	<b>Preferred DNS Server</b>	IP address of the preferred DNS Server.
	<b>Alternate DNS Server</b>	IP address of the alternate DNS Server.

## 4.6.2 Interface Status

This section provides an overview of the interface for the administrator including **WAN1**, **WAN2**, **Controlled Port** and **Uncontrolled Port**.

Interface Status		
WAN1	MAC Address	00:06:78:AA:BB:CE
	IP Address	10.2.3.127
	Subnet Mask	255.255.255.0
WAN2	MAC Address	00:06:78:AA:BB:CD
	IP Address	10.0.2.2
	Subnet Mask	255.255.0.0
Controlled	Mode	NAT
	MAC Address	00:06:78:AA:BB:CC
	IP Address	192.168.10.254
	Subnet Mask	255.255.255.0
Controlled DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.10.1
	End IP Address	192.168.10.100
	Lease Time	1440 Min(s)
Uncontrolled	Mode	NAT
	MAC Address	00:06:78:AA:BB:CC
	IP Address	192.168.2.254
	Subnet Mask	255.255.255.0
Uncontrolled DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.2.1
	End IP Address	192.168.2.100
	Lease Time	1440 Min(s)

The description of the table is as follows.

<u>Item</u>		<u>Description</u>
WAN1	MAC Address	The MAC address of the WAN1 port.
	IP Address	The IP address of the WAN1 port.
	Subnet Mask	The Subnet Mask of the WAN1 port.

<b>WAN2</b>	<b>MAC Address</b>	The MAC address of the WAN2 port.
	<b>IP Address</b>	The IP address of the WAN2 port.
	<b>Subnet Mask</b>	The Subnet Mask of the WAN2 port.
<b>Controlled</b>	<b>Mode</b>	The mode of the controlled port.
	<b>MAC Address</b>	The MAC address of the controlled port.
	<b>IP Address</b>	The IP address of the controlled port.
	<b>Subnet Mask</b>	The Subnet Mask of the controlled port.
<b>Controlled DHCP Server</b>	<b>Status</b>	Enable/disable stands for status of the DHCP server on the controlled port.
	<b>WINS IP Address</b>	The WINS server IP. <b>N/A</b> means that it is not configured.
	<b>Start IP Address</b>	The start IP address of the DHCP IP range.
	<b>End IP address</b>	The end IP address of the DHCP IP range.
	<b>Lease Time</b>	Minutes of the lease time of the IP address.
<b>Uncontrolled</b>	<b>Mode</b>	The mode of the uncontrolled port.
	<b>MAC Address</b>	The MAC address of the uncontrolled port.
	<b>IP Address</b>	The IP address of the uncontrolled port.
	<b>Subnet Mask</b>	The Subnet Mask of the uncontrolled port.
<b>Uncontrolled DHCP Server</b>	<b>Status</b>	Enable/disable stands for status of the DHCP server on the uncontrolled port
	<b>WINS IP Address</b>	The WINS server IP. <b>N/A</b> means that it is not configured.
	<b>Start IP Address</b>	The start IP address of the DHCP IP range.
	<b>End IP address</b>	The end IP Address of the DHCP IP range.
	<b>Lease Time</b>	Minutes of the lease time of the IP address.

### 4.6.3 Current Users

In this function, each online user's information including **Username**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **Idle**, **Source AP** and **Kick Out** can be obtained. Administrator can use this function to force a specific online user to log out. Just click the hyperlink of **Kick Out** next to the online user's name to logout that particular user. Click **Refresh** to renew the current users list.

Current Users List						
Item	Username		Pkts In	Bytes In	Idle	Source AP
	IP	MAC	Pkts Out	Bytes Out		Kick Out

✓ Refresh

## 4.6.4 Traffic History

This function is used to check the history of PLANET WLS-1280. The history of each day will be saved separately in the DRAM for 3 days.

Traffic History	
Date	Size (Byte)
<a href="#">2007-01-05</a>	65

On-demand User Log	
Date	Size (Byte)
<a href="#">2007-01-05</a>	239

Roaming Out Traffic History	
Date	Size (Byte)
<a href="#">2007-01-05</a>	106

Roaming In Traffic History	
Date	Size (Byte)
<a href="#">2007-01-05</a>	112



**Caution:** Since the history is saved in the DRAM, if you need to restart the system and also keep the history, then please manually copy and save the information before restarting.

If the **History Email** has been entered under the **Notify Configuration** page, then the system will automatically send out the history information to that email address.

- **Traffic History**

As shown in the following figure, each line is a traffic history record consisting of 9 fields, **Date**, **Type**, **Name**, **IP**,

**MAC, Pkts In, Bytes In, Pkts Out, and Bytes Out**, of user activities.

Traffic History 2005-03-22									
Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	
2005-03-22 19:12:21 +0800	LOGIN	user1@local.tw	192.168.1.143	00:D0:C9:42:37:20	0	0	0	0	
2005-03-22 19:12:24 +0800	LOGOUT	user1@local.tw	192.168.1.143	00:D0:C9:42:37:20	3	252	3	252	
2005-03-22 19:12:29 +0800	LOGIN	user2@local.tw	192.168.1.143	00:D0:C9:42:37:20	0	0	0	0	
2005-03-22 19:12:32 +0800	LOGOUT	user2@local.tw	192.168.1.143	00:D0:C9:42:37:20	3	252	3	252	
2005-03-22 19:13:51 +0800	LOGIN	user1@local.tw	192.168.1.1	00:D0:C9:60:01:01	0	0	0	0	

- **On-demand User Log**

As shown in the following figure, each line is a on-demand user log record consisting of 13 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **Expiretime**, **Validtime** and **Remark**, of user activities.

On-demand User Log 2005-03-22												
Date	System Name	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	Expiretime	Validtime	Remark
2005-03-22 17:55:58 +0800	My Service	Create_OD_User	P4SP	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:55:58	None	2 hrs 0 mins
2005-03-22 17:56:03 +0800	My Service	Create_OD_User	62H6	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:56:03	None	2 hrs 0 mins
2005-03-22 17:56:07 +0800	My Service	Create_OD_User	886D	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:56:07	None	2 hrs 0 mins

- **Roaming Out Traffic History**

As shown in the following figure, each line is a roaming out traffic history record consisting of 14 fields, **Date**, **Type**, **Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

Roaming Out Traffic History 2005-03-22													
Date	Type	Name	NASID	NASIP	NASPort	UserMAC	sessionID	sessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

- **Roaming In Traffic History**

As shown in the following figure, each line is a roaming in traffic history record consisting of 15 fields, **Date**, **Type**, **Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **UserIP**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

Roaming In Traffic History 2005-03-22														
Date	Type	Name	NASID	NASIP	NASPort	UserMAC	UserIP	SessionID	SessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

## 4.6.5 Notification Configuration

PLANET WLS-1280 will save the traffic history into the internal DRAM. If the administrator wants the system to automatically send out the history to a particular email address, please enter the related information in these fields.

E-mail Notification Configuration				
Send To	Monitor IP Report	Traffic History	On-demand User Log	AP Status
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Interval	1 Hour <input type="button" value="v"/>	1 Hour <input type="button" value="v"/>	1 Hour <input type="button" value="v"/>	N/A
Send Test Email	<input type="button" value="Send"/>	<input type="button" value="Send"/>	<input type="button" value="Send"/>	<input type="button" value="Send"/>
Send From	<input type="text"/>			
SMTP	<input type="text"/>			
Auth Method	None <input type="button" value="v"/>			

Syslog Configuration	
Traffic History	IP: <input type="text"/> Port: <input type="text"/>
On-demand User Log	IP: <input type="text"/> Port: <input type="text"/>

- **Send To:** The e-mail address of the person whom the history email is for. This will be the receiver's e-mail. Check which type of report to be sent—Monitor IP Report, Traffic History, On-demand User Log, and AP Status.
- **Interval:** The time interval to send the e-mail report. Choose a proper number from the drop-down box.
- **Send Test Email:** To test the settings correct or not.
- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **SMTP Server:** The IP address of the SMTP server.
- **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or "**None**" to use none of the above. Depending on which authentication method you select, you have to enter the **Account Name**, **Password** and **Domain**.

**NTLMv1** is not currently available for general use.

**Plain** and **CRAM-MD5** are standardized authentication mechanisms while **Login** and **NTLMv1** are Microsoft proprietary mechanisms. Only **Plain** and **Login** can use the UNIX login password. Netscape uses **Plain**.

Outlook and Outlook express uses **Login** as default, although they can be set to use **NTLMv1**.

Pegasus uses **CRAM-MD5** or **Login** but can not be configured which method to use.

**Syslog Configuration:** There are 2 parts: Traffic History and On-demand User Log. Enter the IP address and Port to specify which and from where the report should be sent. .

•

## 4.7 Help

On the screen, the **Help** button is on the upper right corner.

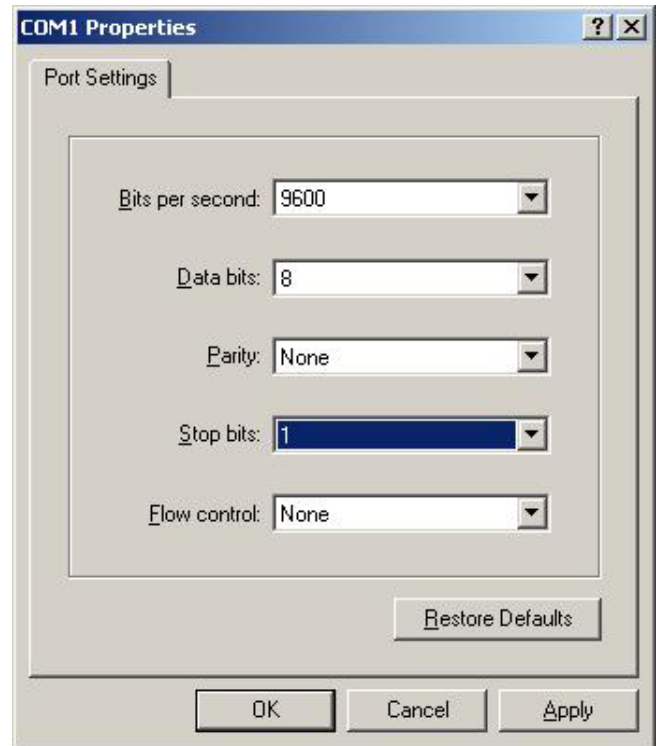
Click **Help** to the **Online Help** window and then click the hyperlink of the items to get the information.



## 5. Appendix A – Console Interface

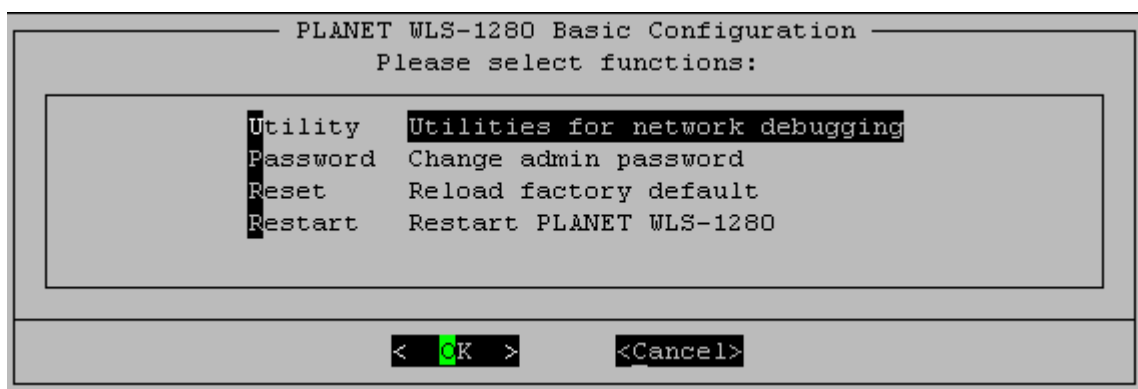
Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

1. To connect the console port of PLANET WLS-1280, you need a console, modem cable and a terminal simulation program, such as the Hyper Terminal.
2. If you use Hyper Terminal, please set the parameters as **9600,8,n,1**.



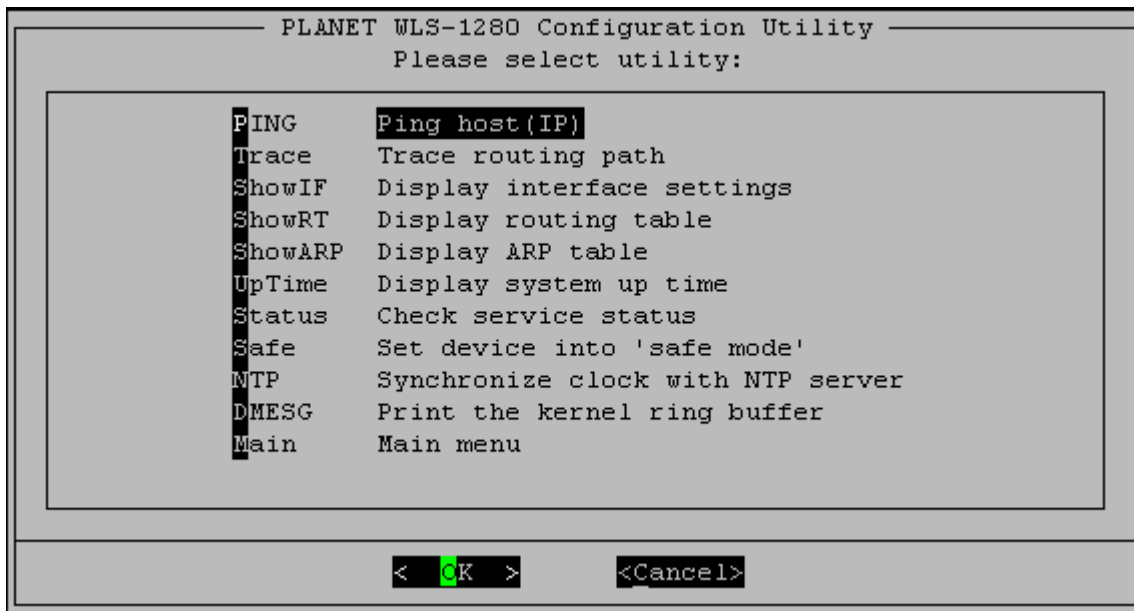
**Caution:** the main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the **Enter** key to make selection or confirm what you enter.

3. Once the console port of PLANET WLS-1280 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys, so that the terminal simulation program will send some messages to the system and the welcome screen or the main menu should appear. If you are still unable to see the welcome screen or the main menu of the console, please check the connection of the cables and the settings of the terminal simulation program.



- **Utilities for network debugging**

The console interface provides several utilities to assist the Administrator to check the system conditions and to debug any problems. The utilities are described as follow:



- Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
- Trace routing path: Trace and inquire the routing path to a specific target.
- Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and netmask.
- Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
- Display ARP table: The internal ARP table of the system is displayed.
- Display system up time: The system live time (time for system being turn on) is displayed.
- Check service status: Check and display the status of the system.
- Set device into "safe mode": If administrator is unable to use Web Management Interface via the browser for the system failed inexplicitly. Administrator can choose this utility and set PLANET WLS-1280 into safe mode, then administrator can management this device with browser again.
- Synchronize clock with NTP server: Immediately synchronize the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, therefore we must reset the internal clock through the NTP.
- Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their bootup messages instead of copying the messages by hand.
- Main menu: Go back to the main menu.

- **Change admin password**

Besides supporting the use of console management interface through the connection of null modem, the

system also supports the SSH online connection for the setup. When using a null modem to connect to the system console, we do not need to enter administrator's password to enter the console management interface. But connecting the system by SSH, we have to enter the username and password.

The username is "admin" and the default password is also "admin", which is the same as for the web management interface. You can use this option to change the administrator's password. Even if you forgot the password and are unable to log in the management interface from the web or the remote end of the SSH, you can still use the null modem to connect the console management interface and set the administrator's password again.



**Caution:** Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change PLANET WLS-1280 Admin username and password after logging in the system for the first time.

- **Reload factory default**

Choosing this option will reset the system configuration to the factory defaults.

- **Restart Cipherium PLANET WLS-1280**

Choosing this option will restart PLANET WLS-1280.

## 6. Appendix B – Network Configuration on PC

After PLANET WLS-1280 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

- **Internet Connection Setup**

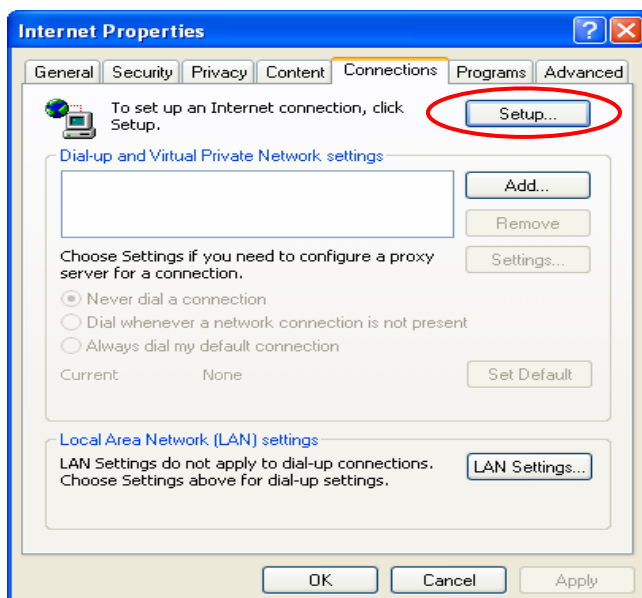
If the Internet Connection of this client PC has been configured as use local area network already, you can skip this setup.

- ◆ **Windows XP**

1. Choose **Start > Control Panel > Internet Option**.



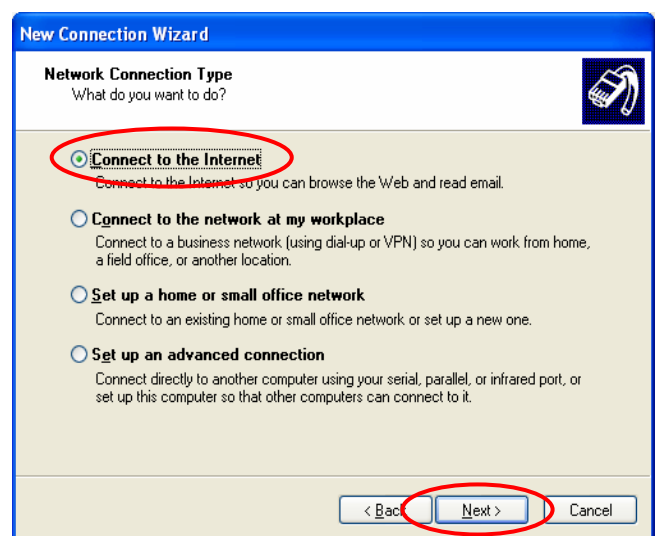
2. Choose the “**Connections**” label, and then click **Setup**.



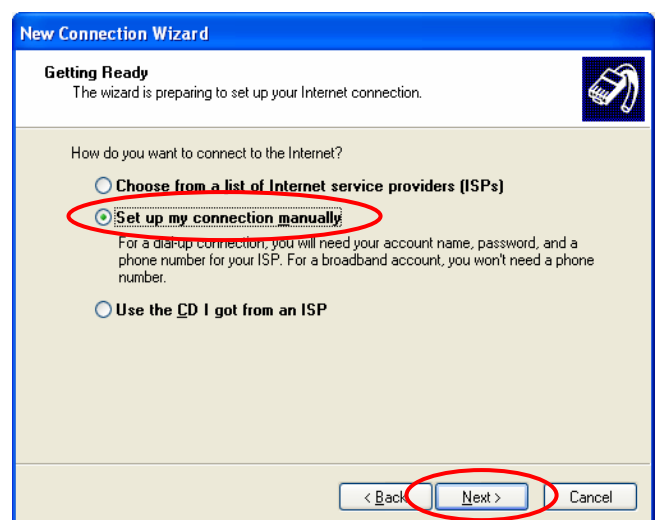
3. Click **Next** when **Welcome to the New Connection Wizard** screen appears.



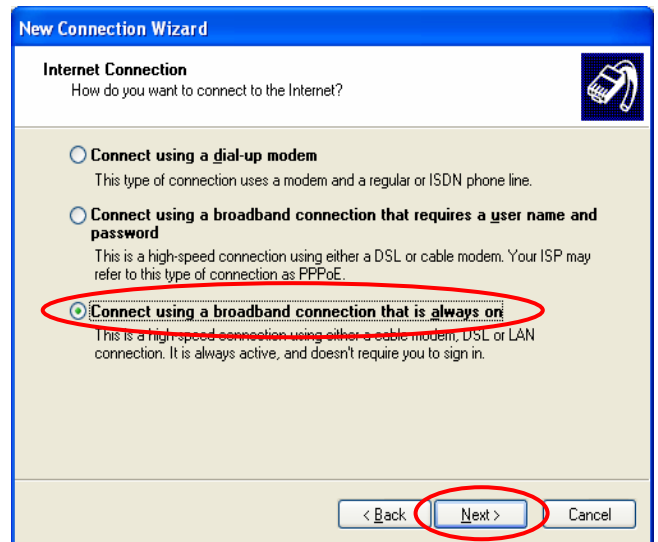
4. Choose “**Connect to the Internet**” and then click **Next**.



5. Choose “**Set up my connection manually**” and then click **Next**.



6. Choose “**Connect using a broadband connection that is always on**” and then click **Next**.



7. Finally, click **Finish** to exit the **Connection Wizard**. Now, you have completed the setup.



- **TCP/IP Network Setup**

In the default configuration, PLANET WLS-1280 will assign an appropriate IP address to a client PC which uses DHCP to obtain IP address automatically. Windows 95/98/2000/XP configures IP setup to “**Obtain an IP address automatically**” in default settings.

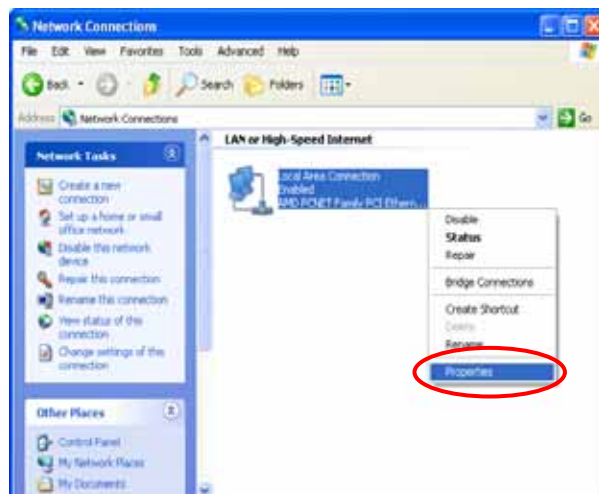
If you want to check the TCP/IP setup or use a static IP to connect to PLANET WLS-1280 LAN port, please follow the following steps:

◆ **Check the TCP/IP Setup of Window XP**

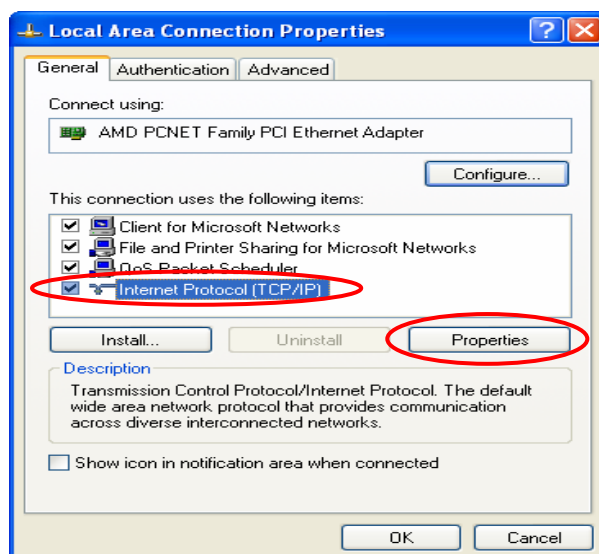
1. Select **Start > Control Panel > Network Connection**.



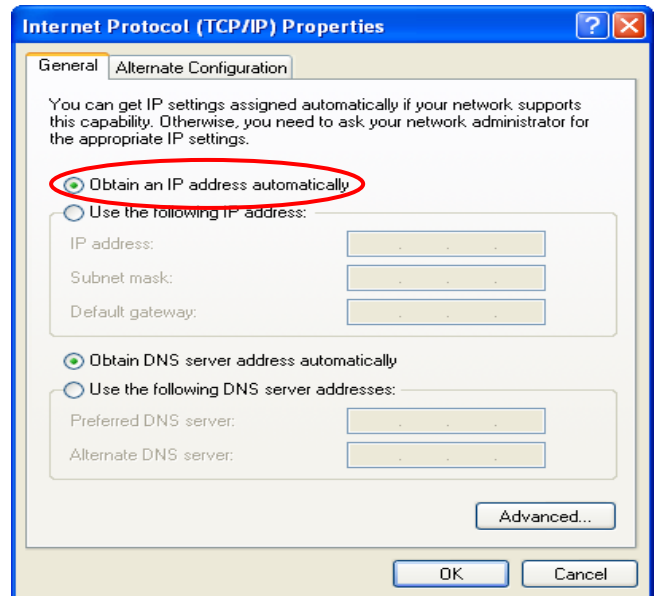
2. Click the right button of the mouse on the “**Local Area Connection**” icon and select “**Properties**”



3. Select “**General**” label and choose “**Internet Protocol (TCP/IP)**” and then click **Properties**.  
Now, you can choose to use **DHCP** or **specific IP address**, please proceed to the following steps.

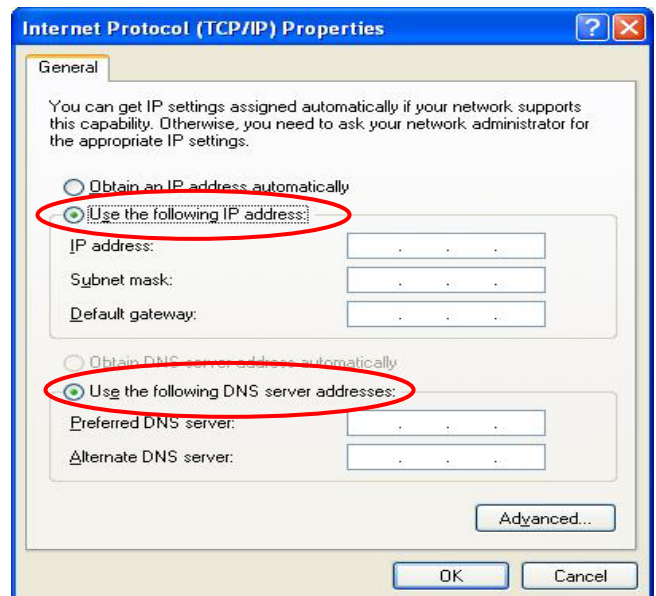


- 1-2. **Using DHCP:** If want to use DHCP, please choose “**Obtain an IP address automatically**” and click **OK**. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from PLANET WLS-1280.



- 2-2. **Using Specific IP Address:** If want to use specific IP address, you have to ask the network administrator for the information of PLANET WLS-1280: **IP address**, **Subnet Mask**, **New gateway** and **DNS server address**.

- Please choose “**Use the following IP address**” and enter the information given from the network administrator in “**IP address**”, “**Subnet mask**” and the “**DNS address(es)**” and then click **OK**.



## 7. Appendix C – IPsec VPN

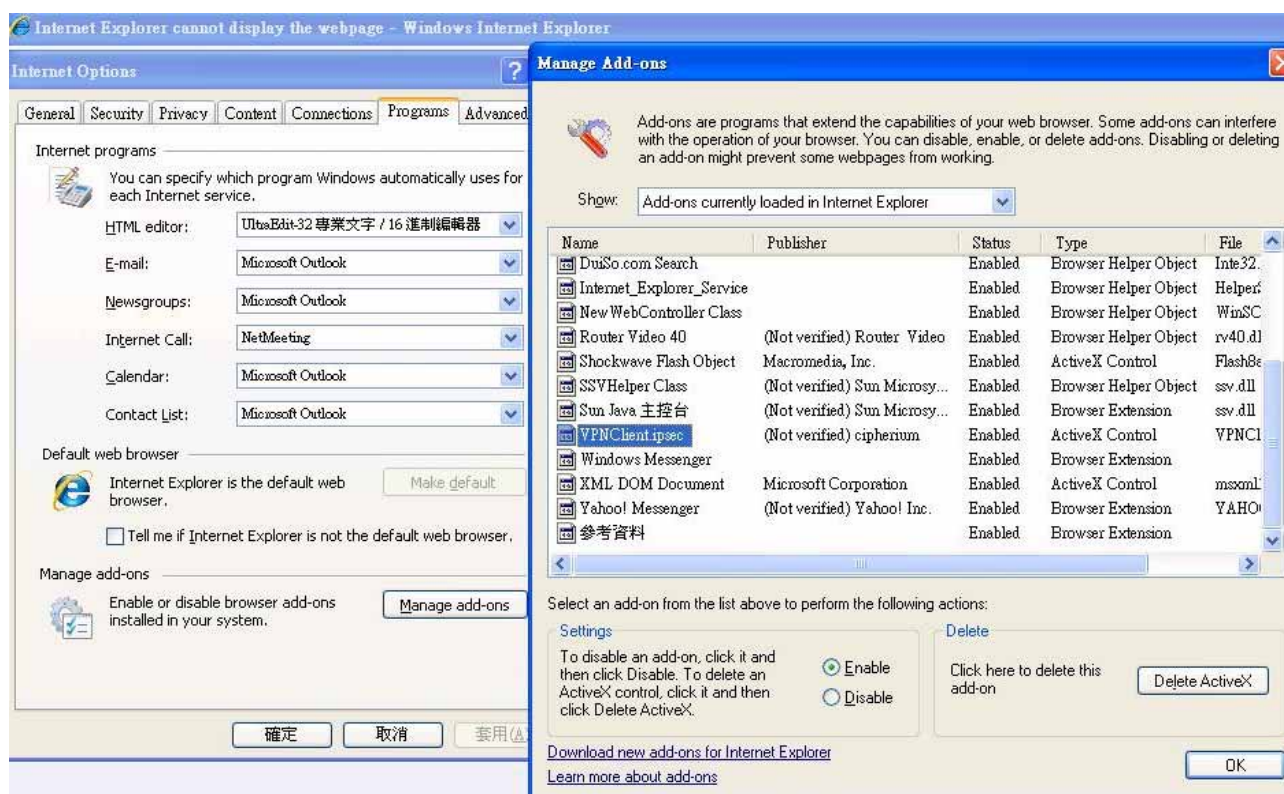
PLANET WLS-1280 has equipped with IPsec VPN feature starts from release version v1.00. To fully utilize the nature supported IPsec VPN by Microsoft Windows XP SP2 (with patch) and Windows 2000 operating systems, PLANET WLS-1280 implement IPsec VPN tunneling technology between client's windows devices and PLANET WLS-1280 itself, no matter of through wired or wireless network.

By pushing down ActiveX to the client's Windows device from PLANET WLS-1280, no extra client software to be installed except ActiveX, in which a so-called "clientless" IPsec VPN setting is configured automatically. At the end of this setup, a build-in IPsec VPN feature was enabled to be ready to serve once it is called to be setup.

The design goal is to eliminate the configuration difficulty from IPsec VPN users. At the client side, the IPsec VPN implementation of PLANET WLS-1280 is based on ActiveX and the built-in IPsec VPN client of Windows OS.

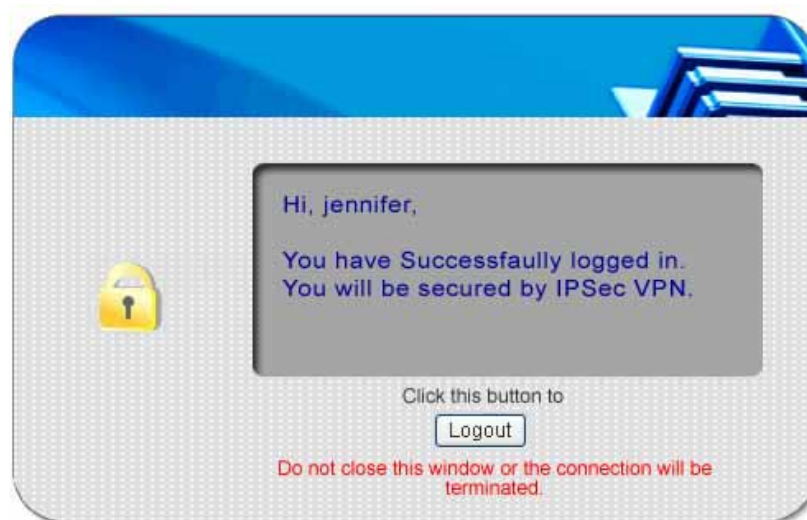
### 1. ActiveX component

The ActiveX is a software component running inside Internet Explorer. The ActiveX component can be checked by the following windows.



From Windows Internet Explorer, click "Manage add-ons" button inside "Programs" page under "Tools" to show the add-ons programs list. You can see VPNClient.ipsec was enabled.

During the first-time login to PLANET WLS-1280, Internet Explorer will ask user to download the ActiveX component of IPsec VPN. This ActiveX component once downloaded will be running paralleled with the “Login Success Page” after the page being brought up successfully. The ActiveX component helps to setup the IPsec VPN tunnel between client’s device and PLANET WLS-1280 controller, and to check the validity of the IPsec VPN tunnel between them. If the connection is down, the ActiveX component will detect the broken link and decompose the IPsec tunnel. Once the IPsec VPN tunnel was built, any packet sent will be encrypted. Without connecting to the original IPsec VPN tunnel, user or client device has no alternative to gain network connection beyond this. The design of PLANET WLS-1280’s IPsec VPN feature directly solves possible data security leak problem between client and the controller via either wireless or wired connection without extra hardware or client software installed.



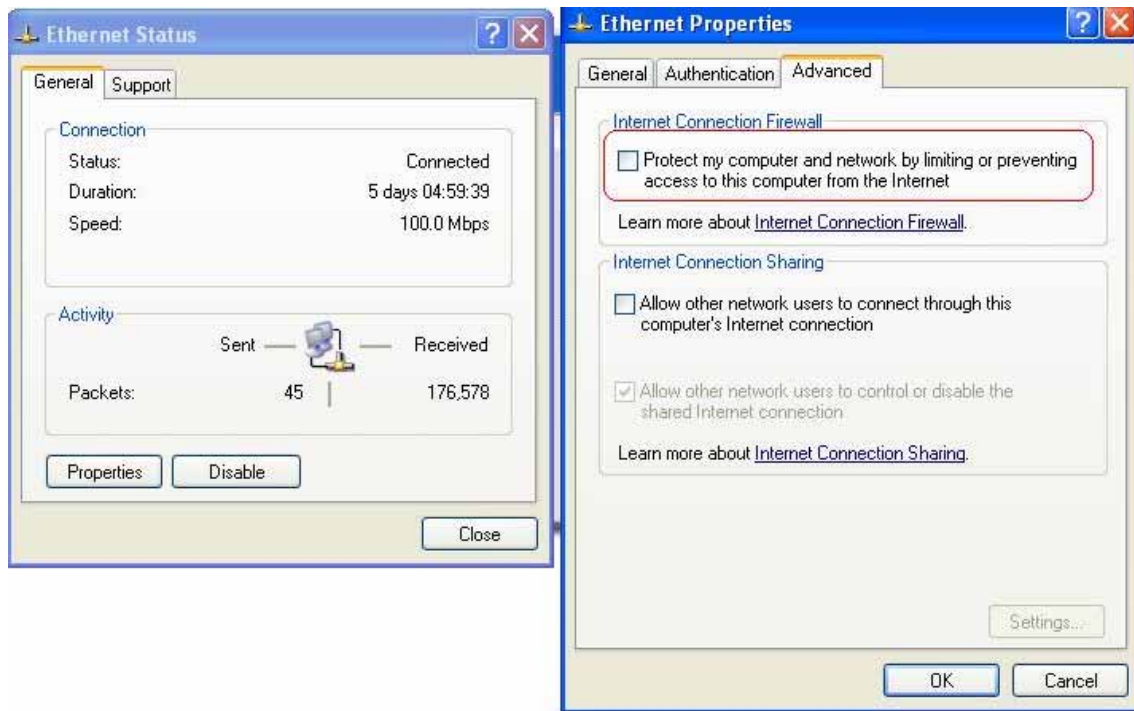
## 2. Limitations

The limitation of the client side due to ActiveX and Windows OS includes:

- a. Internet Connection Firewall of Windows XP or Windows XP SP1 is not compatible with IPsec protocol. It shall be turned off to allow IPsec packets to pass through.
- b. Without patch, ICMP (Ping) and PORT command of FTP can not work in Windows XP SP2.
- c. The Forced termination (through CTRL+ALT+DEL, Task Manager) of the Internet Explorer will stop the running of ActiveX. It causes IPsec tunnel can't be cleared properly at client's device. A reboot of client's device is needed to clear the IPsec tunnel.
- d. The crash of Windows Internet Explorer may cause the same result.

## 3. Internet Connection Firewall

In Windows XP and Windows XP SP1, the Internet Connection Firewall is not compatible with IPsec. Internet Connection Firewall will drop packets from tunneling of IPsec VPN.



**Suggestion:** Please **TURN OFF** Internet Connection Firewall feature or upgrade the Windows OS into Windows XP SP2.

#### 4. ICMP and Active Mode FTP

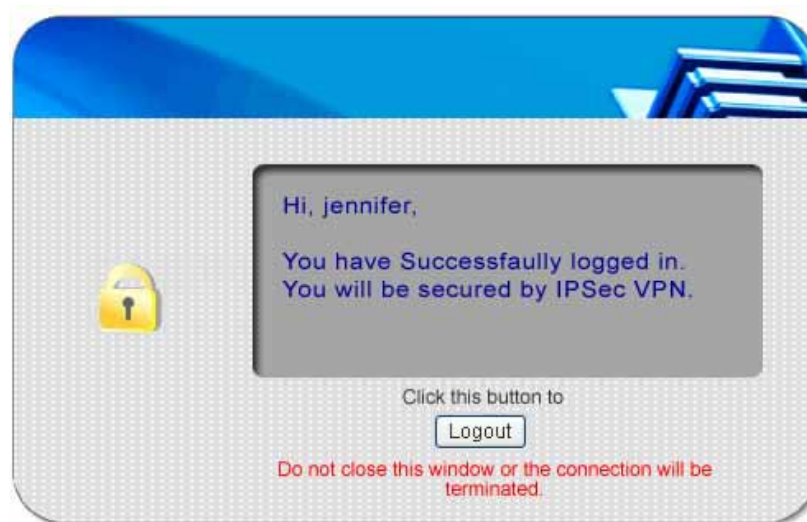
On Windows XP SP2 without patching by KB889527, it will drop ICMP packets from IPsec tunnel. This problem can be fixed by upgrading patch KB889527. Before enabling IPsec VPN function on client device, please access the patch from Microsoft's web at <http://support.microsoft.com/default.aspx?scid=kb;en-us;889527>.

This patch also fixes the problem of supporting active mode FTP inside IPsec VPN tunnel of Windows XP SP2.

**Suggestion:** Please **UPDATE** client's Windows XP SP2 with this patch.

#### 5. The Termination of ActiveX

The ActiveX component for IPsec VPN is running paralleled with the web page of "Login Success". Unless user decides to close the session and to disconnect with PLANET WLS-1280, the following conditions or behaviors of using browser shall be avoided in order to maintain the built IPsec VPN tunnel always alive.



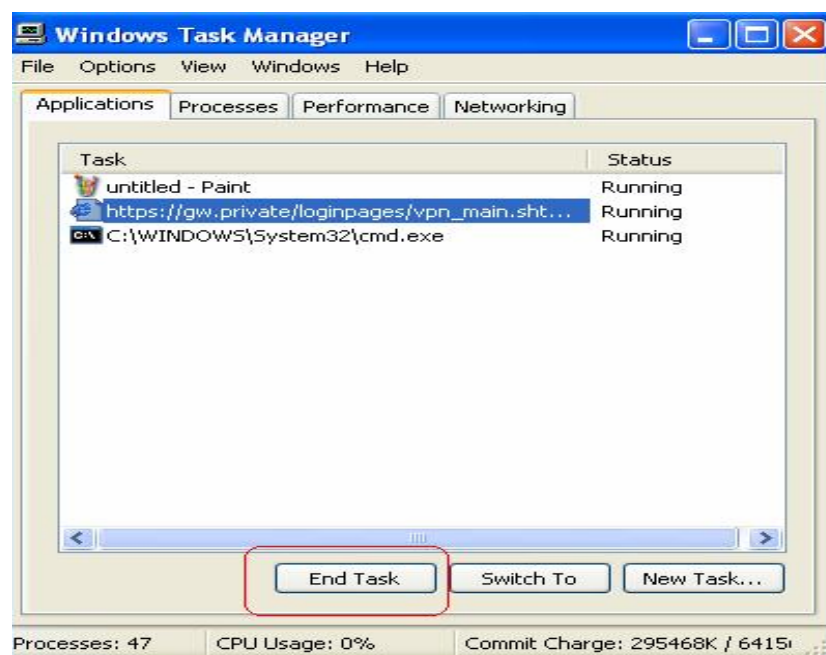
Reasons may cause the Internet Explorer to stop the ActiveX unexpectedly as followings:

**a. The crash of Internet Explorer on running ActiveX**

**Suggestion:** Please reboot client's computer, once Windows service is resumed, go through the login process again.

**b. Terminate the Internet Explorer Task from Windows Task Manager**

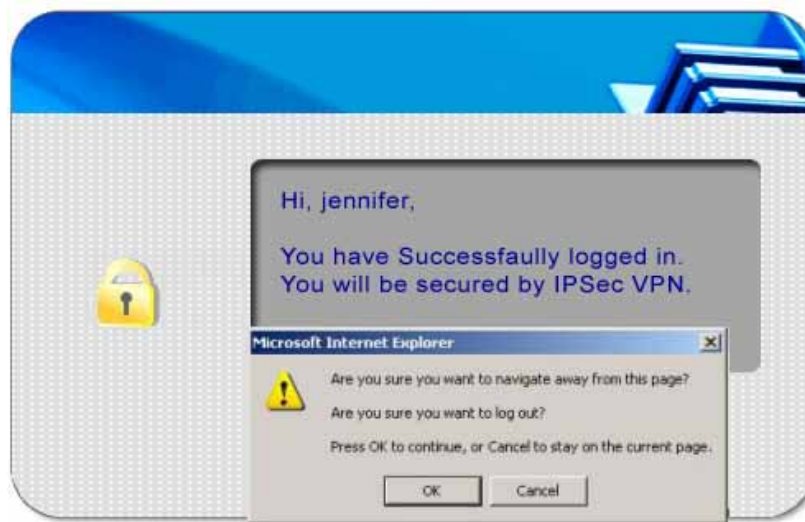
**Suggestion:** Don't terminate this VPN task of Internet Explorer.



**c. There are some cases of Windows messages by which PLANET WLS-1280 will hint current user to:**

- (1) Close the Windows Internet Explorer,

- (2) Click "logout" button on "login success" page,
- (3) Click "back" or "refresh" of the same Internet Explorer,
- (4) Enter new URL in the same Internet Explorer,
- (5) Open a URL from the other application (e.g. email of Outlook) that occupies this existing Internet Explorer.



**That shall all cause the termination of IPSec VPN tunneling if user chooses to click "Yes".** The user has to log in again to regain the network access.

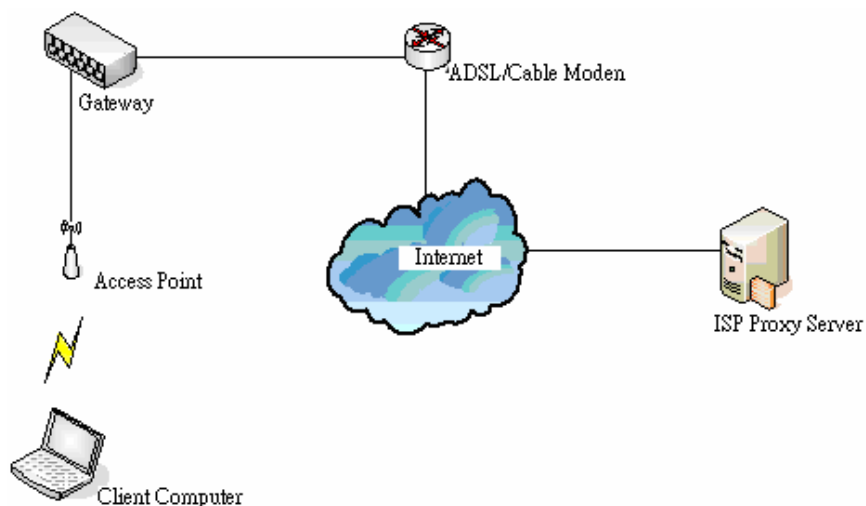
**Suggestion:** Click "Cancel" if you do not intend to stop the IPSec VPN connection yet.

## 6. Non-supported OS and Browser

In current version, Windows Internet Explorer is the only browser supported by PLANET WLS-1280. Windows XP and Windows 2000 are the only two supported OS along with this release.

## 8. Appendix D –Proxy Setting for Hotspot

HotSpot is a place such as a coffee shop, hotel, or a public area where provides Wi-Fi service for mobile and temporary users. HotSpot is usually implemented without complicated network architecture and using some proxy servers provided by Internet Service Providers.



In Hotspots, users usually enable their proxy setting of the browsers such as IE and Firefox. Therefore, so we need to set some proxy configuration in the Gateway need to be set. Please follow the steps to complete the proxy configuration :

6. Login Gateway by using “**admin**”.
7. Click the **Network Configuration from top menu** and the homepage of the **Network Configuration** will appear.

Network Configuration	
Network Address Translation	PLANET WLS-1280 provides 3 types of network address translation: DMZ (Demilitarized Zone), Public Accessible Server and IP/Port Redirect.
Privilege List	System provides Privilege IP Address List and Privilege MAC Address List. System will NOT authenticate those listed devices.
Monitor IP List	System can monitor up to 40 network devices online status with an option to add them as public access servers via HTTP or HTTPS. Even under NAT mode, after added the devices as public access servers, the devices can be accessed by clicking the hypertext.
Walled Garden List	Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication.
Proxy Server Properties	PLANET WLS-1280 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
Dynamic DNS	PLANET WLS-1280 supports dynamic DNS (DDNS) feature.
IP Mobility	System supports IP PNP Configuration.
VPN Termination	VPN tunnels using IPSec can be terminated locally on PLANET WLS-1280.

8. Click the **Proxy Server Properties** from left menu and the homepage of the **Proxy Server Properties** will appear.

External Proxy Server		
Item	Server IP	Port
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Internal Proxy Server	
Built-in Proxy Server	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

9. Add the ISP's proxy Server IP and Port into **External Proxy Server** Setting.

External Proxy Server		
Item	Server IP	Port
1	<input type="text" value="10.2.3.203"/>	<input type="text" value="6588"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Internal Proxy Server	
Built-in Proxy Server	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

10. **Enable Built-in Proxy Server** in **Internal Proxy Server** Setting.

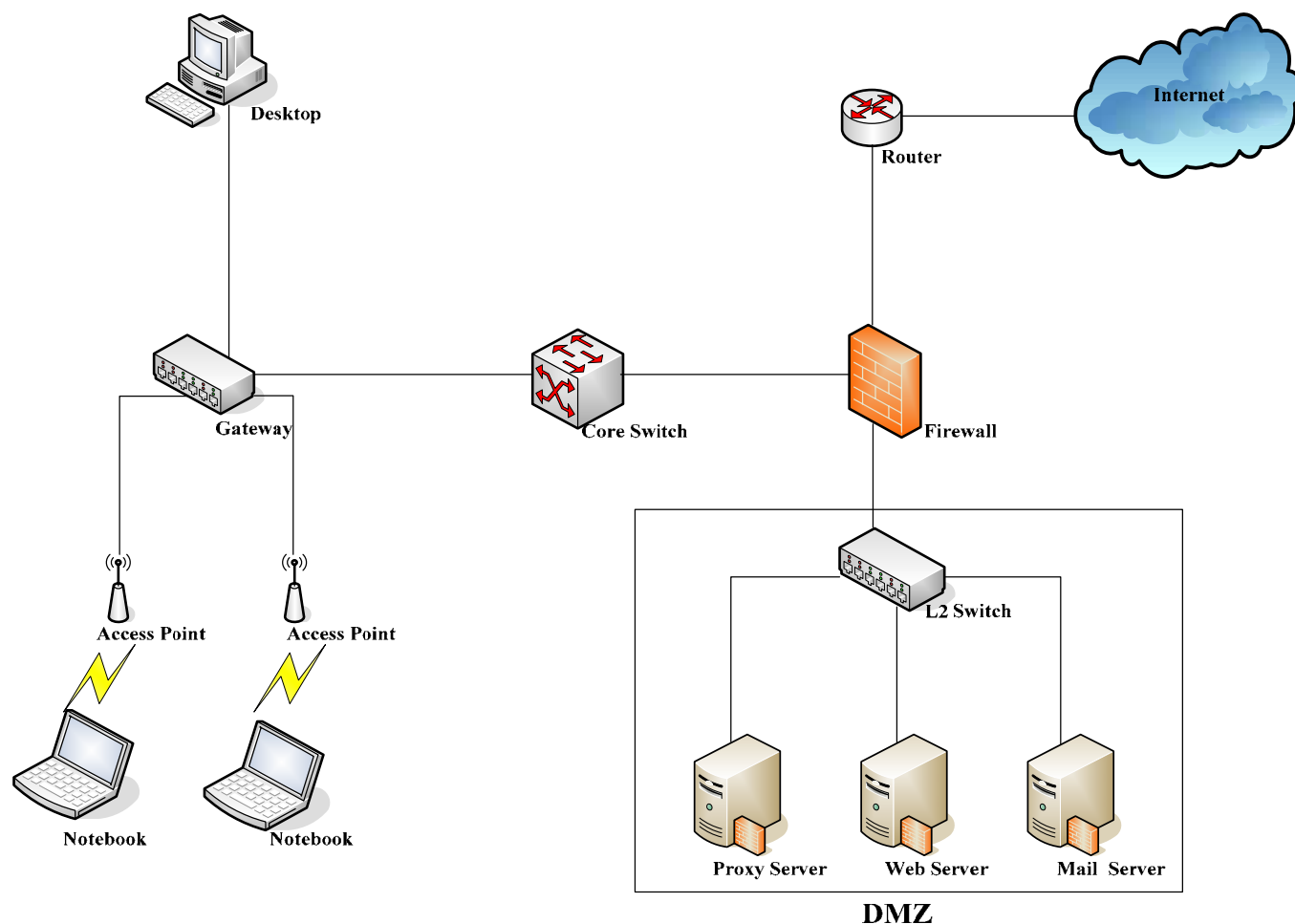
External Proxy Server		
Item	Server IP	Port
1	<input type="text" value="10.2.3.203"/>	<input type="text" value="6588"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Internal Proxy Server	
<b>Built-in Proxy Server</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

11. Click **Apply** to save the settings.

## 9. Appendix E –Proxy Setting for Enterprise

Enterprises usually isolate their intranet and internet by using more elaborated network architecture. Many enterprises have their own proxy server which is usually at intranet or DMZ under the firewall protection.



In enterprises, network managers or MIS staff may often ask their users to enable their proxy setting of the browsers such as IE and Firefox to reduce the internet access loading. Therefore some proxy configurations in the Gateway need to be set.

	<b>Caution :</b> Some enterprises will automatically redirect packets to proxy server by using core switch or Layer 7 devices. By the way, the clients don't need to enable their browsers' proxy settings, and administrators don't need to set any proxy configuration in the Gateway.
--	--

Please follow the steps to complete the proxy configuration :

### ■ Gateway setting

1. Login Gateway by using "**admin**".
2. Click the **Network Configuration from top menu** and the homepage of the **Network Configuration** will

appear.

The screenshot shows the 'Network Configuration' page. The sidebar on the left contains the following links: Network Address Translation, Privilege List, Monitor IP List, Walled Garden List, Proxy Server Properties, Dynamic DNS, IP Mobility, and VPN Termination. The main content area is titled 'Network Configuration' and contains a table with the following data:

Network Configuration	
Network Address Translation	PLANET WLS-1280 provides 3 types of network address translation: DMZ (Demilitarized Zone), Public Accessible Server and IP/Port Redirect.
Privilege List	System provides Privilege IP Address List and Privilege MAC Address List. System will NOT authenticate those listed devices.
Monitor IP List	System can monitor up to 40 network devices online status with an option to add them as public access servers via HTTP or HTTPS. Even under NAT mode, after added the devices as public access servers, the devices can be accessed by clicking the hypertext.
Walled Garden List	Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication.
Proxy Server Properties	PLANET WLS-1280 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
Dynamic DNS	PLANET WLS-1280 supports dynamic DNS (DDNS) feature.
IP Mobility	System supports IP PNP Configuration.
VPN Termination	VPN tunnels using IPSec can be terminated locally on PLANET WLS-1280.

- Click the **Proxy Server Properties** from left menu and the homepage of the **Proxy Server Properties** will appear.

External Proxy Server		
Item	Server IP	Port
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Internal Proxy Server	
Built-in Proxy Server	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

- Add your proxy Server IP and Port into **External Proxy Server** Setting.

External Proxy Server		
Item	Server IP	Port
1	<input type="text" value="10.2.3.203"/>	<input type="text" value="6588"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Internal Proxy Server	
Built-in Proxy Server	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

5. **Disable Built-in Proxy Server** in **Internal Proxy Server** Setting.

External Proxy Server		
Item	Server IP	Port
1	<input type="text" value="10.2.3.203"/>	<input type="text" value="6588"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Internal Proxy Server	
Built-in Proxy Server	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

6. Click **Apply** to save the settings.

**Warning :** If your proxy server is disabled, it will make the user authentication operation abnormal. When users open the browser, the login page won't appear because the proxy server is down. Please make sure your proxy server is always available.

## ■ Client setting

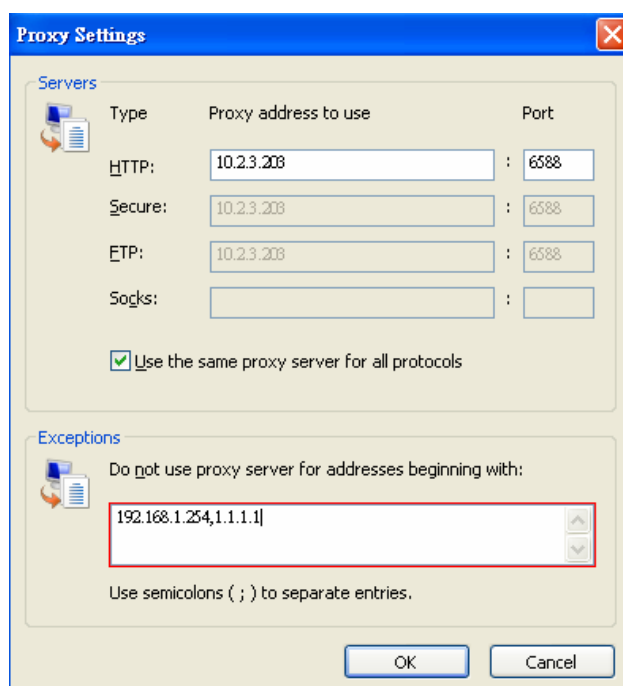
It is necessary for clients to add default gateway IP address into proxy exception information so the user login successful page can show up normally.

1. Use command "**ipconfig**" to get Default Gateway IP Address.




2. Open browser to add **default gateway IP address (e.g. 192.168.1.254)** and **logout page IP address "1.1.1.1"** into proxy exception information.

- For I.E



- For firefox

**Connection Settings** 

Configure Proxies to Access the Internet

☐ Direct connection to the Internet

☐ Auto-detect proxy settings for this network

☒ Manual proxy configuration:

HTTP Proxy:  Port:

☒ Use this proxy server for all protocols

SSL Proxy:  Port:

FTP Proxy:  Port:

Gopher Proxy:  Port:

SOCKS Host:  Port:

☐ SOCKS v4 ☒ SOCKS v5

No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

☐ Automatic proxy configuration URL:

## 10. *Appendix F –Disclaimer for Users*

PLANET WLS-1280,supports in some situations, that the hotspot owners or MIS staff may want to display “terms of use” or announcement information before the login page. Hotspot owners or MIS staff can design a new disclaimer/announcement page and save the page in their local server. After the agreement shown on the page is read, users are asked whether they agree or disagree with the disclaimer. By clicking “I agree,” users are able to log in. If users choose to decline, they will get a popup window saying they are unable to log in. The basic design is to have the disclaimer and login function in the same page but with the login function hidden until users agree with the disclaimer.

Here the codes are supplied. Please note that the blue part is for the login feature, the red part is the disclaimer, and the green part can be modified freely by administrators to suit the situation better. Now the default is set to “I disagree” with the disclaimer. Administrators can change the purple part to set “agree” as the default or set no default. These codes should be saved in local storage with a name followed by .html, such as login\_with\_disclaimer.html.

```
<html>
<head>
<META HTTP-EQUIV="Pragma" CONTENT="no-cache">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<META HTTP-EQUIV="Cache-Control" CONTENT="no-cache">
<link href="../include/style.css" rel="stylesheet" type="text/css">
<title>Login</title>

<script language="javascript1.2">
    var pham = document.cookie;
    var disableButton=false;

    function getCookie(name)
    {
        name += "="; // append '=' to name string
        var i = 0; // index of first name=value pair
        while (i < pham.length) {
            var offset = i + name.length; // end of section to compare name string
            if (pham.substring(i, offset) == name) { // if string matches
                var endstr = pham.indexOf(";", offset); //end of name=value pair
                if (endstr == -1) endstr = pham.length;
                return unescape(pham.substring(offset, endstr));
            }
            i = offset;
        }
    }
</script>
```

```

// return cookie value section
    }
    i = pham.indexOf(" ", i) + 1; // move i to next name=value pair
    if (i == 0) break; // no more values in cookie string
    }
    return null; // cookie not found
}

```

```

function CodeCookie(str)

```

```

{
var strRtn="";

for (var i=str.length-1;i>=0;i--)
{
    strRtn+=str.charCodeAt(i);
    if (i) strRtn+="a";
}
return strRtn;
}

```

```

function DecodeCookie(str)

```

```

{
var strArr;
var strRtn="";

strArr=str.split("a");

for(var i=strArr.length-1;i>=0;i--)
strRtn+=String.fromCharCode(eval(strArr[i]));

return strRtn;

}

```

```

function MM_swapImgRestore() { //v3.0

```

```

var i,x,a=document.MM_sr; for(i=0;a&&i<a.length&&(x=a[i])&&x.oSrc;i++) x.src=x.oSrc;
}

```

```

function MM_preloadImages() { //v3.0

```

```

var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();
var i,j=d.MM_p.length,a=MM_preloadImages.arguments; for(i=0; i<a.length; i++)

```

```

if (a[i].indexOf("#")!=0){ d.MM_p[j]=new Image; d.MM_p[j++].src=a[i];}}
}

```

```

function MM_findObj(n, d) { //v4.01
var p,i,x;  if(!d) d=document; if((p=n.indexOf("?"))>0&&parent.frames.length) {
d=parent.frames[n.substring(p+1)].document; n=n.substring(0,p);}
if(!(x=d[n])&&d.all) x=d.all[n]; for (i=0;!x&&i<d.forms.length;i++) x=d.forms[i][n];
for(i=0;!x&&d.layers&&i<d.layers.length;i++) x=MM_findObj(n,d.layers[i].document);
if(!x && d.getElementById) x=d.getElementById(n); return x;
}

```

```

function MM_swapImage() { //v3.0
var i,j=0,x,a=MM_swapImage.arguments; document.MM_sr=new Array; for(i=0;i<(a.length-2);i+=3)
if ((x=MM_findObj(a[i]))!=null){document.MM_sr[j++]=x; if(!x.oSrc) x.oSrc=x.src; x.src=a[i+2];}
}

```

```

function init(form)
{
    id = getCookie("username");
    if(id!="" && id!=null)
    {
        form.myusername.value = id;
    }

    disclaimer.style.display="";
    login.style.display='none';

}

```

```

function Before_Submit(form)
{
    if(form.myusername.value == "")
    {
        alert("Please enter username.");
        form.myusername.focus();
        form.myusername.select();
        disableButton=false;

        return false;
    }
    if(form.mypassword.value == "")

```

```

    {
        alert("Please enter password.");
        form.mypassword.focus();
        form.mypassword.select();
        disableButton=false;

        return false;
    }

    if(disableButton==true)
    {
        alert("The system is now logging you in, please wait a moment.");
        return false;
    }
    else
    {
        disableButton=true;
        return true;
    }
    return true;
}

function reminder_onclick(form)
{
    Reminder.myusername.value = form.myusername.value;
    Reminder.mypassword.value = form.mypassword.value;
    Reminder.submit();
}

function cancel_onclick(form)
{
    form.reset();
}

function check_agree(form)
{
    if(form.selection[1].checked == true)
    {
        alert("You disagree with the disclaimer, therefore you will NOT be able to log in.");
        return false;
    }
}

```

```
disclaimer.style.display='none';
login.style.display="";
```

```
        return true;
    }
}
```

```
</script>
```

```
</head>
```

```
<body style="font-family: Arial" bgcolor="#FFFFFF"
```

```
onload="init(Enter);MM_preloadImages('../images/submit0.gif','../images/clear0.gif','../images/remaining0.gif')">
```

```
    <ilayer width=&{marquee_width}; height=&{marquee_height}; name="cmarquee01">
```

```
        <layer name="cmarquee02" width=&{marquee_width}; height=&{marquee_height};></layer>
```

```
    </ilayer>
```

```
<form action="userlogin.shtml" method="post" name="Enter">
```

```
<table name="disclaimer" id="disclaimer" width="460" height="430" border="0" align="center"
```

```
background="../images/agreement.gif">
```

```
    <tr>
```

```
        <td height="50" align="center" valign="middle"><div align="center" class="style5">Service  
Disclaimer</div></td>
```

```
    </tr>
```

```
    <tr>
```

```
        <td height="260" align="center" valign="middle"><table width="370" height="260" border="0" align="center">
```

```
            <tr>
```

```
                <td>
```

```
                    <textarea name="textarea" cols="50" rows="15" align="center" readonly>
```

We may collect and store the following personal information:

e-mail address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)

Our primary purpose in collecting personal information is to provide you with a safe, smooth, efficient, and customized experience. You agree that we may use your personal information to: provide the services and customer support you request; resolve disputes, collect fees, and troubleshoot problems; prevent potentially prohibited or illegal activities; customize, measure, and improve our services and the site's content and layout; compare

information for accuracy, and verify it with third parties.

We may disclose personal information to respond to legal requirements, enforce our policies, respond to claims that an activity violates the rights of others, or protect anyone's rights, property, or safety.

We may also share your personal information with:

members of our corporate family to help detect and prevent potentially illegal acts; service providers under contract who help with our business operations; (such as fraud investigations and bill collection) other third parties to whom you explicitly ask us to send your information; (or about whom you are otherwise explicitly notified and consent to when using a specific service) law enforcement or other governmental officials, in response to a verified request relating to a criminal investigation or alleged illegal activity; (In such events we will disclose name, city, state, telephone number, email address, User ID history, and fraud complaints)

xxxxx participants under confidentiality agreement, as we in our sole discretion believe necessary or appropriate in connection with an investigation of fraud, intellectual property infringement, piracy, or other unlawful activity; (In such events we will disclose name, street address, city, state, zip code, country, phone number, email, and company name.) and other business entities, should we plan to merge with, or be acquired by that business entity. (Should such a combination occur, we will require that the new combined entity follow this privacy policy with respect to your personal information. If your personal information will be used contrary to this policy, you will receive prior notice.)

Without limiting the above, in an effort to respect your privacy and our ability to keep the community free from bad actors, we will not otherwise disclose your personal information to law enforcement, other government officials, or other third parties without a subpoena, court order or substantially similar legal procedure, except when we believe in good faith that the disclosure of information is necessary to prevent imminent physical harm or financial loss or to report suspected illegal activity.

Your password is the key to your account. Do not disclose your password to anyone. Your information is stored on our servers. We treat data as an asset that must be protected and use lots of tools (encryption, passwords, physical security, etc.) to protect your personal information against unauthorized access and disclosure. However, as you probably know, third parties may unlawfully intercept or access transmissions or private communications, and other users may abuse or misuse your personal information that they collect from the site. Therefore, although we work very hard to protect your privacy, we do not promise, and you should not expect, that your personal information or private communications will always remain private.

By agreeing above, I hereby authorize xxxxx to process my service charge(s) by way of my credit card.

</textarea>

</td>

</tr>

</table></td>

</tr>

```

<tr>
  <td height="40"><table width="170" height="20" border="0" align="center" cellpadding="2">

    <tr>
      <td align="left"><input name="selection" value="1" type="radio"></td>
      <td><span class="style4">I agree.</span></td>
    </tr>

    <tr>
      <td align="left"><input name="selection" value="2" checked type="radio"></td>
      <td><span class="style4">I disagree.</span></td>
    </tr>
  </table></td>
</tr>
<tr>
  <td height="30"><table width="110" height="20" border="0" align="center" cellpadding="2">
    <tr>
      <td width="45" align="center" valign="middle"><input name="next_button" type="button" value="Next"
onclick="javascript:check_agree(Enter)"></td>
    </tr>
  </table></td>
</tr>
<tr>
  <td height="20">&nbsp;</td>
</tr>
</table>

<div align="center">
<table name="login" id="login" width="497" height="328" border="0" align="center" cellpadding="2" cellspacing="0"
background=" ../images/userlogin.gif">
  <tr>
    <td height="146" colspan="2">&nbsp;</td>
  </tr>
  <tr>
    <td width="43%" height="53">&nbsp;</td>
    <td><input type="text" name="myusername" size="20"></td>
  </tr>
  <tr>
    <td height="42">&nbsp;</td>
    <td><input type="password" name="mypassword" size="20"></td>
  </tr>

```

```

<tr>
  <td colspan="2">
    <div align="center">
      <a onclick="javascript:if(Before_Submit(Enter)){Enter.submit();}" onMouseOut="MM_swapImgRestore()"
onMouseOver="MM_swapImage('Image3','../images/submit0.gif',1)">
        
      </a>
      <a onclick="cancel_onclick(Enter)" onMouseOut="MM_swapImgRestore()"
onMouseOver="MM_swapImage('Image5','../images/clear0.gif',1)">
        
      </a>
      <a onclick="javascript:if(Before_Submit(Enter)){reminder_onclick(Enter);}"
onMouseOut="MM_swapImgRestore()" onMouseOver="MM_swapImage('Image4','../images/remaining0.gif',1)">
        
      </a>
    </div>
  </td>
</tr>
</table>

```

```

<table>
  <tr>
    <td width="100%">
      <font color="#808080" size="2"><script language="JavaScript">if( creditcardenable == "Enabled" )
document.write("<a href='../loginpages/credit_agree.shtml'">Click here to purchase by Credit Card
Online.<a>");</script></font>
    </td>
  </tr>
</table>

```

```

</div>
</form>
<form action="reminder.shtml" method="post" name="Reminder">
  <input type="hidden" name="myusername" value="">
  <input type="hidden" name="mypassword" value="">
</form>
<br>
<div align="center">
  <table>
  <tr>

```

```
<td width="100%">
<font color="#808080" size="2"><script language="JavaScript">document.write(copyright);</script></font></td>
</tr>
</table>
</div>
</body>

</html>
```

P/N: V10020061002